IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 July 2024, accepted 15 August 2024, date of publication 19 August 2024, date of current version 29 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3445956

RESEARCH ARTICLE

Key-Indexed Channel Phase Extended Permutation for Secure Physical Layer Authentication in Correlated Sub-Channels

KYOUNGYEON GO[1,2], SEUNGNAM HAN[2], (Graduate Student Member, IEEE), AND EUISEOK HWANG[2], (Senior Member, IEEE)

[1]Department of Physics and Photon Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea
[2]School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea

Corresponding author: Euiseok Hwang (euiseokh@gist.ac.kr)

This work was supported in part by the Ministry of Science and Information and Communication Technology (MSIT), South Korea, under the Information Technology Research Center (ITRC) Support Program supervised by the Institute of Information Communications Technology Planning Evaluation (IITP) under Grant IITP-2024-2021-0-01835; and in part by the National Research Foundation (NRF) Grants, Basic Research Laboratory, under Grant RS-2023-00218908.

ABSTRACT In this paper, we present a novel key-indexed channel phase permutation method designed to enhance the security of physical-layer (PHY) authentication in the presence of correlated sub-channels. In wireless communication, secret keys should be protected from eavesdroppers, as unauthorized access to these keys may compromise user security, expose sensitive information, and allow attackers to impersonate legitimate users, bypassing authentication mechanisms. To avoid the malicious interception of the pre-shared secret keys in wireless communication, the proposed scheme takes advantage of the inherent characteristics of reciprocal radio frequency channel phases and the key indices between authorized users. This ensures the completion of PHY authentication process at the PHY layer without divulging the actual secret key to potential attackers. Channel phase data are permuted based on binary key indices and concealed within phase information, thwarting unauthorized access. Through extensive testing using a Universal Software Radio Peripheral testbed, we validate the robustness of our scheme to various attacks, ensuring the confidentiality of secret keys and distinguishing legitimate users from attackers attempting illicit authentication. This method strengthens PHY layer security, offering practical applicability in wireless communication scenarios.

INDEX TERMS Physical-layer authentication, wireless security, universal software radio peripheral.

I. INTRODUCTION

Physical layer authentication (PLA) is a wireless security technique that authenticates users by leveraging the unique characteristics of signals in the physical layer (PHY). Using specific signal properties in the PHY, PLA provides several advantages such as real-time operation, efficient resource usage, and simple implementation [1]. Because PLA offers high attack defense capability that enhances cryptography-based security [2], low resource consumption, and fast execution time because of its small computational effort [3], it has been widely researched in the field of wireless security [4].

In wireless communication, users can easily access signals, so important information used for user authentication may be exposed to unauthorized users. Therefore, PLA scheme must effectively protect this information from eavesdropping [4]. PLA includes methods for sharing secret keys between legitimate users and methods for not sharing such keys. Methods in the latter category proposed by [5], [6], and [7] check user legitimacy by comparing the channel data with the data from the legitimate user at the adjacent transmission

The associate editor coordinating the review of this manuscript and approving it for publication was Yuli Yang.

© 2024 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

time. Several other methods attempt authentication without the secret key. Moreover, schemes that can be used to distinguish legitimate users from unauthorized users using secret keys have been proposed [8], [9], [10], [11], [12], [13]. The PHY phase challenge-response authentication scheme (PHY-PCRAS) [8] encapsulates secret keys by subtracting the channel phase between two users from the phase of the secret key (0 or π). Artificial-noise-aided PHY-PCRAS (ANA-PHY-PCRAS) [9] encapsulates secret keys by adding an artificial noise to the concealment method used in PHY-PCRAS. The PLA scheme PHY-PPECRAS [10] quantizes a secret key into 2^M pieces. For example, in the case of $M = 2$, the secret key is hidden by dividing the secret key by M bits and quantizing the key phase to $[0\ \frac{\pi}{2}\ \pi\ \frac{3\pi}{2}]$. Three of the aforementioned schemes exhibit excellent security performance when an attacker attempts to eavesdrop on a legitimate signal in independent channel fading environments. However, they do not solve problems related to sub-channel correlation and channel reciprocity. PHY phase secret key encapsulation in correlated sub-channels (PHY-PSIONICS) [11] encapsulates secret keys by quantizing the channel phase between legitimate users. PHY-PSIONICS shows notable security performance against eavesdropping and replay attacks in correlated sub-channels, but it cannot prevent man-in-the-middle attacks.

In this paper, we present a novel key permutation method designed to conceal secret keys effectively in the presence of correlated sub-channels. We conduct experiments in a real communication environment to collect channel phase data specifically within the context of correlated sub-channels, and we leverage these data to assess the security performance of our proposed scheme within such an environment. We evaluate various attack scenarios may reveal vulnerabilities and rigorously examine the security performance of the approach in each case. Furthermore, we introduce a robust method for quantifying criteria that can be used to distinguish authenticated users from potential attackers. These criteria play an important role in our experimental evaluation, providing a basis for assessing the effectiveness of the proposed approach. The contributions of this paper are as follows:

- We verify the security performance of the proposed method using channel data in an actual indoor environment using a universal software radio peripheral (USRP). Specifically, we check its performance in a correlated sub-channel environment, which is similar to an actual communication environment. Results confirm that the method can be used sufficiently in reality.
- In our design, the secret key is safely hidden without complex calculations. An attacker cannot infer the secret key through eavesdropping and can be distinguished from a legitimate user despite a brute-force attack.
- We propose criteria for distinguishing attackers from legitimate users. Our finding confirms that the security performance of the proposed approach, evaluated through the proposed criteria, makes the method sufficiently useful in a real communication environment.

The remainder of this paper is structured as follows: Section II provides an overview of PHY-PCRAS and the necessary calculations for integrating channel phase data. Section III introduces our novel system model, phase extended permutation approach, and authentication method of the proposed scheme. Section IV outlines our experimental setup, and Section V presents results obtained in various attack scenarios. We conclude our work in Section VI. Throughout the paper, we denote $\exp(\cdot)$ as the natural exponential function (i.e., $e^{(\cdot)}$), $\odot$ as the element-wise multiplication, $(\cdot)^T$ as the transpose operation, and j as $\sqrt{-1}$, respectively.

II. PRELIMINARIES

This section provides a concise overview of the PHY-PCRAS system model, which is integral to our proposed method, along with essential calculations needed for integrating URSP-measured channel phase data.

A. PHASE CHALLENGE-RESPONSE AUTHENTICATION

In authentication systems, secret keys should remain impervious to deduction, even in the event of eavesdropping. The proposed scheme conceals the secret key so that an attacker cannot infer it even if they eavesdrop in a communication environment with a high correlation between sub-channels. In the PLA scheme, the secret key shared with legitimate users follows binary phase-shift keying (BPSK) modulation or quadrature phase shift keying (QPSK) modulation, so it is composed of 0 and 1. In this scheme, channel phase data between users are permuted for sub-channels using the indexes of 0 and 1 of the secret key to conceal the key. The conditions of the proposed scheme are as follows:

- This scheme is based on multi-carrier transmission in the frequency domain.
- The signal transmitted in this system are of the following form:

$$\mathbf{s} = \mathbf{r} \odot \exp(j\boldsymbol{\theta}), \tag{1}$$

  where $\mathbf{r} = [r_1, r_2, \ldots, r_N]^T$ and $\boldsymbol{\theta} = [\theta_1, \theta_2, \ldots, \theta_N]^T$ represent amplitudes and phases of the signal of $\mathbf{s}$ in N sub-carriers transmission, respectively.
- Alice and Bob are legitimate users who share the secret key $\boldsymbol{\varphi}$, and Bob requests authentication from Alice. Eve is an illegitimate user (attacker).
- The channel without noise between Alice and Bob, $\mathbf{h}_{\mathrm{AB}}$, is of the following form:

$$\mathbf{h}_{\mathrm{AB}} = \mathbf{r}_{\mathrm{AB}} \odot \exp(j\boldsymbol{\theta}_{\mathrm{AB}}), \tag{2}$$

  where $\mathbf{r}_{\mathrm{AB}} = [r_{\mathrm{AB},1}, r_{\mathrm{AB},2}, \ldots, r_{\mathrm{AB},N}]^T$ and $\boldsymbol{\theta}_{\mathrm{AB}} = [\theta_{\mathrm{AB},1}, \theta_{\mathrm{AB},2}, \ldots, \theta_{\mathrm{AB},N}]^T$ represent the amplitude and the phase responses of the channel, respectively.
- Due to the noise between Alice and Bob, estimated channel $\hat{\mathbf{h}}_{\mathrm{AB}}$, is of the following form:

$$\hat{\mathbf{h}}_{\mathrm{AB}} = \mathbf{h}_{\mathrm{AB}} + \mathbf{w}_{\mathrm{AB}}, \tag{3}$$

where $\mathbf{w}_{\mathrm{AB}}$ is noise that occurs when Alice transmits the signal to Bob. Here, $\hat{\mathbf{h}}_{\mathrm{AB}} \approx \hat{\mathbf{h}}_{\mathrm{BA}}$ holds assuming channel reciprocity.

- As the signal used in this scheme has N sub-carriers, each i^{th} sub-carrier in $\mathbf{s} = [s_1, s_2, \ldots, s_N]$ suffers from channel noise.

B. PHY-PCRAS [8]

Upon Bob's request for authentication, Alice transmits a challenge signal to Bob, and the phase of this signal is set to 0 ($\theta_{chal_i} = 0$). Bob receives the signal containing the channel information between Alice and Bob, including the noise generated during the communication process. Using this signal, Bob can estimate the channel information ($\hat{\theta}_{\mathrm{AB}_i}$) between Alice and Bob. Then, Bob transmits the response signal ($\theta_{res_i} = \varphi_i - \hat{\theta}_{\mathrm{AB}_i}$) to Alice. As the channel phase between Alice and Bob satisfies reciprocity, Alice receives a response signal similar to φ_i. Therefore, Alice distinguishes whether the user requesting authentication is Bob or Eve by examining the similarity between the secret key and received response signal.

C. PHASE FINGERPRINTING

We cannot directly execute phase challenge-response authentication scheme in actual environments. The symbol time offset (STO), sampling frequency offset (SFO), carrier frequency offset (CFO), and initial phase caused by unsynchronized transmitters and receivers distort channel data [14]. Therefore, after correcting the measured channel phase using method proposed in [15], we confirmed the security performance of the proposed method in this paper. The channel phase of sub-carrier i is expressed as follows:

$$\breve{\theta}_i = \theta_i + 2\pi i \Delta t + \beta + w, \tag{4}$$

where $\breve{\theta}_i$ is the measured channel phase and θ_i is the actual channel phase. Δt is a variable caused by STO and SFO, β is the initial phase, and w is random noise generated during signal propagation. Accurately measuring Δt and β is difficult. However, as the values of Δt and β are constant for all $i = 1, 2, \ldots, N$ for each measurement, we can infer the value of $\theta_i + w$ using the method shown in [11]. We denote this process as phase fingerprinting, and $\theta_i + w$ is expressed as $\hat{\theta}_i$.

D. CHANNEL RECIPROCITY FOR PRACTICAL IMPLEMENTATION

For practical implementation of the proposed authentication, we considered temporal wireless channel correlation between Alice and Bob where the channel coherence depend on their relative movement. As in [20], the temporal channel correlation can be expressed as follows:

$$\rho = J_0(2\pi f_D T_{A-B}), \tag{5}$$

where J_0 is the zero-order Bessel function of the first kind, f_D is the Doppler shift, and T_{A-B} is the time period for authentication process, respectively. Considering that the relative speed of Alice and Bob is likely to be slow in indoor environments, f_D can be expected to be generally insignificant for within coherence time in the proposed system model.

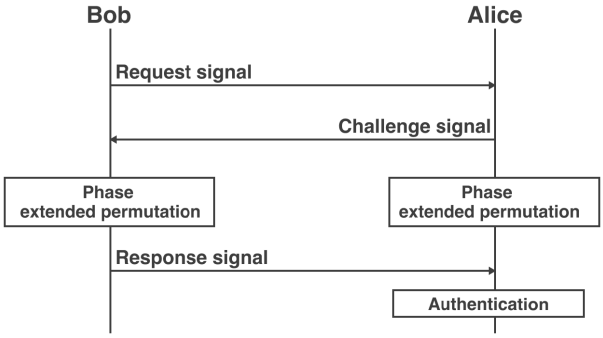

FIGURE 1. System model of the proposed scheme.

III. METHOD

The system model, phase extended permutation method, and user authentication method of the proposed scheme are as follows.

A. SYSTEM MODEL

Fig. 1 shows the system model of the proposed scheme. Upon Bob's request for authentication, he simultaneously transmits a request signal to Alice, and the phase of this signal is set to 0 ($\theta_{req_i} = 0$). Then, Alice receives the signal containing the channel data between Bob and Alice, including the noise generated during the communication process. Using this information, Alice estimates the channel phase ($\hat{\theta}_{\mathrm{BA}_i}$) between Bob and Alice. Subsequently, Alice transmits a challenge signal to Bob, and the phase of this signal is also set to 0 ($\theta_{chal_i} = 0$). Bob receives the signal containing the channel data between Alice and Bob, including the noise. Using this signal, Bob estimates the channel phase ($\hat{\theta}_{\mathrm{AB}_i}$) between Alice and Bob.

Alice and Bob undergo the phase extended permutation process using the channel phase between them and the secret key they share. Because their obtained channel phases have reciprocity, they both have similar permuted phases. The phase extended permutation method is detailed in Section III-B. Bob transmits the response signal ($\theta_{res_i} = \tilde{\theta}_{\mathrm{B}_i} - \hat{\theta}_{\mathrm{AB}_i}$) to Alice using the permuted phase $\tilde{\theta}_{\mathrm{B}_i}$. Upon receiving the response signal, Alice subtracts her permuted phase ($\tilde{\theta}_{\mathrm{A}_i}$) from the phase of the received response signal (θ_{res_i}) and performs calibration. Using the phase of the calibrated signal (θ_{aut_i}), Alice proceeds with the authentication process.

If Alice and Bob rearrange the phases identically, then the authentication signal after calibration will contain only noise. Therefore, Alice can evaluate the legitimacy of the user using the standard deviation of $\hat{\boldsymbol{\theta}}_{aut}$.

B. PHASE EXTENDED PERMUTATION

We present the phase extended permutation algorithm designed to enhance security by rearranging phase

information based on the calibrated channel phase and the phase of the secret key. The algorithm takes $\hat{\theta}_i$ and the phase of the secret key φ_i as inputs and produces the rearranged phase $\tilde{\theta}_i$ as the output.

First, depending on the modulation scheme, the algorithm initializes the number of bits per symbol (sys) and phase boundaries. For example, in BPSK modulation, $sys = 1$ and ϕ_1 and ϕ_2 are defined as 0 and π, respectively. In QPSK modulation, $sys = 2$ and the phase values ϕ_1, ϕ_2, ϕ_3, and ϕ_4 are defined as $\frac{\pi}{4}$, $\frac{3\pi}{4}$, $\frac{5\pi}{4}$, and $\frac{7\pi}{4}$, respectively.

Next, the algorithm iterates over each sub-carrier (i) from 1 to N/sys, calculating the number of sub-carriers satisfying $\varphi_i = \phi_k$ that is defined by n_k. If i is identified as the m^{th} sub-carrier satisfying $\varphi_i = \phi_k$, it assigns $l_{k,m} = i$. Next, for each phase value ϕ_k ($1 \leq k \leq 2^{sys}$), the algorithm calculates the starting index: $firstNum = 1 + \sum_{n=1}^{k-1} n_k$.

Finally, for each ($1 <= n <= n_k$), set $num = firstNum + n - 1$. Meanwhile, for each system variable p ($1 \leq p \leq sys$), it calculates x as $sys \cdot (num - 1) + p$ and y as $sys \cdot (l_{k,n} - 1) + p$. If k is odd, the algorithm sets the rearranged phase $\tilde{\theta}_x = y/num + (-1)^y \hat{\theta}_y$. If k is even, it calculates NUM as $firstNum + n_k - 1$ and sets the rearranged phase $\tilde{\theta}_x = (NUM - y)/num + (-1)^y \hat{\theta}_y$.

By following these steps, the algorithm ensures that the exchanged signal contains no secret information against both eavesdropping and man-in-the-middle attacks. The details is described in **Algorithm 1**.

C. USER AUTHENTICATION

If the user requesting authentication is legitimate (Bob), then Alice and Bob will use the same channel data and same secret key to undergo phase rearranging; consequently, the standard deviation of $\hat{\theta}_{aut_i}$ will be close to zero, with only noise remaining. By contrast, as Eve does not know the secret key, she will attempt authentication using a randomly generated key. Because that key differs from the secret key, the rearranged keys created by Alice and Eve are different. Therefore, the standard deviation $\hat{\theta}_{aut_i}$ calculated by Alice for authentication will be much greater than the noise.

Consequently, Alice can distinguish whether the requested user for authentication is Bob or Eve using the standard deviation of $\hat{\theta}_{aut_i}$. Therefore, in this case, the test statistic for authentication is as follows:

$$\zeta = \text{std}(\hat{\theta}_{aut}). \tag{6}$$

To check the security performance of the proposed scheme, a binary hypothesis testing based on the test statistic reported by [16] is employed in this paper. The hypothesis test Alice conducts is as follows:

$$\mathcal{H}_0 : \zeta \leq \tau \tag{7}$$

and

$$\mathcal{H}_1 : \zeta > \tau, \tag{8}$$

Algorithm 1 Phase Extended Permutation

Input: calibrated channel phase ($\hat{\theta}_i$), phase of the secret key (φ_i)
Output: rearranged phase ($\tilde{\theta}_i$)

```
if BPSK modulation then
    sys = 1
    φ1 = 0 and φ2 = π
end if
if QPSK modulation then
    sys = 2
    φ1 = π/4, φ2 = 3π/4, φ3 = 5π/4 and φ4 = 7π/4
end if
for i = 1, 2, ..., N/sys do
    n_k: Number of i satisfying φ_i = φ_k
    if i is m^th sub-carrier satisfying φ_i = φ_k then
        l_{k,m} = i
    end if
end for
for k = 1, 2, ..., 2^sys do
    firstNum = 1 + Σ_{n=1}^{k-1} n_k
    for n = 1, 2, ..., n_k do
        num = firstNum + n − 1
        for p = 1, 2, ..., sys do
            x = sys · (num − 1) + p
            y = sys · (l_{k,n} − 1) + p
        end for
        if mod(k, 2) = 1 then
            θ̃_x = y/num + (−1)^y θ̂_y
        end if
        if mod(k, 2) = 0 then
            NUM = firstNum + n_k − 1
            θ̃_x = (NUM − y)/num + (−1)^y θ̂_y
        end if
    end for
end for
```

where $\mathcal{H}_0$ and $\mathcal{H}_1$ are the test results obtained when the legitimate user (Bob) and the attacker (Eve), respectively, transmit the response signal. Here, τ is the threshold distinguishing Bob and Eve. In this case, the specific threshold should ensure that Eve can be never mistaken for Bob [16]. The specific threshold τ_E is set as follows:

$$\tau_E = \underset{\tau}{\text{argmax}}\, F_{\zeta|\mathcal{H}_1}(\tau) = 0, \tag{9}$$

where τ_E is the threshold from Eve's data and $F_{\zeta|\mathcal{H}_1}(\tau)$ is the value of the cumulative distribution function (CDF) of Eve at that point. However, because Eve's data cannot be collected in a situation where the threshold is set, the threshold must be collected from Bob's data, and it is as follows:

$$\tau_B = \underset{\tau}{\text{argmin}}\, F_{\zeta|\mathcal{H}_0}(\tau) \geq P_\alpha, \tag{10}$$

where τ_B is the threshold from Bob's test statistic and P_α is the level of significance α.

TABLE 1. USRP and testbed settings.

LTE application framework (LabVIEW NXG 4.0)	Bandwidth		20 MHz
	Center frequency		915 MHz
	Transmission power (coerced)	Alice	6.12 dBm
		Bob	7.50 dBm
		Eve	7.25 dBm
Position	Distance between Alice and Bob		3.6 m
	Eve		2.5 cm × 40 = 1 m
Obstacle specifications	Cube type	Quantity	Size (cm × cm × cm)
	Aluminum	1	30 × 30 × 30
		1	20 × 20 × 20
		1	10 × 10 × 10
	Plastic	8	30 × 35.3 × 33
		1	30 × 37.3 × 33
		1	29 × 34 × 23.8

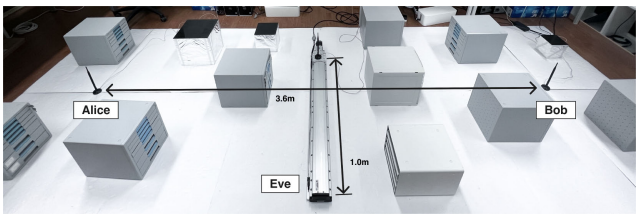

FIGURE 2. USRP testbed for measuring channel data in indoor communication environments.

IV. EXPERIMENTAL SETUP

A. SETTINGS

We investigated the security performance of the proposed scheme in two environments: a computer simulation environment and an actual communication environment. In the simulation, the signal-to-noise ratio (SNR) was set to 5 dB and the test was performed in the same manner as that reported by [8]. In the experiment, we used a USRP to measure channel state information (CSI) in an actual indoor environment. Because USRPs facilitate the manipulation of communication parameters in a software-defined environment, they are widely employed by researchers to measure CSI [11], [12], [17], [18], [19]. We employed the testbed configuration as described in [19]. We considered three USRP-2944R devices as three users (Alice, Bob, and Eve), and a total of 120,000 pieces of data were collected by fixing the positions of Alice and Bob while moving the position of Eve by 2.5 cm 40 times, with 3,000 pieces collected at each position. For the experiment, we relied on the LTE application framework on LabVIEW NXG 4.0 for digital waveform and baseband signal processing. Each user was equipped with a VERT900 vertical antenna, which supports a carrier frequency of 824-960 MHz. The detailed parameter settings are described in TABLE 1. Fig. 2 shows the experimental environment where we measured indoor channel data.

In an actual communication environment, data are stored in all the 200 sub-carriers of the experimental device for transmission and reception, but not all the data stored in these sub-carriers are used in the authentication process. From the 200 sub-carriers, only N sub-carriers are extracted using a certain rule, and the data stored in these N sub-carriers are used. Because we extracted data from the 200 sub-carriers of the experimental device, we extracted N at evenly spaced intervals as much as possible to assume the most general situation. In this paper, N was set to 32, 64, 96, 128, and 200, and the experiment was conducted. Because the value of N did not significantly affect the experimental results, for convenient analysis of the experimental results, as in ordinary wireless communication standards, in this paper, the discussed results were obtained at $N = 64$ at a bandwidth of 20 MHz.

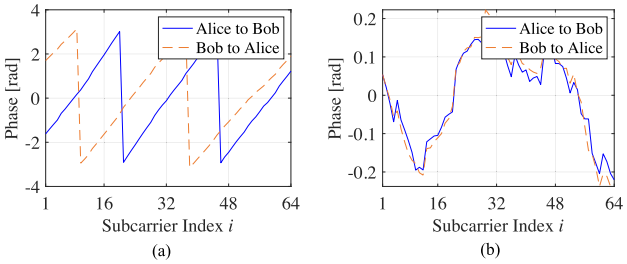

FIGURE 3. Channel phase data between two users: (a) raw channel phase data, and (b) fingerprinted channel phase data.

B. FINGERPRINTING

According to Section II-C, we processed the measured channel phase into desired data through fingerprinting. The desired data were usable channel phase data (i.e., reciprocity of channel phase data was established between two users). Fig. 3 shows the raw and fingerprinted channel phases between two users.

V. RESULTS

The authentication signals calculated by Alice from Bob and Eve are shown in Fig. 4. As mentioned in Section III-C, in the case of the response signal transmitted by Bob, the signal processed by Alice for authentication remains only as noise. The response signal transmitted by Eve is processed into a signal with a much larger phase than noise.

Eve can attempt two types of attacks [13]: a passive attack, in which Eve does not take any action to infer or obtain the secret key, and an active attack, in which a signal is transmitted to Bob or Alice to infer or obtain the secret key. Fig. 5 shows the system model of Eve's eavesdropping on Bob's signal. Eve can eavesdrop on the request signal through a man-in-the-middle attack or eavesdrop on the response signal via an eavesdropping attack or a replay attack.

A. PASSIVE ATTACK

1) EAVESDROPPING ATTACK

Eve eavesdrops on Bob's response signal transmitted to Alice and infers the secret key. During the eavesdropping, Eve receives the signal shown in Fig. 6. By checking the phase

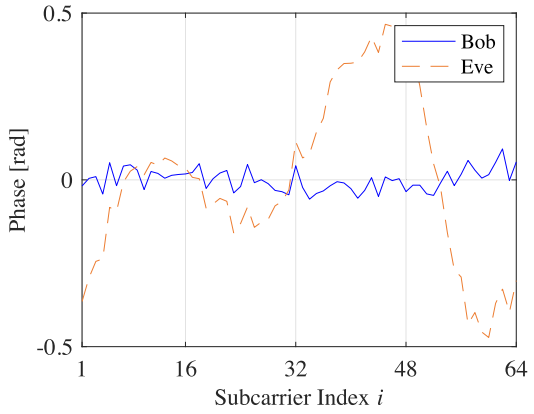

FIGURE 4. Authentication signals of Bob and Eve calculated by Alice.

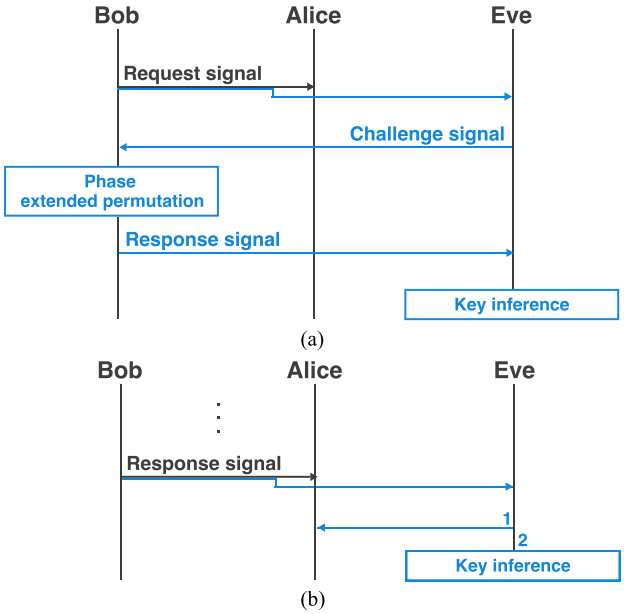

FIGURE 5. System models for (a) man-in-the-middle attacks, (b)(1) replay attacks, and (b)(2) eavesdropping attacks.

difference between two continuous sub-carriers, we confirm that under the use of PHY-PCRAS, the secret key, following BPSK modulation, can be inferred from the eavesdropped signal. By contrast, under our proposed scheme, Eve cannot infer the secret key from the eavesdropped response signal. Assuming that Eve infers indexes where the key changes to consecutive points on the sub-carriers according to the phase extended permutation method, Eve's unit key inference accuracy expressed as probability mass function (PMF) is as shown in Fig. 7. The accuracy of randomly generating a unit key in BPSK (QPSK) modulation is 50% (25%). Thus, the experimental results do not differ considerably from those obtained when randomly generating a unit key. As the number of sub-carriers increases, the unit key accuracy graph becomes increasingly similar to a normal-distribution graph. As the unit key guessing accuracy in BPSK modulation is 50%, the probability of correctly guessing the entire key is

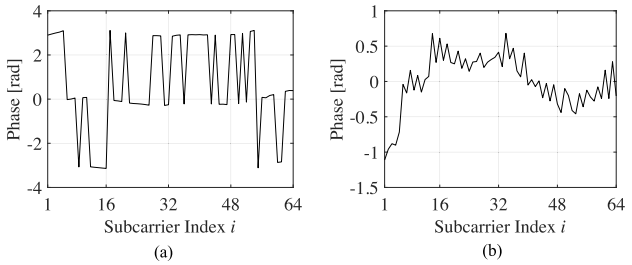

FIGURE 6. Channel phase during Eve's eavesdropping on the Bob's response signal out of the secret key following BPSK modulation: (a) PHY-PCRAS, and (b) proposed scheme.

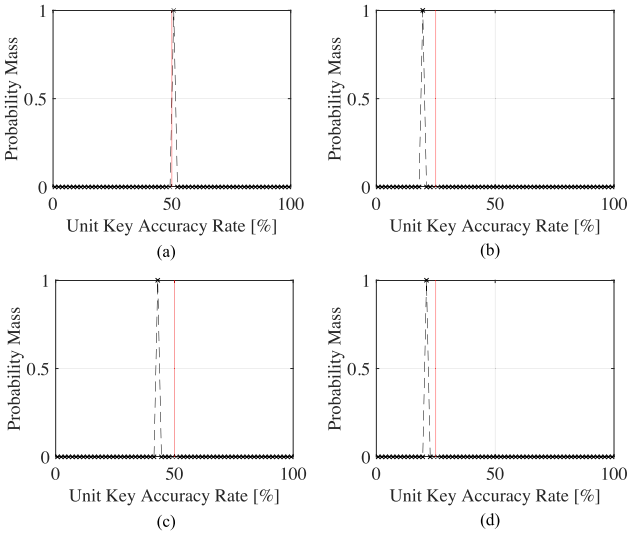

FIGURE 7. PMF of the accuracy of key inferred by Eve via eavesdropping attack: (a) BPSK modulation, (b) QPSK modulation in actual communication environments, (c) BPSK modulation, and (d) QPSK modulation in simulation environments.

$(\frac{1}{2})^N$; in QPSK modulation, it is $(\frac{1}{4})^{\frac{N}{2}}$, which is the same as that in BPSK modulation.

2) MAN-IN-THE-MIDDLE ATTACK

In the man-in-the-middle attack, Eve eavesdrops on Bob's request signal and pretends to be Alice. Eve makes Bob rearrange the key with the channel phase data between him and Eve and then transmit the response signal. Eve infers the key from the response signal received from Bob, and attempts authentication using the inferred key.

As with our analysis of the eavesdropping attack, we check whether Eve can infer the secret key from the response signal she obtains from Bob. As shown in Fig. 8, with PHY-PCRAS, the secret key following BPSK modulation can be inferred from the obtained by Eve, but it cannot be inferred under our scheme. Assuming that Eve infers indexes where the key changes to consecutive points on the sub-carriers according to the phase extended permutation method, Eve's unit key inference accuracy is as shown in Fig. 9. In the man-in-the-middle attack, Eve's unit key guessing accuracy is similar to that of randomly generating the unit key, as in the eavesdropping attack. Therefore, the probability that Eve

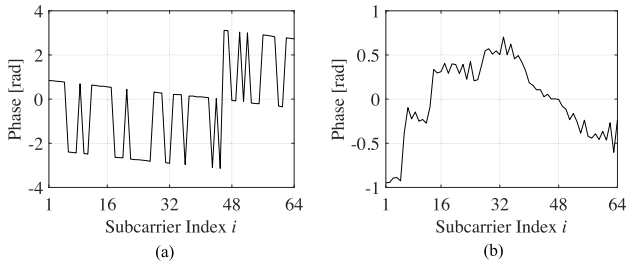

FIGURE 8. Channel phase during Eve's impersonation by Alice using a man-in-the-middle attack and receipt of the response signal from Bob obtained out of the key following BPSK modulation: (a) PHY-PCRAS, and (b) proposed scheme.

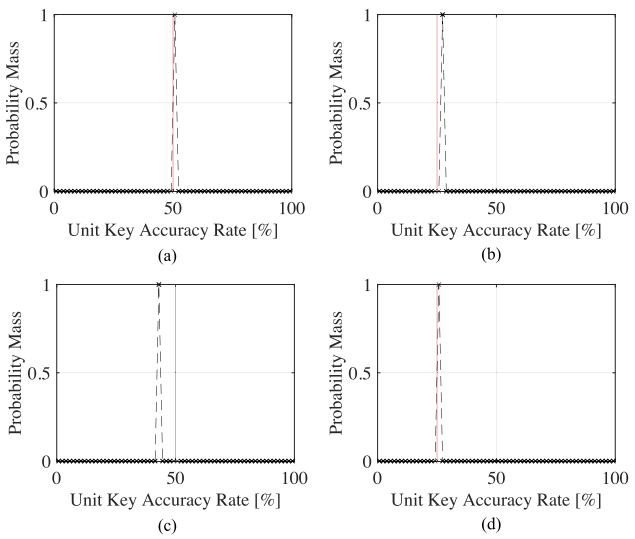

FIGURE 9. PMF of the accuracy of key inferred by Eve infers via man-in-the-middle attack: (a) BPSK modulation, (b) QPSK modulation in actual communication environments, (c) BPSK modulation, and (d) QPSK modulation in simulation environments.

will correctly guesses the entire authentication key through a man-in-the-middle attack is approximately $(\frac{1}{2})^N$, which is similar to that obtained through a brute-force attack.

B. ACTIVE ATTACK

1) REPLAY ATTACK

In the replay attack, Eve eavesdrops on the response signal that Bob sends to Alice, and then replays it to Alice for authenticating as Bob. The signal sent by Eve in this attack differs from that sent by Bob to Alice for authentication, just like in the brute-force attack. The CDF of the Bob and Eve's test statistic in the replay attack is shown in Fig. 10 (b). The threshold obtained using Eve's data τ_B is -2.1705 with $\alpha = 0$ for $N = 64$.

2) BRUTE-FORCE ATTACK

A brute-force attack is a technique in which an attacker, Eve, tries to gain authentication by generating keys randomly, without any prior knowledge of the correct key. Eve's approach to authentication is similar to that of Bob's, as she uses her randomly generated key for the authentication. However, because Eve's key differs from the secret key that Alice shares with Bob, Alice can distinguish Eve from Bob

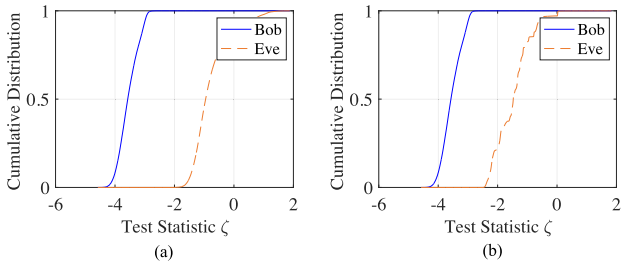

FIGURE 10. CDF of test statistic during Eve's (a) brute-force attack and (b) replay attack.

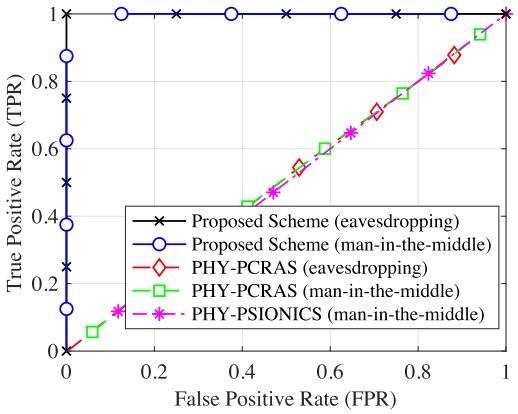

FIGURE 11. ROC curve of proposed scheme, PHY-PCRAS, and PHY-PSIONICS approaches in correlated indoor channel.

by computing $\bar{\boldsymbol{\theta}}_{aut}$. Fig. 10 (a) illustrates the CDF of the test statistic ζ calculated by Alice using the signals of Bob and Eve. From eq. (10), we find that the threshold τ_B is -2.1987 with $\alpha = 0$ for $N = 64$. To assess the security performance of our scheme, we randomly generate Eve's data and compute the threshold. In the absence of Eve's data, as mentioned in Section III-C, the threshold can be set sufficiently using Bob's data.

C. RECEIVER OPERATING CHARACTERISTIC (ROC) CURVE

In attack scenarios, Eve attempts to authenticate as legitimate users using the authentication key inferred through eavesdropping or man-in-the-middle attack. Fig. 11 shows the ROC curves for PHY-PCRAS-based approaches where the sub-channels are correlated in indoor environment. PHY-PCRAS [8] is highly vulnerable even to eavesdropping since the attacker can distinguish the secret key from the received signal. Additionally, Eve can acquire the secret key in a man-in-the-middle attack by intercepting the request signal between legitimate users, which degrades authentication reliability. PHY-PSIONICS [11] employs secret key encapsulation using quantized channel phase to prevent the key from being revealed in correlated sub-channels; however, it has low reliability in man-in-the-middle attack since the legitimate users still transmit the secret primitive over the air. In contrast, the proposed scheme achieves excellent security performance against both attacks by ensuring that the exchanged signal contains no secret information after extended permutation.

VI. CONCLUSION

In this paper, we proposed a PLA scheme for practical communication scenarios. This scheme employs key indexes to permute channel phases and hide the secret keys shared by legitimate users. The proposed method effectively differentiates between legitimate users and potential attackers by leveraging channel data and secret keys shared by authorized users. We verified the security performance of this scheme in a real communication environment, which has correlated sub-channels, by collecting channel data from such an environment using USRP. We verified that this scheme can effectively determine if an unauthorized user attempts authentication. We comprehensively examined the security of our scheme under various attack scenarios: eavesdropping attacks, man-in-the-middle attacks, brute-force attacks, and replay attacks. Our analysis results show that the proposed scheme adequately enhances the margin to set the security threshold, enabling clear distinction between legitimate users and potential attackers. Similar to other wireless channel PLA, the proposed scheme may exhibit performance degradation in high dynamic communication networks.

REFERENCES

[1] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[2] P. L. Yu and B. M. Sadler, "MIMO authentication via deliberate fingerprinting at the physical layer," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 606–615, Sep. 2011.

[3] P. Hao, X. Wang, and W. Shen, "A collaborative PHY-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42279–42293, 2018.

[4] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *J. Commun. Inf. Netw.*, vol. 5, no. 3, pp. 237–264, Sep. 2020.

[5] C. Pei, N. Zhang, X. S. Shen, and J. W. Mark, "Channel-based physical layer authentication," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 4114–4119.

[6] F. Pan, H. Wen, R. Liao, Y. Jiang, A. Xu, K. Ouyang, and X. Zhu, "Physical layer authentication based on channel information and machine learning," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 364–365.

[7] S. Van Vaerenbergh, Ó. González, J. Vía, and I. Santamaría, "Physical layer authentication based on channel response tracking using Gaussian processes," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2014, pp. 2410–2414.

[8] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 74–77, Jan. 2015.

[9] X. Wu, Z. Yang, C. Ling, and X.-G. Xia, "Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6611–6625, Oct. 2016.

[10] 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 Inf. Syst.*, vol. 2017, pp. 1–13, Jul. 2017.

[11] S. Han, J. Choi, and E. Hwang, "PHY-PSIONICS: Physical-layer phase secret key encapsulation in correlated subchannels," *IEEE Wireless Commun. Lett.*, vol. 12, no. 8, pp. 1409–1413, Aug. 2023.

[12] S. Yoon, S. Han, and E. Hwang, "Joint heterogeneous PUF-based security-enhanced IoT authentication," *IEEE Internet Things J.*, vol. 10, no. 20, pp. 18082–18096, Oct. 2023.

[13] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, Sep. 2013.

[14] S. Sen, B. Radunovic, R. R. Choudhury, and T. Minka, "You are facing the Mona lisa: Spot localization using PHY layer information," in *Proc. 10th Int. Conf. Mobile Syst., Appl., Services*, Jun. 2012, pp. 183–196.

[15] W. Wei, J. Yan, X. Wu, C. Wang, and G. Zhang, "CSI fingerprinting for device-free localization: Phase calibration and SSIM-based augmentation," *IEEE Wireless Commun. Lett.*, vol. 11, no. 6, pp. 1137–1141, Jun. 2022.

[16] Y. Lee, J. Yoon, J. Choi, and E. Hwang, "A novel cross-layer authentication protocol for the Internet of Things," *IEEE Access*, vol. 8, pp. 196135–196150, 2020.

[17] Q. Wang, H. Li, D. Zhao, Z. Chen, S. Ye, and J. Cai, "Deep neural networks for CSI-based authentication," *IEEE Access*, vol. 7, pp. 123026–123034, 2019.

[18] F. Gringoli, M. Cominelli, A. Blanco, and J. Widmer, "AX-CSI: Enabling CSI extraction on commercial 802.11 ax Wi-Fi platforms," in *Proc. ACM Workshop Wireless Netw. Testbeds, Experim. Eval. Characterization (WiNTECH)*, 2022, pp. 46–53.

[19] S. Han, H. Lee, J. Choi, and E. Hwang, "Multi-frequency band physical-layer authentication in indoor environment," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2023, pp. 1741–1746.

[20] A. Albehadili, K. A. Al Shamaileh, A. Y. Javaid, and V. K. Devabhakuni, "Link-signature-based discriminatory channel estimation (LS-DCE) for physical layer security in stationary and mobile OFDM transceivers," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8119–8131, Aug. 2020.

KYOUNGYEON GO received the double degree in physics and in electrical engineering and computer science from Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, in 2024. Her research interests include signal processing and wireless communication.

SEUNGNAM HAN (Graduate Student Member, IEEE) received the B.E. degree in mechanical engineering from Chungnam National University, Daejeon, South Korea, in 2019, and the M.S. degree in electrical engineering and computer science from Gwangju Institute of Science and Technology, Gwangju, South Korea, in 2021, where he is currently pursuing the Ph.D. degree. His research interests include signal processing, wireless security, physical layer, and software-defined radio (SDR).

EUISEOK HWANG (Senior Member, IEEE) received the bachelor's and first master's degrees from Seoul National University, in 1998 and 2000, respectively, and the second master's and Ph.D. degrees in electrical and computer engineering from Carnegie Mellon University (CMU), Pittsburgh, PA, USA, in 2010 and 2011, respectively. He is a Professor with the School of Electrical Engineering and Computer Science (EECS) and the AI Graduate School, Gwangju Institute of Science and Technology (GIST), South Korea. He was with the Digital Media Research Center, Daewoo Electronics Company Ltd., South Korea, from 2000 to 2006; and the Channel Architecture Group, Data Controller Division, LSI (currently Broadcom), San Jose, CA, USA, from 2011 to 2014. Since 2015, he has been an Assistant/Associate/Full Professor with the School of EECS/AI Graduate School/School of Mechatronics, GIST. From 2021 to 2022, he was a Visiting Scholar with the Department of Computer Science and Engineering, University of Michigan, Ann Arbor. His research interests include statistical signal processing, machine learning and channel coding for data storage and communication systems, and their emerging information and communication technology applications, particularly in areas such as the Internet of Things and smart grids.