Physical Layer Authentication Based on Channel Polarization Response in Dual-Polarized Antenna Communication Systems

Yuemei Wu, *Student Member, IEEE*, Dong Wei, Caili Guo, *Senior Member, IEEE*, and Weiqing Huang

***Abstract*— This study presents a novel approach for physical layer authentication based on channel polarization response (CPR). CPR is sensitive to variation in the physical properties of scatterers, and the CPR difference between various channels is higher than the channel frequency response (CFR) under rich scattering scenarios. Additionally, the estimation of CPR is continuous, the authentication interval can be adjusted according to the channel coherence time, then the proposed scheme can be applied to any rich scattering scenarios, including highly dynamic scenarios. Since the received polarization state is fixed during the channel coherence time, we can coherently stack the received polarization state to improve the signal to noise ratio (SNR) and the estimation accuracy of CPR, thereby achieving high authentication accuracy under ultra-low SNR. Moreover, since the transmitted polarization state of various transmitters is different, because of their unique hardware deficiencies, and since the CPR is dependent on the transmitted polarization state, the CPR of other transmitters is different, allowing the resolution of co-located attacks. We theoretically drive the false alarm probability, detection probability, optimal discriminant threshold, computational complexity, optimal stacking numbers, and optimal CPR points for authentication. Furthermore, extensive simulations and experiments are performed to verify the validity and effectiveness of the proposed scheme.**

***Index Terms*— Physical layer authentication, channel polarization response, highly dynamic scenarios, ultra-low SNR, co-located attacks.**

I. Introduction

THE broadcast nature of wireless channels makes them vulnerable to spoofing attacks, as both legitimate and illegitimate transmitters have the ability to access them. Conventional wireless communication systems resort to upper-layer authentication algorithms that relies on a symmetric or asymmetric key shared between the legitimate transmitter and receiver [1]. However, this paradigm suffers from security vulnerabilities in the key generation, distribution, and management processes, and the assumption of limited computational power for the adversary is becoming increasingly invalid with advancements in computational power and cryptanalysis algorithms [2].

To address these issues, physical layer authentication schemes have emerged as a promising alternative, offering high security, low computational complexity, and compatibility with future wireless communication networks [2]. These schemes utilize the inherent attributes of the physical layer and are divided into two categories: hardware impairment-based schemes [3], [4], [5], [6], [7] and channel-based schemes [2], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30]. The former ones make use of device information, including power amplifier nonlinearity [3], phase noise [4], clock deviation [5], carrier frequency offset (CFO) [6], and in-phase-quadrature-phase imbalance (IQI) [7]), for authentication, but their application is limited by their sensitivity to channel variations. On the other hand, channel-based schemes, which utilize channel information such as received signal strength (RSS) [8], [9], power spectral density (PSD) [10], channel impulse response (CIR) [2], [11], [12], [13], [14], [15], [16], [17], [28], [29], [30], channel frequency response (CFR) [18], [19], [20], [21], [22], [23], [24], [25], [27], and angle of arrival (AOA) [26]), are more robust in rich scattering channels and are the focus of this paper.

According to the authentication parameters used, channel based schemes include schemes based on statistical channel information (SCI), instantaneous channel information (ICI), and multiple physical layer attributes. In terms of schemes based on SCI, [8], [9] proposed using RSS to provide secure pairing between devices. Reference [10] proposed using both the PSD and the generalized likelihood ratio test for authentication.

In terms of schemes based on ICI, there are CIR based schemes, CFR based schemes, and AOA based schemes. Among the CIR based schemes, [11] initially proposed to use the gain of CIR for authentication in the time-invariant channel. Then, [13] extended it to the time varying channel. In order to improve the authentication performance, [14], [15] proposed to use the gain of CIR and multipath delay for authentication, and a two-dimensional quantizer was proposed to simplify the calculation. However, this introduced quantization errors, which negatively impacted the authentication performance. To overcome this limitation, [2] proposed multiple CIRs physical layer authentication (MCP) and enhanced multiple CIRs physical layer authentication (EMCP)

Manuscript received 9 September 2022; revised 4 December 2022 and 19 February 2023; accepted 19 March 2023. Date of publication 31 March 2023; date of current version 11 April 2023. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Hossein Pishro-Nik. *(Corresponding author: Dong Wei.)*

Yuemei Wu, Dong Wei, and Weiqing Huang are with the School of Cyberspace Security, University of Chinese Academy of Sciences, Beijing 100049, China, and also with the Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: wuyuemei@iie.ac.cn; weidong@iie.ac.cn; huangweiqing@iie.ac.cn).

Caili Guo is with the Beijing Key Laboratory of Network System Architecture and Convergence, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: guocaili@bupt.edu.cn).

Digital Object Identifier 10.1109/TIFS.2023.3263624

schemes. Reference [28] proposed using machine learning to further improve authentication performance. Among the CFR based schemes, [18], [20] initially proposed using the amplitude of CFR for authentication in the time-invariant channels. Then, it was extended to time varying channels [19], mobile scenarios [21], and frequency-selective Rayleigh channels [22]. In order to improve the authentication performance, the amplitude and phase of CFR were used to make an authentication in the OFDM [23] and CDMA systems [24]. Moreover, phase differences between the two CFRs were used for authentication in a multi-carrier transmission systems [12]. Among the AOA based schemes, [26] proposed using AOA for authentication, where a deep autoencoder was trained to learn the features from a training dataset.

In terms of schemes based on multiple physical layer attributes, [16], [17] proposed to use channel gain and phase noise for authentication in Multiple Input Multiple Output (MIMO) and massive MIMO systems. Reference [29] proposed to use CIR, CFO, RSS, and IQI for authentication. Moreover, the fuzzy theory was explored for modeling multiple physical layer attributes with imperfection and uncertainty, and a hybrid learning-based adaptive authentication algorithm was proposed to update system parameters. Reference [30] proposed to use CFO, CIR, and RSS for authentication, and a kernel machine was used for combining multiple physical layer attributes.

Here, we analyze and compare the channel based authentication schemes in table I. We can see that the existing schemes have some limitations under highly dynamic scenarios, co-located attack scenarios, and ultra-low signal to noise ratio (SNR) scenarios.

A. Highly Dynamic Scenarios

All the ICI based schemes rely on the pilot to estimate channel parameters and assume the channel is invariant in the pilot interval. When the channel is rapidly fluctuates, the channel parameters vary during the pilot interval, and the correlation between successive pilot intervals with the same transmitter is extremely low. Then, the authentication performance of ICI based schemes will significantly degrade, which is unacceptable for industrial applications. Reducing the pilot interval may seem like a solution, but this is not practical as the pilot, which is primarily designed for channel equalization and demodulation, instead of authentication, can only occupy limited channel resources. Although schemes based on SCI do not require a pilot signal, but they only depict path loss and shadow fading of the wireless channel, making it easier for attackers to duplicate and rendering their authentication performance inferior to that of ICI based schemes, as noted in [31].

B. Co-Located Attacks Scenarios

Since all the ICI and SCI based schemes assume that transmitters are located at different locations, they cannot handle the co-located attacks. Although schemes based on multiple physical layer attributes can use device features to authenticate transmitters at the same location. However, those devices with the same brand and model can have insufficient feature differences, leading to the possibility of misjudgment and reduced authentication performance.

C. Ultra-Low SNR Scenarios

The authentication accuracy of the channel based schemes under ultra-low SNR is very low. For example, when $SNR \leq -10dB$, the detect probability is less than 40% [2], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30].

To overcome the above shortcomings, we propose a scheme based on channel polarization response (CPR) under dual-polarized antenna systems. CPR describes the fading of the channel to signal polarization state, reflects the physical properties of the scatterers in the channel, e.g., material, orientation, attitude, etc. [32], and changes with the physical properties of the scatterers. Compared with CIR and CFR, which describe the fading of the channel to signal amplitude and phase, reflect spatial fading of the channel, and change with the distance between the transmitter and receiver, CPR is more sensitive to the change of the channel, and the difference between various channels is greater.

Since the polarization state of the signal does not carry information [33], the transmitting polarization state can be used as a "continuous pilot" to estimate CPR. The continuity of the transmitting polarization state enables continuous CPR estimation. On the one hand, we can adaptively adjust the authentication interval of the CPR based scheme according to the coherence time, allowing it to be applied to any rich scattering scenarios, including highly dynamic scenarios. So as to solve the authentication problem in highly dynamic scenarios. On the other hand, we can coherently stack the received polarization state according to the SNR and the required authentication performance to improve the accuracy of the CPR estimation. This is feasible as the transmitted polarization state of the signal is fixed. The problem of authentication with ultra-low SNR can thus be solved.

Under the influence of transmitter hardware deficiencies, the transmitting polarization state will deviate from the expected polarization state, making the polarization states transmitted by different transmitters slightly different [34]. The CPR is dependent on the transmitted polarization state [35], [36], resulting in differing CPR values for different transmitters located at the same location. The CPR difference caused by channel polarization fading is larger than the discriminant threshold, enabling the proposed scheme to distinguish between even two transmitters located at the same location.

To the best of our knowledge, we are the first one to utilize the CPR for physical layer authentication. Such an introduction of CPR to the physical security is not a straightforward effort, where the challenge is lack of the fundamental study, including the theoretical analysis on the CPR characteristic and the performance of the corresponding authentication scheme. The main contributions of this paper are summarized as follows:

- A physical layer authentication scheme based on CPR is proposed, which can solve the problems of authentication

TABLE I
PHYSICAL LAYER AUTHENTICATION BASED ON CHANNEL

Authentication parameters		Works	Domain of authentication parameters: Time domain	Frequency domain	Space domain	Polarization domain	Pilot is need?	The channel is invariant in pilot interval?	Can counter co-located attacks?	Can be authenticated under ultra low SNR?
SCI	RSS	[8], [9]	✓	×	×	×	×	×	×	×
	PSD	[10]	×	✓	×	×	×	×	×	×
ICI	CIR (channel gain)	[11], [13] [2], [28]	✓	×	×	×	✓	✓	×	×
	CIR (channel gain, multipath delay)	[14], [15]	✓	×	×	×	✓	✓	×	×
	CFR (amplitude)	[18]–[22] [27]	×	✓	×	×	✓	✓	×	×
	CFR (amplitude, phase)	[23], [24]	×	✓	×	×	✓	✓	×	×
	CFR (phase differences)	[12]	×	✓	×	×	✓	✓	×	×
	AOA	[26]	×	×	✓	×	×	×	×	×
	CPR	This paper	×	×	×	✓	×	×	✓	✓
Multiple physical attributes	CIR, Phase noise	[16], [17]	✓	×	×	×	✓	✓	✓	×
	CIR, CFO, RSSI, IQI	[29]	✓	×	×	×	✓	✓	✓	×
	CIR, CFO, RSSI	[30]	✓	×	×	×	✓	✓	✓	×

✓means yes, and × means no.

in highly dynamic scenarios and co-located attacks, while maintaining good authentication performance under ultra-low SNR.

- The false alarm probability, detection probability, optimal threshold, optimal stacking numbers, optimal CPR points for authentication, and computational complexity are theoretically derived for the proposed scheme. Additionally, co-located attacks and Doppler effect on authentication performance are evaluated.
- Extensive simulations and experiments are performed to verify the theoretical correctness and feasibility of the proposed scheme.

The rest of this paper is organized as follows. Section II introduces the communication network model and channel model. Section III presents the proposed authentication scheme based on CPR. The performance of the proposed scheme is analyzed in section IV. The numerical simulations and experiments are carried out in section V. Finally, section VI concludes this paper.

II. SYSTEM MODEL

A. Network Model

Consider the traditional secure communication scenario, shown in Fig. 1. There are three entities in the communication network, in which Alice is the legitimate transmitter and Bob is the intended receiver, whereas Eve is the spoofer, attempting to impersonate Alice and sending false messages to Bob. It is assumed that Eve possesses some publicly known and repetitively used information, such as training sequences, pilot symbols [37], and the type of polarization used by the transmitting antennas.

The goal in this work is to construct authentication between Alice and Bob, in the presence of an adversary, Eve, who seeks to impersonate Alice and send false messages to Bob. To this

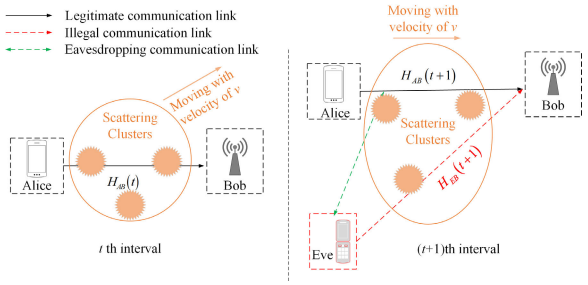


Fig. 1. Secure communication scenario. Alice and Bob are legitimate communicators, and Eve is the spoofer. The channel will be time-varying due to the movement of scatterers in the environment.

end, consider the scenario where Bob receives signals at the tth and $(t+1)$th intervals, with a time interval $\Delta T \leq T_c$, where T_c is the channel coherence time. Through pre-sharing secret, physical measures (e.g., by manually executing the setup phase) [28], or communication on a parallel and secure channel [38], [39], Bob authenticates that the transmitter of the tth interval is Alice. The pre-sharing secret can be a key used one time for initial authentication or the channel information stored by Alice and Bob before the communication is interrupted. Then, Bob stores the CPR at the tth interval. Since CPRs from the same transmitter are highly correlated during the coherence time, CPRs from different transmitters are independent. In $(t+1)$th interval, Bob can distinguish the unknown transmitter by comparing the similarity of CPRs at $(t+1)$th and tth interval.

B. Channel Model

Assuming the receiver is equipped with horizontal and vertical dual-polarized antennas, this paper considers the dual-polarized Rayleigh fading channel [40],

which is modeled as

$$\vec{H}(t,f)=\begin{bmatrix}H_{vv}(t,f) & H_{vh}(t,f)\\ H_{hv}(t,f) & H_{hh}(t,f)\end{bmatrix}=G(t,f)\cdot\vec{S}$$
$$=\sum_{l=1}^{L}A_l\cdot e^{j(2\pi f_m t-2\pi f\iota_l)}\cdot\begin{bmatrix}S_{lvv} & S_{lvh}\\ S_{lhv} & S_{lhh}\end{bmatrix},\quad(1)$$

where $H_{xy}(t,f)$ represents the channel transmission function when the transmitting component is y-polarized and the receiving antenna is x-polarized. $G(t,f)$ represents the spatial fading, and varies with the distance of the transceiver, which is the CFR used in previous works. $\vec{S}$ represents the polarization fading, and varies with the physical properties of the scatterers (e.g., attitude adjustment, azimuth change), which is defined as CPR. We can see that CPR is more sensitive to the change of channel than CFR, and the CPR difference between various channels is greater under rich scattering scenarios. L is the number of multipath. A_l is the channel gain of the lth path. f is the carrier frequency. $f_m=\frac{V\cdot\cos\theta}{c}\cdot f$ is the Doppler shift, V is the velocity of the scatterer, c is the speed of the light, θ is the angle between the scatterer and the incident wave. ι_l is the delay of the lth path. S_{lxy} is the polarization fading of the lth path when the transmitting component is y-polarized and the receiving antenna is x-polarized, which is determined by the transmitted polarization state and communication signal frequency [35], [36].

Suppose the transmitting signal is

$$\vec{x}(t)=\begin{bmatrix}x_v(t) & x_h(t)\end{bmatrix}^{\mathrm{T}},\quad(2)$$

where $x_v(t)=|x_v(t)|\,e^{j\phi_{xv}(t)}$ and $x_h(t)=|x_h(t)|\,e^{j\phi_{xh}(t)}$ are the vertical component and horizontal component of the transmitting signal, respectively; $|\cdot|$ is the modular operator; $\phi_{xv}(t)$ is the phase of $x_v(t)$; $\phi_{xh}(t)$ is the phase of $x_h(t)$.

After the signal in (2) propagating through the channel given by (1), the received signal is

$$\vec{r}(t)=\begin{bmatrix}r_v(t) & r_h(t)\end{bmatrix}^{\mathrm{T}}=\vec{h}(t,\iota)*\vec{x}(t),\quad(3)$$

where $\vec{h}(t,\iota)$ is the inverse Fourier transform of $\vec{H}(t,f)$ on f, $*$ represents convolution. Hereafter, for convenience of notation, we will omit t, ι, and f in the signal or channel parameters and use uppercase letters for the frequency domain, and lowercase letters for the time domain. The time interval index t will be resumed in Section III-C. Sampling $\vec{r}$ at N points to get $\underline{\vec{r}}=\begin{bmatrix}\vec{r}_1,\vec{r}_2,\cdots,\vec{r}_n,\cdots,\vec{r}_N\end{bmatrix}$, where $\vec{r}_n$ represents the nth sample of the received signal, $N=S_a\cdot T_s$, S_a is the sample rate, T_s is the sampling period. We performed N point discrete Fourier transform (DFT) on $\underline{\vec{r}}$ to obtain

$$\underline{\vec{R}}=\begin{bmatrix}\underline{R}_v & \underline{R}_h\end{bmatrix}^{\mathrm{T}}=\vec{H}\cdot\underline{\vec{X}},\quad(4)$$

where $R_{vk}=\sum_{n=0}^{N-1}e^{-j\frac{2\pi}{N}nk}r_{vn}$, $k=0,1,\cdots,N-1$, $R_{hk}=\sum_{n=0}^{N-1}e^{-j\frac{2\pi}{N}nk}r_{hn}$, $k=0,1,\cdots,N-1$, $\underline{\vec{X}}$ is the DFT of $\underline{\vec{x}}$.

Substituting (1) into (4), we can obtain

$$\underline{\vec{R}}=G\cdot\left|\underline{X}_h\right|e^{j\phi_{\underline{X}_h}}\cdot\vec{S}\cdot\begin{bmatrix}\frac{\left|\underline{X}_v\right|}{\left|\underline{X}_h\right|}e^{j(\phi_{\underline{X}_v}-\phi_{\underline{X}_h})}\\ 1\end{bmatrix},\quad(5)$$

where $X_J=\left(\left|\underline{X}_v\right|/\left|\underline{X}_h\right|\right)e^{jX_P}$ is the polarization state of the transmitted signal, $X_F=\left|\underline{X}_v\right|/\left|\underline{X}_h\right|$ is the amplitude ratio, $X_P=\phi_{\underline{X}_v}-\phi_{\underline{X}_h}$ is the phase difference, $\phi_{\underline{X}_v}$ is the phase of $\underline{X}_v$, and $\phi_{\underline{X}_h}$ is the phase of $\underline{X}_h$. It can be observed that the transmitted signal experiences both spatial and polarization fading, with independence between each other. Existing research has predominantly focused on utilizing the spatial fading, however, this paper takes a different approach by leveraging polarization fading.

III. Physical Layer Authentication Scheme

In this section, we present the details of the proposed CPR-based Authentication Scheme, which encompasses three key stages. The first stage aims to enhance the SNR by stacking the received polarization state over the channel coherence time. The second stage estimates the CPR, and the logarithmic amplitude and phase of CPR are used as authentication parameters. The final stage performs the authentication process according to a hypothesis testing model, where the logarithmic likelihood ratio test is used to determine the test statistic.

A. Polarization State Coherent Stacking

Suppose the vertical and horizontal components of the noise powers at the receiver are σ_v^2 and σ_h^2, respectively. The received signal is represented as

$$\hat{\underline{r}}=\begin{bmatrix}\hat{\underline{r}}_v\\ \hat{\underline{r}}_h\end{bmatrix}=\begin{bmatrix}\underline{r}_v+\underline{w}_v\\ \underline{r}_h+\underline{w}_h\end{bmatrix},\quad(6)$$

where $\underline{w}_v$ and $\underline{w}_h$ represent orthogonal receiver noise after sampling; w_v and w_h follow a cyclic complex Gaussian distribution with a mean of 0 and variance of σ_v^2 and σ_h^2, respectively. Then, the received polarization state is

$$\hat{\underline{r}}_J=\frac{\left|\hat{\underline{r}}_v\right|}{\left|\hat{\underline{r}}_h\right|}e^{j(\phi_{\hat{\underline{r}}_v}-\phi_{\hat{\underline{r}}_h})},\quad(7)$$

where $\hat{r}_F=\left|\hat{\underline{r}}_v\right|/\left|\hat{\underline{r}}_h\right|$ is the amplitude ratio of the received orthogonally polarized components. $\hat{r}_P=\phi_{\hat{\underline{r}}_v}-\phi_{\hat{\underline{r}}_h}$ is the phase difference of the received orthogonally polarized components, $\phi_{\hat{\underline{r}}_v}$ is the phase of $\hat{\underline{r}}_v$, $\phi_{\hat{\underline{r}}_h}$ is the phase of $\hat{\underline{r}}_h$.

Since the transmitted polarization state is fixed, and the channel can be considered approximately time-invariant during the coherence time. The received polarization state within the the coherence time can then be uniformly segmented and stacked in the time domain to reduce the impact of noise.

Assuming that the received polarization state between tth and $(t+1)$th interval is divided into C segments, and the sample point of each segment is M, i.e. $C\times M=N$. Then $\hat{\underline{r}}'_J=\begin{bmatrix}\hat{r}_{J1},\hat{r}_{J2},\cdots,\hat{r}_{Jc},\cdots,\hat{r}_{JC}\end{bmatrix}$, where $\hat{r}_{Jc}=\hat{r}_J\left[t\cdot\Delta T+c\cdot\Delta r\right]$, $\Delta r=\frac{\Delta T}{C}$. Using coherent stacking to denoise the signal, the stacked polarization state becomes

$$\hat{\underline{r}}_{Je}=\frac{1}{C}\sum_{c=1}^{C}\hat{r}_{Jc}.\quad(8)$$

The SNR after stacking is represented as

$$SNR=C\times SNR_0=C\left(|r_v|^2+|r_h|^2\right)/\left(\sigma_v^2+\sigma_h^2\right),\quad(9)$$

where $|r_v|^2 + |r_h|^2$ is the power of the signal after stacking, $\frac{\sigma_v^2+\sigma_h^2}{C}$ is the power of the noise after stacking. It can be observed that the stacking process results in a direct transfer of the SNR to C times the original SNR_0. How to optimally select C and M will be discussed in Section IV-C.

B. CPR Estimation

After stacking the received polarization state, Bob performs M points DFT on $\hat{\underline{r}}_{Je}$ to obtain $\hat{\underline{R}}_{Je}$. Based on X_J and $\hat{\underline{R}}_{Je}$, which describe the polarization state of the transmitted signal and received signal, the CPR can be estimated as outlined in equation (10).It is worth noting that the form of $\vec{S}$ in equation (10) is distinct from that in equation (1). This difference is due to the use of the polarization ratio here, rather than the Jones vector in (1), to represent the polarization state for the purpose of facilitating subsequent calculations. The Jones vector and polarization ratio are two representations of the polarization state. So both $\vec{S}$ in (1) and (10) uniquely represent the polarization fading of the channel.

$$\vec{S} = X_J^{-1} \cdot \hat{R}_{Je}, \tag{10}$$

where the upper subscript -1 denotes inverse. Bring $\hat{R}_{Je}$ and X_J in (5) into (10), we can obtain

$$\begin{aligned} \hat{S}_F &= \hat{R}_{Fe}/X_F \\ \hat{S}_P &= \hat{R}_{Pe} - X_P. \end{aligned} \tag{11}$$

Here X_J is the ideal transmitting polarization state. Actually, the transmitted polarization state is affected by the transmitter hardware deficiency and noise, and deviates from X_J [34]. Then, S_F and S_P are affected by the deficiency and noise of transmitter and receiver hardware.

$$\begin{aligned} \hat{S}_F &= S_F + F_{WX} + F_{WR} \\ \hat{S}_P &= S_P + P_{WX} + P_{WR}, \end{aligned} \tag{12}$$

where S_F and S_P are true channel polarization fading. F_{WX} and P_{WX} are the estimation error of S_F and S_P caused by transmitter hardware deficiency and transmitter noise. F_{WR} and P_{WR} are the estimation error of S_F and S_P caused by receiver hardware deficiency and receiver noise.

According to [41], under dual polarization Rayleigh channel, $log(S_F)$ approximately follows normal distribution, that is, $log(S_F) \sim N\left(\mu_{SF}, \sigma_{SF}^2\right)$, and

$$\mu_{SF} = log(\xi)$$
$$\sigma_{SF}^2 = \begin{cases} \dfrac{1}{ln10}\left[\dfrac{\pi^2}{6} - \displaystyle\sum_{k=1}^{\infty}\dfrac{\rho^{2k}}{k^2}\right] & \rho < 0.5 \\ \dfrac{1}{ln10}\left[\ln(\rho^2)\ln(1-\rho^2) + \displaystyle\sum_{k=1}^{\infty}\dfrac{(1-\rho^2)^k}{k^2}\right] & \rho \geq 0.5, \end{cases} \tag{13}$$

where $\xi = \left|\underline{R}_{ve}\right|^2 / \left|\underline{R}_{he}\right|^2$ represents the power ratio of the received signal; $\rho = \frac{\underline{R}_{ve} \cdot \underline{R}_{he}^{\dagger}}{\sqrt{\left|\underline{R}_{ve}\right|^2 \cdot \left|\underline{R}_{he}\right|^2}}$ represents the correlation between the orthogonal components of the received signal, and $\dagger$ represents conjugate. $\rho = \left(\frac{\tan^2\vartheta \cdot \cos^2\varphi - \xi^{-1}}{\tan^2\vartheta \cdot \cos^2\varphi + \xi^{-1}}\right)^2$, where ϑ is the slant angle of receiving antenna, φ is the slant angle of the transmitting antenna [42].

Based on [43] and [44], the mean value of S_P is determined by $\beta_{vh} = arg[\sigma_{ve,he}]$, where $\sigma_{ve,he} = R_{ve} \cdot R_{he}^{\dagger}$, $arg(\cdot)$ is phase operator, the variance of S_P is determined by ρ. When $\rho = 0$, the orthogonal signal components are independent of each other, and S_P follows uniform distribution, that is, $S_P \sim U[0, 2\pi)$. When $\rho = 1$, the orthogonal signal components are completely correlated, and S_P follows delta distribution. When $0 < \rho < 1$, S_P follows normal distribution, that is, $S_P \sim N(\mu_{SP}, \sigma_{SP}^2)$, and

$$\begin{aligned} \mu_{SP} &= \beta_{vh} \\ \sigma_{SP}^2 &= 2\left(1 - \frac{\Gamma^2(1.5)}{\Gamma^2(1)}\sqrt{\rho} \times_2 F_1(0.5; 0.5; 2; \rho)\right), \end{aligned} \tag{14}$$

where ${}_2F_1(\cdot;\cdot;\cdot;\cdot)$ is the confluent hypergeometric functions.

To facilitate later derivation, the characteristics of CPR used for authentication is

$$\vec{S}_l = log(\vec{S}) = log(S_F) + jS_P. \tag{15}$$

We use S_{lF} to replace $log(S_F)$, then,

$$\begin{aligned} \hat{S}_{lF} &= S_{lF} + F_X + F_R \\ \hat{S}_P &= S_P + P_X + P_R, \end{aligned} \tag{16}$$

where F_X and P_X are the estimation error of S_{lF} and S_P caused by transmitter hardware deficiency and transmitter noise, which follow Gaussian distribution with a mean of μ_{FX} and μ_{PX}, and variance of σ_{FX}^2 and σ_{PX}^2, that is, $F_X \sim N(\mu_{FX}, \sigma_{FX}^2)$, $P_X \sim N(\mu_{PX}, \sigma_{PX}^2)$. μ_{FX} and μ_{PX} are determined by transmitter hardware structure, $\sigma_{FX}^2 = \sigma_{PX}^2 = KT_0BF_{NX}$, where $K = 1.38 \times 10^{-23} J/K$, $T_0 = 290K$, B is the measurement noise bandwidth per tone, F_{NX} is the transmitter noise figure. F_R and P_R are the estimation error of S_F and S_P caused by receiver hardware deficiency and receiver noise, which follow Gaussian distribution with a mean of μ_{FR} and μ_{PR}, and variance of σ_{FR}^2 and σ_{PR}^2, that is, $F_R \sim N(\mu_{FR}, \sigma_{FR}^2)$, $P_R \sim N(\mu_{PR}, \sigma_{PR}^2)$. μ_{FR} and μ_{PR} are determined by receiver hardware structure, $\sigma_{FR}^2 = \sigma_{PR}^2 = KT_0BF_{NR}$, F_{NR} is the receiver noise figure.

For wireless communications, the relative movement between transmitters and scatterers results in correlated temporal variations of channels. Similar to [17], we use the first-order Gauss-Markov process to approximate the temporal channel variations. Then represented as

$$\begin{aligned} S_{lF}[t+1] &= \alpha_F S_{lF}[t] + \sqrt{\left(1-\alpha_F^2\right)\sigma_{SF}^2}u[t+1] \\ S_P[t+1] &= \alpha_P S_P[t] + \sqrt{\left(1-\alpha_P^2\right)\sigma_{SP}^2}u[t+1], \end{aligned} \tag{17}$$

where $S_{lF}[t+1]$ and $S_P[t+1]$ represent S_{lF} and S_P at $(t+1)$th interval. $S_{lF}[t]$ and $S_P[t]$ represent S_{lF} and S_P at tth interval. α_F represents the correlation between $S_{lF}[t+1]$ and $S_{lF}[t]$, α_P represents the correlation between $S_P[t+1]$ and $S_P[t]$. A larger value of α_F and α_P results in a higher degree of correlation. Without losing generality, it is assumed that $\alpha_F = \alpha_P = \alpha$. Since CPR is continuous, ΔT can be adjusted adaptively according to channel coherence time, and a large α can always be obtained. $u[t+1]$ represents a Gaussian

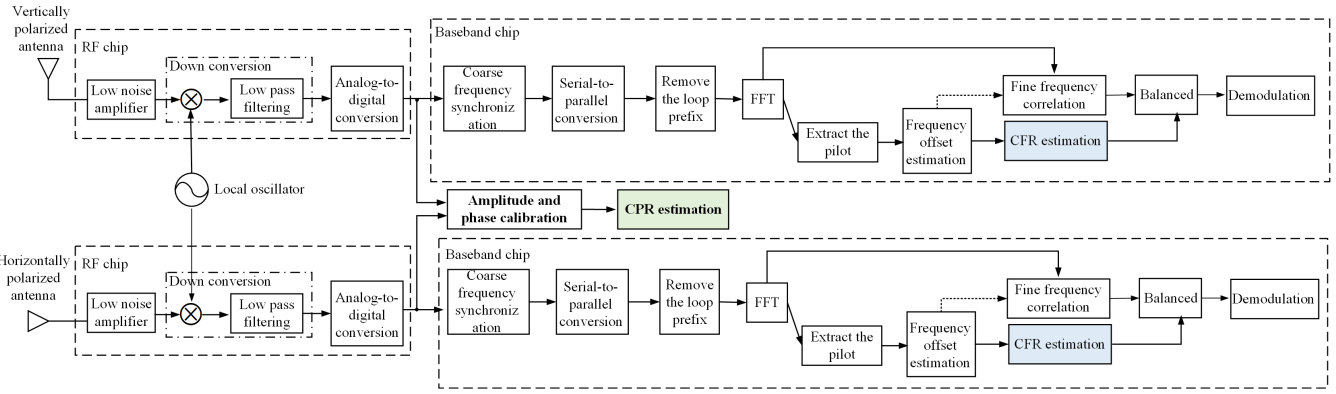


Fig. 2. The diagram of CPR estimation.

random variable with mean of 0 and variance of 1, that is, $u[t+1] \sim N(0,1)$.

As shown in Fig. 2, we demonstrate the estimation of CPR. The CPR estimation only needs to use the original baseband signal and can be completed only by embedding a digital signal processing module in the existing commercial systems. However, the extraction of CFR requires customization of the existing commercial baseband signal processing chips. Therefore, the CPR extraction is more compatible with current commercial systems than CFR.

C. Authentication Based on CPR

Assuming that the transmitted signal frequency range is $[f_{min}, f_{max}]$, $\hat{S}_{lF}$ and $\hat{S}_P$ that Bob stored are $\underline{\hat{S}}_{lF} = [\hat{S}_{lF1}, \hat{S}_{lF2}, \cdots, \hat{S}_{lFm}, \cdots, \hat{S}_{lFM}]$ and $\underline{\hat{S}}_P = [\hat{S}_{P1}, \hat{S}_{P2}, \cdots, \hat{S}_{Pm}, \cdots, \hat{S}_{PM}]$, where $\hat{S}_{lFm} = \hat{S}_{lF}(f_m)$, $\hat{S}_{Pm} = \hat{S}_P(f_m)$, $f_m = f_{min} + m \cdot \Delta f$, $\Delta f = (f_{max} - f_{min})/M$.

Bob uses the logarithmic likelihood ratio test to determine the test statistic T that evaluates the difference of CPRs between adjacent time intervals [21]. Specifically, the logarithm likelihood ratio rule is:

$$T = log \frac{P(\hat{\underline{S}}_l[t+1]|H_1)}{P(\hat{\underline{S}}_l[t+1]|H_0)}, \tag{18}$$

where $P(\cdot)$ denotes a probability density function; the null hypothesis, H_0, denotes that the transmitter is Alice; the alternative hypothesis, H_1, denotes that the transmitter is not Alice and we assume that the transmitter is Eve. According to (16) and (17), $\hat{\underline{S}}_l[t+1]$ follows complex Gaussian distribution with mean of $\alpha_A \hat{\underline{S}}_l[t]$ and variance of $\sigma_0^2 = \left(1-\alpha_A^2\right)\left(\sigma_{SFA}^2 + \sigma_{SPA}^2\right) + \left(1+\alpha_A^2\right)\left(\sigma_{FXA}^2 + \sigma_{PXA}^2 + \sigma_{FR}^2 + \sigma_{PR}^2\right)$ under H_0, where α_A is the correlation coefficient of S_{lF} (S_P) between Alice and Bob, σ_{SFA}^2 (σ_{SPA}^2) represents the variance of S_{lF} (S_P) between Alice and Bob, σ_{FXA}^2 and σ_{PXA}^2 represent the estimation error of S_{lF} and S_P caused by the Alice transmitter noise. According to (16), $\hat{\underline{S}}_l[t+1]$ follows complex Gaussian distribution with mean of $\mu_{SE} = \mu_{SFE} + j\mu_{SPE}$ and variance of $\sigma_1^2 = \sigma_{SFE}^2 + \sigma_{SPE}^2 + \sigma_{FXE}^2 + \sigma_{PXE}^2 + \sigma_{FR}^2 + \sigma_{PR}^2$ under H_1, where σ_{SFE}^2 (σ_{SPE}^2) represents the variance of S_{lF} (S_P) between Eve and Bob, and σ_{FXE}^2 and σ_{PXE}^2 represent the estimation errors of S_{lF} and S_P caused by the Eve transmitter noise. Then,

$$T = \frac{\left|\hat{\underline{S}}_l[t+1] - \alpha_A \hat{\underline{S}}_l[t]\right|^2}{\sigma_0^2} - \frac{\left|\hat{\underline{S}}_l[t+1] - \mu_{SE}\right|}{\sigma_1^2} + log\frac{\sigma_0^2}{\sigma_1^2}. \tag{19}$$

The location uncertainty of Eve makes $\sigma_{SFE}^2 \gg \sigma_{SFA}^2$ and $\sigma_{SPE}^2 \gg \sigma_{SPA}^2$ [14], then (19) can be simplified as

$$T \approx \left|\hat{\underline{S}}_l[t+1] - \alpha_A \hat{\underline{S}}_l[t]\right|^2 / \sigma_0^2. \tag{20}$$

Bring (15) into (20), we can obtain

$$T \approx \frac{\left|\hat{S}_{lF}[t+1] - \alpha_A \hat{S}_{lF}[t]\right|^2}{\sigma_0^2} + \frac{\left|\hat{S}_P[t+1] - \alpha_A \hat{S}_P[t]\right|^2}{\sigma_0^2}. \tag{21}$$

According to the typical statistical decision method, Bob uses a hypothesis test model to determine whether the transmitter at the $(t+1)$th interval continues to be Alice. When T is less than or equal to the threshold δ, Bob accepts the hypothesis H_0. Otherwise, Bob accepts the hypothesis H_1.

$$\begin{aligned} H_0 &: T \le \delta \\ H_1 &: T > \delta. \end{aligned} \tag{22}$$

We show the authentication process of the proposed scheme in Fig. 3. Combining Fig. 2 and Fig. 3, we can see that the proposed authentication scheme only needs to add a CPR estimation module and an authentication module to the existing dual-polarized antenna communication systems, which is easy to implement.

IV. Performance Analysis

In this section, we first derive the false alarm probability, detection probability, and optimal threshold. Subsequently, the computational complexity of the proposed authentication scheme is analyzed, and the optimal stacking numbers and the optimal CPR points for authentication are also given in a closed-form manner. Finally, the impact of co-located attacks and Doppler effect on the authentication performance is emphatically discussed.

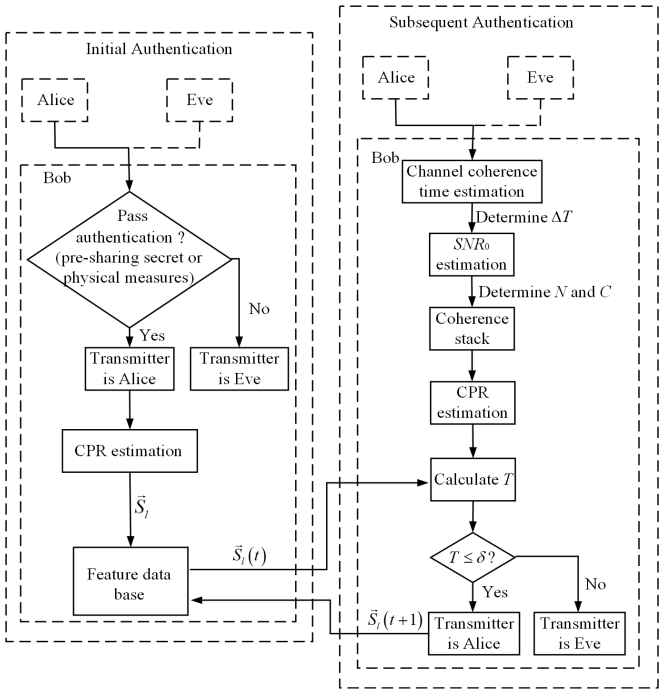


Fig. 3. The diagram of CPR based authentication scheme.

A. Derivation of False Alarm and Detection Probability

1) False Alarm Probability: Based on (21) and (22), the false alarm probability (P_{FA}) of the proposed scheme is

$$P_{FA}=1-\frac{e^{-\frac{\delta}{2\beta}}}{(2\beta)^{\frac{v}{2}+1}}\frac{\delta^{\frac{v}{2}}}{\Gamma(\frac{v}{2}+1)}\sum_{k\geq 0}\frac{k!m_k}{(\frac{v}{2}+1)_k}L_k^{v/2}\left(\frac{(v+2)\delta}{4\beta\mu_0}\right). \tag{23}$$

Proof: P_{FA} refers to that under H_0, T is greater than δ, Bob misjudges Alice as Eve,

$$P_{FA}=P(T>\delta|H_0)=1-F_{FA}(\delta), \tag{24}$$

where $F_{FA}(\delta)=P(T\leq\delta|H_0)$ is the cumulative distribution function of T under H_0, which will be derived below. For the sake of analysis, T is represented as

$$\begin{aligned} T &= T_F+T_P \\ T_F &= \sum_{m=1}^{M}\frac{\left|\hat{S}_{lFm}[t+1]-\alpha_A\hat{S}_{lFm}[t]\right|^2}{\sigma_0^2} \\ T_P &= \sum_{m=1}^{M}\frac{\left|\hat{S}_{Pm}[t+1]-\alpha_A\hat{S}_{Pm}[t]\right|^2}{\sigma_0^2}. \end{aligned} \tag{25}$$

Under H_0, the transmitter is still Alice at $(t+1)$th interval. The CPR estimated at the $(t+1)$th interval can be characterized by the first-order Gauss-Markov model. Then, T_F becomes:

$$T_F=F_1\sum_{m=1}^{M}\left|\underbrace{\frac{\sqrt{\left(1-\alpha_A^2\right)\sigma_{SFA}^2}u[t+1]+\Delta F_{1m}}{\sigma_{F1}}}_{T_{Fm}}\right|^2, \tag{26}$$

where $\sigma_{F1}^2=\left(1-\alpha_A^2\right)\sigma_{SFA}^2+\left(1+\alpha_A^2\right)\left(\sigma_{FXA}^2+\sigma_{FR}^2\right)$, $F_1=\sigma_{F1}^2/\sigma_0^2$, $\Delta F_{1m}=\Delta F_{Xm}+F_{Rm}$, $\Delta F_{Xm}=F_{XAm}[t+1]-\alpha_A F_{XAm}[t]$, and $\Delta F_{Rm}=F_{Rm}[t+1]-\alpha_A F_{Rm}[t]$. Since $u[t+1]\sim N(0,1)$, $F_{XAm}\sim N(\mu_{FXAm},\sigma_{FXA}^2)$, $F_{Rm}\sim N(\mu_{FRm},\sigma_{FR}^2)$, T_{Fm} follows Gaussian distribution with mean of 0 and variance of 1. Then, T_F follows the central chi-square distribution with M degrees of freedom, that is, $T_F\sim F_1\chi_M^2$.

Under H_0, T_P becomes:

$$T_P=P_1\sum_{m=1}^{M}\left|\frac{\sqrt{\left(1-\alpha_A^2\right)\sigma_{SPA}^2}u[t+1]+\Delta P_{1m}}{\sigma_{P1}}\right|^2, \tag{27}$$

where $\sigma_{P1}^2=\left(1-\alpha_A^2\right)\sigma_{SPA}^2+\left(1+\alpha_A^2\right)\left(\sigma_{PXA}^2+\sigma_{PR}^2\right)$, $P_1=\sigma_{P1}^2/\sigma_0^2$, $\Delta P_{1m}=\Delta P_{Xm}+\Delta P_{Rm}$, $\Delta P_{Xm}=P_{XAm}[t+1]-\alpha_A P_{XAm}[t]$, and $\Delta P_{Rm}=P_{Rm}[t+1]-\alpha_A P_{Rm}[t]$. Since $P_{XAm}\sim N(\mu_{PXAm},\sigma_{PXA}^2)$, $P_{Rm}\sim N(\mu_{PRm},\sigma_{PR}^2)$, T_P follows the central chi-square distribution with M degrees of freedom, that is, $T_P\sim P_1\chi_M^2$.

When a variable is the linear weighted sum of two chi-square variable, its cumulative distribution function can be approximated by Laguerre polynomials [45]. Therefore, according to (26) and (27), the cumulative distribution function of T is

$$F_{FA}(\delta)=\frac{e^{-\frac{\delta}{2\beta}}}{(2\beta)^{\frac{v}{2}+1}}\frac{\delta^{\frac{v}{2}}}{\Gamma(\frac{v}{2}+1)}\sum_{k\geq 0}\frac{k!m_k}{(\frac{v}{2}+1)_k}L_k^{v/2}\left(\frac{(v+2)\delta}{4\beta\mu_0}\right), \tag{28}$$

where $\beta=\frac{2\cdot\alpha_1\cdot\alpha_2}{\alpha_1+\alpha_2}$, $\alpha_1=F_1$, $\alpha_2=P_1$. $\Gamma(\cdot)$ is the gamma function. $v_1=v_2=M$ and $v=v_1+v_2$. $(u)_v=\Gamma(u+v)/\Gamma(u)$ is the Pochhammer symbol [46]. $0<\mu_0<p/2$ and $p=v/2+1$. m_k can be expressed as in (29-a)-(29-c), shown at the bottom of the next page, and $\delta_1=0$, $\delta_2=0$. $L_n^v(y)=\frac{\Gamma(v+n+1)}{n!}\sum_{q=0}^{n}\frac{(-n)_q y^q}{q!\Gamma(v+q+1)}$ is the generalized Laguerre polynomial.

The proof is complete.

2) Detection Probability: Based on (21) and (22), the detection probability (P_D) of the proposed scheme is

$$\begin{aligned} P_D=1-&\frac{e^{-\frac{\delta}{2\beta'}}}{(2\beta')^{\frac{v'}{2}+1}}\frac{\delta^{\frac{v'}{2}}}{\Gamma(\frac{v'}{2}+1)} \\ &\times\sum_{k\geq 0}\frac{k!m_k'}{(\frac{v'}{2}+1)_k}L_k^{v'/2}\left(\frac{(v'+2)\delta}{4\beta'\mu_0'}\right). \end{aligned} \tag{30}$$

Proof: P_D refers to that under the hypothesis of H_1, T is greater than δ, and Bob correctly detects the existence of Eve,

$$P_D=P(T>\delta|H_1)=1-F_D(\delta), \tag{31}$$

where $F_D(\delta)=P(T\leq\delta|H_1)$ is the cumulative distribution function of T under H_1, which will be derived below.

Under H_1, the transmitter is Eve. In this case, the CPRs estimated by Bob at the tth and $(t+1)$th interval are independent of each other. Then, T_F becomes

$$T_F=F_2\sum_{m=1}^{M}\left|\frac{S_{lFEm}[t+1]-\alpha_A S_{lFAm}[t]+\Delta F_{2m}}{\sigma_{F2}}\right|^2, \tag{32}$$

where $\sigma_{F2}^2 = \sigma_{SFE}^2 + \alpha_A^2\sigma_{SFA}^2 + \sigma_{FXE}^2 + \alpha_A^2\sigma_{FXA}^2 + \sigma_{FR}^2 + \alpha_A^2\sigma_{FR}^2$, $F_2 = \sigma_{F2}^2/\sigma_0^2$, $\Delta F_{2m} = \Delta F'_{Xm} + \Delta F_{Rm}$, and $\Delta F'_{Xm} = F_{XEm}[t+1] - \alpha_A F_{XAm}[t]$. Since $S_{lFEm} \sim N(\mu_{SFEm}, \sigma_{SFE}^2)$, $F_{XEm} \sim N(\mu_{FXEm}, \sigma_{FXE}^2)$, T_F follows the non-central chi-square distribution with M degrees of freedom, that is, $T_F \sim F_2\chi_M^2(\eta_F)$, where $\eta_F = \sum_{m=1}^{M}\left[\frac{\mu_{SFEm}-\alpha_A\mu_{SFAm}+\mu_{FXEm}-\alpha_A\mu_{FXAm}}{\sigma_{F2}}\right]^2$.

Under H_1, T_P becomes

$$T_P = P_2\sum_{m=1}^{M}\left|\frac{S_{PEm}[t+1]-\alpha_A S_{PAm}[t]+\Delta P_{2m}}{\sigma_{P2}}\right|^2, \quad (33)$$

where $\sigma_{P2}^2 = \sigma_{SPE}^2 + \alpha_A^2\sigma_{SPA}^2 + \sigma_{PXE}^2 + \alpha_A^2\sigma_{PXA}^2 + \sigma_{PR}^2 + \alpha_A^2\sigma_{PR}^2$, $P_2 = \sigma_{P2}^2/\sigma_0^2$, $\Delta P_{2m} = \Delta P'_{Xm} + \Delta P_{Rm}$, and $\Delta P'_{Xm} = P_{XEm}[t+1] - \alpha_A P_{XAm}[t]$. Since $S_{PEm} \sim N(\mu_{SPEm}, \sigma_{SPE}^2)$, $P_{XEm} \sim N(\mu_{PXEm}, \sigma_{PXE}^2)$, T_P follows the non-central chi-square distribution with M degrees of freedom, that is $T_P \sim P_2\chi_M^2(\eta_P)$, where $\eta_P = \sum_{m=1}^{M}\left[\frac{\mu_{SPEm}-\alpha_A\mu_{SPAm}+\mu_{PXEm}-\alpha_A\mu_{PXAm}}{\sigma_{P2}}\right]^2$.

According to (25), (32), and (33), the cumulative distribution function of T is

$$F_D(\delta) = \frac{e^{-\frac{\delta}{2\beta'}}}{(2\beta')^{\frac{v'}{2}+1}}\frac{\delta^{\frac{v'}{2}}}{\Gamma(\frac{v'}{2}+1)} \times\sum_{k\geq 0}\frac{k!m'_k}{(\frac{v'}{2}+1)_k}L_k^{v/2}\left(\frac{(v'+2)\delta}{4\beta'\mu'_0}\right), \quad (34)$$

where $\beta' = \frac{2\cdot\alpha'_1\cdot\alpha'_2}{\alpha'_1+\alpha'_2}$, $\alpha'_1 = F_2$, and $\alpha'_2 = P_2$. $v'_1 = v'_2 = M$ and $v' = v'_1 + v'_2$. $0 < \mu'_0 < p'/2$ and $p' = v'/2 + 1$. $\delta'_1 = \eta_F$, $\delta'_2 = \eta_P$. Bring β', v', p', μ'_0, δ'_1, and δ'_2 into (29-a)-(29-c), we can obtain m'_k.

The proof is complete.

B. Optimal Threshold

According to the Neyman-Pearson (NP) theorem, P_D increases as P_{FA} increases. Then, the optimal threshold can be obtained by solving $P_{FA} = \epsilon$, where ϵ is the maximum P_{FA} that Bob can tolerate. However, when we take a closer look at (23), we find that the threshold δ exists multiple places of the closed-form expression of the P_{FA}. Then, it is challenging to obtain the optimal threshold directly from (23). Thus, we first derive the approximated expression of P_{FA} to replace (23) for calculating the optimal threshold.

Here, we adopt the Log-Normal distribution to approximate the chi-square distribution in (26) and (27). This approximation is based on the observation that the probability density function of the chi-square distribution is nearly identical to that of the Log-Normal distribution when the degree of freedom of the chi-square distribution is large [2], [47]. Thus, we obtain $T \sim F_1 LogN(\mu_F, \sigma_F^2) + P_1 LogN(\mu_P, \sigma_P^2)$, where $\mu_F = \mu_P = log(M) - \frac{\sigma_F^2}{2}$ and $\sigma_F^2 = \sigma_P^2 = log\left(1+\frac{2}{M}\right)$.

The log-shifted Gamma approximation is also employed to model the sum of two lognormally distributed random variables according to [48] and [49]. Then, the cumulative distribution function of T can be approximated as

$$P(T \leq \delta|H_0) \approx \frac{\gamma\left(\varpi, \frac{log(\delta)-\varrho}{\varsigma}\right)}{\Gamma(\varpi)}. \quad (35)$$

$\varpi, \varrho, \varsigma$ can be obtained by the following expressions

$$\begin{aligned}\frac{e^{\varrho}}{(1-\varsigma)^{\varrho}} &= e^{\mu_F + log(F_1) + \sigma_F^2/2} + e^{\mu_P + log(P_1) + \sigma_P^2/2}\\ \varrho + \varpi\varsigma &= \mu_F + log(F_1) + G_1\left(\mu, \sigma^2\right)\\ \varpi\varsigma^2 &= \sigma_F^2 - G_1^2\left(\mu,\sigma^2\right) + G_2\left(\mu,\sigma^2\right) - \frac{2\sigma_F^2 G_3\left(\mu,\sigma^2\right)}{\sigma^2},\end{aligned} \quad (36)$$

where $\mu = \mu_P - \mu_F + log(P_1) - log(F_1)$, $\sigma^2 = \sigma_F^2 + \sigma_P^2$. G_1, G_2, and G_3 can be represented as in (37-a)-(37-c), shown at the bottom of the next page, where

$$\begin{aligned}F(\sigma,\mu,k) &= e^{-k\mu + \frac{k^2\sigma^2}{2}}\Phi\frac{\mu - k\sigma^2}{\sigma}\\ \Phi(x) &= \frac{1}{2\pi}\int_{-\infty}^{x} e^{-\frac{t^2}{2}}dt\\ C_k &= \frac{(-1)^{k+1}}{k}\\ B_k &= \frac{2(-1)^{k+1}}{k+1}\sum_{j=1}^{k}\frac{1}{j}.\end{aligned}$$

Bring (23) and (35) into $P_{FA} = \epsilon$, we can obtain the optimal threshold

$$\delta^* = e^{F^{-1}_{\Gamma(\varpi,\varsigma)}(1-\epsilon)+\varrho}, \quad (38)$$

where $F^{-1}_{\Gamma(\varpi,\varsigma)}(1-\epsilon)$ is the inverse of the cumulative distribution function of $\Gamma(\varpi,\varsigma)$, which can be calculated by $gaminv(1-\epsilon,\varpi,\varsigma))$ in Matlab.

Substituting (38) into (30), we can see that P_D is determined by $SNR_0, \xi_A, \xi_E, \alpha_{FA}, \alpha_{PA}, C, M$ under specific P_{FA}, where SNR_0, C, M can be adjusted according to specific performance requirement and channel parameters of $(\xi_A, \xi_E, \alpha_{FA}, \alpha_{PA})$. In the simulations, we analyze the impact of those factors on authentication performance.

$$m_k = \frac{\sum_{k=0}^{k-1} m_j d_{k-j}}{k}, \quad k \geq 1 \quad (29\text{-a})$$

$$m_0 = 2\left(\frac{v}{2}+1\right)^{\frac{v}{2}+1} exp\left(-\frac{1}{2}\sum_{i=1}^{2}\frac{\delta_i\alpha_i(p-\mu_0)}{\beta\mu_0+\alpha_i(p-\mu_0)}\right)\frac{\beta^{\frac{v}{2}+1}}{p-\mu_0}\prod_{i=1}^{2}(\beta\mu_0+\alpha_i(p-\mu_0)) - \frac{v_i}{2} \quad (29\text{-b})$$

$$d_j = -\frac{j\beta p}{2\mu_0}\sum_{i=1}^{2}\delta_i\alpha_i(\beta-\alpha_i)^{j-1}\left(\frac{\mu_0}{\beta\mu_0+\alpha_i(p-\mu_0)}\right)^{j+1} + \left(\frac{-\mu_0}{p-\mu_0}\right)^j + \sum_i^2\frac{v_i}{2}\left(\frac{\mu_0(\beta-\alpha_i)}{\beta\mu_0+\alpha_i(p-\mu_0)}\right)^j, \quad j \geq 1 \quad (29\text{-c})$$

C. Computational Complexity and Optimal (C, M)

1) Computational Complexity: We use C^{CM} and C^{ADD} to represent the number of multiplications and additions of various schemes, and $COM = C^{CM} + C^{ADD}$ represents the total computation. The computation of the proposed scheme comes from three parts: authentication, CPR estimation, and coherent stacking.

According to (21), C^{CM} required for authentication is $(4M + 6) \times \tau$, where $\tau = S_t/T_c$ represents the time varying speed of the channel, S_t is the duration of a pilot, and $T_c = c/(Vf_c)$. The reason for multiplying τ is that as the time varying speed of the channel increases, the number of authentications will also linearly increase. C^{ADD} required for authentication is $(4M+3)\times\tau$. The total computation required for authentication is $COM_{au} = (8M + 9) \times \tau$.

According to (11), C^{CM} required for CPR estimation is $(M^2 + 2M + 1) \times \tau$. C^{ADD} required for CPR estimation is $(M(M-1)+1)\times\tau$. The total computation required for CPR estimation is $COM_{es} = (2M^2 + M + 2) \times \tau$.

According to (7) and (8), C^{CM} required for coherent stacking is $(2CM + 1) \times \tau$. C^{ADD} required for coherent stacking is $(CM+C)\times\tau$. The total computation required for coherent stacking is $COM_{st} = (3CM + C + 1) \times \tau$.

Then, the total computation required for CPR based scheme is $COM_{CPR} = (2M^2+9M+3CM+C+12)\times\tau$. According to (7) in [2], the computation required for the CFR based scheme is $COM_{CFR} = 4M$. We can observe that for the same M, the proposed scheme requires more computation. For wireless communication systems such as IoT and 5G, these extra computations are acceptable.

2) Optimal C and M: In order to optimize COM under the specific performance requirements (P_{FAs},P_{Ds}) and channel parameters (τ_s, SNR_0). We need to select the appropriate C and M. The mathematical model is

$$\begin{aligned} &\min_{C,M} \ COM_{CPR} \\ &\text{s.t. } P_D = P_{Ds}, \quad P_{FA} = P_{FAs}, \quad \tau = \tau_s, \quad SNR = SNR_0, \\ &\quad C \times M = N, \quad N = Sa \cdot T_s, \quad T_s \le \frac{S_t}{\tau}. \end{aligned} \tag{39}$$

Since COM_{CPR} increases monotonically with the increases of C and M under certain τ. The above optimization problem can be simplified to solve C and M with $P_D(\delta = e^{F^{-1}_{\Gamma(\varpi,\varsigma)}(1-P_{FAs})+\varrho}, SNR = SNR_0) = P_{Ds}$. Through exhaustive search method we can find the optimal C^* and M^*.

D. Impact of Co-Located Attacks and Doppler Effect

1) Impact of Co-Located Attacks: Assuming that Alice and Eve are located at the same position, and that Eve has perfect knowledge of the ideal transmitting polarization state that Alice wants to transmit. Alice and Eve complete the information transmission at tth and $(t + 1)$th interval, respectively. Since the receiver of both Alice and Eve is the same, μ_{PR} and μ_{FR} can be eliminated according to (21). Therefore, we only need to analyze the impact of transmitter hardware deficiencies and channel polarization fading on CPR. We denote that $\zeta(f)$ represents the polarization deflection difference between Alice and Eve owing to their different hardware deficiency, as shown in Fig. 4. We can then obtain the CPR of Eve using [50]

$$\vec{S}_E = \vec{S}_A \cdot \begin{bmatrix} cos\zeta(f) & sin\zeta(f) \\ -sin\zeta(f) & cos\zeta(f) \end{bmatrix}, \tag{40}$$

where $\vec{S}_A$ is the CPR between Alice and Bob. Substituting (10) and (11) into (40), we can get the CPR difference between Alice and Eve is

$$\begin{aligned} \Delta\vec{S} &= \vec{S}_E - \vec{S}_A \\ &= S_{FeA} \cdot e^{jS_{PeA}} \cdot (cos\zeta(f) + sin\zeta(f) - 1) \\ &\quad + X_F \cdot e^{-jX_P} \cdot (sin\zeta(f) - cos\zeta(f)) - 1. \end{aligned} \tag{41}$$

Here $\Delta\vec{S}$ represents the CPR difference caused by channel polarization fading under the specific polarization deflection difference $\zeta(f)$ between transmitters. To simplify the analysis, we assume that the transmitted polarization state of Alice is an ideal vertical polarization. Then (41) can be simplified as

$$\Delta\vec{S} = S_{FeA} \cdot e^{jS_{PeA}} \cdot (cos\zeta - sin\zeta - 1) + (sin\zeta + cos\zeta - 1). \tag{42}$$

In Fig. 5, we show the impact of ζ and ξ on $|\Delta\vec{S}|^2$ at a frequency, such result is also valid at other frequency, which is the three-dimensional surface, the red line on the surface is δ of (38). We can see that $|\Delta\vec{S}|^2$ increases with the increase of ζ and ξ. We can also see that, the CPR difference is larger than the threshold when $\zeta \ge 0.3$ and $\xi \ge 3.25$. According to [34], [42], [51], [52], $\zeta \ge 0.3$ and $\xi \ge 6$ can always be obtained. Then, our proposed scheme can distinguish different transmitters at the same location.

Actually, the transmitter hardware deficiency can also cause CFO, which also affects the CFR under the frequency selective fading channels. However, the CFO is much smaller than the

$$G_1(\mu,\sigma) = \mu\Phi\left(\frac{\mu}{\sigma}\right) + \frac{\sigma}{\sqrt{2\pi}} e^{-\frac{\mu^2}{2\sigma^2}} + \sum_{k=1}^{\infty} C_k \left[(F(\sigma,\mu,k) + F(\sigma,-\mu,k))\right] \tag{37-a}$$

$$G_2(\mu,\sigma) = \left(\mu^2+\sigma^2\right)\Phi\left(\frac{\mu}{\sigma}\right) + \frac{(\mu+ln4)\,\sigma}{\sqrt{2\pi}} e^{-\frac{\mu^2}{2\sigma^2}} + 2\sum_{k=1}^{\infty} C_k \left(\mu - k\sigma^2\right) F(\sigma,\mu,k) + \sum_{k=2}^{\infty} B_{k-1}\left(F(\sigma,\mu,k) + F(\sigma,-\mu,k)\right) \tag{37-b}$$

$$G_3(\mu,\sigma) = \sigma^2 \sum_{k=1}^{\infty} \left[(-1)^k \left(F(\sigma,\mu,k) + F(\sigma,-\mu,k+1)\right)\right] \tag{37-c}$$

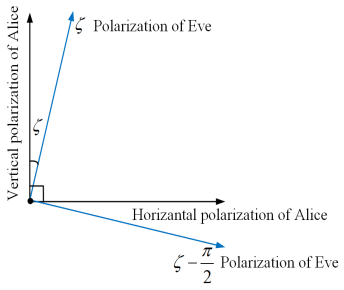


Fig. 4. Polarization deflection of transmitter at a specific frequency, which is various at different frequency.

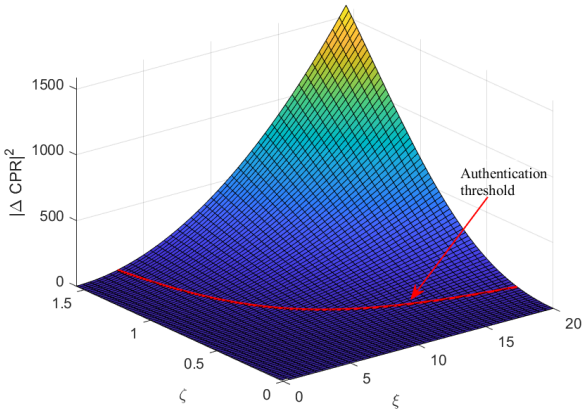


Fig. 5. CPR difference between transmitters at the same location.

channel coherence bandwidth [53], [54], and the CFR can be approximately regarded as constant. Then, the schemes based on CFR cannot distinguish the transmitters at the same location.

2) Impact of Doppler Effect: In time-varying scenarios, the presence of the Doppler shift can impact the authentication performance. While the CPR estimation shown in Fig. 2 does not involve the estimation of frequency offset, thus the effect of the Doppler effect on authentication performance is required to be carefully considered. Specifically, in the time domain, the Doppler effect causes time-varying channels, which leads to variation in α and τ. In the frequency domain, the Doppler effect causes spectrum extension, which results in the overlap of signals at different frequencies.

In our proposed scheme, ΔT is adjusted according to T_c to ensure that large α_F and α_P are always satisfied. This adjustment helps to eliminate the influence of the Doppler effect on the authentication performance in the time domain. In the following, we will analyze the impact of the Doppler effect on authentication performance in the frequency domain.

We consider two cases, where the relative velocity of scatterers in the channel is either constant or increases linearly.

1) *Uniform motion*. Under this case, the overlap of signal at tth interval and $(t+1)$th interval are the same, that is, the CPRs are highly correlated in the coherence time, and the authentication performance is not affected by the Doppler effect.

2) *Uniformly accelerated motion*. Considering an acceleration of a and a velocity of scatterers in tth interval as V, the velocity of scatterers in $(t+1)$th interval is $V + a\Delta T$. The maximum Doppler shift at tth interval is $f_m[t] = \frac{V\cdot\cos\theta}{c} \cdot f_c$, and the maximum Doppler shift at $(t+1)$th interval is $f_m[t+1] = \frac{(V+a\Delta T)\cdot\cos\theta}{c} \cdot f_c$, then the Doppler shift difference between tth interval and $(t+1)$th interval is $\Delta f = \frac{a\cdot\Delta T\cdot\cos\theta}{c} \cdot f_c$. In our paper $\Delta T = T_c$, then $\Delta f = \frac{a\cdot T_c\cdot\cos\theta}{c} \cdot f_c$. Under the worst case scenario (high-speed rail scenarios) with $\theta = 0$, $a = 7.78m/s^2$, $T_c = 500/f_c$ [55], we can obtain $\Delta f = 1.297 \times 10^{-5} Hz$. According to polarization mode dispersion, the polarization state on the Poincare sphere spirally deflects with frequency, and the polarization states of adjacent frequencies are highly correlated. Since Δf is much smaller than coherence bandwidth [53], [54], the CPRs at the tth interval and $(t+1)$th interval are highly correlated, and the authentication performance is not affected by Doppler effect.

V. Simulation and Experimental Results

A. Simulation Setting

According to (30) and (38), Table II lists the primary system parameters that affect authentication performance. Here, $\Delta\xi = |\xi_E - \xi_A|$ reflects the polarization power imbalance difference between various channels. Assume that Alice is equipped with a vertically polarized antenna and Bob is equipped with $\pm 45°$ dual polarized antennas. Considering a Rayleigh fading channel. We compare the authentication performance of the proposed scheme with that of CFR based scheme. The authentication model of the CFR scheme is based on the EMCP scheme proposed in [2], which is the same as this paper. So as to demonstrate the advantages of CPR over CFR in authentication.

We use Matlab for Monte Carlo simulations. Assume that the distance between Alice and Bob is d_A, and the distance between Eve and Bob is d_E. The channel gain is calculated by $\sigma_Y^2 = P_0 d_Y^{-n}, Y \in A, E$, n is the path loss exponent, which is the same as the measured value of the experiments in section V-B. Based on (5), (13), and (14), we calculate the mean and variance of S_{lF} and S_P, where ξ is the same as the measured value of the experiments in section V-B. Additionally, we also need to consider the transmitter and receiver hardware deficiencies and noise, which are the same as the measured value of the experiments in section V-B. Then, based on (3) in [2] and (17), the CFR and CPR between Alice and Bob are generated by the "randn" function in Matlab. If the signal at $(t+1)$th interval is still from Alice, the CPR is generated based on (17), and the CFR is generated based on (2) in [2], where α_F and α_P are the same as experiments. If the signal at $(t+1)$th interval comes from Eve, the CFR and CPR are generated by independent "randn" function. If the signal at $(t+1)$th interval comes from Eve and Eve modifies its transmitting signal to attack the authentication systems, the CFR and CPR are generated based on (19) in [56], where the channel correlation coefficient is obtained based on (55) in [57]. Based on the authentication process shown in Fig. 3, we conduct 10000 independent Monte Carlo simulations, and the average P_{FA} and P_D are counted.

Based on (23), (30), and (38), we use numerical simulation to obtain the theoretical P_{FA} and P_D of the proposed scheme.

TABLE II
SYSTEM PARAMETERS

Parameter	Description
SNR	Signal to noise ratio
$\Delta\xi$	Difference between ξ_E and ξ_A
α_F	The correlation between $S_F[t+1]$ and $S_F[t]$
α_P	The correlation between $S_P[t+1]$ and $S_P[t]$
τ	Channel time varying speed
C	Stacking numbers
M	CPR authentication points

The correctness of the theoretical analysis is verified by comparing them with the Monte Carlo results.

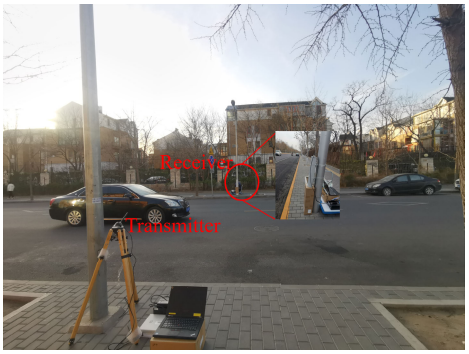
B. Experiment Setting

In order to further verify the effectiveness of the proposed scheme, we performed experiments in real communication scenarios. Due to the limited space of the paper, we only show four typical experiments, including experiments on slow time varying channel, ultra-low SNR, co-located attacks, and fast time varying channel. The first three experiments were performed in the office with a maximum speed of 1m/s, as shown in Fig. 6(a). The last experiment was performed on a highway at a average vehicle speed of 50km/h, as shown in Fig. 6(b). The scatterers shown in Fig. 6(a) are composed of metal, paper boxes, etc., and there are people movement. The scatterers shown in Fig. 6(b) consist of trees, vehicles, etc.

We use $\pm 45°$ dual polarized antennas as the receiving antenna and a vertically polarized antenna as the transmitting antenna, both of which are placed at a height of 1.5m. USRP X310 and GNU radio are used to send wireless signals with 1.9GHz and 32MHz bandwidth, in which a frame consists of 140 OFDM symbols and the frame duration is 10ms. Moreover, the OFDM symbol comprises 64 subcarriers, and the pilot is located at the [-21,-7,7,21] subcarrier of the first OFDM symbol. The sample rate S_a is 30.72MHz, which is the sample rate of Long Term Evolution (LTE) systems. According to [54], Fig. 6(a) is a low dynamic scenario with $\tau \ll 1$, and Fig. 6(b) is a highly dynamic scenario with $\tau > 1$.

Based on the received signal, we can calculate ξ by $\frac{|R_v|^2}{|R_h|^2}$, and calculate α_I by $\frac{cov(S_I[t],S_I[t+1])}{\sqrt{var(S_I[t])var(S_I[t+1])}}$, where $I \in (F, P)$, $cov(S_I[t], S_I[t+1])$ is the covariance between $S_I[t]$ and $S_I[t+1]$, $var(S_I[t])$ is the variance of $S_I[t]$, $var(S_I[t+1])$ is the variance of $S_I[t+1]$. By placing the transmitter next to the receiver, the hardware deficiency can be obtained by comparing the receiving polarization state with the ideal transmitting polarization state. Besides, the path loss exponent is calculated by $n = log(\frac{P_r}{P_t \cdot K})/log(\frac{d_0}{d})$, where $d_0 = 1m$ is the distance between transmitter and reference point, d is the distance between transmitter and receiver, P_r, P_t, and K are the received signal power, transmitted signal power, and signal power at distance of d_0, which are measured by spectrum analyzer (ROHDE SCHWARZ FSH8), and the signal is transmitted by signal generator (ROHDE SCHWARZ SMW 200A). Bring F_{NX} and F_{NR} of the used transmitters and receiver into $\sigma^2_{FO} = \sigma^2_{PO} = KT_0BF_{NO}$, where $O \in (X, R)$, we can obtain σ^2_{FO} and σ^2_{PO}. The above parameters are also used for simulations.

(a)



(b)

Fig. 6. Experimental scenarios. (a) Indoor office. (b) Urban highway.

Based on Fig. 3, we collect the signal data and conduct authentication, where $T_s = \Delta T = T_c$, N and C are determined by (39). In order to eliminate the randomness introduced by the noise, we conduct 10000 repeated experiments for each test point, then take the average value as the result.

C. Impact of SNR_0

In Fig. 7, we show the simulation and experiment results of the proposed scheme under different SNR_0. We can observe the following conclusions. First, the closed-form expressions of the theoretical results of various schemes perfectly match the corresponding simulation results as we expected. Second, the experiment results are slightly different from the simulation and theoretical results, which is caused by the fluctuation of SNR_0 during the measurement, with a maximum fluctuation of $0.2dB$. However, the maximum performance difference is less than 4%, which is consistent with the simulation result. Third, the P_Ds of various schemes improve as the value of SNR_0 increases. This is because the effect of estimation error significantly decreases as the value of SNR_0 increases. Fourth, the authentication performance of the proposed scheme is better than that of the EMCP scheme. This is evident at low SNR_0. For example, in the simulation, when $SNR_0 = -4dB$ and $C = 1$, $P_D = 99.8\%$ of the CPR based scheme, and $P_D = 61.5\%$ of the EMCP scheme. This is because the CPR is more sensitive to the change of channel, and CPR difference between various channels is greater, then Eve can

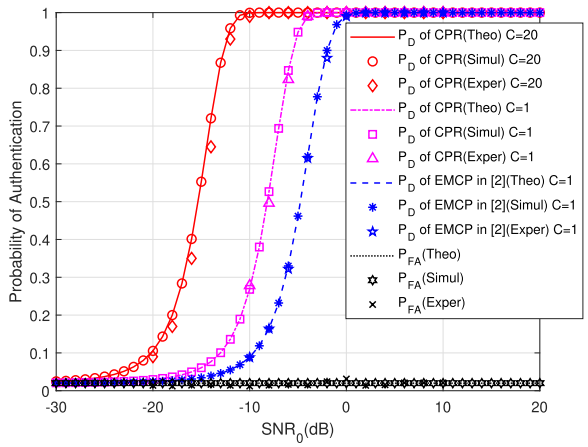


Fig. 7. (P_{FA}, P_D) of various schemes vs. SNR_0 and C with the setting of $\alpha_A = \alpha_{EMCP} = \alpha_{FA} = \alpha_{PA} = 0.924, M = 13, \epsilon = 0.02, d_A = d_E, \xi = 7.15$.

be easily detected. Fifth, the proposed scheme can still achieve good authentication performance when SNR_0 is very low. For example, when $SNR_0 = -10dB$ and $C = 20$, $P_D = 99.7\%$ of our proposed scheme, while $P_D = 9.8\%$ of the EMCP scheme. This is because coherent stacking improves the estimation accuracy of CPR.

D. Impact of C and M

In Fig. 8, we analyze the impact of C and M on the authentication performance.

In Fig. 8(a), we analyze the impact of C on the authentication performance of the proposed scheme. We can see that the P_D of the proposed scheme increases with the increase of C. This is because the improvement of SNR is proportional to C. Besides, P_D reaches saturation at $C = 21$ when $SNR_0 = -10dB$. This is because SNR reaches the value that is sufficiently accurate to estimate CPR. Since the computation of the proposed scheme is proportional to C, it is sufficient to select the value of C that makes the P_D reach saturation. We can also see that, with the increase of SNR_0, the required C is less to make P_D reach saturation. This is because with the increase of SNR_0, the required improvement of SNR is small under certain authentication performance.

In Fig. 8(b), we analyze the impact of M on the authentication performance. We can see that under the same P_D, the CPR based scheme requires less M than the EMCP scheme. Specifically, when $P_D \geq 98\%$ and $SNR_0 = 0dB$, the CPR based scheme needs $M \geq 13$, and the EMCP scheme needs $M \geq 24$. This is because the CPR is more sensitive to the change of channel, and the difference between various channels is greater. In practice, we can select appropriate M according to the authentication performance requirements to reduce the computational complexity. We can also see that under the same P_D, the increase of SNR_0 will reduce the required M. For example, under the condition of $P_D = 98\%$, our proposed scheme needs $M = 43$ when $SNR_0 = -5dB$, $M = 13$ when $SNR_0 = 0dB$, and $M = 6$ when $SNR_0 = 5dB$. This is because the effect of estimation error significantly decreases as the value of SNR_0 increases.

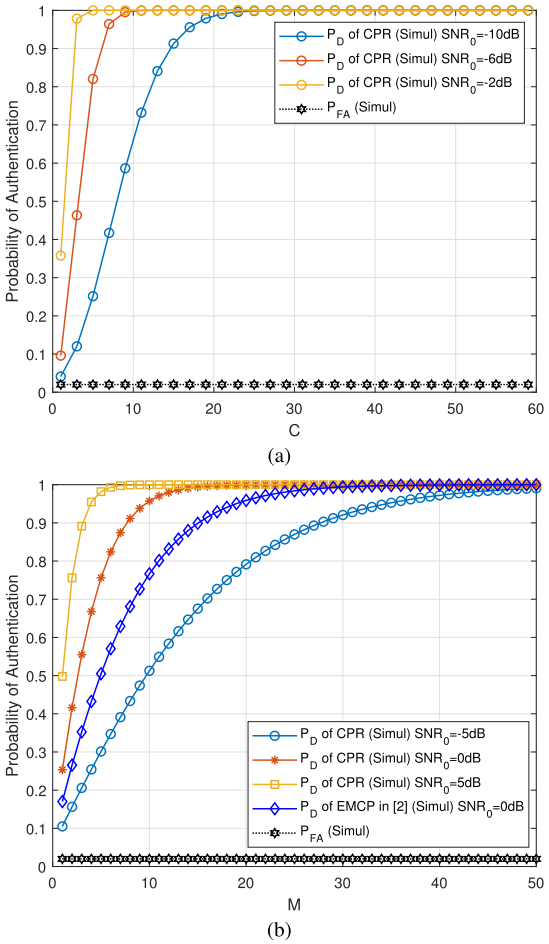


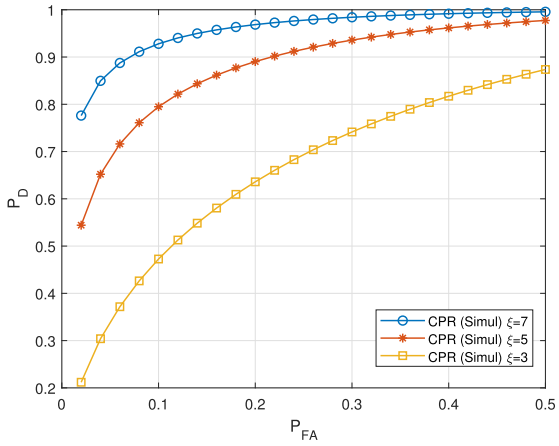
Fig. 8. Impact of C, M, and SNR_0 on (P_{FA}, P_D) of various schemes with $\alpha_A = \alpha_{EMCP} = \alpha_{FA} = \alpha_{PA} = 0.924, \epsilon = 0.02, d_A = d_E, \xi = 7.15$. (a) Impact of C and SNR_0 on (P_{FA}, P_D) with $M = 13$. (b) Impact of M and SNR_0 on (P_{FA}, P_D) with $C = 1$.

From Fig. 8(a) and (b), we can learn that when $SNR_0 = 0dB$ and $C = 1$, the P_D reaches saturation. This means when $SNR_0 \geq 0dB$, increase C cannot improve P_D. This is because $SNR_0 \geq 0dB$ is sufficient for accurate CPR estimation. However, when $SNR_0 \geq 0dB$, P_D can still increase with the increase of M. This is because the available CPR frequency attribute increases with the increase of M. Since compared with the increase of C, the increase of M will bring more COM increase. In practical applications, when the SNR_0 is small, we should first increase C to make the SNR_0 reach the SNR that can estimate CPR accurately. Generally, CPR can be estimated accurately when $SNR = 0dB$. Then, on the basis of this SNR, increase M to further improve authentication performance.

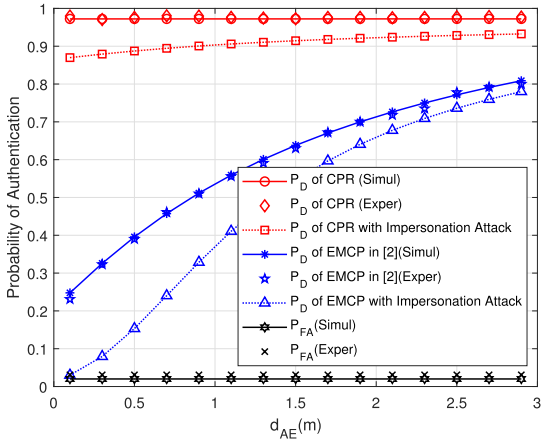
Under the sample rate of 30.72MHz, and the worst case (high-speed rail scenarios) with $V = 603km/h$, the maximum available N is 325. When $SNR_0 = -15dB$, we only need $N = 130$ to make $P_D = 98\%$ and $P_{FA} = 2\%$. Therefore, it is reasonable to analyze the impact of C and M separately, and we can always obtain the optimal C and M.

E. Impact of $\Delta\xi$

In Fig. 9, we analyze the impact of $\Delta\xi$ on the authentication performance of the proposed scheme. Since $\Delta\xi$ is effected by



(a)



(b)

Fig. 9. Impact of $\Delta\xi$ on (P_{FA}, P_D) of CPR scheme with the setting of $SNR_0 = -5dB, M = 13, C = 1, \epsilon = 0.02, \alpha_A = \alpha_{EMCP} = \alpha_{FA} = \alpha_{PA} = 0.924$. (a) ROC curves of CPR based scheme under different $\Delta\xi$ with $d_A = d_E$. (b) Impact of d_{AE} and impersonation attack on (P_{FA}, P_D) of various schemes with $\xi = 7.15$.

ξ, the distance between Alice and Eve, which is represented by d_{AE}, and the impersonation attack that Eve performed, i.e. Eve may modify its transmitting signal to make $\Delta\xi$ as small as possible [56]. Next, we will analyze the impact of $\Delta\xi$ from those three aspects.

In Fig. 9(a), we analyze the impact of polarization fading degree ξ on authentication performance with fixed position of transmitter and receiver. We can see that the performance of the proposed scheme improves with the increases of ξ. This is because $\Delta\xi$ increases with the increase of ξ. The larger ξ is, the greater CPR difference between Alice and Eve, and Bob can easily detect Eve. Therefore, when Alice, Eve, and Bob fixed, the proposed scheme can achieve better performance in channel with obvious polarization fading. Such as, non-line-of-sight (NLOS) Macrocell and NLOS Microcell.

In Fig. 9(b), we analyze the impact of d_{AE} and impersonation attack on authentication performance. We can see that the experimental results are basically consistent with the simulation and theoretical results, which verifies the effectiveness of the proposed scheme. We can also see that d_{AE} has little effect on the authentication performance of the proposed scheme when Eve do not modify its transmitting signal. Even

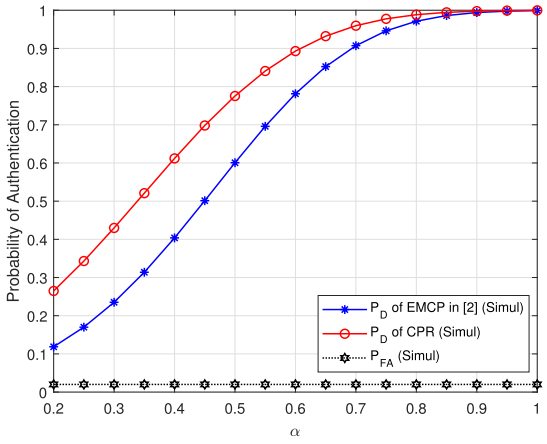


Fig. 10. Impact of α on (P_{FA}, P_D) of various schemes with the settings of $SNR_0 = 0dB, M = 13, C = 1, \epsilon = 0.02, d_A = d_E, \xi = 7.15$, $\Delta T = T_c = S_t$.

when $d_{AE} = 0$, we can still achieve $P_D = 98.7\%$, which proves that the proposed scheme can well solve the problem of co-located attacks. The reason for this is that the polarization state transmitted by Alice and Eve are different due to their different hardware deficiencies, and CPR is depended on the transmitted polarization state. Then, the CPRs of Alice and Eve are different, and Bob can distinguish Alice and Eve. While the authentication performance of the EMCP scheme declines with the decrease of d_{AE}. When $d_{AE} = 0$, P_D is less than 30%, which cannot be accepted by industry.

In Fig. 9(b), we can also see that the authentication performance of the CPR based scheme and the EMCP scheme decrease under impersonation attack. This is because Eve can modify its transmitting signal to make the CPR or CFR between Eve and Bob is similar to that of Alice and Bob, then Bob may identify Eve as Alice [56]. However, under the same d_{AE}, the performance degradation of CPR based scheme is smaller than that of EMCP scheme, and the CPR based scheme can better counter the impersonation attack. Even when $d_{AE} = 0$, i.e. there is a co-located attack, our propose scheme can still achieve $P_D = 88.7\%$. The reason is that the probability of Eve's successful attack is proportional to the correlation between the channel of Eve-Bob and that of Alice-Bob. The polarization dependence of CPR makes the correlation of CPR between different channels being less than CFR. Even if Eve and Alice are co-located, there are still large differences between the CPR of Eve-Bob and Alice-Bob. In addition, we can see that the performance difference between impersonation attack and without attack decreases with the increase of d_{AE}. This is because the correlation between the channel of Eve-Bob and that of Alice-Bob decreases with the increase of d_{AE} [57].

F. Impact of α

In Fig. 10, we demonstrate the impact of α on the authentication performance of various schemes. We can see that the performance of various schemes improves as α increases under a fixed ΔT. This is because the correlation of the same channel at adjacent intervals increases as α increases, then δ becomes

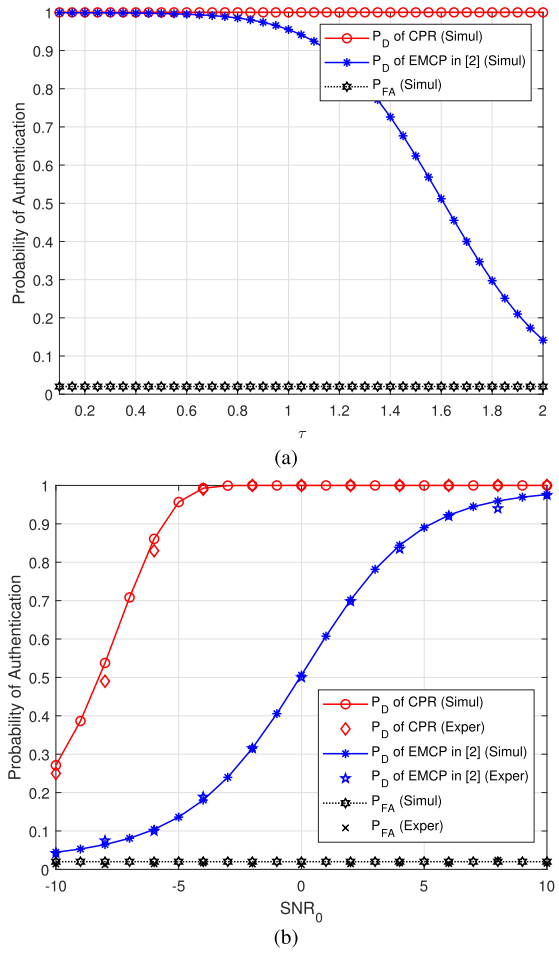


Fig. 11. Impact of τ on (P_{FA}, P_D) of various scheme with the settings of $SNR_0 = 0dB, M = 13, C = 1, \epsilon = 0.02, d_A = d_E, \xi = 7.15$. (a) Impact of τ on (P_{FA}, P_D) of various scheme. (b) (P_{FA}, P_D) of various schemes.

small, and Eve can be easily detected. Therefore, in order to achieve high authentication performance, ΔT needs to be adjusted according to the channel coherence time to ensure that large α can always be obtained, which will be discussed in the next subsection. In addition, under the same α, the proposed scheme can achieve higher authentication accuracy. This is because CPR is more sensitive to change of channel, and the difference between various channels is more significant.

G. Impact of τ

In Fig. 11, we demonstrate the impact of τ on the authentication performance of various schemes.

In Fig. 11(a), we can see that the P_D of our proposed based scheme remains unchanged with the increase of τ. This is because CPR can be estimated continuously, and the authentication interval can be adaptively adjusted according to the channel coherence time. The P_D of the EMCP scheme rapidly declines as τ increases. The reason is that the estimation interval of CFR is equal to the pilot period, when $T_c < \Delta T$, where $\Delta T = S_t$, that is, $\tau \geq 1$, CFRs at adjacent interval are weakly correlated or even independent of each other. Although the computational complexity of our proposed scheme also increases with the increase of τ, the increased computation can be accepted by engineering practices.

In Fig. 11(b), we can see that the experimental results are basically consistent with the simulation and theoretical results, which verifies the effectiveness of the proposed scheme. We can also see that, the authentication performance of our proposed scheme can still achieve the same performance as Fig. 7 with $C = 1$, while the EMCP scheme has a significant performance degradation compared with Fig. 7 with $C = 1$. This is because our proposed scheme can adjust ΔT according to T_c, whereas ΔT of the EMCP scheme is fixed as S_t. Then, $\alpha_{FA} = \alpha_{PA} = 0.924$ can also be obtain, whereas α_{EMCP} is only 0.415 under experiment.

VI. Conclusion

We propose a novel physical authentication scheme based on CPR. It can be applied to any rich scattering scenarios, including high dynamic scenarios, and can still achieve high authentication accuracy under ultra-low SNR. Besides, we skillfully solve the co-located attacks problem. We theoretically derive the false alarm probability, detection probability, optimal threshold, computation complexity, optimal stacking numbers, and optimal authentication points of the proposed scheme. In addition, through extensive simulations and experiments, we get that the authentication performance of CPR based scheme is better than that of CFR based scheme, also our proposed scheme can still achieve good authentication performance in high dynamic scenarios and ultra-low SNR, and can distinguish Alice and Eve even they are located at the same position. In the future, we will further study the authentication scheme in massive MIMO systems. How to counter Eve's various attacks is also the focus of our future research.

Acknowledgment

The authors would like to thank Dr. Yue Wang from the Department of Electrical and Computer Engineering, George Mason University, for his constructive comments and helpful suggestions.

References

[1] D. Chen et al., "An LDPC code based physical layer message authentication scheme with prefect security," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 748–761, Apr. 2018.

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

[3] A. C. Polak, C. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, Aug. 2011.

[4] Y.-F. Wang and J.-H. Lee, "A simple phase noise suppression scheme for massive MIMO uplink systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4769–4780, Jun. 2017.

[5] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Trans. Mobile Comput.*, vol. 9, no. 3, pp. 449–462, Mar. 2010.

[6] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 2014.

[7] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[8] A. Kalamandeen, A. Scannell, E. De Lara, A. Sheth, and A. LaMarca, "Ensemble: Cooperative proximity-based authentication," in *Proc. 8th Int. Conf. Mobile Syst., Appl., Services*, Jun. 2010, pp. 331–344.

[9] Q. Wang, "A novel physical layer assisted authentication scheme for mobile wireless sensor networks," *Sensors*, vol. 17, no. 2, p. 289, Feb. 2017.

[10] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[11] J. K. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proc. 2nd Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2010, pp. 1–9.

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

[13] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. Mil. Commun. Conf. (MILCOM)*, Nov. 2011, pp. 538–542.

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

[15] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, Jun. 2016.

[16] P. Zhang, Y. Shen, X. Jiang, and B. Wu, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2446–2458, Apr. 2020.

[17] P. Zhang, J. Liu, Y. Shen, and X. Jiang, "Exploiting channel gain and phase noise for PHY-layer authentication in massive MIMO systems," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4265–4279, 2021.

[18] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 4646–4651.

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

[20] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," in *Proc. 42nd Annu. Conf. Inf. Sci. Syst.*, Mar. 2008, pp. 642–646.

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

[22] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948–5956, Dec. 2009.

[23] F. He, H. Man, D. Kivanc, and B. McNair, "EPSON: Enhanced physical security in OFDM networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.

[24] F. He, W. Wang, and H. Man, "REAM: RAKE receiver enhanced authentication method," in *Proc. Mil. Commun. Conf. (MILCOM)*, Nov. 2010, pp. 2205–2210.

[25] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676–1687, Mar. 2017.

[26] T. M. Hoang, T. Van Chien, T. van Luong, S. Chatzinotas, B. Ottersten, and L. Hanzo, "Detection of spoofing attacks in aeronautical ad-hoc networks using deep autoencoders," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1010–1023, 2022.

[27] F. Pan et al., "Threshold-free physical layer authentication based on machine learning for industrial wireless CPS," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6481–6491, Dec. 2019.

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

[29] H. Fang, X. Wang, and L. Xu, "Fuzzy learning for multi-dimensional adaptive physical layer authentication: A compact and robust approach," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5420–5432, Aug. 2020.

[30] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

[31] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 282–310, 1st Quart., 2021.

[32] J. R. Huynen, "Phenomenological theory of radar targets," Tech. Rep., 1970.

[33] D. Wei, L. Liang, M. Zhang, R. Qiao, and W. Huang, "A polarization state modulation based physical layer security scheme for wireless communications," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2016, pp. 1195–1201.

[34] J. Xu, D. Wei, and W. Huang, "Polarization fingerprint: A novel physical-layer authentication in wireless IoT," in *Proc. IEEE 23rd Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2022, pp. 434–443.

[35] W.-M. Boerner and H. Überall, *Radar Target Imaging*, vol. 13. Springer, 2012.

[36] S. Gong, C. Xing, S. Chen, and Z. Fei, "Polarization sensitive array based physical-layer security," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 3964–3981, May 2018.

[37] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[38] M. M. U. Rahman, Q. H. Abbasi, N. Chopra, K. Qaraqe, and A. Alomainy, "Physical layer authentication in Nano networks at terahertz frequencies for biomedical applications," *IEEE Access*, vol. 5, pp. 7808–7815, 2017.

[39] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 359–371, Apr. 2012.

[40] C. Oestges, B. Clerckx, M. Guillaud, and M. Debbah, "Dual-polarized wireless communications: From propagation models to system performance evaluation," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 4019–4031, Oct. 2008.

[41] V. N. Bringi, T. A. Seliga, and S. M. Cherry, "Statistical properties of the dual-polarization differential reflectivity (ZDR) radar signal," *IEEE Trans. Geosci. Remote Sens.*, vol. GE-21, no. 2, pp. 215–220, Apr. 1983.

[42] S. Kozono, T. Tsuruhara, and M. Sakamoto, "Base station polarization diversity reception for mobile radio," *IEEE Trans. Veh. Technol.*, vol. VT-33, no. 4, pp. 301–306, Nov. 1984.

[43] J.-S. Lee, K. W. Hoppel, S. A. Mango, and A. R. Miller, "Intensity and phase statistics of multilook polarimetric and interferometric SAR imagery," *IEEE Trans. Geosci. Remote Sens.*, vol. 32, no. 5, pp. 1017–1028, Sep. 1994.

[44] C. Polprasert and J. A. Ritcey, "Phase difference statistics for Nakagami-*m* fading channels," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process. (PACRIM)*, Aug. 2005, pp. 593–596.

[45] A. Castaño-Martínez and F. López-Blázquez, "Distribution of a sum of weighted noncentral chi-square variables," *Test*, vol. 14, no. 2, pp. 397–415, 2005.

[46] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2014.

[47] W. Jouini, D. Le Guennec, C. Moy, and J. Palicot, "Log-normal approximation of chi-square distributions for signal processing," in *Proc. 30th URSI Gen. Assem. Sci. Symp.*, Aug. 2011, pp. 1–4.

[48] X. Li, "A novel accurate approximation method of lognormal sum random variables," Ph.D. dissertation, Wright State Univ., Dayton, OH, USA, 2008.

[49] C. L. J. Lam and T. Le-Ngoc, "Log-shifted gamma approximation to lognormal sum distributions," *IEEE Trans. Veh. Technol.*, vol. 56, no. 4, pp. 2121–2129, Jul. 2007.

[50] R. Bhagavatula, C. Oestges, and R. W. Heath, "A new double-directional channel model including antenna patterns, array orientation, and depolarization," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2219–2231, Jun. 2010.

[51] J. J. A. Lempiainen and J. K. Laiho-Steffens, "The performance of polarization diversity schemes at a base station in small/micro cells at 1800 MHz," *IEEE Trans. Veh. Technol.*, vol. 47, no. 3, pp. 1087–1092, Aug. 1998.

[52] F. Lotse, J.-E. Berg, U. Forssen, and P. Idahl, "Base station polarization diversity reception in macrocellular systems at 1800 MHz," in *Proc. Veh. Technol. Conf. (VTC)*, vol. 3, 1996, pp. 1643–1646.

[53] *IEEE Standard for Local and Metropolitan Area Networks*, IEEE Standard 802.16e–2005 IEEE Standard 802.16-2004/Cor 1–2005 (Amendment Corrigendum to IEEE Standard 802.16–2004), 2006.

[54] T. S. Rappaport, K. Blankenship, and H. Xu, "Propagation and radio system design issues in mobile radio systems for the GloMo project," Virginia Polytech. Inst. State Univ., Blacksburg, VA, USA, Tech. Rep., 1997.
[55] K. Matsuoka, A. Collina, C. Somaschini, and M. Sogabe, "Influence of local deck vibrations on the evaluation of the maximum acceleration of a steel-concrete composite bridge for a high-speed railway," *Eng. Struct.*, vol. 200, Dec. 2019, Art. no. 109736.
[56] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.
[57] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-free massive MIMO versus small cells," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1834–1850, Jan. 2017.

Yuemei Wu (Student Member, IEEE) received the B.S. degree in electronic science and technology from the Beijing University of Chemical Technology, Beijing, China, in 2019. She is currently pursuing the Ph.D. degree with the Institute of Information Engineering, Chinese Academy of Sciences. Her current research interests include wireless communications and physical layer security.

Dong Wei received the Ph.D. degree in computer architecture from the Beijing University of Posts and Telecommunications, Beijing, China, in 2013. He is currently a Researcher and a Master's Tutor with the Institute of Information Engineering, Chinese Academy of Sciences. His research interests include wireless communication security and wireless signal processing.

Caili Guo (Senior Member, IEEE) received the Ph.D. degree in communication and information systems from the Beijing University of Posts and Telecommunications (BUPT) in 2008. She is currently a Professor with the School of Information and Communication Engineering, BUPT. Her research interests include machine learning and statistical signal processing for wireless communications. In these related areas, she has published over 200 papers and holds over 30 granted patents. She won Diamond Best Paper Award of IEEE ICME 2018 and Best Paper Award of IEEE WCNC 2021.

Weiqing Huang received the M.S. degree in communication and information systems from the Beijing University of Posts and Telecommunications (BUPT) in 2002. He is currently a Senior Engineer with the Institute of Information Engineering, Chinese Academy of Sciences. His research interests include electromagnetic leakage emission detection, wireless communication security, and electromagnetic information security.