Robust Channel-Phase Based Physical-Layer Authentication for Multi-Carriers Transmission

Xinjin Lu, Yuxin Shi, Ru-Han Chen, Zhifei Yang, Kang An and Symeon Chatzinotas, *Fellow, IEEE.*

***Abstract*—This paper focuses on the serious threat posed by an eavesdropper using a well-designed impersonation attack, which aims to pass the physical-layer authentication (PLA) illegally. To prevent Eve from decreasing the authentication performance, we propose a robust channel-phase based PLA scheme for multi-carriers transmission, which contains a novel two-level decision. Specifically, the first level decision is used to prevent Eve from high transmit power and the second one is used to further authenticate the user. The optimal threshold for accurately detecting the response signal with high transmit power is derived. Moreover, we provide the theoretical performance analysis for the proposed scheme, and derive the closed-form expressions of the probability of detection and false alarm via the numerical statistic and the proper approximation. Simulation results show the robustness of our proposed scheme and verify the effectiveness of the theoretical analysis.**

***Index Terms*—Physical-Layer Authentication (PLA), channel-phase, authentication performance, probability of false alarm.**

I. Introduction

A. Background

The pervasiveness of commercial Internet of Things (IoT) around the globe is expected to reach significant levels with the upcoming sixth generation of mobile networks (6G). Nonetheless, the openness of wireless transmissions and the forecasted overwhelm in connected devices will provoke unprecedented security leakages and vulnerabilities [1].

Physical-layer authentication (PLA) has attracted lots of attentions due to its unique advantages, e.g., security and low-complexity. The information theoretic security can be obtained by the PLA since the physical layer introduces uncertainty into the adversary, whilst the low-complexity of PLA is because the intrinsic physical-layer features can be utilized to authentication instead of the complex encryption algorithm [2]. Hence, upper-layer authentication mechanisms ensuring the security by using conventional cryptography-based algorithms, PLA is more applicable for emerging wireless communication systems, e.g., internet of vehicles (IoV), smart grids (SG) networks, cognitive radio (CR) networks, and unmanned aerial vehicles (UAV) [3]. To this end, a secure and lightweight continuous authentication scheme for IoT device authentication was proposed in [4], which utilized the inherent properties of the IoT devices' transmission model as its source for seed generation and device authentication. In [5], an adaptive PLA scheme for IoT was proposed to exploit the antenna diversity inherent in multiple-input multiple-output (MIMO) systems by using a one-class classification support vector machine. In [6], a mobile UAV aided PLA framework was proposed based on the physical layer channel characteristics and geographical locations of different transmitters. [7] exploited two intrinsic hardware-specific fingerprints in terms of carrier frequency offset (CFO) and phase noise to propose a PLA scheme in the UAV aided communication systems. In [8], the polarization fingerprint (PF) was deeply studied and a PF-based LoRaWAN PLA solution was designed.

Inspired by the rapid development in Artificial intelligence (AI), [9] proposed a federated learning based cooperative PLA scheme that utilizes a group of edge devices to jointly build an authenticator, which ensures privacy preservation and higher robustness. In [10], a transfer learning-based PLA scheme was proposed to achieve fast online user authentication for latency sensitive applications such as edge computing. In [11], ResNet was employed to extract channel features of channel state information (CSI) from different transmitters and classify them at the network output layer, enabling authentication decisions based on classification results. [12] proposed a lightweight cross-domain authentication scheme for securing wireless IoT devices using backscatter communication where a federated learning model was designed to aggregate device identity information across domains. Based on deep learning methods, [13] presented a fingerprint exploitation modality to leverage RF fingerprints originating from symbol transition trajectories for transmitter authentication. Though the potential performance improvement can be achieved by using AI, the extra high burdens of complexity introduced by the training process should be noticed.

Different from the general scenario of PLA, various scenarios or functions of PLA were considered in [13]–[18]. Specifically, [14] concerned the problem of authenticating different transmitters at the physical layer in a multi-user scenario and proposed two tag-based PLA schemes in a multi-user scenario. [15] concerned the problem of ensuring the security of the tag-based PLA schemes under multiple cooperative attackers. To defending against the jamming attack for the PLA, [16] proposed two jamming detection schemes called jamming-attack detection (JAD) and composite jamming-attack detection (CJAD), which exploited the difference of

Xinjin Lu is with the National University of Defense Technology, Changsha 410000, China, and is also with State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System, Luoyang 471003, China (luxinjin2023@163.com). Yuxin Shi, Ru-Han Chen and Kang An are with the Sixty-Third Research Institute, National University of Defense Technology, Nanjing 210000, China (e-mail: shiyuxin13@nudt.edu.cn, tx_rhc22@nudt.edu.cn, ankang89@nudt.edu.cn). Zhifei Yang is with State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System, Luoyang 471003, China (e-mail: zhifeiyang@163.com). Symeon Chatzinotas is with the Institute of Informatics and Telecommunications, NCSR 'Demokritos', 153 41 Athens, Greece (e-mail: schatzin@ieee.org). *Corresponding author: Yuxin Shi.*

noise variances to well detect jamming attacks. To improve authentication reliability, [17] proposed a knowledge-enhanced PLA algorithm, which used prior knowledge of mobile devices and wireless channels to verify mobility patterns and extract stable features. Evaluation results show that the proposed algorithm can achieve higher reliability than two state-of-the-art algorithms in three mobile scenarios. [18] developed an enhancement framework consisting of analysis, enhancement, and assessment to improve the transferability and immunity of PLA, where superior reliability of the proposed algorithm transferring across various scenarios and immunizing against attacks forging CSI was shown.

B. Related Works and Our Motivation

As a main category of PLA, the identity authentication mechanism based on the physical layer wireless channel can be divided into key-based PLA and key-less PLA [19]. Noting that key-less PLA is more or less based on upper layers security mechanisms to ensure the security of the previous timeslot [20], key-based PLA can use secret keys shared by legitimate users to employ the complete authentication process without upper layers security mechanisms, which has unique advantages on security in the context of rapidly increasing computing power. However, more requirements of robustness should be considered in key-less PLA schemes.

The researches on key-based PLA technology originated from [21], which utilized the randomness, reciprocal, and location decorrelation features of the wireless fading channel to defend various passive and active attacks. In [21], the randomness of the channel amplitude was used to protect the inquiry and response signals. Wu. *et al* proposed channel-phase response based PLA scheme, which enhanced the authentication performance [22]. In general, the channel-phase based PLA scheme has two main advantages compared with amplitude-based scheme. First, channel amplitude responses usually undergo great changes in high speed mobile wireless systems due to Doppler spread, but the changes of phase values are predictable [23]. Second, the recent channel-phase based PLA researches have shown better authentication performance by well-designed testing statistics [24]–[27], which are suitable for multi-carriers transmission.

Against the background and related works, our motivation is to solve the two main challenges in this paper. First, the prior channel-phase based PLA schemes considered that the malicious eavesdropper employed the impersonation attack without secret keys using the same steps and the same transmit power as legitimate users. However, it is possible for the eavesdropper to employ the well-designed impersonation attack to decrease the authentication performance. It is challenging to find this attack and enhance the robustness of the channel-phase based PLA scheme. Second, it is challenging to theoretically analyze the performance of our proposed scheme. Noticing the performance analysis for the prior channel-phase based PLA scheme has been very complex, the extra design on the channel-phase based PLA scheme will inevitably increases the difficulty of quantitative analysis.

C. Threat Model

In this paper, we consider that Bob is a center of the authentication and Alice is a legitimate user. Here, the eavesdropper (Eve) has known the all details of the authentication protocols shared by Alice and Bob, except the shared secret keys. Then, Eve aims to conduct the same steps of authentication protocols as Alice to pass the authentication illegally. Since Eve has owned the details of the authentication protocols, it is possible for Eve to impersonate Alice and well design the signals (response or inquiry signals) in the authentication process to successfully pass the authentication process illegally. Though the prior schemes have investigated this issue in [25], [27], which has improved the authentication performance, the potential threats from extremely high transmit power used by Eve are still ignored.

D. Key Contributions and Results

The main contributions and results of this paper are summarized as below:

- We investigate a well-designed impersonation attack, which poses a serious threat posed for the key-based PLA schemes. Specifically, Eve employs the first step of authentication process as the general impersonation attack, i.e., the authentication request, and then sends the authentication response by using an extremely high transmit power, which will decrease the authentication performance.
- We propose a novel two-level decision channel-phase based PLA. To be specific, the first level decision is used to prevent Eve from high transmit power and the second one is used to authenticate the user. Moreover, the optimal threshold of the decision for detecting response signal with high transmit power is derived. Through the two-level decision, the robustness of the channel-phase based PLA scheme is ensured.
- Theoretical performance analysis is provided for accurately estimating the authentication performance. Here, the theoretical results of the proposed scheme, i.e., the closed-form expressions of the probability of detection and false alarm are derived via the numerical statistic and the proper approximation.
- Comprehensive simulation results in terms of the receiver operator characteristic (ROC), probabilities of detection and false alarm under various parameters are provided to validate the robustness of the proposed scheme compared with the benchmark scheme. Moreover, the effectiveness of the theoretical performance analysis is verified by the comparison between the simulated results and the theoretical ones.

The rest of the paper is organized as follows. In Section II, we provide the system model and the problem statement. In Section III, the proposed scheme containing the two-level decision process is provided. Theoretical performance analysis of the proposed scheme is given in Section IV. Section V provides the comprehensive simulation results. Section VI concludes this paper.

Notation: Transpose and its Hermitian transpose are denoted as $(\cdot)^T$ and $(\cdot)^H$, respectively. $|\cdot|$ denotes the absolute value of a variable. $\mathcal{I}(\cdot)$ and $\mathcal{R}(\cdot)$ denotes the imaginary part and the real part of a vector, respectively. $\mathbb{E}(\cdot)$ and $\mathrm{Var}(\cdot)$ denotes the expectation and variance of a vector or variable, respectively.

II. System Model and Problem Statement

A. System Model

The details of the channel-phase based authentication process are given in Fig. 1, which contains three main steps: authentication request, authentication inquiry and authentication response.

1) Authentication Request: First of all, we consider a legitimate user Alice aims to start the authentication, and then sends an authentication request by an N-subcarrier signal. The request signal $\mathbf{s}_R$ usually contains some public information of a user, such as the user's request, type, number, and state.

2) Authentication Inquiry: After receiving the request signal, Bob realizes there exists a user requesting for authentication. Then, Bob sends an inquiry signal $\mathbf{s}_b$, where $\mathbf{s}_b = [s_{b,1}, s_{b,2}, \ldots, s_{b,N}]^T$ and $s_{b,i} = \exp(j\theta_{b,i})$. Here, $\theta_{b,i}$ is a random phase generated by Bob, where $\theta_{b,i} \in U[0, 2\pi]$ for $i = 1, 2, \ldots, N$. Then, the received inquiry signal from the i-th subcarrier can be represented by

$$r_{a,i} = h_{BA,i} s_{b,i} + w_{ab,i}, \tag{1}$$

where $h_{BA,i}$ and $w_{a,i}$ denote the channel coefficient and the additional white Gaussian noise (AWGN). Note that

$$h_{BA,i} = |h_{BA,i}| \exp(j\theta_{h_{BA,i}}), \tag{2}$$

where $\theta_{h_{BA,i}}$ is the phase response of the channel coefficient. Then, the phase extracted from $r_{a,i}$ can be denoted as

$$\theta_{a,i} = \theta_{h_{BA,i}} + \theta_{b,i} + \varepsilon_{ab,i}, \tag{3}$$

where $\theta_{b,i}$ and $\varepsilon_{ab,i}$ denote the phase of $s_{b,i}$ and the phase noise introduced by $w_{ab,i}$, respectively.

3) Authentication Response: Then, Alice generates the response signal $\mathbf{s}_a$, where $\mathbf{s}_a = [s_{a,1}, s_{a,2}, \ldots, s_{a,N}]^T$. Here, Alice uses the secret key $\mathbf{K}_A = [k_{a,1}, k_{a,2}, \ldots k_{a,N}]$ to produce the response signal $\mathbf{s}_a$. The i-th element of $\mathbf{s}_a$ can be given by

$$s_{a,i} = \exp\left(j\mathcal{M}(k_{a,i}) - j\theta_{a,i}\right), \tag{4}$$

where $k_{a,i}$ is the i-th pair-wise 0-1 secret key owned by Alice. $\mathcal{M}(k_i)$ denotes the mapping function, given by

$$\mathcal{M}(k_i) = \begin{cases} 0, & k_i = [0\ 0] \\ \pi/2, & k_i = [0\ 1] \\ \pi, & k_i = [1\ 1] \\ 3\pi/2, & k_i = [1\ 0] \end{cases} \tag{5}$$

The response signal received by Bob can be represented by

$$r_{b,i} = h_{AB,i} s_{a,i} + w_{ba,i}, \tag{6}$$

where $h_{AB,i}$ and $w_{ba,i}$ denote the channel coefficient and the AWGN from Alice to Bob. Due to the reciprocity of wireless channels, i.e., $h_{AB,i} = h_{BA,i} = h_i$, Eq. (6) can be rewritten as

$$r_{b,i} = |h_i| \exp\left(j\left(\mathcal{M}(k_{a,i}) - \theta_{b,i} - \varepsilon_{ab,i}\right)\right) + w_{ba,i}. \tag{7}$$

Next, Bob will multiply the inquiry signal by $\mathbf{s}_b$ to get $\mathbf{y}$, which aims to remove the preset random phase, and i-th element of $\mathbf{y}$ obtained from Alice can be represented by

$$y_{i,a} = |h_i| \exp\left(j\left(\mathcal{M}(k_{a,i}) - \varepsilon_{ab,i}\right)\right) + w_{ba,i} s_{b,i}. \tag{8}$$

Note that Eve will learn and impersonate the behavior of Alice with randomly generated $\mathbf{K}_E = [k_{e,1}, k_{e,2}, \ldots k_{e,N}]$, where $\mathbf{K}_E \neq \mathbf{K}_B$. In this case, Eq. (8) can be rewritten as

$$y_{i,e} = |h_i| \exp\left(j\left(\mathcal{M}(k_{e,i}) - \varepsilon_{eb,i}\right)\right) + w_{be,i} s_{b,i}, \tag{9}$$

where the variables are similar to that of (8), except that the sender is Eve. Finally, Bob calculates the hypothesis testing statistics for making decision. According to [27], a well-designed hypothesis testing statistics can be represented by

$$C_R = \mathcal{R}\left\{e^{-j\mathcal{M}(\mathbf{K}_B)}\mathbf{y}\right\}, \tag{10}$$

where $\mathbf{K}_B$ is the secret key of Bob, and $\mathbf{K}_B = \mathbf{K}_A = [k_{b,1}, k_{b,2}, \ldots k_{b,N}]$. Here, the authentication decision can be summarized as a binary hypothesis testing problem, given by

$$\begin{cases} \mathcal{H}_0: & \text{The user is illegal (Eve)}, \\ \mathcal{H}_1: & \text{The user is legitimate (Alice)}. \end{cases} \tag{11}$$

Under $\mathcal{H}_0$, it indicates that the authenticated user is illegal. Under $\mathcal{H}_1$, it indicates that the authenticated user is legitimate. Substituting (8) and (9) into (10), we obtain the hypothesis testing statistics under $\mathcal{H}_0$ and $\mathcal{H}_1$, expressed as

$$\begin{aligned} C_{R,\mathcal{H}_0} &= \mathcal{R}\left\{\sum_{i=1}^{N}\left(|h_{BE,i}|\, e^{j(\Delta\mathcal{M}(k_{eb,i}) - \varepsilon_{eb,i})} + \tilde{\omega}_{b,i}\right)\right\}, \\ C_{R,\mathcal{H}_1} &= \mathcal{R}\left\{\sum_{i=1}^{N}\left(|h_{BA,i}|\, e^{j(\Delta\mathcal{M}(k_{ab,i}) - \varepsilon_{ab,i})} + \tilde{\omega}_{b,i}\right)\right\}, \end{aligned} \tag{12}$$

where $\Delta\mathcal{M}$ denotes the phase offset introduced by the secret key, i.e., $\Delta\mathcal{M}(k_{ab,i}) = \mathcal{M}(k_{a,i}) - \mathcal{M}(k_{b,i})$. $\tilde{\omega}_{b,i}$ denotes the AWGN rotated by $s_{b,i}$ and $e^{-j\mathcal{M}(k_{b,i})}$, where $\tilde{\omega}_{b,i} = \exp\left(-j\mathcal{M}(k_{b,i})\right)\omega_{bx,i} s_{b,i}$ and $x \in \{a, b\}$. Here, we assume that $\tilde{\omega}_{b,i}$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ has the same probability density function (PDF) , i.e., $\tilde{\omega}_{b,i} \sim \mathcal{CN}\left(0, \sigma_n^2\right)$ for the sake of convenience.

Finally, Bob uses a preset threshold to determine the accepted hypothesis, given by

$$C_R \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} T. \tag{13}$$

If C_R is larger than T, Bob will accept $\mathcal{H}_1$; otherwise Bob will accept $\mathcal{H}_0$.

B. Problem Statement

Taking a closer look on Eq. (12), we observe that $C_{R,\mathcal{H}_1}$ is easily larger than $C_{R,\mathcal{H}_0}$ due to $\Delta\mathcal{M}(k_{ab,i}) = 0$ for $i =$

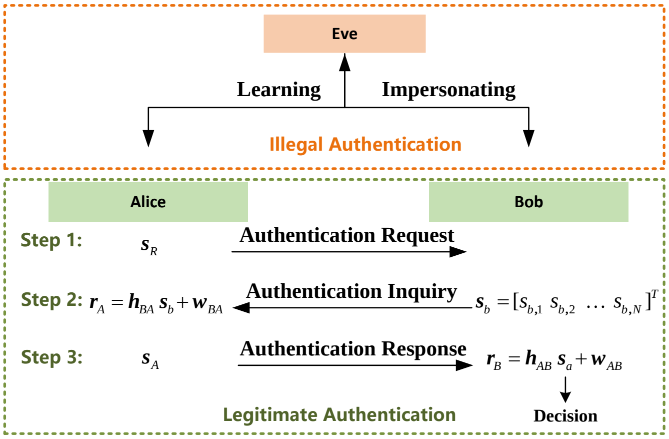

Fig. 1. Diagram of the channel-phase based authentication process.

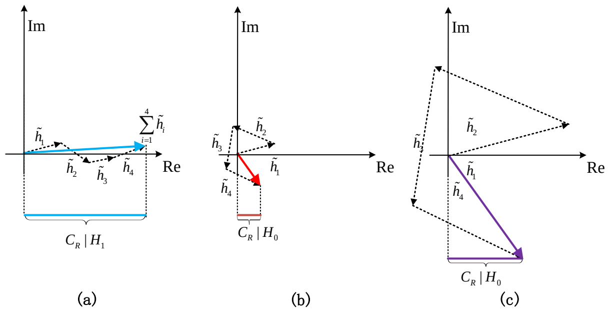

Fig. 2. The statistic comparisons with $N = 4$: (a) under $\mathcal{H}_1$ with unit transmit power (b) under $\mathcal{H}_0$ with unit transmit power (c) under $\mathcal{H}_0$ with higher transmit power.

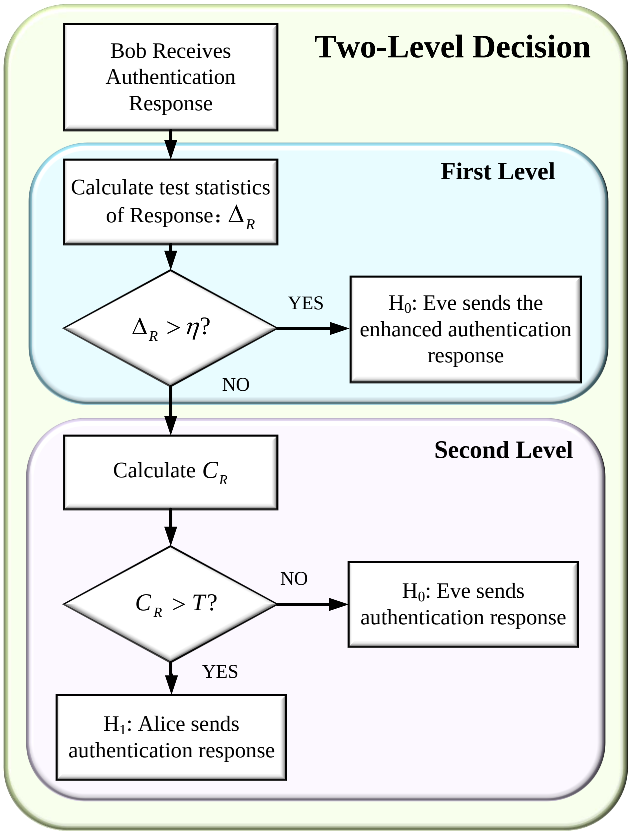
Two-Level Decision
Bob Receives Authentication Response
First Level
Calculate test statistics of Response: Δ_R
$\Delta_R > \eta$?
YES
H_0: Eve sends the enhanced authentication response
NO
Second Level
Calculate C_R
$C_R > T$?
NO
H_0: Eve sends authentication response
YES
H_1: Alice sends authentication response

Fig. 3. Flow chart of the proposed channel-phase based authentication process.

$1, 2, \dots, N$. As shown in Fig. 2 (a) and Fig. 2 (b), Alice can remove the phase offset $\Delta\mathcal{M}(k_{ab,i})$ introduced by secret keys, whilst Eve cannot remove $\Delta\mathcal{M}(k_{eb,i})$. Therefore, the better authentication performance can be obtained.

Note that the prior schemes consider that Eve uses the same transmit power as Alice, as shown in Eq. (9). However, if Eve increases its transmit power of its authentication response, Eve has higher probability to illegally pass the authentication. From Fig. 2 (b) and Fig. 2 (c), it can be observed that $C_{R,\mathcal{H}_0}$ becomes closer to $C_{R,\mathcal{H}_1}$ after using higher transmit power, which will makes it difficult for Bob to distinguish. Hence, the authentication performance will be seriously threatened. To well represent the effect of transmit power, (12) can be renewed as

$$C_{R,\mathcal{H}_0} = \mathcal{R}\left\{\sum_{i=1}^{N}\left(\sqrt{E_e}|h_{BE,i}|\,e^{j(\Delta\mathcal{M}(k_{eb,i})-\varepsilon_{eb,i})} + \tilde{\omega}_{b,i}\right)\right\},$$
$$C_{R,\mathcal{H}_1} = \mathcal{R}\left\{\sum_{i=1}^{N}\left(\sqrt{E_a}|h_{BA,i}|\,e^{j(\Delta\mathcal{M}(k_{ab,i})-\varepsilon_{ab,i})} + \tilde{\omega}_{b,i}\right)\right\}, \tag{14}$$

where E_a and E_e denote the transmit power used by Alice and Eve, respectively. To measure the degree of Eve's high transmit power, we define the energy ratio (ER) between Eve and Alice, expressed as

$$\text{ER (dB)} = 10\log_{10}\left(\frac{E_e}{E_a}\right). \tag{15}$$

Without loss of generality, we set $E_a = 1$ in the following discussions.

III. Proposed Scheme

According to the discussion above, it is urgent for Bob to prevent Eve from using the higher transmit power. To this end, we propose a two-level decision process for the authentication process, as shown in Fig. 3. The basic idea of the decision process is to detect the high transmit power of Eve by estimating the average energy of a response signal at the first level decision. Then, the second level decision can be used to distinguish the legitimate user with the shared secret keys from the illegal one without the shared secret keys.

A. First Level Decision

Specifically, after receiving the response signal, Bob first calculates the testing statistic

$$\Delta = \frac{1}{N}\mathbf{y}^H\mathbf{y}, \tag{16}$$

where Δ can be seen as the average energy of the response signal. If Δ is larger than the preset threshold η, Bob will accept $\mathcal{H}_0$ that there exists an illegal user using a large transmit power; otherwise, Bob will continue to the next decision.

It is worth noting that Bob will determine η based on the type, user's number, and state given in authentication request. For example, Bob will record the average energy used by the authenticated legitimate user. Once a user sends the authentication request claiming the same user's number as the authenticated one, Bob will calculate η according to the recorded average energy. Thereafter, we provide the optimal η for accurately employ the first level decision.

Proposition 1. *The optimal value of the first level decision for the proposed scheme is expressed as*

$$\eta_{op} = Q_{\chi^2}^{-1}\left(P_{F,1,thre}, 2N\right)\frac{\sigma_h^2+\sigma_n^2}{2N}, \tag{17}$$

where $Q_{\chi^2}^{-1}(p,\nu)$ denotes the inverse tail probability function of a Chi-Square distribution with Degree of Freedom (DoF) ν at the probability values in p. $P_{F,1,thre}$ denotes the preset threshold of the probability that Alice is falsely regarded as Eve in the first level decision.

Proof. Based on the Neyman Pearson (NP) theorem, the optimal threshold can be calculated by ensuring the maximum probability of false alarm. Here, we ensure

$$\Pr\left(\Delta_{\mathcal{H}_1} > \eta_{\text{op}}\right) = P_{F,1,thre}, \tag{18}$$

where $\Delta_{\mathcal{H}_1}$ denotes the testing statistic Δ under $\mathcal{H}_1$. Based on (8) and (9), we have $y_{i,a} \sim \mathcal{CN}\left(0, \sigma_h^2+\sigma_n^2\right)$, and

$$\frac{2N\Delta_{\mathcal{H}_1}}{\sigma_h^2+\sigma_n^2} \sim \chi^2\left(2N\right). \tag{19}$$

Substituting (19) into (18), it can be obtained that

$$Q_{\chi^2}\left(\frac{2N\eta_{\text{op}}}{\sigma_h^2+\sigma_n^2}, 2N\right) = P_{F,1,thre}, \tag{20}$$

where $Q_{\chi^2}(z,\nu)$ denotes tail probability function of a Chi-Square distribution with DoF ν at z. Based on [28], we have

$$Q_{\chi^2}\left(z,\nu\right) = \exp\left(-\frac{1}{2z}\right)\sum_{k=0}^{\frac{\nu}{2}-1}\frac{1}{k!}\left(\frac{1}{2}z\right)^k, \nu \geqslant 2. \tag{21}$$

Through some mathematical calculations of (20), we finally obtain (17).

The proposition is proved. □

B. Second Level Decision

After the first level decision, Bob will calculate C_R by (10) for the case that $\Delta < \eta_{\text{op}}$. Then, Bob uses a threshold T to determine the accepted hypothesis, expressed as

$$C_R|\,\Delta < \eta_{\text{op}} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} T. \tag{22}$$

where $C_R|\,\Delta < \eta_{\text{op}}$ denotes the testing statistic C_R meeting $\Delta < \eta_{\text{op}}$ in the first level decision. If $C_R|\,\Delta < \eta_{\text{op}}$ is larger than T, Bob will accept $\mathcal{H}_1$; otherwise Bob will accept $\mathcal{H}_0$. Noting that T is used to distinguish the user with the acceptable transmit power, Bob can determine the proper value of T as [27].

IV. Performance Analysis

After the thresholds η and T of the two-level decision are given, the authentication performance of the proposed scheme is determined. In this section, we analyze the authentication performance of the proposed scheme, where the closed-form expressions of the probability of detection and the probability of false alarm are involved. Here, the major difficulty of performance analysis lies in the derivations of the PDF and numerical characteristic of the testing statistic C_R, which have been changed after the selection of the first level decision.

Specifically, Alice should pass the two-level decision to successfully complete the authentication. Here, the probability of detection for Alice in the proposed scheme can be given by

$$P_D = \Pr\left(\mathcal{H}_1|\mathcal{H}_1\right) = \left(1-P_{F,1,thre}\right)P_{D,2}, \tag{23}$$

where $1 - P_{F,1,thre}$ denotes the probability that Alice can successfully pass the first level decision. $P_{D,2}$ denotes the probability of detection in the second level decision for Alice after successfully passing the first level decision. Noting that the first level decision will affect the PDF of the original C_R, the probability of detection in the second level decision becomes a conditional probability, given by

$$P_{D,2} = \Pr\left(C_{R,\mathcal{H}_0} > \eta_{\text{op}}|\Delta_{\mathcal{H}_1} < T\right). \tag{24}$$

Since Bob will set a very small value of $P_{F,1,thre}$ to decrease the impact on probability of detection, we have the approximation

$$P_{D,2} \approx \Pr\left(C_{R,\mathcal{H}_0} > \eta_{\text{op}}|\text{without first threshold}\right). \tag{25}$$

According to [26], we have

$$P_{D,2} \approx Q\left(\frac{T-\mathbb{E}(C_{R,\mathcal{H}_1})}{\sqrt{N\left(\left(2-\frac{\pi}{2}\right)\frac{\sigma_h^2}{2}+\sigma_n^2\right)}}\right), \tag{26}$$

where $Q(\cdot)$ denotes the Q-function. $\mathbb{E}(C_{R,\mathcal{H}_1})$ denotes the expectation of $C_{R,\mathcal{H}_1}$, where $\mathbb{E}(C_{R,\mathcal{H}_1}) = \frac{N}{2}\sqrt{\frac{\pi\sigma_h^4}{\sigma_n^2\sigma_h^2}}$.

Moreover, the probability of false alarm of the proposed scheme can be expressed as

$$\rho_{\text{FA}} = \Pr\left(\mathcal{H}_1|\mathcal{H}_0\right) = \left(1-P_{D,1,\text{eve}}\right)\cdot\rho_{\text{FA},2}, \tag{27}$$

where $P_{D,1,\text{eve}}$ denotes the probability that Eve is correctly detected in the first level decision. $\rho_{\text{FA},2}$ denotes the probability that Eve passes the second level decision after successfully passing the first level decision.

Corollary 1. *$P_{D,1,eve}$ can be represented by*

$$P_{D,1,eve} = Q_{\chi^2}\left(\frac{Q_{\chi^2}^{-1}\left(P_{F,1,thre}, 2N\right)\left(\sigma_h^2+\sigma_n^2\right)}{E_e\sigma_h^2+\sigma_n^2}, 2N\right). \tag{28}$$

Proof. According to definition of $P_{D,1,\text{eve}}$, we have

$$P_{D,1,\text{eve}} = \Pr\left(\Delta_{\mathcal{H}_0} > \eta_{\text{op}}\right). \tag{29}$$

Recall that $y_{i,e} \sim \mathcal{CN}\left(0, E_e\sigma_h^2+\sigma_n^2\right)$. Similar to (19), we easily have

$$\frac{2N\Delta_{\mathcal{H}_0}}{E_e\sigma_h^2+\sigma_n^2}\sim\chi^2\left(2N\right). \tag{30}$$

Substituting (30) into (29), we have

$$P_{D,1,\text{eve}}=Q_{\chi^2}\left(\frac{2N\eta_{\text{op}}}{E_e\sigma_h^2+\sigma_n^2},2N\right). \tag{31}$$

Substituting (17) into (31), we finally obtain (28).

The corollary is proved. □

Note that the probability of false alarm $\rho_{\text{FA},2}$ can be obtained from the PDF of $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}$. However, the effect of the constraint $\Delta_{\mathcal{H}_0}<\eta_{\text{op}}$ on $C_{R,\mathcal{H}_0}$ seems complex, which makes it difficult to obtain the simple expression of the PDF of $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}$. Fortunately, $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}$ is the sum of $2N$ independent random variables. When N is sufficiently large, we have the approximation that $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}$ follows the Gaussian distribution based on the well-known central-limit theorem (CLT). Here, the PDF of $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}$ can be obtained by calculating its expectation and variance.

Proposition 2. *The expectation of $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{op}$ is given by*

$$\mathbb{E}\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{op}\right)=0. \tag{32}$$

Proof. Based on (10) and the symmetry of the Gaussian distribution, we obtain

$$\mathbb{E}\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right)=\frac{1}{2}\mathbb{E}\left(\sum_{i=1}^{N}y_{i,e}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right), \tag{33}$$

where $y_{i,e}\sim\mathcal{CN}(0,\sigma_n^2+E_e\sigma_h^2)$ and thus $\sum\limits_{i=1}^{N}y_{i,e}\sim\mathcal{CN}\left(0,N\left(\sigma_n^2+E_e\sigma_h^2\right)\right)$. According to (16), $\Delta_{\mathcal{H}_0}<\eta_{\text{op}}$ can be seen as an energy-constraint of $\sum\limits_{i=1}^{N}y_{i,e}$, the PDF of $\sum\limits_{i=1}^{N}y_{i,e}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}$ is still symmetrical about zero. Then, it can be achieved that

$$\mathbb{E}\left(\sum_{i=1}^{N}y_{i,e}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right)=0. \tag{34}$$

Substituting (34) into (33), we finally obtain (32).

The proposition is proved. □

Thereafter, we begin to calculate the expression of the variance of $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}$. To simplify the calculation of the variance, we have the following proposition.

Proposition 3. *The variance of $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{op}$ can be rewritten as*

$$Var\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{op}\right)=\frac{N}{2}\mathbb{E}\left(\Delta_{\mathcal{H}_0}|\,\Delta_{\mathcal{H}_0}<\eta_{op}\right). \tag{35}$$

Proof. Due to the result in **Proposition 2**, we easily have

$$\text{Var}\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right)=\mathbb{E}\left(C_{R,\mathcal{H}_0}^2|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right). \tag{36}$$

Substituting (12) into (36), we further have

$$\begin{aligned}&\text{Var}\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right)\\&=\mathbb{E}\left(\left(\mathcal{R}\left\{\sum_{i=1}^{N}\left(\sqrt{E_e}\left|h_{BE,i}\right|e^{j(\Delta\mathcal{M}(k_{eb,i})-\varepsilon_{eb,i})}+\right.\right.\right.\right.\\&\left.\left.\left.\tilde{\omega}_{b,i})\}\right)^2|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right)\\&=\frac{1}{2}\mathbb{E}\left(\left(\sum_{i=1}^{N}\left(\sqrt{E_e}\left|h_{BE,i}\right|e^{j(\Delta\mathcal{M}(k_{eb,i})-\varepsilon_{eb,i})}+\right.\right.\right.\\&\left.\left.\tilde{\omega}_{b,i})\right)^2|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right),\end{aligned} \tag{37}$$

where $\mathcal{R}(\cdot)$ can be replaced with $\frac{1}{2}$ in (37) due to the symmetry of $e^{-j\mathcal{M}(\mathbf{K}_B)}\mathbf{y}$ under $\mathcal{H}_0$ in terms of the real and the imaginary parts. In other words, $\mathcal{R}\left\{e^{-j\mathcal{M}(\mathbf{K}_B)}\mathbf{y}\right\}$ has the same PDF as that of $\mathcal{I}\left\{e^{-j\mathcal{M}(\mathbf{K}_B)}\mathbf{y}\right\}$ under $\mathcal{H}_0$, which leads to the same value of expectation.

Since the AWGN and channel response on different subcarriers are independent of each other, it can be obtained that

$$\mathbb{E}\left(\tilde{\omega}_{b,i}\tilde{\omega}_{b,k}|\,\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right)=0 \tag{38}$$

and

$$\begin{aligned}&\mathbb{E}\left(\left|h_{BE,i}\right|e^{j(\Delta\mathcal{M}(k_{eb,i})-\varepsilon_{eb,i})}\times\right.\\&\left.\left|h_{BE,k}\right|e^{j(\Delta\mathcal{M}(k_{eb,k})-\varepsilon_{eb,k})}\right|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\Big)=0,\end{aligned} \tag{39}$$

when $i\neq k$. Substituting (38) and (39) into (37), we have

$$\begin{aligned}&\text{Var}\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right)=\\&=\frac{1}{2}\mathbb{E}\left(\sum_{i=1}^{N}\left(E_e|h_{BE,i}|^2+|\tilde{\omega}_{b,i}|^2\right)\right|\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\Bigg)\\&=\frac{N}{2}\mathbb{E}\left(\Delta_{\mathcal{H}_0}|\,\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right).\end{aligned} \tag{40}$$

The proposition is proved. □

Taking a closer look at (40), it is necessary to provide the expression of $\mathbb{E}\left(\Delta_{\mathcal{H}_0}|\,\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right)$. To begin with, we consider a simple example that $\mathbb{E}\left(X|\,X<T_X\right)$, where X is a random variable following a Chi-Square distribution with DoF ν, and T_X is the constant threshold. We have the following proposition.

Proposition 4. *The closed-form expression of* $\mathbb{E}\left(X|\,X<T_X\right)$ *can be represented by*

$$\begin{aligned}&\mathbb{E}\left(X|\,X<T_X\right)=\frac{\frac{\nu}{2}\exp\left(-\frac{T_X}{2}\right)}{1-Q_{\chi^2}\left(T_X,\nu\right)}\times\\&\left(\left(-2\sum_{j=1}^{\frac{\nu}{2}-1}\left(2^{-(j+1)}\frac{T_X^{j+1}}{(j+1)!}\right)-\left(T_X+2\right)\right)+\nu\right).\end{aligned} \tag{41}$$

Proof. See Appendix A.

□

Now, we need to convert $\mathbb{E}\left(\Delta_{\mathcal{H}_0}|\,\Delta_{\mathcal{H}_0}<\eta_{\text{op}}\right)$ in (40) to the closed-form expression of $\mathbb{E}\left(X|\,X<T_X\right)$ as provided in

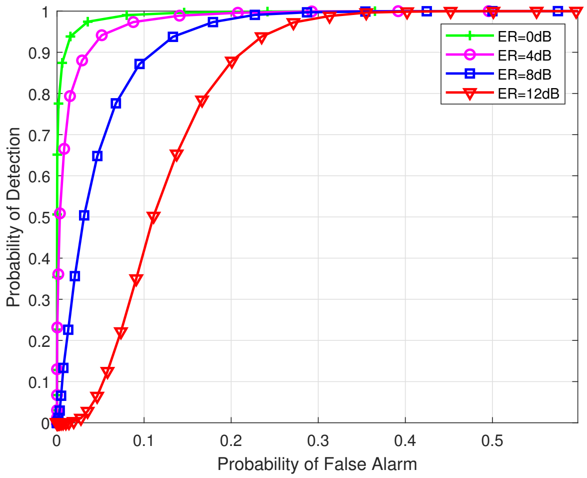

Fig. 4. ROC performance comparisons of the traditional channel-phase based PLA scheme under various values of ERs.

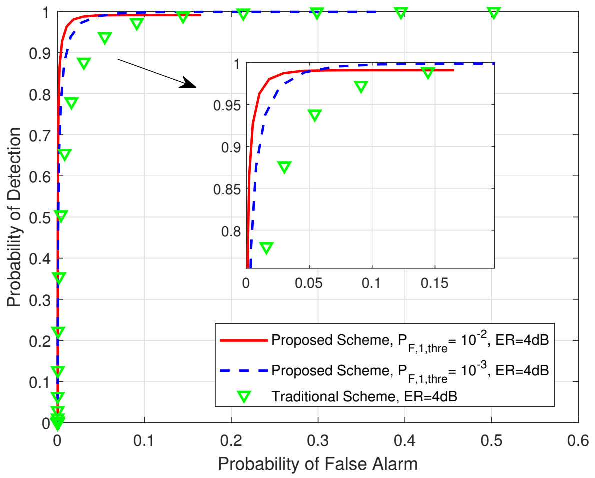

Fig. 5. ROC performance comparisons between the traditional channel-phase based PLA scheme and the proposed scheme under ER $= 4$dB.

Proposition 4. According to the relationship between X and $\Delta_{\mathcal{H}_0}$, we rewrite (40) as

$$\begin{aligned}&\mathrm{Var}\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\mathrm{op}}\right)=\frac{N}{2}\mathbb{E}\left(\Delta_{\mathcal{H}_0}|\,\Delta_{\mathcal{H}_0}<\eta_{\mathrm{op}}\right)\\&=\frac{N}{2}\mathbb{E}\left(\Delta_{\mathcal{H}_0}|\,\frac{\Delta_{\mathcal{H}_0}}{\Omega}<\frac{\eta_{\mathrm{op}}}{\Omega}\right)\\&=\frac{N}{2}\Omega\mathbb{E}\left(X|\,X<\frac{\eta_{\mathrm{op}}}{\Omega}\right),\end{aligned}\tag{42}$$

where Ω denotes the coefficient between X and $\Delta_{\mathcal{H}_0}$, i.e., $\Delta_{\mathcal{H}_0}=\Omega X$. Based on the definition of $\Delta_{\mathcal{H}_0}$, we have

$$\Omega=\frac{E_e\sigma_h^2+\sigma_n^2}{2N}.\tag{43}$$

Ensuring $T_X=\frac{\eta_{\mathrm{op}}}{\Omega}$ and $\nu=2N$ in (41) and then substituting (41) into (42), we finally obtain the closed-form expression of $\mathrm{Var}\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\mathrm{op}}\right)$.

Since $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\mathrm{op}}$ approximately follows the Gaussian distribution according to CLT, i.e., $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\mathrm{op}}\sim\mathcal{N}\left(0,\mathrm{Var}\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\mathrm{op}}\right)\right)$, we obtain

$$\rho_{\mathrm{FA},2}\approx Q\left(\frac{T}{\sqrt{\mathrm{Var}\left(C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0}<\eta_{\mathrm{op}}\right)}}\right).\tag{44}$$

Substituting (44) and (28) into (27), we finally achieve the probability of false alarm of the proposed scheme.

V. Simulation Results

In simulations, we utilize the state-of-the-art channel-phase based PLA scheme in [27] as the benchmark scheme, which is termed as the traditional scheme in the following discussions for short. In the proposed scheme, we first calculate the first threshold η by fixing $P_{F,1,thre}$ and then use different values of T to calculate the probabilities of detection and false alarm for the proposed scheme. Moreover, the receiver operator characteristic (ROC) is further used as the metric for performance comparisons.

In Fig. 4, we provide the ROC performance of the traditional channel-phase based PLA scheme under various ERs, where SNR is set as 0dB and $N=32$. It can be seen that the ROC performance decreases as the increase of ER, which represents the serious threats as mentioned in Section II. For example, let us focus on $\rho_{\mathrm{FA}}=0.1$. Compared with the case that Eve uses the normal transmit power, i.e., ER $=$ 0dB, the probability of detection drops substantially from about 99% to 40% at the case of ER $=$ 12dB. Therefore, it is urgent for legitimate users to resist Eve with high transmit power during the authentication process.

In Fig. 5, the ROC performance comparison between the proposed scheme and the traditional channel-phase based PLA scheme are provided under ER $=$ 4dB. Here, the simulation parameters are set as $P_{F,1,thre}=10^{-2}$ and 10^{-3}, SNR $=$ 0dB and $N=32$. We have the following conclusions. First, the ROC performances of the proposed scheme under both $P_{F,1,thre}=10^{-2}$ and 10^{-3} are better than the traditional channel-phase based PLA scheme at the regular value of probability of false alarm, such as $\rho_{\mathrm{FA}}=10^{-2}$, which demonstrates the superiority of the proposed scheme under high transmit power aided impersonation attack from Eve. Second, the ROC performances of the proposed scheme under $P_{F,1,thre}=10^{-2}$ and 10^{-3} are different, which requires to well select according to the requirement of Bob. Specifically, the proposed scheme under $P_{F,1,thre}=10^{-2}$ has the better authentication performance under the constraint of $\rho_{\mathrm{FA}}<0.05$ whilst the proposed scheme under $P_{F,1,thre}=10^{-3}$ is better at the rest range of ρ_{FA}.

In Fig. 6, we illustrate the ROC performance comparisons between the traditional channel-phase based PLA scheme and the proposed scheme under ER $=$ 0dB. Here, the parameter settings are the same as Fig. 5 except for ER. We have the following conclusions. First, the ROC performance of the proposed scheme is close to that of the traditional channel-phase based PLA scheme as the decrease of $P_{F,1,thre}$. Especially when $P_{F,1,thre}=10^{-3}$, the ROC performance of the proposed scheme is very close to that of the traditional scheme, which indicates that the first level decision has few impact on the authentication performance when Eve uses the same transmit

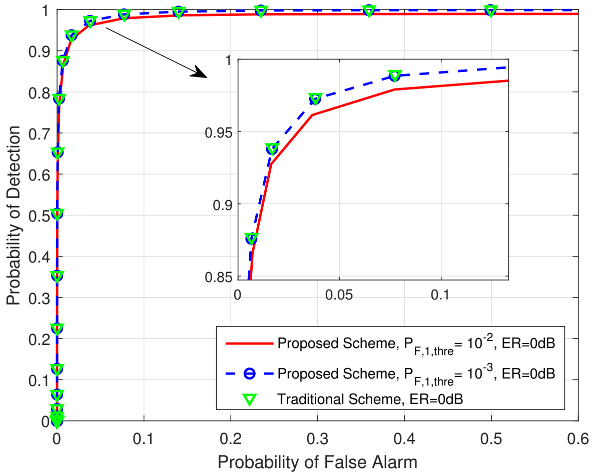

Fig. 6. ROC performance comparisons between the traditional channel-phase based PLA scheme and the proposed scheme under ER = 0dB.

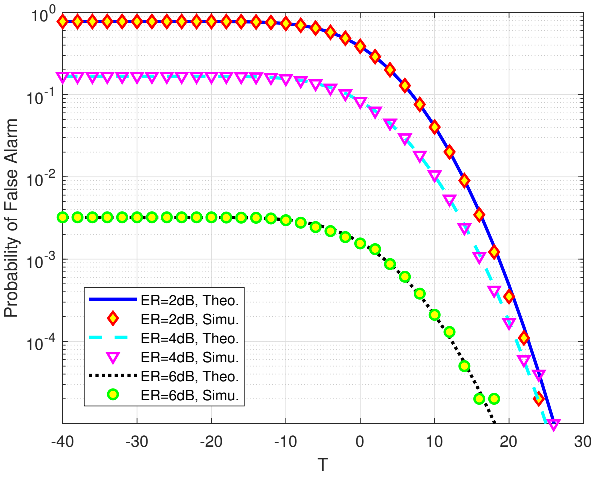

Fig. 8. Simulated and theoretical probabilities of false alarm of the proposed scheme under various values of T.

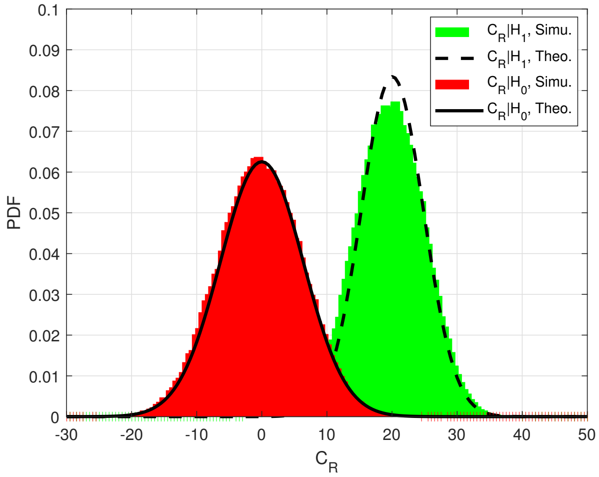

Fig. 7. Comparison between simulated results and the approximated theoretical results of C_R after passing the first level decision.

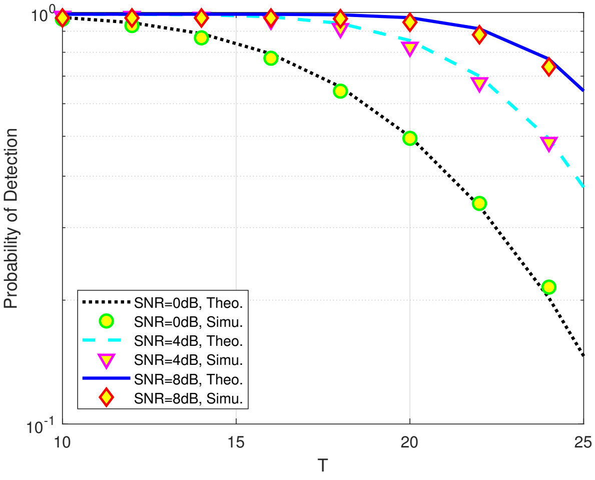

Fig. 9. Simulated and theoretical probabilities of detection of the proposed scheme under various values of T.

power as Alice. Finally, considering Fig. 5 and Fig. 6, the robustness of the proposed scheme are verified.

To verify the theoretical results in performance analysis, we illustrate the comparison between simulated results and the approximated theoretical results of C_R after passing the first level decision in Fig. 7. Here, we use 2×10^5 samples to obtain the simulated results, and set $N = 32$, $P_{F,1,thre} = 0.01$, SNR = 0dB and ER = 6dB. It can be observed that the approximated theoretical results of $C_{R,\mathcal{H}_1}|\Delta_{\mathcal{H}_1} < \eta_{\text{op}}$ is very close to the simulated ones, which shows that the approximated theoretical results in [26] can be used to well estimate the authentication performance though the PDF of $C_{R,\mathcal{H}_1}$ is affected by the first level decision. The small deviation here is due to the approximated error in variance as stated in [26]. Moreover, we observe that the approximated theoretical results of $C_{R,\mathcal{H}_0}|\Delta_{\mathcal{H}_0} < \eta_{\text{op}}$ fit very well with the simulated ones, which verifies the effectiveness of (32) and (42).

Fig. 8 investigates the comparison between the simulated and theoretical probabilities of false alarm under various values of T. Here, we set SNR = 0dB, $N = 32$ and $P_{F,1,thre} = 0.01$. ER is set as 2dB, 4dB and 6dB, respectively. We have the following observations. To begin with, the probability of false alarm decreases as the increase of ER, which indicates that the higher transmit power used by Eve will not decrease the authentication performance of the proposed scheme. On the contrary, the authentication performance of the proposed scheme is improved since the higher transmit power of response signals can not pass the first level decision, which demonstrates the significance of our proposed scheme. Moreover, the theoretical probabilities of false alarm match very well with the simulated ones, which indicates the effectiveness of our theoretical performance analysis.

Fig. 9 investigates the comparison between the simulated and theoretical probabilities of detection under various values of T. Here, we set ER = 2dB, $N = 32$ and $P_{F,1,thre} = 0.01$. Meanwhile, SNR is set as 0dB, 4dB and 8dB, respectively. We

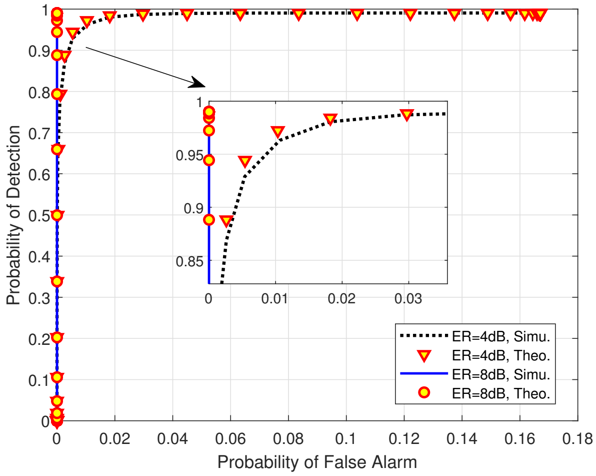

Fig. 10. Comparisons between simulated and theoretical ROC performance of the proposed scheme.

observe that the theoretical probability of detection improves as the increase of SNR, which can be explained by the fact that the impact of AWGN on authentication performance decreases. Moreover, the theoretical probability of detection is also close to the simulated one, where the small deviation is due to the approximation error of the variance. Hence, the effectiveness of the theoretical performance analysis is demonstrated.

Fig. 10 provides the comparisons between simulated and theoretical ROC performance of the proposed scheme. Here, we set SNR $=$ 0dB, $N = 32$ and $P_{F,1,thre} = 0.01$, whilst ER is set as 4dB and 8dB, respectively. We have the following conclusions. First, the ROC performance of the proposed scheme improves as the increase of ER, which contributes to the proposed first level decision. Second, the theoretical ROC curves are close to the simulated curves under both ER = 4dB and ER = 8dB, which demonstrates effectiveness of the performance analysis. Finally, the small deviation between theoretical ROC and simulated ROC curves exists due to the small approximation error of the approximated theoretical probability of detection.

VI. Conclusion

In this paper, we considered the serious threat that Eve used an extremely high transmit power in the authentication process, which attempts to pass the authentication illegally. To solve this issue, we proposed a robust channel-phase based PLA scheme by using the novel two-level decision in the PLA process. Specifically, Bob first calculated the average energy of a user's response and derived an optimal threshold to prevent Eve from using high transmit power. Then, the second level decision was used to distinguish the legitimate users. Moreover, the theoretical performance analysis was provided for the proposed scheme to accurately estimate the authentication performance. Simulation results indicated the significant improvement on the authentication performance of our proposed scheme, and demonstrated the effectiveness of the theoretical results.

One of our future plans is to consider the multiple users scenario, which aims to enhance the efficiency of authentication for more legitimate users cases and avoid the unnecessary information leakage in the authentication request. Moreover, another future plan is to evaluate our proposed scheme in a real system.

Appendix A
Proof of Proposition 4

Through the definition of $\mathbb{E}\left(X|\,X<T_X\right)$, we obtain

$$\mathbb{E}\left(X|\,X<T_X\right)=\frac{\int\limits_0^{T_X} xf(x)dx}{\int\limits_0^{T_X} f(x)dx}, \tag{45}$$

where $f(x)$ denotes the PDF of X, which can be expressed as [28]

$$f(x)=\begin{cases}\dfrac{1}{2^{\frac{\nu}{2}}\Gamma\left(\frac{\nu}{2}\right)}x^{\frac{\nu}{2}-1}\exp\left(-\dfrac{1}{2}x\right) & ,x>0,\\ & 0,x<0.\end{cases} \tag{46}$$

Substituting (46) into the numerator of (45), we further have

$$\begin{aligned}\int\limits_0^{T_X} xf(x)dx &= \frac{1}{2^{\frac{\nu}{2}}\Gamma\left(\frac{\nu}{2}\right)}\int\limits_0^{T_X} x^{\frac{\nu}{2}}\exp\left(-\frac{1}{2}x\right)dx\\ &= \frac{1}{2^{\frac{\nu}{2}}\Gamma\left(\frac{\nu}{2}\right)}\left(\underbrace{-2T_X{}^{\frac{\nu}{2}}\exp\left(-\frac{1}{2}T_X\right)}_{A_0}+\right.\\ &\qquad\left.\underbrace{\nu\int\limits_0^{T_X} x^{\frac{\nu}{2}-1}\exp\left(-\frac{1}{2}x\right)dx}_{B_0}\right),\end{aligned} \tag{47}$$

where B_0 can be further derived as

$$\begin{aligned}B_0 = &\underbrace{-2\cdot 2\cdot\frac{\nu}{2}T_X{}^{\frac{\nu}{2}-1}\exp\left(-\frac{1}{2}T_X\right)}_{A_1}+\\ &\underbrace{2^2\frac{\nu}{2}\left(\frac{\nu}{2}-1\right)\int\limits_0^{T_X} x^{\frac{\nu}{2}-2}\exp\left(-\frac{1}{2}x\right)dx}_{B_1}.\end{aligned} \tag{48}$$

Similarly, B_1 can be further derived as

$$\begin{aligned}B_1 = &\underbrace{-2\cdot 2^2\cdot\frac{\nu}{2}\left(\frac{\nu}{2}-1\right)T_X{}^{\frac{\nu}{2}-2}\exp\left(-\frac{1}{2}T_X\right)}_{A_2}+\\ &\underbrace{2^3\frac{\nu}{2}\left(\frac{\nu}{2}-1\right)\left(\frac{\nu}{2}-2\right)\int\limits_0^{T_X} x^{\frac{\nu}{2}-3}\exp\left(-\frac{1}{2}x\right)dx}_{B_2}.\end{aligned} \tag{49}$$

From (47) to (49), we can observe that each item of B can be divided into a new A and B. Based on the rule of A and B, we have the $\frac{\nu}{2} - 2$-th item

$$\begin{aligned}
&A_{\frac{\nu}{2}-2} = -2 \cdot 2^{\frac{\nu}{2}-2} \cdot \left(\frac{\nu}{2}!\right) \cdot \frac{1}{2} {T_X}^2 \exp\left(-\frac{1}{2} T_X\right), \\
&B_{\frac{\nu}{2}-2} = 2^{\frac{\nu}{2}-1} \left(\frac{\nu}{2}!\right) \int\limits_0^{T_X} x \exp\left(-\frac{1}{2} x\right) dx.
\end{aligned} \tag{50}$$

Then, we easily have

$$\begin{aligned}
\frac{1}{2^{\frac{\nu}{2}} \Gamma\left(\frac{\nu}{2}\right)} B_{\frac{\nu}{2}-2} &= \frac{\nu}{4} \int\limits_0^{T_X} x \exp\left(-\frac{1}{2} x\right) dx \\
&= -\left(T_X + 2\right) \frac{\nu}{2} \exp\left(-\frac{1}{2} T_X\right) + \nu.
\end{aligned} \tag{51}$$

Based on (47)-(51), we have

$$\begin{aligned}
&\int\limits_0^{T_X} x f(x) dx = \frac{1}{2^{\frac{\nu}{2}} \Gamma\left(\frac{\nu}{2}\right)} \left(\sum_{i=0}^{\frac{\nu}{2}-2} A_i + B_{\frac{\nu}{2}-2} \right) \\
&= -\left(T_X + 2\right) \frac{\nu}{2} \exp\left(-\frac{T_X}{2}\right) + \nu \\
&+ \frac{1}{2^{\frac{\nu}{2}} \Gamma\left(\frac{\nu}{2}\right)} \sum_{i=0}^{\frac{\nu}{2}-2} A_i.
\end{aligned} \tag{52}$$

For the sake of simplicity, let $A_{\frac{\nu}{2}-2}$ be the first item of $A^{\dagger}$, i.e., $A_{\frac{\nu}{2}-2} = A_1^{\dagger}$, and then we obtain

$$\begin{aligned}
&\sum_{i=0}^{\frac{\nu}{2}-2} A_i = \sum_{j=1}^{\frac{\nu}{2}-1} A_j^{\dagger} \\
&= -2 \exp\left(-\frac{T_X}{2}\right) \sum_{j=1}^{\frac{\nu}{2}-1} \left(\frac{\nu}{2}\right) \frac{1}{(j+1)!} {T_X}^{j+1}.
\end{aligned} \tag{53}$$

Substituting (53) into (52), we finally have

$$\begin{aligned}
&\int\limits_0^{T_X} x f(x) dx = -2 \exp\left(-\frac{T_X}{2}\right) \frac{\nu}{2} \sum_{j=1}^{\frac{\nu}{2}-1} \left(2^{-(j+1)} \frac{{T_X}^{j+1}}{(j+1)!} \right) \\
&- \left(T_X + 2\right) \frac{\nu}{2} \exp\left(-\frac{T_X}{2}\right) + \nu \\
&= \frac{\nu}{2} \exp\left(-\frac{T_X}{2}\right) \left(-2 \sum_{j=1}^{\frac{\nu}{2}-1} \left(2^{-(j+1)} \frac{{T_X}^{j+1}}{(j+1)!} \right) - \left(T_X + 2\right) \right) + \nu.
\end{aligned} \tag{54}$$

Here, the denominator of (45) can be calculated by

$$\int\limits_0^{T_X} f(x) dx = 1 - Q_{\chi^2}\left(T_X, \nu\right). \tag{55}$$

Substituting (54) and (55) into (45), we finally obtain (41). The proposition is proved.

□

References

[1] E. Illi, M. Qaraqe, S. Althunibat, A. Alhasanat, M. Alsafasfeh, M. de Ree, G. Mantas, J. Rodriguez, W. Aman, and S. Al-Kuwari, "Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 347–388, 2024.

[2] N. Xie, J. Zhang, Q. Zhang, H. Tan, A. X. Liu, and D. Niyato, "Hybrid physical-layer authentication," *IEEE Transactions on Mobile Computing*, vol. 23, no. 2, pp. 1295–1311, 2024.

[3] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[4] S. Khan, C. Thapa, S. Durrani, and S. Camtepe, "Access-based lightweight physical-layer authentication for the internet of things devices," *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 11 312–11 326, 2024.

[5] M. Abdrabou and T. A. Gulliver, "Adaptive physical-layer authentication for IoT in MIMO communication systems using support vector machine," *IEEE Internet of Things Journal*, vol. 10, no. 22, pp. 19 861–19 873, 2023.

[6] Y. Zhou, Z. Ma, H. Liu, P. L. Yeoh, Y. Li, B. Vucetic, and P. Fan, "A UAV-aided physical layer authentication based on channel characteristics and geographical locations," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 1053–1064, 2024.

[7] Y. Teng, P. Zhang, Y. Liu, J. Dong, and F. Xiao, "Exploiting carrier frequency offset and phase noise for physical layer authentication in UAV-aided communication systems," *IEEE Transactions on Communications*, pp. 1–1, 2024.

[8] J. Xu and D. Wei, "Polarization fingerprint-based lorawan physical layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 4593–4608, 2023.

[9] T. Zhang, Y. Huo, Q. Gao, L. Ma, Y. Wu, and R. Li, "Cooperative physical layer authentication with reputation-inspired collaborator selection," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 22 165–22 181, 2023.

[10] Y. Chen, P.-H. Ho, H. Wen, S. Y. Chang, and S. Real, "On physical-layer authentication via online transfer learning," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 1374–1385, 2022.

[11] T. Jing, H. Huang, Q. Gao, Y. Wu, Y. Huo, and Y. Wang, "Multi-user physical layer authentication based on CSI using resnet in mobile IIoT," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1896–1907, 2024.

[12] G. Zhang, Q. Hu, Y. Zhang, Y. Dai, and T. Jiang, "Lightweight cross-domain authentication scheme for securing wireless IoT devices using backscatter communication," *IEEE Internet of Things Journal*, pp. 1–1, 2024.

[13] D. Huang, A. Al-Hourani, K. Sithamparanathan, and W. S. Rowe, "Deep learning methods for IoT device authentication using symbols density trace plot," *IEEE Internet of Things Journal*, pp. 1–1, 2024.

[14] N. Xie, M. Sha, T. Hu, and H. Tan, "Multi-user physical-layer authentication and classification," *IEEE Transactions on Wireless Communications*, vol. 22, no. 9, pp. 6171–6184, 2023.

[15] Y. Cai, W. Wang, Y. Chen, H. Tan, N. Xie, and J. Wang, "Multiple cooperative attackers for tag-based physical layer authentication," *IEEE Communications Magazine*, vol. 61, no. 7, pp. 165–171, 2023.

[16] H. Tan, Z. Li, N. Xie, J. Lu, and D. Niyato, "Detection of jamming attacks for the physical-layer authentication," *IEEE Transactions on Wireless Communications*, vol. 22, no. 12, pp. 9579–9594, 2023.

[17] Q. Wang, W. Liang, J. Zhang, K. Wang, and X. Jiang, "Knowledge-enhanced physical layer authentication for mobile devices," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2024.

[18] Q. Wang, W. Liang, Z. Pang, J. Zhang, K. Wang, and Y. Yu, "Improving transferability and immunity of physical layer authentication by the channel time-varying pattern," *IEEE Wireless Communications Letters*, vol. 13, no. 3, pp. 751–755, 2024.

[19] S. Tomasin, "Analysis of channel-based user authentication by key-less and key-based approaches," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 5700–5712, 2018.

[20] N. Xie, J. Chen, and L. Huang, "Physical-layer authentication using multiple channel-based features," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2356–2366, 2021.

[21] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1817–1827, 2013.

[22] X. Wu and Z. Yang, “Physical-layer authentication for multi-carrier transmission,” *IEEE Communications Letters*, vol. 19, no. 1, pp. 74–77, 2015.

[23] Y. Liu, H.-H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[24] L. Cheng, L. Zhou, B. C. Seet, W. Li, D. Ma, and J. Wei, “Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase,” *Mobile Information Systems,2017,(2017-7-10)*, vol. 2017, no. pt.3, pp. 1–13, 2017.

[25] X. Lu, J. Lei, Y. Shi, and W. Li, “Improved physical layer authentication scheme based on wireless channel phase,” *IEEE Wireless Communications Letters*, vol. 11, no. 1, pp. 198–202, 2022.

[26] X. Lu, J. Lei, Y. Shi, H. Fang, and W. Li, “Analytical method of physical layer authentication for performance evaluation,” in *2022 IEEE GLOBECOM Workshops, (GC Wkshps 2022)*, 2022.

[27] X. Lu, J. Lei, Y. Shi, and W. Li, “Physical-layer authentication based on channel phase responses for multi-carriers transmission,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1734–1748, 2023.

[28] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Englewood Cliffs, NJ, USA:Prentice-Hall, 1998.