Wireless Communications and Mobile Computing

Next-Generation Wireless Networks Communication Sustainability, Efficiency, and Security from a Physical Layer Perspective

Lead Guest Editor: Jia Liu
Guest Editors: Zhao Li, Yang Xu, Xiaoying Liu, and Kechen Zheng

Next-Generation Wireless Networks Communication Sustainability, Efficiency, and Security from a Physical Layer Perspective

Wireless Communications and Mobile Computing

Next-Generation Wireless Networks Communication Sustainability, Efficiency, and Security from a Physical Layer Perspective

Lead Guest Editor: Jia Liu
Guest Editors: Zhao Li, Yang Xu, Xiaoying Liu, and Kechen Zheng

Chief Editor

Associate Editors

Academic Editors

Contents

Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 3178335, 14 pages
https://doi.org/10.1155/2023/3178335

WILEY | Hindawi

Research Article

Analysis of Eavesdropping Region in Hybrid mmWave-Microwave Wireless Systems

Qianyue Qu,[1] **Yuanyu Zhang**,[2,3] **and Shoji Kasahara**[1]

[1]*Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma, Japan*
[2]*School of Computer Science and Technology, Xidian University, Xi'an, China*
[3]*Shannxi Key Laboratory of Network and System Security, Beijing Sunwise Information Technology Ltd, Beijing, China*

Correspondence should be addressed to Yuanyu Zhang; yyuzhang@xidian.edu.cn

Received 5 January 2023; Revised 24 April 2023; Accepted 31 May 2023; Published 2 September 2023

Academic Editor: Kechen Zheng

Hybrid communication systems, where millimeter-wave (mmWave) links coexist with microwave links, have been an essential component in the fifth-generation (5G) wireless networks. Nevertheless, the open feature of the wireless medium makes hybrid systems vulnerable to eavesdropping attacks. Eavesdroppers in hybrid communication systems can enhance their attack performance by opportunistically eavesdropping on mmWave or microwave links. This paper, therefore, aims to answer a natural question: in which region do eavesdroppers prefer the mmWave links? To this end, we first formulate this question as an eavesdropping region characterization problem from the physical layer security perspective, where eavesdroppers select the link to eavesdrop based on the ratio between the security performances of the mmWave and microwave links. To model the security performances of both the mmWave and microwave links, we derive closed-form expressions for the secrecy outage probabilities and lower bounds/exact expressions for the secrecy rates of both links. Finally, we provide numerical results to validate our theoretical analysis and also illustrate the mmWave eavesdropping region under various network parameter settings.

1. Introduction

In the past decade, the number of wireless devices is increasing exponentially, leading to a critical spectrum scarcity issue in current wireless communication systems. One of the promising solutions is to transmit information over the much wider millimeter-wave (mmWave) frequency band for significantly improved capacity and increased data rate in the fifth-generation (5G) wireless networks [1, 2]. Despite the great capacity and high data rate, mmWave communication suffers from high signal attenuation when mmWave signals encounter obstacles [3]. In this case, users may choose to transmit over conventional microwave links. Therefore, hybrid wireless communication systems, where the mmWave links coexist with microwave links, are expected to be a typical component in the ongoing 5G era [4].

However, due to the open nature of the wireless medium, hybrid communication systems are also vulnerable to eavesdropping attacks like other wireless systems [5–7]. Recent research has shown that the emerging physical layer security (PLS) technology can achieve a stronger form of security with less computational cost [8, 9]. The key idea of the PLS technology is to exploit physical layer characteristics of wireless channels (e.g., fading and noise) to ensure that almost no information is leaked to eavesdroppers [10]. Moreover, the PLS technology can be combined with existing cryptographic methods to provide a critical security solution that can combat eavesdropping attacks [11, 12].

Motivated by the benefits of the PLS technology, extensive research efforts have been devoted to the PLS performance analysis and/or PLS scheme design in wireless communication systems [13–23]. For instance, Zhu et al. [15] explored the potential of PLS in mmWave ad hoc networks. Zhang et al. [16] proposed a sight-based cooperative jamming scheme to improve the PLS performance of mmWave ad hoc networks. Zhang et al. [17] examined the problem of mode selection and spectrum partition in cellular networks with inband device-to-device communication. Some authors analyzed the PLS performance of nonorthogonal multiple access networks [18]. In addition, some researchers discussed

the joint resource allocation of artificial noise-assisted multiuser wiretap orthogonal frequency division multiplexing channel [20]. The optimization problem of wireless communication systems with intelligent reflecting surfaces was addressed by Chen et al. [21], Makarfi et al. [22], Shen et al. [23].

Recently, the PLS performance analysis of hybrid wireless communication systems has also attracted considerable attention [24–29]. Tokgoz et al. [24] investigated the hybrid free-space optical (FSO) and mmWave wireless system from the perspective of PLS, and different fading channels were considered for FSO and mmWave links, respectively. Vuppala et al. [25, 26] analyzed the performance of mmWave-overlaid microwave cellular networks. They developed a mathematical framework to analyze the connection outage probability, secrecy outage probability (SOP), and achievable secrecy rate of the hybrid mmWave network. Umer et al. [27] proposed a tractable method using stochastic geometry to analyze the SOP and secrecy energy efficiency of a hybrid heterogeneous network (HetNet). They also explored the PLS performance of the hybrid HetNet, where mmWave links coexist with sub-6 GHz (microwave) links. Wang et al. [28] first proposed a secure mobile association policy based on an access threshold and then investigated the connection probability and security probability of a randomly located user based on the proposed policy. The results showed that introducing an appropriate access threshold can significantly improve the security throughput performance of heterogeneous cellular networks. Wang et al. [29] studied the PLS of two-tier HetNets with sub-6 GHz massive multi-input multioutput macrocells and mmWave small cells. In contrast to previous studies, the eavesdroppers of this paper sent pilot signals during the channel training phase to improve the quality of the intercepted signals.

The previous studies investigated the security performance of legitimate transmitters but did not consider the possible behavior of eavesdroppers. Eavesdroppers in hybrid systems behave differently than eavesdroppers in systems with only one link type (i.e., mmWave link or microwave link). They can improve their eavesdropping performance by opportunistically selecting the wave (i.e., mmWave or microwave) to eavesdrop on. For example, eavesdroppers may prefer to eavesdrop on mmWave links when they have better connections to mmWave transmitters than microwave transmitters.

Motivated by the above finding, this paper aims to answer a natural question in hybrid communication systems: in which region do eavesdroppers prefer the mmWave links? Specifically, this paper considers a hybrid communication system with a mmWave communication pair, a microwave communication pair, and an eavesdropper. We focus on characterizing the region where the eavesdropper prefers to eavesdrop on the mmWave link. We first formulate an eavesdropping region characterization problem, where the eavesdropper selects the link to eavesdrop based on the ratio between the security performance of the mmWave and microwave links. To model the security performance of mmWave and microwave links, we derive a closed-form expression for the SOP and lower bound/exact expressions for the secrecy rate of both links. Finally, we provide numerical results to validate our theoretical analysis and also illustrate the millimeter-wave eavesdropping region under various network parameter settings. A preliminary version of this paper can be found by Qu et al. [30], which only focuses on the SOP performance.

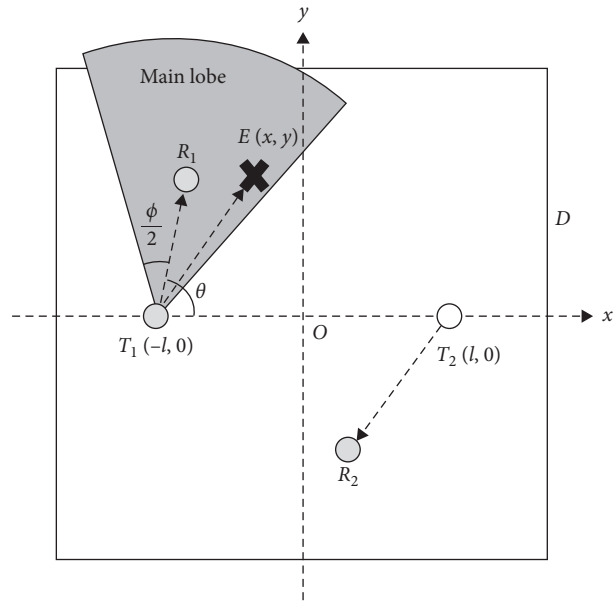


FIGURE 1: System model: one mmWave transmission pair $T_1(-l, 0) \longrightarrow R_1(x_1, y_1)$, one microwave transmission pair $T_2(l, 0) \longrightarrow R_2(x_2, y_2)$, and one eavesdropper $E(x, y)$.

The rest of the paper is structured as follows. Section 2 presents the preliminaries, including the system model and wave selection scheme. In Section 3, we derive the SOPs and secrecy rates of the mmWave link and microwave link and characterize the mmWave eavesdropping regions. We formulate the optimization problem to find the optimal eavesdropping locations in Section 4. Section 5 presents numerical results to validate our theoretical analysis and reveal our findings. Finally, we conclude the paper in Section 6.

2. Preliminaries

In this section, we introduce the preliminaries of this paper, including the system model, antenna model, and blockage and propagation models. In addition, we present the metrics used in this paper and the wave selection scheme of the eavesdropper.

2.1. System Model. Figure 1 shows the system model of this paper, and we consider a square network model with the side length D, which consists of one mmWave transmission pair $T_1 \longrightarrow R_1$, one microwave transmission pair $T_2 \longrightarrow R_2$, and one eavesdropper E which can wiretap on mmWave or microwave link, respectively. We assume the distance between T_1 and T_2 is $2l$ and construct a coordinate system with the origin at the middle point between them. Thus, the coordinate of T_1 and T_2 are $(-l, 0)$ and $(l, 0)$, respectively. In addition, we define the coordinate of R_1 by (x_1, y_1), the coordinate of R_2 by (x_2, y_2), the coordinate of E by (x, y). As shown in Figure 1, the angle between $\overrightarrow{T_1R_1}$ and the x-axis

is defined by θ. Note that we use $d_{i,j}$ to denote the distance between nodes i and j.

2.2. Antenna Model. To approximate the antenna patterns of mmWave transmitter T_1, we adopt the sectored antenna model by Bai and Heath [31] and Thornburg et al. [32], where the antenna of T_1 consists of a main lobe and a back lobe. We use ϕ, A_m, and a_m ($A_m > a_m$) to define the beam width of the main lobe, the main lobe gain, and back lobe gain, respectively. We assume that to obtain the maximum antenna gain, T_1 and T_2 have guided their antennas correctly so that $\overrightarrow{T_1R_1}$ coincides with the aperture of the antenna. Unlike T_1, the microwave transmitter T_2 uses an omnidirectional antenna with an antenna gain of A_u.

To simplify the analysis, we assume that the eavesdropper E uses an omnidirectional antenna with antenna gain of A_E. Note that the effective channel gain G between T_1 and E depends on the location of E. When E is within the main lobe of the antenna of T, G is A_mA_E. Otherwise, G is a_mA_E. We need to compare the angle of $\overrightarrow{T_1R_1}$ with x-axis and the angle between x-axis and $\overrightarrow{T_1E}$ to determine whether E is inside the main lobe of T_1's antenna.

Based on the locations of T_1 and E as well as the angle θ, we have $\overrightarrow{T_1E} = (x + \ell, y)$ and $\overrightarrow{T_1R_1} = (r_0 \cos\theta, r_0 \sin\theta)$, where r_0 denotes the distance between T_1 and R_1. Thus, the angle between $\overrightarrow{T_1R_1}$ and $\overrightarrow{T_1E}$ can given by the following:

$$\vartheta(x, y) = \arccos\left(\frac{(x + \ell)\cos\theta + y \sin\theta}{\sqrt{(x + \ell)^2 + y^2}}\right). \tag{1}$$

If and only if $\vartheta(x, y)$ is smaller than or equal to half of the beamwidth of the main lobe, i.e., $\phi/2$, E is inside the main lobe of T's antenna. Formally, we can give the effective channel gain $\mathcal{G}$ between T_1 and E by the following:

$$G(x, y) = \begin{cases} A_mA_E, & \vartheta(x, y) \le \phi/2, \\ a_mA_E, & \text{otherwise.} \end{cases} \tag{2}$$

2.3. Blockage and Propagation Model. To describe the blockage effect, we use an exponential line-of-sight (LoS) model, where a mmWave link of length r is LoS with a probability

$$p_L(r) = e^{-\beta r}, \tag{3}$$

and is NLoS with probability

$$p_N(r) = 1 - p_L(r), \tag{4}$$

where β represents the blockage density [33]. The blockage effect results in different path losses for LoS and NLoS links, where the exponents are denoted by α_L and α_N, respectively.

In addition, mmWave links are subject to multipath fading, which we characterize with the Nakagami-m fading model. Note that in this paper, we only consider the case where the link $T_1 \longrightarrow R_1$ of the mmWave link transmits information only when the link is LoS. Thus the channel gain of the legitimate channel follows a gamma distribution $\Gamma(N_L, N_L)$ with shape N_L and rate N_L. In contrast, two cases exist for the eavesdropping channel $T_1 \longrightarrow E$. When the link is LoS, it follows a gamma distribution $\Gamma(N_L, N_L)$ with shape N_L and rate N_L, and when the link is NLoS, it follows a gamma distribution $\Gamma(N_N, N_N)$ with shape N_N and rate N_N. Typically, $N_L > N_N$ holds. We use h_{T_1,R_1} to denote the channel gain of the $T_1 \longrightarrow R_1$ link, and $h^L_{T_1,E}$ (resp. $h^N_{T_1,E}$) to denote the channel gain of the $T_1 \longrightarrow E$ link under LoS (resp. NLoS). Thus, the probability density function (PDF) of h_{T_1,R_1} is given by the following:

$$f_{h_{T_1,R_1}}(x) = \frac{N_L^{N_L} x^{N_L - 1} e^{-N_L x}}{\Gamma(N_L)}, \tag{5}$$

and the PDF of $h^b_{T_1,E}$ ($b = L, N$) is given by the following:

$$f_{h^b_{T_1,E}}(x) = \frac{N_b^{N_b} x^{N_b - 1} e^{-N_b x}}{\Gamma(N_b)}, \tag{6}$$

where $\Gamma(\cdot)$ is the gamma function.

To describe the fading effect of microwave links, we use a quasi-static Rayleigh fading model. Thus, the legitimate channel gain h_{T_2,R_2} of the link $T_2 \longrightarrow R_2$ and the eavesdropping channel gain $h_{T_2,E}$ of the link $T_2 \longrightarrow E$ follow the exponential distribution with unit mean, e.g., $h_{T_2,E} \sim \text{Exp}(1)$. In addition, the links of $T_2 \longrightarrow R_2$ and $T_2 \longrightarrow E$ are also impaired by the large-scale path loss. We use α_u to denote the path loss of microwave links.

2.4. Metrics. To measure the secrecy performance of the network, we adopt the commonly-used SOP and secrecy rate as the metrics. Note that SOP represents the probability that E succeeds in decoding the transmitted signals. The secrecy rate denotes the difference between the rate of the main communication channel and the rate of the eavesdropping channel.

We use ε_m and ε_u to denote the minimum required signal-to-noise ratios (SNRs) for decoding the signals from T_1 and T_2, respectively. Formally, the SOP when E eavesdropps on the mmWave (i.e., transmitter T_1) is formulated as follows:

$$p^m_{\text{so}} = \mathbb{P}\left(\text{SNR}_{T_1,E} > \varepsilon_m\right), \tag{7}$$

and that when E eavesdropps on the microwave (i.e., transmitter T_2) is formulated as follows:

$$p^u_{\text{so}} = \mathbb{P}\left(\text{SNR}_{T_2,E} > \varepsilon_u\right). \tag{8}$$

According to Barros and Rodrigues [34], Bloch et al. [35], Geraci et al. [36], Ozan Koyluoglu et al. [37], the secrecy rate of mmWave link is formulated as follows:

$$R_s = \left[\log_2\left(1 + \mathrm{SNR}_{T_1,R_1}\right) - \log_2\left(1 + \mathrm{SNR}_{T_1,E}\right)\right]^+, \quad (9)$$

and the secrecy rate of the microwave link is formulated as follows:

$$R_s^u = \left[\log_2\left(1 + \mathrm{SNR}_{T_2,R_2}\right) - \log_2\left(1 + \mathrm{SNR}_{T_2,E}\right)\right]^+, \quad (10)$$

where $[x]^+ = \max\{x, 0\}$.

2.5. Eavesdropping Wave Selection. Based on the SOPs, E chooses between eavesdropping on the mmWave and eavesdropping on the microwave wave. We assume that E uses the ratio between Equations (7) and (8) as the selection criterion and conducts the selection according to the following rule:

(i) If $p_{\mathrm{so}}^m / p_{\mathrm{so}}^u \geq \rho_{\mathrm{sop}}$, E eavesdrops on the mmWave;
(ii) Otherwise, E eavesdrops on the microwave.

Similarly, E chooses to eavesdrop on mmWave links or microwave links, depending on the secrecy rate. We propose to utilize the ratio between Equations (9) and (10) as the selection criterion and develop the selection scheme of eavesdroppers according to the following rules:

(i) If $R_s^u / R_s \geq \rho_{sr}$, E eavesdrops on the mmWave link;
(ii) Otherwise, E eavesdrops on the microwave link.

Here, the parameter ρ_{sop} and ρ_{sr} represent the preference of E. If $\rho_{\mathrm{sop}}\ (\mathrm{resp.}\ \rho_{sr}) = 1$, E treats eavesdropping on the mmWave links and eavesdropping on microwave links as equally important. If $\rho_{\mathrm{sop}}(\mathrm{resp.}\ \rho_{sr}) < 1$, E prefers to eavesdrop on the mmWave links rather than the microwave links, and vice versa.

3. Eavesdropping Region Characterization Modeling

In this section, we characterize the mmWave eavesdropping regions of the eavesdropper, for which we formulate the eavesdropping regions in Section 3.1, derive the SOP p_{so}^m and p_{so}^u in Section 3.2, and derive the average achievable secrecy rate R_s and R_s^u in Section 3.3, respectively.

3.1. Problem Formulation. In this section, we will formulate the eavesdropping regions characterized by SOPs and secrecy rates, respectively.

3.1.1. Eavesdropping Region Characterized by SOP. Note that both p_{so}^m and p_{so}^u vary with the location of E. Thus, the eavesdropping wave of E, i.e., the wave on which E eavesdrops, varies with its location. Therefore, this paper aims to characterize the eavesdropping region, i.e., the *mmWave eavesdropping region* where E eavesdrops on the mmWave based on the proposed wave selection scheme in Section 2.5. We use $\mathscr{R}_m$ to denote the mmWave eavesdropping regions characterized by SOPs, which can be given by the following:

$$\mathscr{R}_m = \left\{(x, y) : p_{\mathrm{so}}^m(x, y) / p_{\mathrm{so}}^u(x, y) \geq \rho_{\mathrm{sop}}\right\}. \quad (11)$$

We can see that, to determine the mmWave eavesdropping region $\mathscr{R}_m$, we need to derive the SOPs $p_{\mathrm{so}}^m(x, y)$ and $p_{\mathrm{so}}^u(x, y)$ when E is located in an arbitrary location (x, y).

3.1.2. Eavesdropping Region Characterized by Secrecy Rate. Similar to SOPs, both R_s and R_s^u vary with the location of E. Therefore, the wave that E chooses to eavesdrop on varies with its location. Thus, we also use the secrecy rates to characterize the mmWave eavesdropping region. We use $\mathscr{M}_m$ to denote the mmWave eavesdropping regions characterized by secrecy rates, which can be given by the following:

$$\mathscr{M}_m = \left\{(x, y) : R_s^u(x, y) / R_s(x, y) \geq \rho_{sr}\right\}. \quad (12)$$

It is easy to see that we need to derive the secrecy rate R_s and R_s^u to determine the mmWave eavesdropping region $\mathscr{M}_m$.

3.2. SOP Analysis. In this section, we derive the expression of the SOPs $p_{\mathrm{so}}^m(x, y)$ and $p_{\mathrm{so}}^u(x, y)$ to determine the regions $\mathscr{R}_m$. With the help of the SOPs, we show the mmWave eavesdropping regions characterized by SOPs in Section 5.

3.2.1. SOP of mmWave Link. According to Equation (7), to derive the SOP, we first need to determine the $\mathrm{SNR}_{T_1,E}$. Note that $\mathrm{SNR}_{T_1,E}$ varies depending on whether the link $T_1 \longrightarrow E$ is LoS or NLoS. We use $\mathrm{SNR}_{T_1,E}^L$ (resp. $\mathrm{SNR}_{T_1,E}^N$) to denote the SNR when the link is LoS (resp. NLoS). $\mathrm{SNR}_{T_1,E}^L$ and $\mathrm{SNR}_{T_1,E}^N$ can be given by the followings:

$$\mathrm{SNR}_{T_1,E}^L = \frac{P_m G(x, y) h_{T_1,E}^L d_{T_1,E}^{-\alpha_L}}{\sigma^2}, \quad (13)$$

and

$$\mathrm{SNR}_{T_1,E}^N = \frac{P_m G(x, y) h_{T_1,E}^N d_{T_1,E}^{-\alpha_N}}{\sigma^2}, \quad (14)$$

where P_m represents the transmit power of T_1, $d_{T_1,E}$ denotes the distance between T_1 and E, and σ^2 is the noise power.

Theorem 1. *The SOP $p_{\mathrm{so}}^m(x, y)$ when E eavesdrops on the mmWave link is as follows:*

$$p_{so}^m(x, y) = 1 - e^{-\beta d_{T_1,E}} \frac{\gamma\left(N_L, \frac{N_L \varepsilon_m d_{T_1,E}^{\alpha_L} \sigma^2}{P_m G(x,y)}\right)}{\Gamma(N_L)} - \left(1 - e^{-\beta d_{T_1,E}}\right) \frac{\gamma\left(N_N, \frac{N_N \varepsilon_m d_{T_1,E}^{\alpha_N} \sigma^2}{P_m G(x,y)}\right)}{\Gamma(N_N)}, \quad (15)$$

where $d_{T_1,E} = \sqrt{(x + \ell)^2 + y^2}$ and $\gamma(\cdot,\cdot)$ is the lower incomplete gamma function.

Proof. Applying the law of total probability, we have the following:

$$p_{so}^{m} = p_L(d_{T_1,E}) \underbrace{\mathbb{P}\left(\mathrm{SNR}_{T_1,E}^{L} > \varepsilon_m\right)}_{Q_L} + p_N(d_{T_1,E}) \underbrace{\mathbb{P}\left(\mathrm{SNR}_{T_1,E}^{N} > \varepsilon_m\right)}_{Q_N}. \tag{16}$$

Next, we derive Q_L and Q_N. Applying the PDF of gamma random variables, we have the following:

$$\begin{aligned} Q_L &= \mathbb{P}\left(\frac{P_m G(x,y) h_{T_1,E}^{L} d_{T_1,E}^{-\alpha_L}}{\sigma^2} > \varepsilon_m\right) \\ &= \mathbb{P}\left(h_{T_1,E}^{L} > \frac{\varepsilon_m d_{T_1,E}^{\alpha_L} \sigma^2}{P_m G(x,y)}\right) \\ &= 1 - \frac{\gamma\left(N_L, \frac{N_L \varepsilon_m d_{T_1,E}^{\alpha_L} \sigma^2}{P_m G(x,y)}\right)}{\Gamma(N_L)}. \end{aligned} \tag{17}$$

Similarly, we have the following:

$$Q_N = 1 - \frac{\gamma\left(N_N, \frac{N_N \varepsilon_m d_{T_1,E}^{\alpha_N} \sigma^2}{P_m G(x,y)}\right)}{\Gamma(N_N)}. \tag{18}$$

Substituting $p_L\left(d_{T_1,E}\right) = e^{-\beta d_{T_1,E}}$, Equations (17) and (18) into Equation (16) completes the proof. □

3.2.2. SOP of Microwave Link. Likewise, to derive the SOP in this case, we need to determine the SNR $\mathrm{SNR}_{T_2,E}$, which is given by the following:

$$\mathrm{SNR}_{T_2,E} = \frac{P_u A_u A_E h_{T_2,E} d_{T_2,E}^{-\alpha_u}}{\sigma^2}, \tag{19}$$

where $d_{T_2,E}$ is the distance between T_2 and E. Based on $\mathrm{SNR}_{T_2,E}$, we derive the SOP in the following theorem.

Theorem 2. *The SOP $p_{\mathrm{so}}^{u}(x,y)$ when E eavesdrops on the microwave link is as follows:*

$$p_{\mathrm{so}}^{u}(x,y) = \exp\left(-\frac{\varepsilon_u\left((x-\ell)^2 + y^2\right)^{\frac{\alpha_u}{2}} \sigma^2}{P_u A_u A_E}\right). \tag{20}$$

Proof. Following the definition of SOP, we have the following:

$$\begin{aligned} p_{so}^{u}(x,y) &= \mathbb{P}\left(\mathrm{SNR}_{T_2,E} > \varepsilon_u\right) \\ &= \mathbb{P}\left(\frac{P_u A_u A_E h_{T_2,E} d_{T_2,E}^{-\alpha_u}}{\sigma^2} > \varepsilon_u\right) \\ &= \mathbb{P}\left(h_{T_2,E} > \frac{\varepsilon_u d_{T_2,E}^{\alpha_u} \sigma^2}{P_u A_u A_E}\right) \\ &= e^{-\frac{\varepsilon_u d_{T_2,E}^{\alpha_u} \sigma^2}{P_u A_u A_E}}. \end{aligned} \tag{21}$$

Substituting $d_{T_2,E} = \sqrt{(x-\ell)^2 + y^2}$ in Equation (21) completes the proof. □

Using the SOPs in Theorems 1 and 2, we can determine the mmWave eavesdropping region $\mathscr{R}_m$ based on the definition in Equation (11).

3.3. Secrecy Rate Analysis. In this section, we show the derivation steps of the secrecy rates of the mmWave link and microwave link, respectively. With the help of these two rates, we determine the mmWave eavesdropping region characterized by secrecy rates.

3.3.1. Secrecy Rate of mmWave Link. We analyze the average achievable secrecy rate of mmWave communication networks. Based on Equation (9) and [38–40], the average secrecy rate can be lower bounded by the following:

$$\overline{R}_s = \left[\overline{R} - \overline{R}_e\right]^{+}, \tag{22}$$

where $\overline{R} = \mathbb{E}\left[\log_2\left(1 + \mathrm{SNR}_{T_1,R_1}\right)\right]$ is the average achievable secrecy rate of the channel between the transmitter T_1 and its receiver R_1, and $\overline{R}_e = \mathbb{E}\left[\log_2\left(1 + \mathrm{SNR}_{T_1,E}\right)\right]$ is the average achievable rate of the channel between transmitter T_1 and eavesdropper E.

According to Equation (9), to derive the secrecy rate, we first need to determine the SNR_{T_1,R_1} and $\mathrm{SNR}_{T_1,E}$. As mentioned above, the link $T_1 \longrightarrow R_1$ transmits information only when the link is LoS. Thus, the SNR_{T_1,R_1} is as follows:

$$\mathrm{SNR}_{T_1,R_1} = \underbrace{\frac{P_m G(x_1,y_1) d_{T_1,R_1}^{-\alpha_L}}{\sigma^2}}_{C_1} h_{T_1,R_1}, \tag{23}$$

where (x_1, y_1) denotes the coordinate of R_1 and d_{T_1,R_1} denotes the distance between T_1 and R_1.

The $\mathrm{SNR}_{T_1,E}$ varies depending on whether the link $T_1 \longrightarrow E$ is LoS or NLoS. We use $\mathrm{SNR}_{T_1,E}^{L}$ (resp. $\mathrm{SNR}_{T_1,E}^{N}$) to denote the SNR when the link is LoS (resp. NLoS). Thus, the $\mathrm{SNR}_{T_1,E}^{b}$ $(b = L, N)$ is given by the following:

$$\mathrm{SNR}^{b}_{T_1,E} = \underbrace{\frac{P_m G(x,y) d^{-\alpha_b}_{T_1,E}}{\sigma^2}}_{C^b_2} h^{b}_{T_1,E}. \tag{24}$$

Next, we first derive $\overline{R}$, then show the derivation of $\overline{R}_e$, and finally derive $\overline{R}_s$ based on Equation (22).

Lemma 1. *The average rate of the channel between the transmitter T_1 and its receiver R_1 is as follows:*

$$\overline{R} = \frac{\ln \frac{C_1}{N_L} + \psi_0(N_L)}{\ln 2}, \tag{25}$$

where $C_1 = \frac{P_m G(x_R, y_R) d_{T_1,R_1}}{\sigma^2}$ and $\psi_0(x)$ is Polygamma function.

Proof. To simplify the calculation, we ignore the 1 in $\log_2\left(1 + \mathrm{SNR}_{T_1,R_1}\right)$. The reason is that we focus on the high SNR regime, i.e., $\mathrm{SNR} \gg 1$. Then, we have the following:

$$\overline{R} = \mathbb{E}\left[\log_2\left(1 + \mathrm{SNR}_{T_1,R_1}\right)\right] = \mathbb{E}\left[\log_2\left(C_1 \underbrace{h_{T_1,R_1}}_{u}\right)\right]. \tag{26}$$

Applying the PDF of gamma random variables, we have the following:

$$\begin{aligned}
\overline{R} &= \frac{1}{\ln 2}\int_0^{\infty} \ln(C_1 u)\, d\frac{\gamma(N_L, N_L u)}{\Gamma(N_L)} \\
&\overset{(a)}{=} \frac{\ln(C_1 u)\frac{\gamma(N_L,N_L u)}{\Gamma(N_L)}}{\ln 2} - \frac{\int_0^{\infty} \sum_{k=0}^{\infty} (-1)^k \frac{(N_L u)^{N_L+k}}{k!(N_L+k)} \frac{1}{u}\, du}{\Gamma(N_L)\ln 2} \\
&= \frac{\left[\ln(C_1 u)\gamma(N_L, N_L u) - \sum_{k=0}^{\infty} \frac{(-1)^k (N_L u)^{N_L+k}}{k!(N_L+k)^2}\right]\Big|_0^{\infty}}{\Gamma(N_L)\ln 2},
\end{aligned} \tag{27}$$

where (a) follows the series expansions of the *incomplete gamma function* by Olver et al. [41]. Let

$$D(u) = \ln(C_1 u)\gamma(N_L, N_L u) - \sum_{k=0}^{\infty} \frac{(-1)^k (N_L u)^{N_L+k}}{k!(N_L+k)^2}. \tag{28}$$

Then, $\overline{R}$ can be rewritten as follows:

$$\overline{R} = \frac{1}{\Gamma(N_L)\ln 2}\left(\lim_{u\longrightarrow\infty} D(u) - \lim_{u\longrightarrow 0} D(u)\right). \tag{29}$$

Next, we derive the limit $\lim_{u\longrightarrow\infty} D(u)$, which is given by the following:

$$\begin{aligned}
\lim_{u\longrightarrow\infty} D(u) = &\lim_{u\longrightarrow\infty} \left(\ln C_1 \gamma(N_L, N_L u) + \ln u \gamma(N_L, N_L u)\right) \\
&- \lim_{u\longrightarrow\infty} \sum_{k=0}^{\infty} \frac{(-1)^k (N_L u)^{N_L+k}}{k!(N_L+k)^2}.
\end{aligned} \tag{30}$$

Based on the series expansions of *lower incomplete gamma function* by Olver et al. [41], we have the following:

$$\begin{aligned}
\lim_{u\longrightarrow\infty} D(u) = &\lim_{u\longrightarrow\infty} \sum_{k=0}^{\infty} \frac{(-1)^k (N_L u)^{N_L+k} (\ln u(N_L+k) - 1)}{k!(N_L+k)^2} \\
&+ \lim_{u\longrightarrow\infty} \left(\ln C_1 \gamma(N_L, N_L u)\right).
\end{aligned} \tag{31}$$

Letting $\ln u = \ln \frac{N_L u}{N_L} = \ln N_L u - \ln u$, we have the following:

$$\begin{aligned}
\lim_{u\longrightarrow\infty} D(u) &= \lim_{u\longrightarrow\infty} \sum_{k=0}^{\infty} \frac{(-1)^k (N_L u)^{N_L+k} (\ln N_L u(N_L+k) - 1)}{k!(N_L+k)^2} + \lim_{u\longrightarrow\infty} \left(\gamma(N_L, N_L u) \ln\left(\frac{C_1}{N_L}\right)\right) \\
&\overset{(b)}{=} \lim_{u\longrightarrow\infty} \left((\ln(C_1) - \ln(N_L))\gamma(N_L, N_L u)\right) + \lim_{u\longrightarrow\infty} \frac{\partial \gamma(N_L u, N_L)}{\partial N_L} \\
&\overset{(c)}{=} \ln(C_1)\Gamma(N_L) - \ln(N_L)\Gamma(N_L) + \Gamma'(N_L) \\
&= \Gamma(N_L)(\ln(C_1) - \ln(N_L) + \psi_0(N_L)),
\end{aligned} \tag{32}$$

where step (*b*) follows from Equation (33) and step (*c*) follows the Equation (8.8.13) by Olver et al. [41],

$$\begin{aligned}\frac{\partial(\gamma(s,x))}{\partial s} &= \sum_{k=0}^{\infty}\frac{(-1)^k}{k!}\frac{x^{s+k}\ln x(s+k)-x^{s+k}}{(s+k)^2}\\ &= \sum_{k=0}^{\infty}\frac{(-1)^k x^{s+k}}{k!(s+k)}\left(\ln x-\frac{1}{s+k}\right).\end{aligned} \tag{33}$$

Then, we derive the $\lim_{u\longrightarrow 0} D(u)$, which is given by the following:

$$\begin{aligned}\lim_{u\longrightarrow 0} D(u) &= \lim_{u\longrightarrow 0}\ln(C_1u)\gamma(N_L,N_Lu)\\ &- \lim_{u\longrightarrow 0}\sum_{k=0}^{\infty}\frac{(-1)^k(N_Lu)^{N_L+k}}{k!(N_L+k)^2}\\ &\overset{(d)}{=} \lim_{u\longrightarrow 0}\sum_{k=0}^{\infty}\left(\frac{(-1)^k {N_L}^{N_L+k}}{k!(N_L+k)}\frac{\ln(C_1u)}{(u)^{-(N_L+k)}}\right)\\ &\overset{(e)}{=} \sum_{k=0}^{\infty}\lim_{u\longrightarrow 0}\left(\frac{(-1)^k {N_L}^{N_L+k}}{k!(N_L+k)}\frac{u^{N_L+k}}{-(N_L+k)}\right),\end{aligned} \tag{34}$$

where step (*d*) follows from the series expansion of the *lower incomplete gamma function* by Olver et al. [41] and step (*e*) due to the *L'Hospital's* rule. When $u\longrightarrow 0$, Equation (34) is equal to 0. Substituting Equations (32) and (34) into Equation (29) completes the proof. □

Lemma 2. *The average rate of the channel between the transmitter T_1 and the eavesdropper E is as follows:*

$$\begin{aligned}\overline{R}_e &= p_L\left(d_{T_1,E}\right)\left(\ln\frac{C_2^L}{N_L}+\psi_0(N_L)\right)\\ &+p_N\left(d_{T_1,E}\right)\left(\ln\frac{C_2^N}{N_N}+\psi_0(N_N)\right)\Bigg),\end{aligned} \tag{35}$$

where $C_2^b=\frac{P_m G(x,y) d_{T_1,E}^{-\alpha_b}}{\sigma^2}(b=L,N)$.

Proof. To simplify the calculation, we ignore the 1 in $\log_2\left(1+\mathrm{SNR}_{T_1,E}\right)$. Following the definition of $\mathrm{SNR}_{T_1,E}$, Equations (3) and (4), and the law of total probability, we have the following:

$$\begin{aligned}\overline{R}_e &= \mathbb{E}\left[\log_2\left(1+\mathrm{SNR}_{T_1,E}\right)\right]\\ &= p_L\left(d_{T_1,E}^L\right)\mathbb{E}\left[\log_2\left({C_2}^L\underbrace{h_{T_1,E}^L}_{u_L}\right)\right]\\ &+p_N\left(d_{T_1,E}^N\right)\mathbb{E}\left[\log_2\left(C_2^N\underbrace{h_{T_1,E}^N}_{u_N}\right)\right].\end{aligned} \tag{36}$$

Applying the PDF of gamma random variables, we have the following:

$$\overline{R}_e = p_L\left(d_{T_1,E}^L\right)\underbrace{\int_0^{\infty}\log_2(C_2^L u_L)f(u_L)du_L}_{I_L}+p_N\left(d_{T_1,E}^N\right)\underbrace{\int_0^{\infty}\log_2(C_2^N u_N)f(u_N)du_N}_{I_N}. \tag{37}$$

Next, we derive I_L and I_N,

$$I_L=\frac{\ln(C_2^Lu_L)\gamma(N_L,N_Lu_L)-\sum_{k=0}^{\infty}\frac{(-1)^k(N_Lu_L)^{N_L+k}}{k!(N_L+k)^2}\Big|_0^{\infty}}{\Gamma(N_L)\ln 2}. \tag{38}$$

Then, we let

$$D(u_L)=\ln(C_2^Lu_L)\gamma(N_L,N_Lu_L)-\sum_{k=0}^{\infty}\frac{(-1)^k(N_Lu_L)^{N_L+k}}{k!(N_L+k)^2}. \tag{39}$$

Thus, the I_L can be rewritten as follows:

$$\begin{aligned}I_L &= \frac{1}{\Gamma(N_L)\ln 2}\left(\lim_{u_L\longrightarrow\infty}D(u_L)-\lim_{u_L\longrightarrow 0}D(u_L)\right)\\ &\overset{(f)}{=}\frac{\ln(C_2^L)-\ln(N_L)+\psi_0(N_L)}{\ln 2},\end{aligned} \tag{40}$$

where step (*f*) follows after substituting Equations (32) and (34) into $\overline{R}_e$. Similarly, we have the following:

$$I_N=\frac{\ln(C_2^N)-\ln(N_N)+\psi_0(N_N)}{\ln 2}. \tag{41}$$

Substituting Equations (40) and (41) to Equation (37), we complete the proof. □

Theorem 3. *Based on Equation (18), Lemma 1 and 2, the average secrecy rate of mmWave link can be lower bounded by the following:*

$$\overline{R}_s = \frac{1}{\ln 2}\left[\ln \frac{C_1 N_N}{N_L C_2^N} + \psi_0(N_L) - \psi_0(N_N) - p_L\left(d_{T_1,E}\right)\left(\ln \frac{C_2^L N_N}{N_L C_2^N} + \psi_0(N_L) - \psi_0(N_N)\right)\right]^+. \tag{42}$$

Proof. Substituting Equations (3) and (4) to Equation (9) and Equation (4) to Equation (4), we complete the proof. □

3.3.2. Secrecy Rate of Microwave Link. The average achievable secrecy rate of the microwave link is given by the following:

$$\overline{R_s^u} = \mathbb{E}[R_u - R_e^u]^+, \tag{43}$$

where $R_u = \log_2\left(1 + \mathrm{SNR}_{T_2,R_2}\right)$ is the secrecy rate of the channel between the transmitter T_2 and its receiver R_2, and $R_e^u = \log_2\left(1 + \mathrm{SNR}_{T_2,E}\right)$ is the secrecy rate of the channel between transmitter T_2 and eavesdropper E.

According to Equation (10), to derive the secrecy rate of the microwave link, we first need to determine the SNR_{T_2,R_2} and $\mathrm{SNR}_{T_2,E}$. Therefore, the SNR_{T_2,R_2} is as follows:

$$\mathrm{SNR}_{T_2,R_2} = \underbrace{\frac{P_u A_u A_u d_{T_2,R_2}^{-\alpha_u}}{\sigma^2}}_{C_3} \; h_{T_2,R_2}, \tag{44}$$

and the $\mathrm{SNR}_{T_2,E}$ is as follows:

$$\mathrm{SNR}_{T_2,E} = \underbrace{\frac{P_u A_u A_E d_{T_2,E}^{-\alpha_u}}{\sigma^2}}_{C_4} \; h_{T_2,E}, \tag{45}$$

where d_{T_2,R_2} denotes the distance between T_2 and R_2, and $d_{T_2,E}$ denotes the distance between T_2 and E.

We then derive the average achievable secrecy rate of the microwave link, which is given by the following theorem.

Theorem 4. *The average secrecy rate of the microwave link is as follows:*

$$\overline{R_s^u} = \ln\left(1 + \frac{A_u d_{T_2,R_2}^{-\alpha_u}}{A_E d_{T_2,E}^{-\alpha_u}}\right). \tag{46}$$

Proof. Using Equations (10), (44), and (45), we have the following:

$$\begin{aligned}\overline{R_s^u} &= \mathbb{E}\left[\log_2\left(C_3 \underbrace{h_{T_2,R_2}}_{u_3}\right) - \log_2\left(C_4 \underbrace{h_{T_2,E}}_{u_4}\right)\right] \\ &= \frac{1}{\ln 2}\mathbb{E}\left[\ln\left(\frac{C_3 u_3}{C_4 u_4}\right)\right] \\ &\overset{(i)}{=} \frac{1}{\ln 2}\mathbb{E}\left[\ln\left(C\frac{u_3}{u_4}\right)\right],\end{aligned} \tag{47}$$

where step (i) follows after letting $C = \frac{C_3}{C_4}$. Then, applying the PDF of exponential distribution, we have the following:

$$\begin{aligned}\overline{R_s^u} &= \int_0^\infty \int_{\frac{u_4}{C}}^\infty \ln\left(C\frac{u_3}{u_4}\right) e^{-u_3} e^{-u_4}\, du_3\, du_4 \\ &= \int_0^\infty \underbrace{\int_{\frac{u_4}{C}}^\infty \ln\left(C\frac{u_3}{u_4}\right) e^{-u_3}\, du_3}_{A}\; e^{-u_4}\, du_4.\end{aligned} \tag{48}$$

We derive A first,

$$\begin{aligned}A &= \int_{\frac{u_4}{C}}^\infty \ln\left(C\frac{u_3}{u_4}\right) e^{-u_3}\, du_3 \\ &= -\ln\left(C\frac{u_3}{u_4}\right)e^{-u_3}\Big|_{u_3=\frac{u_4}{C}}^{u_3\longrightarrow\infty} + \int_{\frac{u_4}{C}}^\infty \frac{e^{-u_3}}{u_3}\, du_3 \\ &= \ln(1)e^{-\frac{u_4}{C}} - \lim_{x\longrightarrow\infty} \ln\left(C\frac{u_3}{u_4}\right)e^{-u_3} + \int_{\frac{u_4}{C}}^\infty \frac{e^{-u_3}}{u_3}\, du_3 \\ &= 0 - 0 - E_i\left(-\frac{u_4}{C}\right) \\ &= -E_i\left(-\frac{u_4}{C}\right),\end{aligned} \tag{49}$$

where $E_i(-t) = -\int_t^\infty \frac{e^{-x}}{x} dx$ denotes the *Exponential Integral Function* [42]. Hence,

$$\begin{aligned}\overline{R_s^u} &= -\int_0^\infty E_i\left(-\frac{u_4}{C}\right)e^{-u_4}\, du_4 \\ &= -\lim_{t\longrightarrow 0}\int_t^\infty E_i\left(-\frac{u_4}{C}\right)e^{-u_4}\, du_4.\end{aligned} \tag{50}$$

Applying the rule of integral by parts yields,

$$\begin{aligned}\overline{R_s^u} &= \lim_{t\longrightarrow 0} E_i\left(-\left(1+\frac{1}{C}\right)t\right) - e^{-t}E_i\left(-\frac{t}{C}\right) \\ &= \lim_{t\longrightarrow 0} E_i\left(-\left(1+\frac{1}{C}\right)t\right) - E_i\left(-\frac{t}{C}\right).\end{aligned} \tag{51}$$

To calculate the above limit, we can use the following expansion of the exponential integral function [42],

$$E_i(t) = \gamma^* + \ln(t) + \sum_{n=1}^{\infty} \frac{t^n}{nn!}, \tag{52}$$

where γ^* is the *Euler constant*. Therefore, Equation (51) can be expressed as follows:

$$\begin{aligned}\overline{R_s^u} &= \lim_{t\longrightarrow 0} \ln\left(-\left(1+\frac{1}{C}\right)t\right) - \ln\left(-\frac{t}{C}\right) \\ &\quad + \sum_{n=1}^{\infty} \frac{\left(-\left(1+\frac{1}{C}\right)t\right)^n - \left(-\frac{t}{C}\right)^n}{nn!} \\ &= \ln(1+C) + \underbrace{\lim_{t\longrightarrow 0} \sum_{n=1}^{\infty} \frac{\left(-\left(1+\frac{1}{C}\right)\right)^n - \left(-\frac{1}{C}\right)^n}{nn!} t^n}_{=0} \\ &= \ln(1+C).\end{aligned} \tag{53}$$

Substituting Equations (44) and (45) into Equation (53) completes the proof. Using the secrecy rates in Theorems 3 and 4, we can determine the mmWave eavesdropping region $\mathcal{M}_m$ characterized by secrecy rates based on the definition in Equation (12). □

4. Optimal Eavesdropping Location Modeling

4.1. Problem Formulation. To better observe the eavesdropping behavior of eavesdroppers, we propose the optimal eavesdropping location problem to investigate the optimal eavesdropping location in the given network. We formulate the optimization problem as follows:

$$(x*, y*) = \underset{x,y\in\left(-\frac{D}{2},\frac{D}{2}\right)}{\arg\max}\ W_m P_{\mathrm{so}}^m(x,y) + (1-W_m) P_{\mathrm{so}}^u(x,y). \tag{54}$$

Due to the complexity of the optimization problem, it is difficult to obtain closed-form solutions. Thus, we use the Arg max function in *Mathematica* to calculate the numerical results [43]. Lastly, we present the numerical results of the optimization problem in the next section.

5. Numerical Results

In this section, we first provide simulation results to validate the expressions of SOPs and secrecy rates for the mmWave link and microwave link, respectively. We then provide the mmWave eavesdropping regions results characterized by different metrics, i.e., SOPs and secrecy rates, and demonstrate the selection behavior of the eavesdropper in the considered hybrid communication scenario under different parameter settings. Finally, we show the numerical results of the optimal eavesdropping location. Table 1 summarizes the parameter settings used in this section.

5.1. Model Validation

5.1.1. SOP Validation. To validate our theoretical analysis, we compare the simulation and theoretical values of the SOPs in mmWave and microwave, respectively. We set the angle between $\overrightarrow{T_1R_1}$ and the x-axis as $\theta = 2\pi/3$, the blockage density as $\beta = 0.1$ and the beam width of the main lobe of T_1's antenna as $\phi = \pi/6$.

We first show in Figure 2 the simulation results and the theoretical values of the SOP of the mmWave transmission pair for three different locations of the eavesdropper E, i.e., $(-20, 20)$, $(-30, 20)$, and $(-40, 20)$. We can see from Figure 2 that the simulation results are consistent with the theoretical ones under all three eavesdropper locations. This indicates the correctness of the SOP expression of the mmWave transmission. We can also see from Figure 2 that the SOP of mmWave decreases as the decoding threshold ε_m increases.

Table 1: Parameter settings.

Parameter	Value
Beamwidth φ of main lobe of T_1	$\pi/6$
Main (back) lobe gain A_m (a_m) of T_1	10 (0.1)
Antenna gain A_u of T_2	1
Antenna gain A_r of T_1	10
Antenna gain A_E of E	5
Path loss exponent α_L (α_N, α_u)	2 (4, 3)
Nakagami-m fading parameter N_L (N_N)	3 (2)
Transmit power P_m (P_u) of T_1 (T_2)	1 (1) (w)
Noise power σ^2	10^{-5} (w)
Distance 2ℓ between T_1 and T_2	80 (m)
The coordinates of mmWave receiver $R_1(x_1, y_1)$	$(40, 20\sqrt{3})$
The coordinates of microwave receiver $R_2(x_2, y_2)$	$(60, -40)$
Minimum required SNR ε_m for decoding the signals from T_1	0.03
Minimum required SNR ε_u for decoding the signals from T_2	0.1

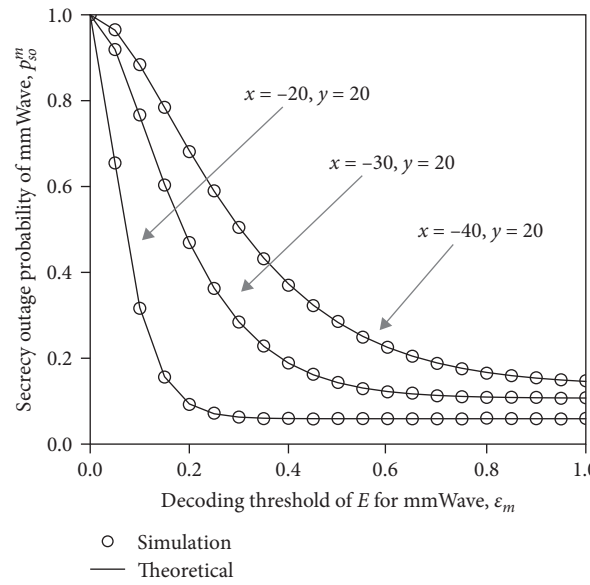


Figure 2: SOP validation of mmWave transmission pair.

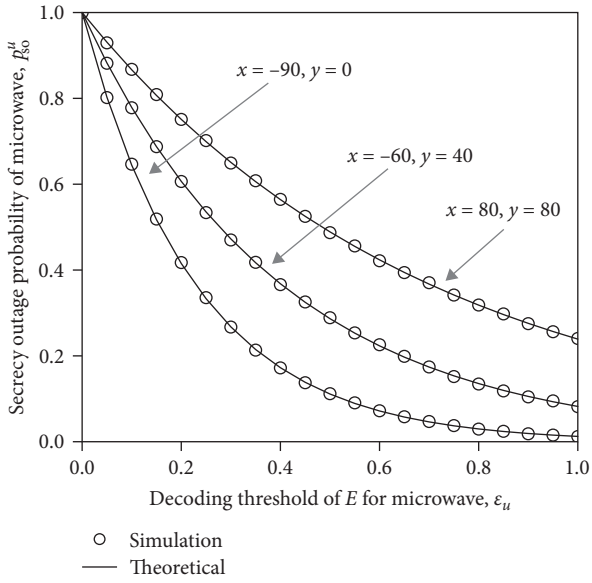


FIGURE 3: SOP validation of microwave transmission pair.

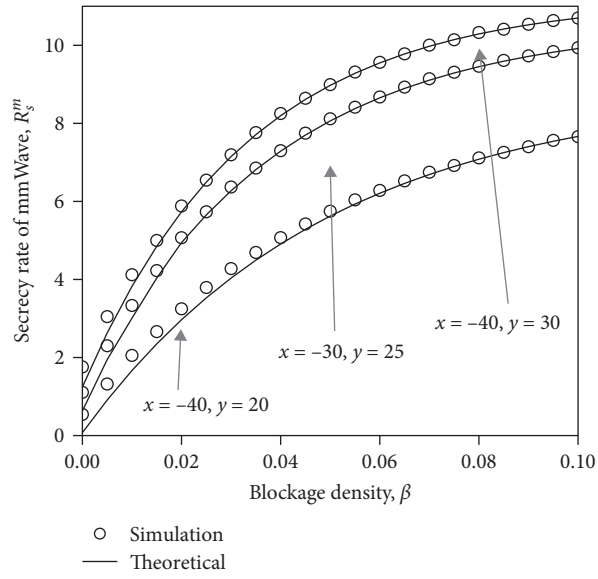


FIGURE 4: Secrecy rate validation of mmWave link.

We next show in Figure 3 the simulation results vs. theoretical ones for the SOP of the microwave transmission. We also consider three different locations of E, which are $(-90, 0)$, $(-60, 40)$, and $(80, 80)$. The results in Figure 3 show that the theoretical results match nicely with the simulation ones, demonstrating the correctness of the SOP expression of the microwave transmission. Similar to the SOP of the mmWave transmission, the results show that the SOP of the microwave also decreases as the decoding threshold ε_u increases.

5.1.2. Secrecy Rate Validation. To validate the theoretical analysis in Section 3, we summarize the simulation and theoretical values of the secrecy rate for the mmWave link and microwave link in Figures 4 and 5, respectively. In both figures, we consider three different locations of the eavesdropper E, i.e., $(-40, 20)$, $(-30, 25)$, and $(-40, 30)$ in Figure 4, and $(-20, 20)$, $(0, 40)$, and $(20, -40)$ in Figure 5. We set the antenna gain of E as $A_E = 5$, the coordinates of mmWave receiver $R_1(x_1, y_1)$ and that of microwave receiver as $(40, 20\sqrt{3})$ and $(60, -40)$, respectively.

The results in Figure 4 show that the theoretical results match the simulation results very well, indicating that the lower bound on the secrecy rate of the mmWave link is tight enough to be used as an approximation. Figure 4 also indicates that the secrecy rate of the mmWave link increases as the blockage density β increases. Figure 5 demonstrates the validation of secrecy rate R_s^u for various target antenna gain A_u of microwave transmitter T_1. Notice that the simulation results match nicely with theoretical values, indicating the correctness of the expression of the secrecy rate of the microwave link. The results in Figure 5 also show that the secrecy rate of the microwave transmission increases as the microwave transmitter T_1's antenna gain A_u increases.

5.2. Performance Evaluation. We investigate the impacts of several important parameters on the mmWave eavesdropping

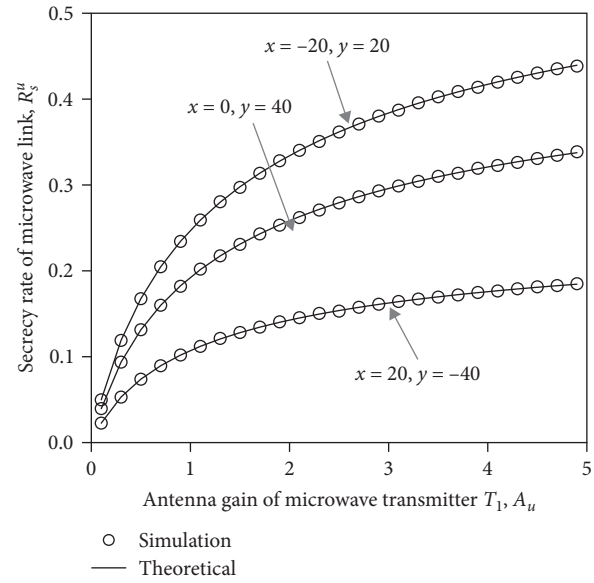


FIGURE 5: Secrecy rate validation of microwave link.

region $\mathscr{R}_m$ characterized by the SOPs and that on the mmWave eavesdropping region $\mathscr{M}_m$ characterized by the secrecy rates.

5.2.1. Eavesdropping Region $\mathscr{R}_m$. To understand the impact of the selection parameter ρ_{sop} on the mmWave eavesdropping region $\mathscr{R}_m$, we summarize in Figure 6 the mmWave eavesdropping region $\mathscr{R}_m$ under three different values of ρ_{sop}. Figure 6 shows that $\mathscr{R}_m$ enlarges as the selection parameter ρ_{sop} decreases. Recall that ρ_{sop} represents the selection preference of E. The smaller ρ_{sop} is, the more E prefers the mmWave over the microwave. Thus, for a fixed location, the SOP of the microwave remains unchanged, and as ρ_{sop} decreases, this location is more likely to be included in the mmWave

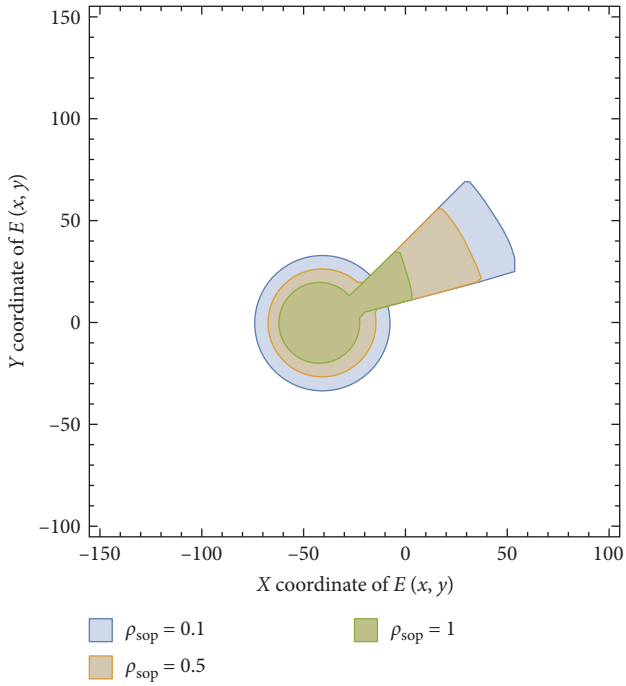


FIGURE 6: Impact of selection parameter ρ_{sop} on mmWave eavesdropping region (SOP).

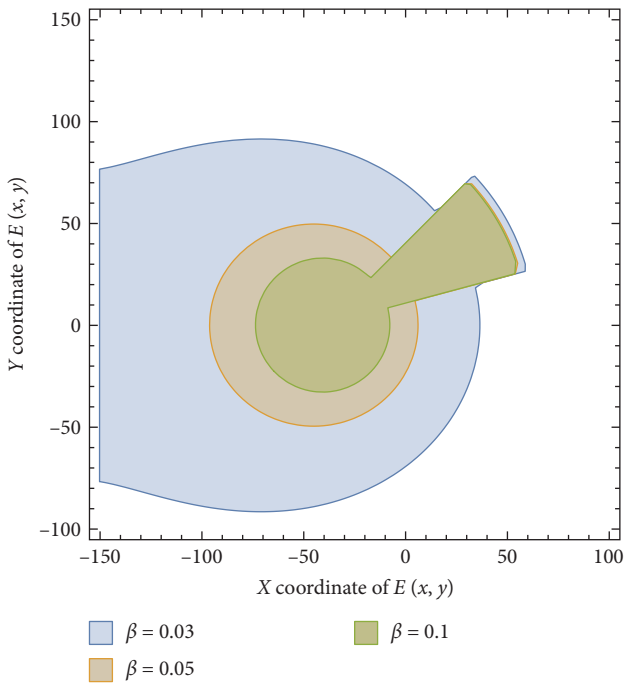


FIGURE 7: Impact of blockage density β on mmWave eavesdropping region (SOP).

eavesdropping region $\mathscr{R}_m$. As a result, the size of the mmWave eavesdropping region $\mathscr{R}_m$ increases.

Figure 7 shows the impact of the blockage density β on the mmWave eavesdropping region $\mathscr{R}_m$. It can be observed that the size of $\mathscr{R}_m$ decreases as β increases. The major

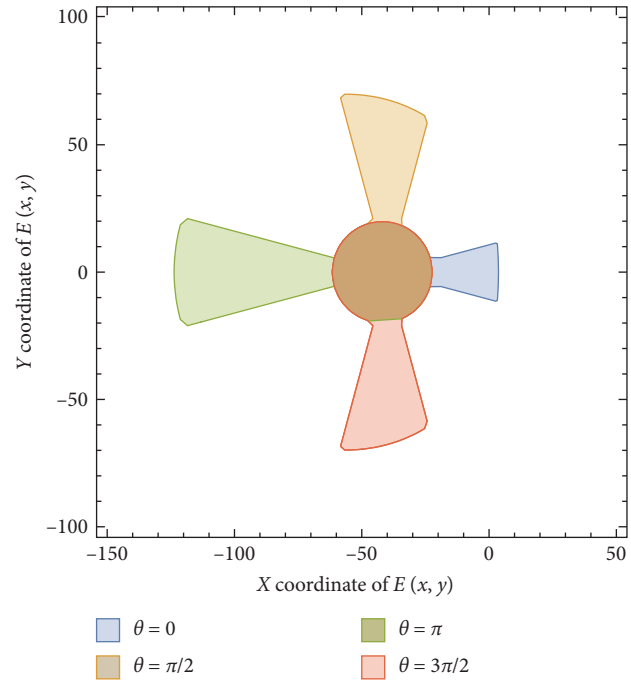


FIGURE 8: Impact of angle θ on mmWave eavesdropping region (SOP).

reason for this phenomenon is that the larger β is, the more blockage exists in the network. As a result, the link from T_1 to E is more likely to be NLoS, leading to a smaller SOP. Thus, the possibility of a fixed location being included in $\mathscr{R}_m$ is reduced, resulting in a smaller $\mathscr{R}_m$.

Finally, we explore the impact of the angle θ between $\overrightarrow{T_1R_1}$ and the x-axis (i.e., the boresight of the mmWave transmitter's antenna) on the mmWave eavesdropping region $\mathscr{R}_m$. As Figure 8 shows, the size of $\mathscr{R}_m$ changes as the angle θ changes. In general, the region size is minimized when the mmWave transmitter's antenna points toward the microwave transmitter (i.e., the case of $\theta = 0$ in Figure 8), while it is maximized when the mmWave transmitter's antenna points towards the opposite direction of the microwave transmitter (i.e., the case of $\theta = \pi$ in Figure 8). This is intuitive since the closer E is to the microwave transmitter, the larger the SOP under the microwave and, thus, the less likely E prefers the mmWave.

5.2.2. Eavesdropping Region $\mathscr{M}_m$. Figure 9 illustrates the impact of the blocking density β on the mmWave eavesdropping region $\mathscr{M}_m$. We can observe that the size of $\mathscr{M}_m$ decreases as β increases. A larger β means that more blockages exist in the network. Consequently, the link from $T_1 \longrightarrow E$ is more likely to be NLoS, which leads to a larger secrecy rate of the mmWave link. Therefore, the likelihood of any location being included in the mmWave eavesdropping region decreases, which leads to a smaller mmWave eavesdropping region $\mathscr{M}_m$.

We then demonstrate the impact of the selection parameter ρ_{sr} on the mmWave eavesdropping region $\mathscr{M}_m$ in Figure 10. It shows that as the selection parameter ρ_{sr}

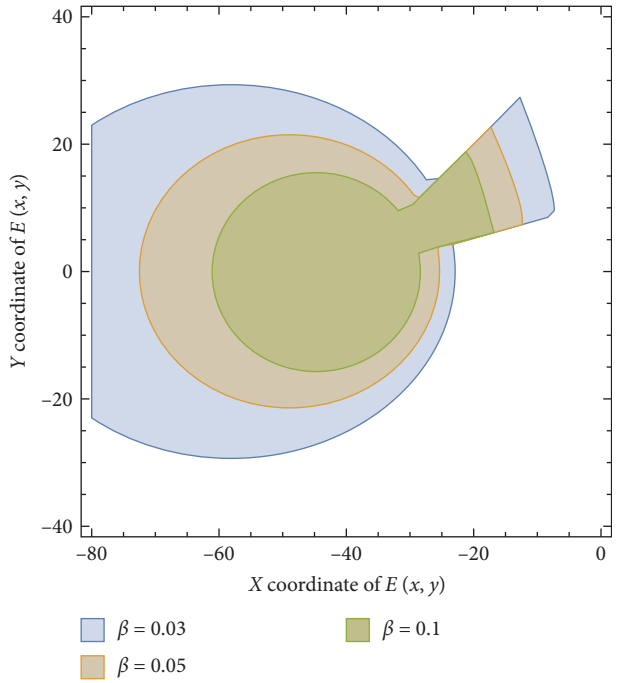


Figure 9: Impact of blockage density β on mmWave eavesdropping region (secrecy rate).

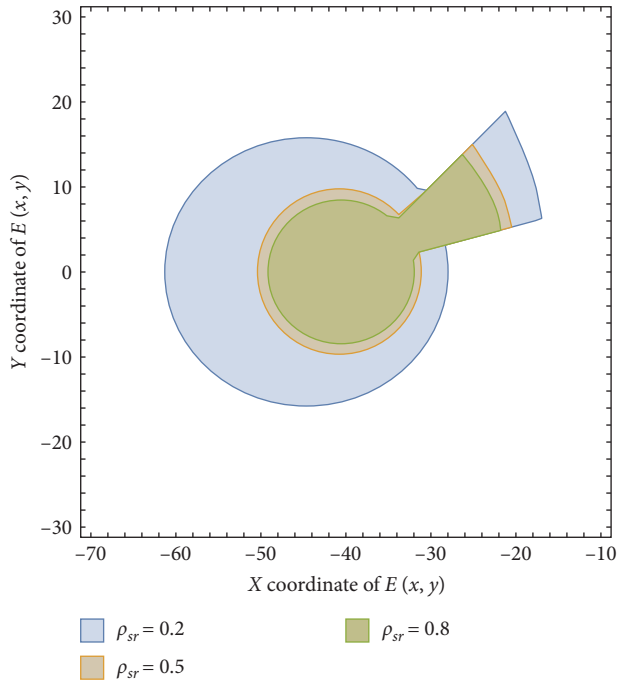


Figure 10: Impact of selection parameter ρ_{sr} on mmWave eavesdropping region (secrecy rate).

increases, the size of $\mathcal{M}_m$ decreases. Note that we use ρ_{sr} to represent the selection preference of E in this paper, and a smaller ρ_{sr} means that E prefers mmWave. Since the secrecy rate of the microwave link remains constant, as ρ_{sr} increases,

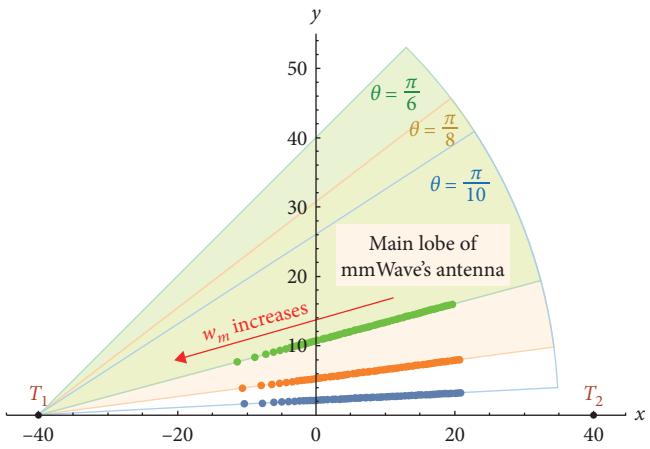


Figure 11: Optimal eavesdropping location.

it is more difficult for any fixed location to be included in the mmWave eavesdropping region. Therefore, the mmWave eavesdropping region $\mathcal{M}_m$ becomes smaller.

An interesting phenomenon can be observed from Figure 10, when $\rho_{sr} = 0.5$ or 1, the change of the mmWave eavesdropping region is extremely small. This is because, in this paper, we assume that the eavesdropper E treats eavesdropping on the mmWave link and the microwave link as equally important when $\rho_{sr} = 1$. Also, the transmit power of the mmWave link is much smaller than that of the microwave link. Therefore, when ρ_{sr} is large (i.e., $0.5 < \rho_{sr} < 1$), although the eavesdropper E is in the vicinity of the mmWave transmitter T_1, it still prefers to eavesdrop on the microwave link with stronger transmit power in order to improve their eavesdropping performance.

5.2.3. Optimal Eavesdropping Location. We demonstrate the numerical result of the optimization eavesdropping locations in Section 4. We set the beam width ϕ of the main lobe of T_1 as $\phi = \pi/6$, the blockage density as $\beta = 0.1$ and the antenna gain A_E of E as 5. Moreover, we set the minimum required SNRs ε_m and ε_u as 0.03 and 0.1, respectively.

We illustrate the optimal eavesdropping locations by considering three different angles of θ (the angle between $\overrightarrow{T_1R_1}$ and x-axis), i.e., $\pi/6$, $\pi/8$, and $\pi/10$. Figure 11 shows the optimal eavesdropping locations of the eavesdropper according to the objective function that we proposed when the angle θ is at three different angles. Note that the sectors represent the main lobe of the mmWave transmitter $T_1(-40, 0)$, $T_2(40, 0)$ represent the microwave transmitter, the three different colors represent three different angles θ, and the continuous dots on the borders denote the optimal eavesdropping locations.

According to Figure 11, we can observe that the optimal eavesdropping location changes as the angle θ changes. Moreover, it is easily seen that the optimal eavesdropping location is always on the lower border of the main lobe of the mmWave transmitter's antenna. As W_m increases, the optimal location is close to mmWave transmitter T_1.

6. Conclusion

This paper investigates the millimeter-wave (mmWave) eavesdropping region characterization problem in hybrid wireless communication systems where mmWave links and microwave links coexist. We first derived the secrecy outage probabilities and secrecy rates of both the mmWave link and microwave link, respectively, based on which we identify the eavesdropping region, where eavesdroppers prefer the mmWave links. We then demonstrate the numerical results of optimization eavesdropping locations. The results in this paper showed that the mmWave eavesdropping region decreases as the selection parameter ρ_{sop} and ρ_{sr} increases. In addition, the eavesdropping region decreases when there are more blockages in the network (i.e., when blockage density β becomes larger).

Data Availability

No underlying data were collected or produced in this study.

Disclosure

This paper was presented in part at the International Conference on Networking and Network Applications (NaNA), Haikou, China, December 2020.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (grant no. 62202354), Qin Chuangyuan Innovation and Entrepreneurship Talent Project of Shaanxi (grant no. QCYRCXM-2022-144), Natural Science Basic Research Program of Shaanxi (program no. 2019JC-17), JST SPRING (grant no. JPMJSP2140) and the Japan Society for the Promotion of Science under Grant-in-Aid for Challenging Research (Exploratory) (grant no. 22K19776).

References

[1] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: potentials and challenges," *Proceedings of the IEEE*, vol. 102, no. 3, pp. 366–385, 2014.

[2] X. Wang, L. Kong, F. Kong et al., "Millimeter wave communication: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1616–1653, 2018.

[3] W. Hong, Z. H. Jiang, C. Yu et al., "The role of millimeter-wave technologies in 5G/6G wireless communications," *IEEE Journal of Microwaves*, vol. 1, no. 1, pp. 101–122, 2021.

[4] M. Shafi, J. Zhang, H. Tataria et al., "Microwave vs. millimeter-wave propagation channels: key differences and impact on 5G cellular systems," *IEEE Communications Magazine*, vol. 56, no. 12, pp. 14–20, 2018.

[5] J. Ma, R. Shrestha, J. Adelberg et al., "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, pp. 89–93, 2018.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

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

[8] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[9] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Network*, vol. 36, no. 3, pp. 98–104, 2022.

[10] S. He, Y. Zhang, J. Wang et al., "A survey of millimeter-wave communication: physical-layer technology specifications and enabling transmission technologies," *Proceedings of the IEEE*, vol. 109, no. 10, pp. 1666–1705, 2021.

[11] J. D. V. Sánchez, L. Urquiza-Aguiar, and M. C. P. Paredes, "Physical layer security for 5G wireless networks: a comprehensive survey," in *2019 3rd Cyber Security in Networking Conference (CSNet)*, pp. 122–129, IEEE, 2019.

[12] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli, and J. M. Chuma, "An overview of key technologies in physical layer security," *Entropy*, vol. 22, no. 11, Article ID 1261, 2020.

[13] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[14] L. Tao, W. Yang, Y. Cai, and D. Chen, "On secrecy outage probability and average secrecy rate of large-scale cellular networks," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 6869189, 14 pages, 2018.

[15] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3205–3217, 2017.

[16] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Secure millimeter-wave ad hoc communications using physical layer security," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 99–114, 2022.

[17] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: a physical layer security perspective," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 623–638, 2019.

[18] S. Huang, M. Xiao, and H. Vincent Poor, "On the physical layer security of millimeter wave noma networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11697–11711, 2020.

[19] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.

[20] L. Fan, B. Tang, Q. Jiang, F. Liu, and C. Yin, "Joint resource allocation for frequency-domain artificial noise assisted multiuser wiretap OFDM channels with finite-alphabet inputs," *Symmetry*, vol. 11, no. 7, Article ID 855, 2019.

[21] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: a programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, 2019.

[22] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with

reconfigurable intelligent surfaces," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–6, IEEE, 2020.

[23] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1488–1492, 2019.

[24] S. C. Tokgoz, S. Althunibat, S. L. Miller, and K. A. Qaraqe, "On the secrecy capacity of hybrid FSO-mmWave links with correlated wiretap channels," *Optics Communications*, vol. 499, Article ID 127252, 2021.

[25] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Transactions on Communications*, vol. 64, no. 8, pp. 3507–3519, 2016.

[26] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1139–1152, 2018.

[27] A. Umer, S. A. Hassan, H. Pervaiz, L. Musavian, Q. Ni, and M. A. Imran, "Secrecy spectrum and energy efficiency analysis in massive MIMO-enabled multi-tier hybrid hetnets," *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 1, pp. 246–262, 2020.

[28] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204–1219, 2016.

[29] W. Wang, K. C. Teh, S. Luo, and K. H. Li, "Physical layer security in heterogeneous networks with pilot attack: a stochastic geometry approach," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6437–6449, 2018.

[30] Q. Qu, Y. Zhang, and S. Kasahara, "On eavesdropping region characterization in hybrid wireless communications," in *2020 International Conference on Networking and Network Applications (NaNA)*, pp. 29–34, IEEE, 2020.

[31] T. Bai and R. W. Heath, "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1100–1114, 2015.

[32] A. Thornburg, T. Bai, and R. W. Heath, "Performance analysis of outdoor mmWave ad hoc networks," *IEEE Transactions on Signal Processing*, vol. 64, no. 15, pp. 4065–4079, 2016.

[33] M. R. Akdeniz, Y. Liu, M. K. Samimi et al., "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1164–1179, 2014.

[34] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, pp. 356–360, IEEE, 2006.

[35] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[36] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3472–3482, 2012.

[37] O. Ozan Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, 2012.

[38] A. F. Darwesh and A. O. Fapojuwo, "Achievable secrecy rate analysis in mmWave ad hoc networks with multi-array antenna transmission and artificial noise," *IET Communications*, vol. 15, no. 16, pp. 2068–2086, 2021.

[39] S. Iwata, T. Ohtsuki, and P.-Y. Kam, "A lower bound on secrecy capacity for MIMO wiretap channel aided by a cooperative jammer with channel estimation error," *IEEE Access*, vol. 5, pp. 4636–4645, 2017.

[40] C. Liu, J.-Y. Wang, J.-B. Wang, J.-X. Zhu, and M. Chen, "Three lower bounds on secrecy capacity for indoor visible light communications," in *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–5, IEEE, 2017.

[41] F. W. J. Olver, A. B. O. Daalhuis, D. W. Lozier et al., 2021, *NIST Digital Library of Mathematical Functions*, http://dlmf.nist.gov/.

[42] M. Abramowitz, *Handbook of Mathematical Functions, With Formulas, Graphs, and Mathematical Tables*, Dover Publications, Inc., USA, 1974.

[43] W. Research, "ArgMax," 2021, https://reference.wolfram.com/language/ref/ArgMax.html.

Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 6980619, 13 pages
https://doi.org/10.1155/2023/6980619

Research Article

Wireless Key Generation Scheme Based on Random Permutation and Perturbation in Quasistatic Environments

Liquan Chen,[1,2] **Yi Lu**,[1] **Tianyu Lu**,[1] **Zhaofa Chen**,[1] **and Aiqun Hu**[1,2]

[1]*School of Cyber Science and Engineering, Southeast University, Nanjing 211102, China*
[2]*Purple Mountain Laboratories, Nanjing 211111, China*

Correspondence should be addressed to Liquan Chen; lqchen@seu.edu.cn

Received 13 August 2022; Revised 19 January 2023; Accepted 8 February 2023; Published 27 April 2023

Academic Editor: Zhao Li

The wireless key generation using wireless channel reciprocity has attracted considerable attention in the past two decades. However, there are many challenges for the key generation in quasistatic wireless environments. The key generation rate (KGR) in a quasistatic environment is low, and the randomness of the key is insufficient, which is difficult to meet the secure communication requirements. To tackle these issues, a random permutation and perturbation-based wireless key generation (RPP-WKG) scheme is proposed to improve the KGR and randomness in quasistatic environments. Unlike existing key generation schemes, the RPP-WKG scheme allows the two legitimate users to generate the same secret key based on their random permuted channel measurements. Besides, the perturbed key sequence will be obtained by combining the initial key generated after quantization and the permutation order sequence through the XOR operation. Simulation results show that the proposed RPP-WKG scheme can generate secret keys with a high generation rate, sufficient randomness, a low mismatch rate, and a low correlation coefficient in quasistatic environments.

1. Introduction

With the rapid development of wireless communication techniques and the wide use of the Internet of Things (IoT) devices, establishing an encrypted and secure communication link between two IoT devices has become an urgent need [1–5]. The traditional encryption methods widely used at present are symmetric or asymmetric cryptographic algorithms. Symmetric cryptographic algorithms usually rely on preshared secret keys, which are not suitable for distributed IoT devices [6]. Asymmetric cryptography requires complex mathematical algorithms. However, due to the limited computing power of IoT devices and the difficulty in establishing a public key infrastructure between devices, these asymmetric cryptographic algorithms are not suitable for secure communication between lightweight IoT devices. In recent years, wireless key generation schemes based on physical layer channel characteristics have received extensive attention due to their low computational complexity and high security. Traditional cryptographic mechanisms can be supplemented and enhanced by taking advantage of the inherent physical properties of wireless channels [7]. Wireless key generation based on physical layer channel reciprocity is a promising solution for secure communication between IoT devices [8–10].

Generally, a wireless key generation scheme contains four steps: channel sampling, quantization, information reconciliation, and privacy amplification [11]. Among the four steps, quantization converts channel measurements into binary bit sequences, which is the core function of the wireless key generation scheme. Various channel characteristics can be used for quantization, such as received signal strength (RSS), channel state information (CSI), time delay amplitude, phase, and angle-of-arrive (AoA) [12–15].

However, unsynchronized channel sampling in time-division duplex systems and environmental noise will impair channel reciprocity in the real system. The nonreciprocity in the channel measurements can be further amplified by ambient noise, adversely causing the inconsistent quantization result between two users. To mitigate the nonreciprocity of a wireless channel, many researchers have proposed solutions. For example, Li et al. [16] designed a mean-value

quantization scheme for RSS to improve the key generation rate (KGR). Zhao et al. [17] proposed performing group quantization and adaptive quantization on the collected RSS measurements. Margelis et al. [18] used discrete cosine transform (DCT) on channel observations to reduce the mismatches caused by quantization. Liu et al. [19] designed a bipartite graph matching-based wireless key generation method to avoid quantization.

In some IoT application scenarios, such as environmental monitoring and smart home, the IoT devices are fixed and the surrounding wireless environment changes very slowly [20, 21]. In these scenarios, wireless channels between the communication users are quasistatic. The KGR based on the characteristics of this quasistatic wireless channel is very low, which is difficult to meet the secure communication requirements. The reason for low KGR is due to the long channel coherence time in the quasistatic channel, and the secret keys are generated within the coherence time, so the similarity of the secret keys is high. At the same time, ambient noise will also cause key inconsistency. Therefore, an efficient and robust solution is required to achieve a low key mismatch rate (KMR) in a quasistatic environment. Various schemes have been proposed to overcome the challenges of wireless key generation in quasistatic environments. [22, 23] proposed key generation protocols with the aid of a reconfigurable intelligent surface (RIS) to boost KGR in quasistatic environments. [24] used singular value decomposition techniques to reconstitute the wireless channels to improve the randomness of the wireless channels. In [25], the two legitimate users independently generated local randomness to be used together with the uniqueness of the wireless channel coefficients in order to enable high-rate secret key generation.

To mitigate the effect of channel nonreciprocity, we use principal component analysis- (PCA-) based processing on the sampled channel measurements. Li et al. [26] proposed two realization algorithms of PCA for preprocessing: PCA algorithm with interaction and PCA algorithm without interaction. The corresponding eigenvalues and eigenvectors of the two legitimate users, Alice and Bob, are different due to the deviation. Alice can send her eigenvectors to Bob via a public channel and both of them use it for signal reconstruction, which is named as the PCA algorithm with interaction. Alice and Bob can also calculate their own eigenvectors and eigenvalues and use their eigenvectors for signal reconstruction without any interaction, which is called the PCA algorithm without interaction. Although the PCA algorithm with interaction can obtain a relatively higher key agreement than the PCA algorithm without interaction, information leakage will be caused by the transmission on an insecure public channel. When the eavesdropper, Eve, obtains enough information such as eigenvalue and eigenvector, he/she can find the secret key by a brute-force search. Li et al. [26] assume Eve can only obtain eigenvectors instead of the covariance matrix, resulting in a low information leakage ratio. In this paper, since broadcasting eigenvectors on a public channel still has security risks, we recommend the two legitimate users perform a processing algorithm based on PCA without interaction on their original channel measurements after channel sampling.

In a quasistatic channel, the secret keys extracted from channel measurements not only have a relatively low KGR but also have poor randomness. The use of PCA processing on the CSI matrices of legitimate users can only obtain good feature amplification and deredundancy effects, but the KGR cannot be improved by PCA processing. In order to solve the problems of the low KGR and the poor randomness of the secret keys, we focus on the preprocessing algorithm of channel measurements and propose a random permutation and perturbation-based wireless key generation (RPP-WKG) scheme, which provides high randomness and low correlation for secret keys. Based on the RPP-WKG scheme, we develop a secret key generation method that is aimed at extracting secret keys from channel measurements at a low KMR and high speed. CSI is chosen as the channel measurement in this paper because the existing work has shown that CSI could provide more channel characteristics than RSS does. The main contributions of this paper are summarized as follows:

(1) A new and practical RPP-WKG scheme is proposed. Based on the scheme, we can mitigate the impact of the quasistatic channel and generate secret keys with high randomness and low correlation

(2) We propose an efficient and secure permutation method, which can help legitimate users perform the same random permutation on their respective CSI to acquire new random sources with high randomness and great fluctuations. In addition, the length of the permutation order can be adjusted by the number of CSI segments. The random sources can be used as the new channel measurements to generate secret keys

(3) A minimum weight-based matching method is proposed to reduce KMR in the RPP-WKG scheme. Legitimate users can obtain an agreement on the permutation order of CSI without revealing it. The permutation order will be obtained by finding the correspondence between the users' CSI, and it can be used as a source of the secret keys

(4) We propose a random perturbation generation method based on the permutation order agreed by the two legitimate users. The correlation between the secret keys is reduced by performing an XOR operation on the random perturbation sequence and the initial key, and the randomness and KGR are further improved

1.1. Notation and Outline. Unless otherwise specified, we use the following notations throughout the manuscript: Upper bold-face letters denote matrices and lower bold-face letters denote vectors. Light-face letters denote scalars. Numeral subscripts of matrices and vectors, if needed, represent their sizes. $\mathbf{I}$ denotes the identity matrix. Matrix superscript $(\cdot)^H$ denotes conjugate-transpose. The $E\{\cdot\}$ denotes ensemble expectation. The $\mathrm{vec}\{\bullet\}$ is the straightening operation by row.

The remainder of this paper is organized as follows: In Section 2, the system model and the related formulations are presented. The basic key generation steps are also introduced in this section. In Section 3, we describe the proposed RPP-WKG scheme in detail. The performance results are evaluated extensively in Section 4. In Section 5, we summarize the paper.

2. System Model

2.1. Channel Estimation. Figure 1 illustrates the system model of a wireless key generation system in the smart home: In an orthogonal frequency division multiplexing (OFDM) communication system, Alice and Bob establish secret keys in the time division duplex (TDD). They take advantage of the reciprocity and time variability of wireless channels to generate consistent security keys at both ends and update them continuously. Eve has a potential security threat to the communication between Alice and Bob.

During the channel sampling process, Alice and Bob alternately transmit pilots to each other. Alice sends a channel probing signal at time slot 1, and Bob receives the signal and stores it locally. Bob sends a channel probing signal at time slot 2, and Alice receives the signal and stores it. Meanwhile, Eve eavesdrops on the signals from Alice and Bob in two-time slots and tries to decrypt the message.

In this paper, we use the CSI as the channel measurements. We assume that the difference in measured values caused by delay and hardware fingerprints has been removed by methods such as interpolation transformation and hardware calibration. The matrices $\boldsymbol{H}^A$ and $\boldsymbol{H}^B$ of size $N \times K$ are defined as the channel measurement matrices of Alice and Bob after channel sampling, where N is the number of subcarriers and K is the number of samples. The relationship between $\boldsymbol{H}^A$ and $\boldsymbol{H}^B$ can be expressed as $\boldsymbol{H}^B = \boldsymbol{H}^A + \boldsymbol{W}$, where $\boldsymbol{W}$ represents the observation deviation caused by the measurement noise and the noise remaining in the calibration process. $\boldsymbol{W}$ is independent of $\boldsymbol{H}^A$ and considered to follow a complex Gaussian distribution.

2.2. Problem Formulation. According to the principle of channel reciprocity, the channel response of Alice and Bob should be highly correlated in practice. Since the ambient noises are usually considered to follow complex Gaussian distribution, the received channel measurements $\boldsymbol{H}^A$ and $\boldsymbol{H}^B$ should also be highly correlated. Based on the above theories, traditional wireless key generation methods allow Alice and Bob to extract the same secret keys by quantizing each channel measurement in $\boldsymbol{H}^A$ and $\boldsymbol{H}^B$, respectively. However, $\boldsymbol{H}^A$ and $\boldsymbol{H}^B$ could be easily affected by random ambient noise and nonsimultaneous channel probing, resulting in inconsistent quantization results and mismatched secret keys between two users.

Besides, the wireless environments between two legitimate devices change slowly in the smart home application scenario, which will result in the two adjacent channel samples in a coherence time being very similar. Figure 2 shows the CSI sampled under the quasistatic environments, which

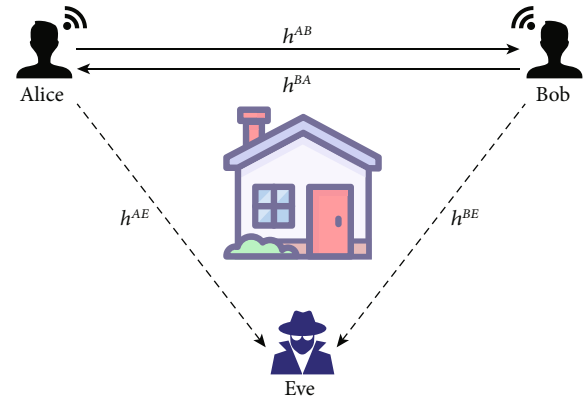


Figure 1: Channel estimation in a smart home.

is in an OFDM model with 56 subcarriers. The SNR in the scenario is 40 dB, and the sampling interval is 0.5 ms. The x-axis and y-axis of Figure 2 represent the real and imaginary parts of the CSI parameter. It can be seen that the CSI measured from two adjacent samples are very similar. This will result in the two generated keys being very similar or even identical. Overall, the above challenges demonstrate the need for a new key generation scheme to achieve efficient key generation in a quasistatic environment.

2.3. Basic Steps of Wireless Key Generation. Generally, the generation of secret keys based on channel measurements between two legitimate users includes four steps.

2.3.1. Channel Sampling. To initiate the key generation, Alice and Bob sample the channel through multiple rounds of probe packet exchanges [27, 28], each controlled within a coherence time to ensure channel reciprocity. After each user receives the probe packets, the channel measurements are extracted from the probe packets to construct reciprocal channel matrices $\boldsymbol{H}^A$ and $\boldsymbol{H}^B$ for Alice and Bob, respectively. The channel sampling process is completed after a sufficient number of probe packets are collected.

2.3.2. Quantization. After channel sampling, Alice and Bob need to adopt the same quantization scheme on channel measurements to obtain the initial keys. The quantization process is an analog-to-digital conversion process, which converts the CSI estimated by the legitimate communication parties into a sequence of key bits [29].

2.3.3. Information Reconciliation. Due to the interference, estimation error, and other facts, the initial keys quantized by Alice and Bob may have inconsistent bits. The main purpose of information reconciliation is to correct the inconsistent bits in the secret keys of the two legitimate users without divulging the key information as much as possible [30, 31]. After information reconciliation, inconsistent bits are eliminated and both Alice and Bob will obtain the consistent initial keys.

2.3.4. Privacy Amplification. Eve can eavesdrop on the information about the secret keys during the communication between Alice and Bob. Privacy amplification needs to be

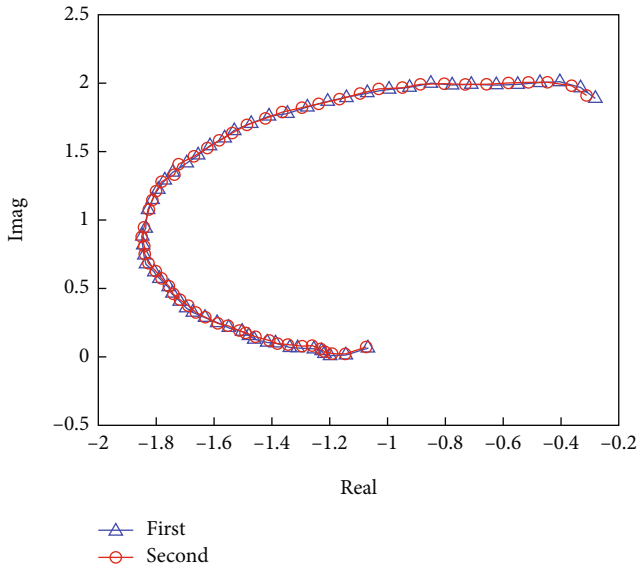


Figure 2: The results of two adjacent channel sampling.

performed to eliminate the information eavesdropped on by Eve [32–34]. After privacy amplification, Alice and Bob will obtain the final secret keys to encrypt their messages.

3. The Proposed RPP-WKG Scheme

3.1. RPP-Based Key Generation. The basic idea of the RPP-based wireless key generation algorithm is to permute channel measurements randomly and match the sorted channel measurement values between pairs of reciprocal users. Then the two reciprocal users perform the wireless key generation scheme according to the channel measurements after permutation and the agreed permutation order. As shown in Figure 3, Alice and Bob collect their respective channel measurement matrices $\boldsymbol{H}^A$ and $\boldsymbol{H}^B$ of size $N \times K$ in the channel sampling stage. Alice and Bob then perform PCA processing without interaction on their respective channel measurement matrices; the channel measurement matrices after PCA processing are $\boldsymbol{Y}^A$ and $\boldsymbol{Y}^B$ of size $P \times K$ and consist of P groups of samples. For the accuracy of statistical information, the number of sample groups and dimensions should satisfy $K \geq P$.

$$\begin{aligned} \boldsymbol{Y}^A &= \left[\boldsymbol{y}_1^A, \boldsymbol{y}_2^A, \cdots, \boldsymbol{y}_P^A\right]^H, \\ \boldsymbol{Y}^B &= \left[\boldsymbol{y}_1^B, \boldsymbol{y}_2^B, \cdots, \boldsymbol{y}_P^B\right]^H. \end{aligned} \tag{1}$$

After PCA processing, Alice applies random permutation to her channel measurement matrix $\boldsymbol{Y}^A$. The channel measurement matrix after permutation is $\widehat{\boldsymbol{Y}}^A$. The permutation order **PO** is determined by Alice according to the size of the matrix $\boldsymbol{Y}^A$. After the straightening transformation of $\widehat{\boldsymbol{Y}}^A$, Alice then sends the permutated channel measurements to Bob via a public channel without revealing the permutation order. Once receiving the permutated channel measurements, Bob can infer the permutation order by finding the correspondence between $\widehat{\boldsymbol{Y}}^A$ and his own channel measurement matrix $\boldsymbol{Y}^B$ through channel reciprocity. Bob then performs the same permutation on $\boldsymbol{Y}^B$ and gets the new channel measurement matrix $\widehat{\boldsymbol{Y}}^B$.

Meanwhile, Alice and Bob use their respective reconstructed signal matrices after random permutation $\widehat{\boldsymbol{Y}}^A$ and $\widehat{\boldsymbol{Y}}^B$ to perform the quantization operation. The permutation order **PO** participates in key generation as a source of randomness perturbation. Last, Alice and Bob perform the information reconciliation and privacy amplification on the origin secret keys to further eliminate occasional errors and generate secret keys with high randomness. The details of these components are elaborated as follows.

Some notions and their descriptions used in the following sections are listed in Table 1.

3.2. Sampling and Preprocessing Model. In the channel sampling phase, Alice and Bob each send pilots to each other and estimate CSI. A vector of length N for the k-th channel estimate can be written as

$$\boldsymbol{h}_k^u = \boldsymbol{h}_k + \boldsymbol{n}_k^u, \tag{2}$$

where $u = \{a, b\}$, a and b denote Alice and Bob, respectively, $\boldsymbol{h}^k$ follows complex Gaussian distribution, and $\boldsymbol{n}^u$ is independent and identically distributed zero-mean complex Gaussian noise with variance $E\{\boldsymbol{n}_k^u(n_k^u)^H\} = \sigma_n^2 \mathbf{I}_N$. After K channel samplings, Alice and Bob can construct the channel measurement matrix $\boldsymbol{H}^u$ as

$$\boldsymbol{H}^u = [\boldsymbol{h}_1^u, \boldsymbol{h}_2^u, \cdots, \boldsymbol{h}_K^u], \tag{3}$$

where $\boldsymbol{h}_k^u$ and $\boldsymbol{h}_l^u$ are assumed to be independent and identically distributed, $k, l \in [1, 2, \cdots, K]$. The subscript is omitted for simplicity, and we define the channel signal-to-noise ratio (SNR) as

$$\mathrm{SNR} = \frac{E\{\boldsymbol{h}^H \boldsymbol{h}\}}{N\sigma_n^2}. \tag{4}$$

After channel sampling, Alice and Bob will get their respective channel measurement matrices $\boldsymbol{H}^A$ and $\boldsymbol{H}^B$ for further preprocessing. The signal preprocessing process is divided into two steps: PCA processing without interaction, random segmentation, and permutation.

3.2.1. PCA Processing without Interaction. Figure 4 shows the process of PCA. In PCA processing without interaction, Alice and Bob calculate the transformation matrices according to the following steps:

(1) Alice and Bob perform eigenvalue decomposition of their covariance matrices $\boldsymbol{R}^A$ and $\boldsymbol{R}^B$, respectively, where $\boldsymbol{\Lambda}^A$, $\boldsymbol{\Lambda}^B$ are eigenvalue matrices and $\boldsymbol{U}^A$, $\boldsymbol{U}^B$

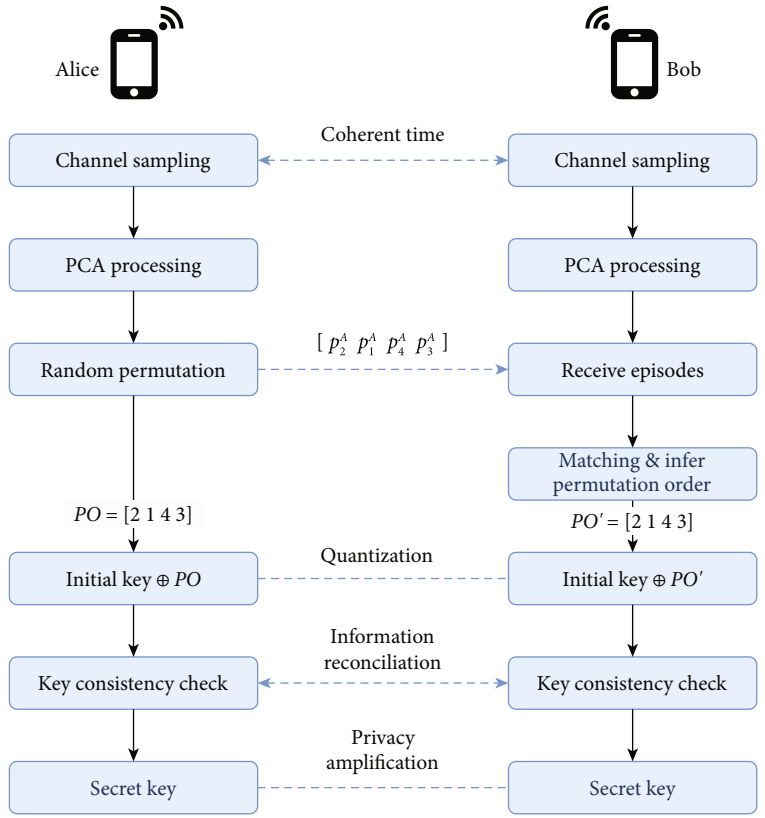


Figure 3: System flow chart.

Table 1: Notion list.

Notation	Descriptions
H	Channel measurement matrix
W	Observation deviation
Y	Channel measurement matrix after PCA processing
R	Covariance matrix
U	Eigenvector matrix
Λ	Eigenvalue matrix
T	Transformation matrix
P	Segmented channel measurement sequence
PO	Permutation order
RS	Random perturbation sequence
IK	Initial key
PK	Perturbed key

are eigenvector matrices. $\boldsymbol{R}^A$ and $\boldsymbol{R}^B$ are given by

$$\begin{aligned}\boldsymbol{R}^A &= \boldsymbol{U}^A \boldsymbol{\Lambda}^A \left(\boldsymbol{U}^A\right)^H,\\ \boldsymbol{R}^B &= \boldsymbol{U}^B \boldsymbol{\Lambda}^B \left(\boldsymbol{U}^B\right)^H.\end{aligned} \tag{5}$$

(2) Alice and Bob sort their eigenvalue matrices and eigenvector matrices in descending order of eigenvalues, respectively. The eigenvalue matrices after sorting are $\tilde{\boldsymbol{\Lambda}}^A, \tilde{\boldsymbol{\Lambda}}^B$, and the eigenvector matrices after sorting are $\tilde{\boldsymbol{U}}^A, \tilde{\boldsymbol{U}}^B$.

(3) Alice and Bob select the first P eigenvectors of their eigenvector matrices to construct the transformation matrices $\boldsymbol{T}^A$ and $\boldsymbol{T}^B$, where P is the number of eigenvectors agreed upon by Alice and Bob in advance

Alice and Bob transform their channel measurement matrices $\boldsymbol{H}^A$ and $\boldsymbol{H}^B$ by using the transformation matrices; the matrices after signal reconstruction are $\boldsymbol{Y}^A$, $\boldsymbol{Y}^B$, which are given by

$$\begin{aligned}\boldsymbol{Y}^A &= \left(\boldsymbol{T}^A\right)^H \boldsymbol{H}^A,\\ \boldsymbol{Y}^B &= \left(\boldsymbol{T}^B\right)^H \boldsymbol{H}^B,\end{aligned} \tag{6}$$

where $\boldsymbol{Y}^A = [\boldsymbol{y}_1^A, \boldsymbol{y}_2^A, \cdots, \boldsymbol{y}_K^A]$ and $\boldsymbol{Y}^B = [\boldsymbol{y}_1^B, \boldsymbol{y}_2^B, \cdots, \boldsymbol{y}_K^B]$ are the reconstructed signal matrices.

3.2.2. Random Segmentation and Permutation. To further increase the complexity and randomness of the collected channel measurements, we perform a random permutation on the channel measurement matrices $\boldsymbol{Y}^A$ and $\boldsymbol{Y}^B$. Figure 5 shows the effect of permutation on the CSI measurements. For ease of calculation and matching, Alice and Bob straighten $\boldsymbol{Y}^A$ and $\boldsymbol{Y}^B$ by row to make them two $1 \times S$, (S

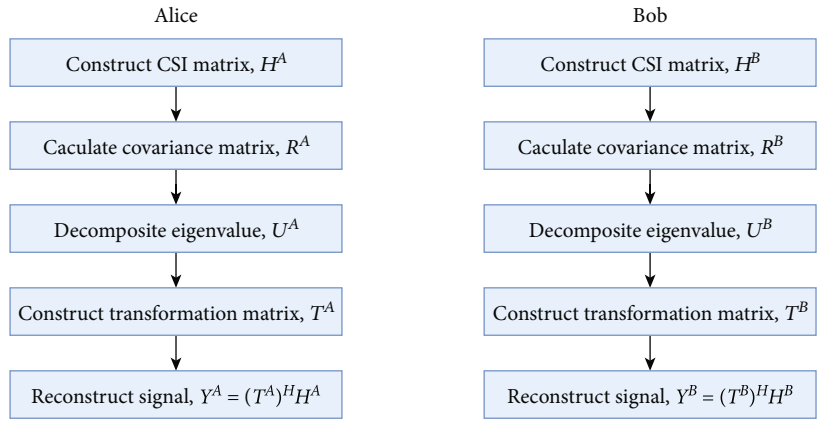


Figure 4: PCA processing steps of CSI.

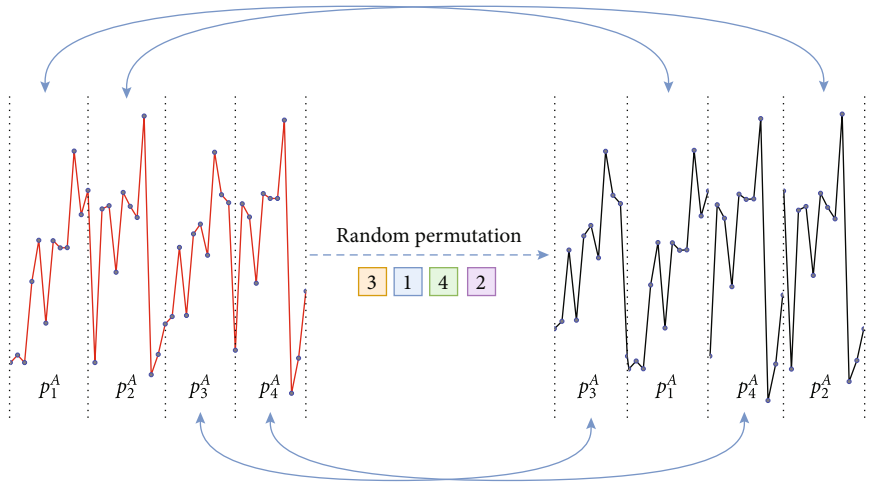


Figure 5: Random permutation on CSI.

$= P \times K$) dimensional vectors $\boldsymbol{v}^A$ and $\boldsymbol{v}^B$

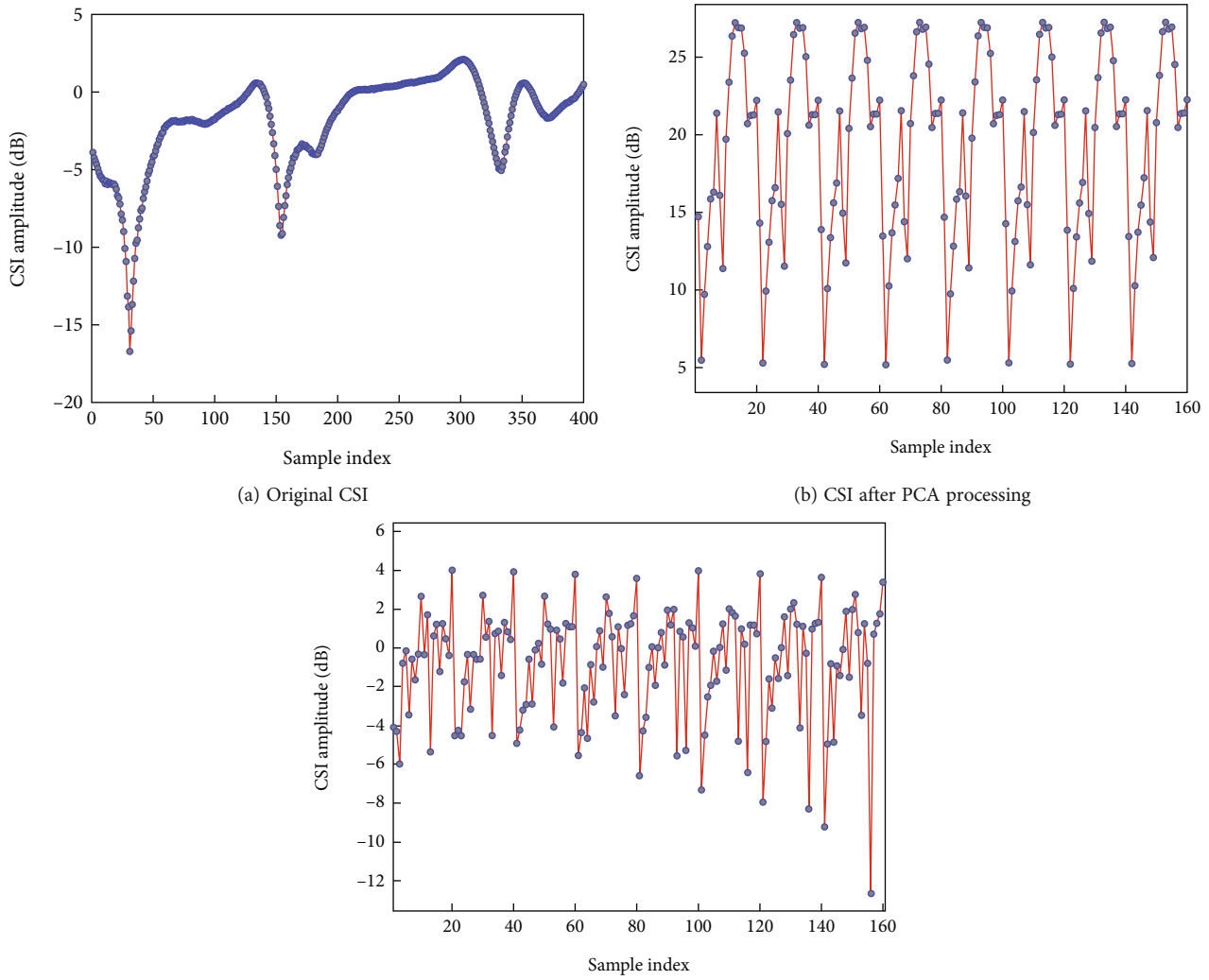
$$\begin{aligned} \boldsymbol{v}^A &= \mathrm{vec}\{\boldsymbol{Y}^A\}, \\ \boldsymbol{v}^B &= \mathrm{vec}\{\boldsymbol{Y}^B\}, \end{aligned} \tag{7}$$

where vec$\{\bullet\}$ is the straightening operation by row.

Alice and Bob segment their vectors $\boldsymbol{v}^A$ and $\boldsymbol{v}^B$ into M episodes of the same length, $\boldsymbol{P}^A = [\boldsymbol{p}_1^A, \boldsymbol{p}_2^A, \cdots, \boldsymbol{p}_M^A]$ and $\boldsymbol{P}^B = [\boldsymbol{p}_1^B, \boldsymbol{p}_2^B, \cdots, \boldsymbol{p}_M^B]$, where $\boldsymbol{p}_m^A$ and $\boldsymbol{p}_m^B$ are the m^{th} episode with length $L = S/M$. Given the segmented channel measurement sequence $\boldsymbol{P}^A$, Alice comes up with a permutation order $\mathbf{PO} = [k_1, k_2, \bullet\bullet\bullet, k_M]$ and applies permutation to $\boldsymbol{P}^A$ to create a new channel measurement sequence $\widehat{\boldsymbol{P}}^A = [\boldsymbol{p}_{k_1}^A, \boldsymbol{p}_{k_2}^A, \cdots, \boldsymbol{p}_{k_M}^A]$, where $k_m \in [1, M]$ is the original index of the episode $\boldsymbol{p}_{k_m}^A$ in $\boldsymbol{P}^A$. Alice then sends $\widehat{\boldsymbol{P}}^A$ to Bob without revealing the permutation order via the public channel, which potential attackers listen to. Each $\boldsymbol{p}_k^B$ in $\boldsymbol{P}^B$ can always find the reciprocal $\boldsymbol{p}_{k_m}^A$ in $\widehat{\boldsymbol{P}}^A$ even permutated due to channel reciprocity. Bob can infer the permutation order $\mathbf{PO} = [k_1, k_2, \bullet\bullet\bullet, k_M]$ of $\widehat{\boldsymbol{P}}^A$ by finding the perfect match between the episodes in $\widehat{\boldsymbol{P}}^A$ and $\boldsymbol{P}^B$ with the minimum discrepancy and use **PO** as part of the secret key. Bob performs the same permutation on $\boldsymbol{P}^B$ and obtains the new sequence $\widehat{\boldsymbol{P}}^B$ after inferring the **PO**. Since the original channel measurement sequence $\boldsymbol{P}^A$ was not made public, the permutation order $\mathbf{PO} = [k_1, k_2, \bullet\bullet\bullet, k_M]$ is a secret between Alice and Bob and is unknown to the potential attackers. Determining the permutation order is also equal to achieving a key agreement between Alice and Bob.

Then, Alice and Bob restore the vectors $\widehat{\boldsymbol{P}}^A$ and $\widehat{\boldsymbol{P}}^B$ to matrices $\widehat{\boldsymbol{Y}}^A$ and $\widehat{\boldsymbol{Y}}^B$ according to the initial segment length, where $\widehat{\boldsymbol{Y}}^A$ and $\widehat{\boldsymbol{Y}}^B$ can be seen as being randomly permutated. As the example shown in Figure 6, the channel measurement matrix after random permutation will have lower regularity and more complexity.

3.3. Matching Algorithm. In order to reduce the time cost of inferring the permutation order, we use the minimum weight bipartite graph matching to find the perfect match. Episodes in $\widehat{\boldsymbol{P}}^A$ and $\boldsymbol{P}^B$ are considered as vertices of a



(a) Original CSI

(b) CSI after PCA processing

(c) CSI after PCA and permutation

FIGURE 6: CSI after different preprocessing schemes.

weighted undirect graph G, and vertices are connected by edges. The edges only exist between the vertices of $\widehat{\boldsymbol{P}}^A$ and $\boldsymbol{P}^B$ in G (i.e., no edge connects the vertices within $\widehat{\boldsymbol{P}}^A$ or $\boldsymbol{P}^B$). The weight of the edges can be denoted as $w_{A,B}(k_m, k) = \|\boldsymbol{p}^A_{k_m} - \boldsymbol{p}^B_k\|$, where $k_m, k \in [1, M]$ and $\|\bullet\|$ represents taking the absolute value. A perfect match in G consists of a set of vertex-disjoint edges with every vertex of G. A perfect match can be always found in G to satisfy the reciprocal mapping between the channel measurement matrices of Alice and Bob due to the channel reciprocity. The sum of weights of the match between Alice and Bob can be denoted as $W_{A,B} = \sum_{k_m,k}^{M} w_{A,B}(k_m, k)$, where $k_m, k \in [1, M]$. The minimum weight matching problem is to find the match with the smallest sum of weights. The minimum weight matching can be transformed into the maximum weight matching problem after converting the weight $w_{A,B}(k_m, k)$ to $\widehat{w}_{A,B}(k_m, k) = C - w_{A,B}(k_m, k)$, where $C \geq \max(w_{A,B}(k_m, k))$. We use the Kuhn-Munkres algorithm to solve the maximum weight matching problem. To minimize the summation of its associated weights, the following linear programming with integer constraints relaxation is formulated:

$$\begin{aligned} \min \quad & \sum_{k_m,k}^{M} (w_{A,B}(k_m, k) - l_A(k_m) - l_B(k)), \\ \text{s.t.} \quad & l_A(k_m) \geq 0, l_B(k) \geq 0, \\ & k_m, \quad k \in [1, M], \end{aligned} \tag{8}$$

where $l_A(k_m), l_B(k)$ are the feasible label with the value equal to the weight of the perfect match output by the algorithm as follows:

$$\begin{aligned} \max \quad & \sum_{k_m \in [1,M]} l_A(k_m) + \sum_{k \in [1,M]} l_B(k), \\ \text{s.t.} \quad & l_A(k_m) + l_B(k) \leq w_{A,B}(k_m, k), \quad \forall (k_m, k) \in E, \end{aligned} \tag{9}$$

where E denotes all the edges in G. Any feasible prime label in a perfect match has a weight as large as the value of any

feasible dual-labeling. If $l_A(k_m) + l_B(k) = w_{A,B}(k_m, k)$, the edge (k_m, k) is tight. A match is optimal if it only uses tight edges when given any dual feasible label.

To find the perfect match, a random feasible dual label l is used to find a maximum-cardinality matching that uses tight edges. The process is over if the match is perfect. If not, the dual label is updated and the process continues until an optimal match is found. After the graph matching, Bob infers the permutation order $\mathbf{PO}' = [k_1', k_2', \bullet\bullet\bullet, k_M']$, where $\mathbf{PO} = \mathbf{PO}'$.

3.4. Wireless Key Generation Based on Random Perturbation. The wireless key generation process based on permutation and matching is divided into the following three steps: obtaining the initial secret key, generating and splicing the random perturbation sequence, and performing the XOR operation.

In this paper, after the preprocessing, different components of channel measurements have different SNRs, which can be expressed as

$$\mathrm{SNR}_i = \frac{\lambda_i^2}{\sigma_n^2}. \tag{10}$$

SNR_i represents the SNRs of different components. As the index of components increases, the SNR decreases. To make full use of the high SNR of dominant components, we employ flexible quantization levels in the quantization algorithm to quantify the initial keys.

The first step is to obtain the initial keys. Alice and Bob get their respective initial keys IK^A and IK^B after the quantization process on their channel measurement matrices $\widehat{\boldsymbol{Y}}^A$ and $\widehat{\boldsymbol{Y}}^B$. The length of the initial keys is L_1.

The second step is to generate the random perturbation sequence through the negotiated permutation order $\mathbf{PO} = [k_1, k_2, \bullet\bullet\bullet, k_M]$. First, convert **PO** into a binary bit sequence RS, and the length of the converted bit sequence RS is $L_2 = c \times M$, where c is the length of each binary bit sequence converted by $k_m, k_m \in [1, M]$ in **PO**. RS then needs to be spliced into RS'. Repeatedly splicing the stochastic perturbation sequence until it is equal to the key length L_1, that is,

$$L_1 = k \times L_2 + k', \tag{11}$$

where k is a positive integer and $0 < L_2 < L_1$.

The last step is to XOR the random perturbation sequence RS' and the initial secret keys. Alice and Bob perform XOR operation between their initial key $\mathrm{IK}^A, \mathrm{IK}^B$ and the perturbation sequence RS' to get the perturbed key PK^A and PK^B, which are given by

$$\begin{aligned} \mathrm{PK}^A &= \mathrm{IK}^A \oplus \mathrm{RS}', \\ \mathrm{PK}^B &= \mathrm{IK}^B \oplus \mathrm{RS}'. \end{aligned} \tag{12}$$

Compared with the key sequence before random perturbation, the number of secret keys does not increase. However, the method based on random perturbation reduces the correlation between the two adjacent sets of secret keys, so it can effectively increase the KGR.

Then Alice and Bob perform information reconciliation on their perturbed keys PK^A and PK^B. The main purpose of information reconciliation is to correct the inconsistent bits in the key bit sequences without divulging the key information as much as possible. After information reconciliation, Alice and Bob will agree on an error-free secret key.

Table 2: Simulation parameters.

Parameter	Value
Channel model	TGn
Scenario	NLOS
SNR	40 dB
Bandwidth	20 MHz
PSDU length	20 bytes
Carrier number	56
RMS delay spread	15 ns
Channel coding	BCC
Maximum delay	80 ns
Sampling interval	0.5 ms

4. Performance Evaluation

To evaluate the performance of our proposed scheme, we conduct numerical simulations. We build the simulation model based on a Matlab implementation of the TGn multipath fading channel. The detailed parameters are summarized in Table 2. Alice and Bob are randomly distributed, and the distance between them is greater than or equal to five meters. We focus on the non-line-of-sight (NLOS) scenario. An OFDM model with 56 subcarriers is utilized. We sample 400 independent channel vectors to perform the key generation process.

In this section, we evaluate the performance of the RPP-WKG scheme and compare it with the wireless key generation without processing (named as "Initial"), and with the wireless key generation scheme based on PCA and without random permutation and perturbation (named as "PCA-WKG"). We evaluate the key performance from 4 aspects: the KGR, the KMR, the correlation between the secret keys, and the randomness of the keys.

4.1. Key Generation Rate. The KGR reflects the speed of the wireless key generation. The actual wireless key generation system has high requirements on the KGR. If the KGR is too low, the time cost required for wireless key generation will be too high, which is not suitable for practical applications. In this section, we test the KGR of the RPP-WKG scheme in the case of different SNRs. The test results are shown in Figure 7. As the SNR increases, the KGR gradually increases. The KGR can reach 480 bits/packet when the SNR is 45 dB. We also compare the KGR performance of the RPP-WKG scheme with the PCA scheme without random permutation and perturbation. The comparison results show

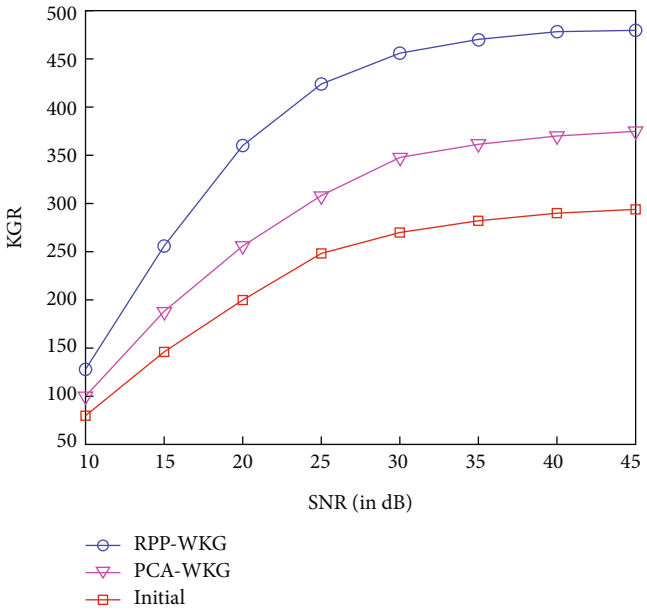


Figure 7: KGR performance under the impact of different SNRs.

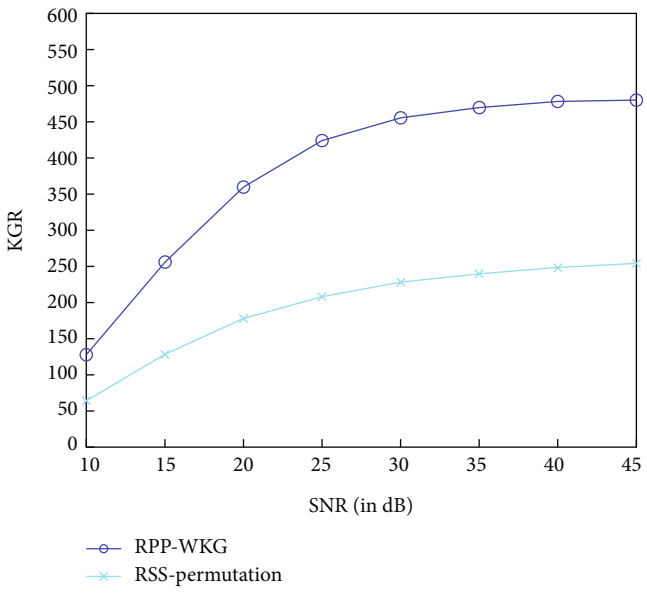


Figure 8: KGR performance for different channel measurements.

that the KGR can be further improved by the random permutation and perturbation scheme.

In addition, we compare the performance of our proposed RPP-WKG scheme with the scheme based on RSS permutation. Based on the comparison results shown in Figure 8, our RPP-WKG scheme will achieve a higher KGR by using CSI as the channel measurements than the traditional RSS permutation-based scheme.

4.2. Key Mismatch Rate. The KMR reflects the inconsistency rate of the secret keys quantified, respectively, by Alice and Bob. Due to the influence of ambient noise and other factors,

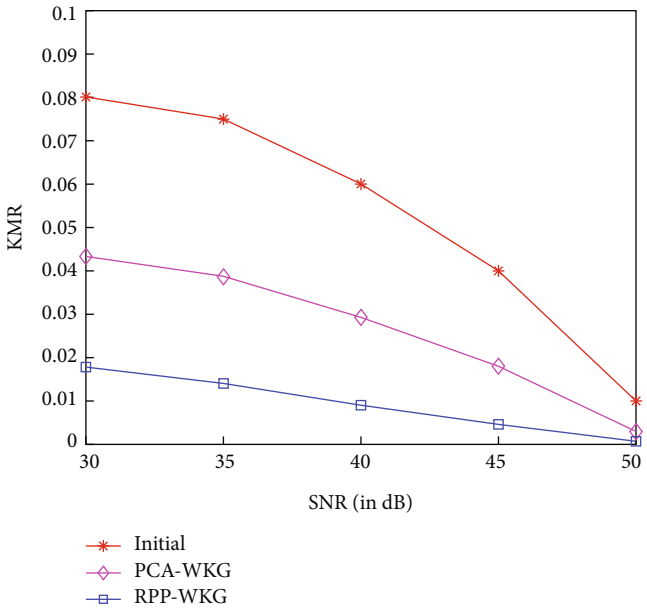


Figure 9: KMR performance under the impact of different SNRs.

there will be certain errors in the bit sequences quantized by Alice and Bob according to their respective CSI. Figure 9 shows the KMR performance of the initially generated secret keys and the secret keys after the RPP-WKG scheme. As the SNR increases, the KMR gradually decreases. According to the comparison results, the RPP-WKG scheme achieves a lower KMR. Figure 10 shows the KMR performance of secret keys generated by the RPP-WKG scheme under the impact of different episode numbers. As the number of permutation episodes increases, the KMR of the secret keys will increase significantly.

4.3. Correlation between the Secret Keys. The correlation between the secret keys represents the degree of linear correlation between adjacent sets of keys. We use the Pearson correlation coefficient [35–37] to calculate the correlation between keys. The Pearson correlation coefficient is defined as

$$\rho_{XY} = \frac{E(XY) - E(X)E(Y)}{\sqrt{E(X^2) - E^2(X)}\sqrt{E(Y^2) - E^2(Y)}}, \quad (13)$$

where X and Y are the two sets of secret key sequences.

The correlation coefficient between two sets of secret keys is a value between -1 and 1. The stronger the correlation between the two sets of secret keys, the closer the absolute value of the correlation coefficient is to 1. If the correlation coefficient is equal to 0, it indicates that there is no linear correlation between the two sets of secret keys.

In this section, we first calculate the correlation coefficient between the secret keys of the three schemes. We display the calculation results in the form of heat maps. The horizontal and vertical coordinates represent the index number of the keys, and the colour of each dot represents the correlation between the secret keys. The yellower the colour, the higher the correlation between the secret keys. The bluer

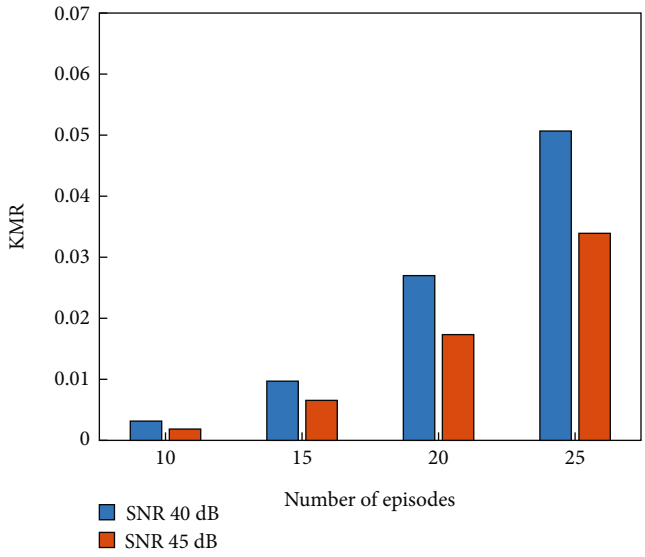


Figure 10: KMR performance of RPP-WKG scheme under the impact of different episode numbers.

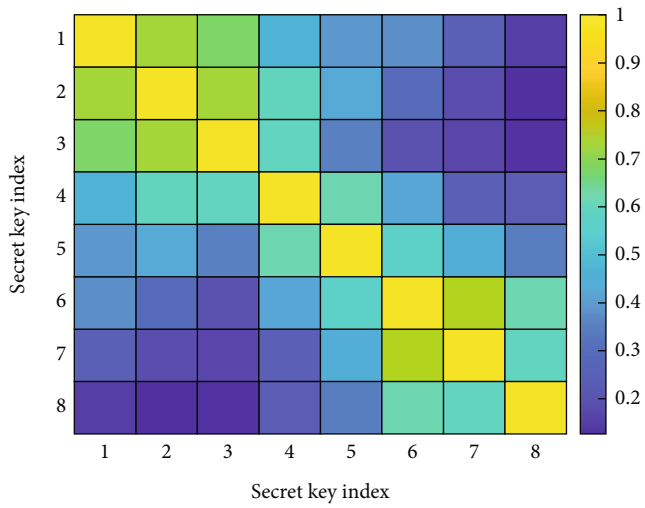


Figure 11: Correlation between initial secret keys.

the colour, the lower the correlation between the secret keys. We test the correlation between the initial secret keys, the secret keys after PCA processing, and the secret keys after random permutation and perturbation. According to the test results, the correlation between initial secret keys is the highest in Figure 11, and the correlation between secret keys after random permutation and perturbation is the lowest. Figure 12 shows that the secret keys quantized by the CSI after PCA processing can obtain a lower correlation than the initial secret keys. Figure 13 shows the advantage of the random permutation and perturbation scheme in the process of key generation. The test results reflect the RPP-WKG scheme has an obvious effect on reducing the correlation between secret keys.

We also calculate how the correlation coefficient changes as the number of episodes increases. As shown in Figure 14, once the CSI is randomly permuted and perturbed, the correlation coefficient between secret keys will drop significantly. As the number of permutation episodes increases, the correlation coefficient between secret keys will slowly decrease. When the number of permutation episodes is greater than 10, a good correlation reduction effect can be obtained. Considering that as the number of permutation episodes increases, the time cost to find the correct permutation order using the matching algorithm will also increase, and the number of permutation episodes should not be set too large.

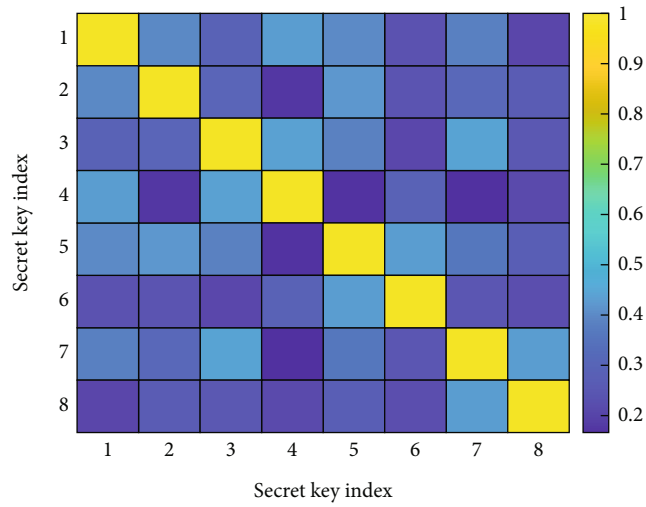


Figure 12: Correlation between secret keys after PCA processing.

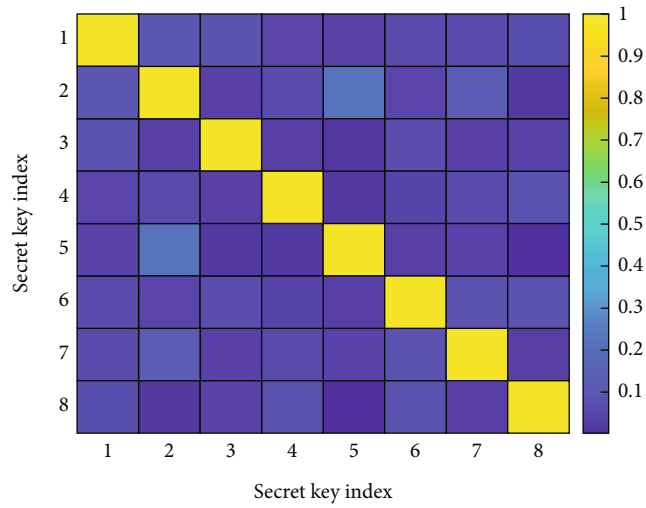


Figure 13: Correlation between secret keys of RPP-WKG scheme.

4.4. Randomness of Secret Keys. The randomness of the key is an important standard to measure the performance of the secret keys. The definition of key randomness is the uniformity of the distribution of 0 and 1 in the generated secret keys. The higher the randomness of the key, the more difficult it is for the eavesdropper to guess the key. To ensure that the secret keys generated are substantially random, the standard randomness test suite from NIST is employed to

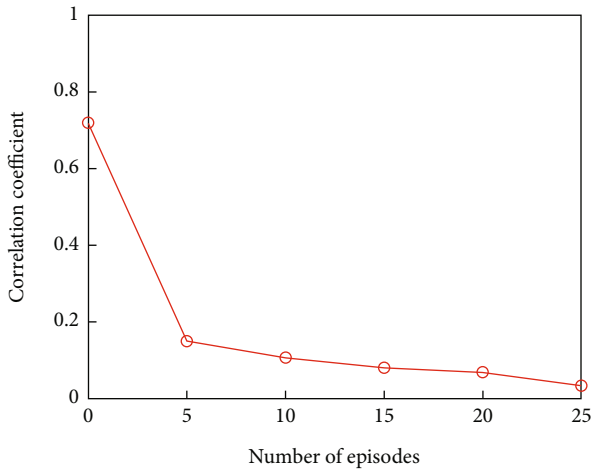


Figure 14: Correlation with the number of episodes.

Table 3: NIST randomness test of RPP-WKG scheme.

Test	p value
Frequency test	0.729034
Frequency test within a block	0.731615
Run test	0.902544
Longest run of ones in a block	0.773102
Discrete Fourier transform	0.791081
Nonoverlapping temple match	0.999959
Serial test	0.561915
Approximate entropy test	1.0
Cumulative sums (forward) test	0.700062
Cumulative sums (reverse) test	0.407770

Table 4: NIST randomness test of different schemes.

Test	Initial	PCA-WKG	RSS-permutation	RPP-WKG
1	0.204023	0.448213	0.446671	0.729034
2	0.457833	0.385534	0.489325	0.731615
3	0.170472	0.395013	0.576431	0.902544
4	0.057768	0.731615	0.663982	0.773102
5	0.063689	0.426776	0.512378	0.791081
6	0.678439	0.827952	0.843564	0.999959
7	0.343128	0.498961	0.378615	0.561915
8	1.0	1.0	1.0	1.0
9	0.211935	0.368282	0.397446	0.700062
10	0.166529	0.297799	0.337512	0.407770

verify the effectiveness of the secret keys extracted after the wireless key generation scheme based on permutation and perturbation [38, 39]. The output result of each test is an indicator called the p value. A tested secret key sequence passes a test when the p value is greater than the threshold, usually chosen as 0.01. We run 10 NIST tests on the secret keys generated on the RPP-WKG scheme, as listed in Table 3. All the results pass the tests, indicating the randomness of the generated secret keys is sufficient for practical key generation. In addition, in this section, we also compare the randomness of the initial secret keys, the secret keys quantified after PCA processing, the secret keys generated by RSS, and the secret keys generated by the RPP-WKG scheme. Table 4 shows the comparison results: the secret key generation scheme based on random permutation and perturbation has obvious advantages in the tests.

5. Conclusions

In this paper, we propose an efficient wireless key generation scheme based on random permutation and perturbation, which achieves high randomness and a high KGR between the legitimate users, Alice and Bob, in a quasistatic environment. In the proposed RPP-WKG scheme, we can mitigate the impact of the quasistatic channel and achieve secret keys with high randomness and low correlation. The efficient and secure permutation method allows legitimate users to perform the same random permutation on their respective CSI to acquire new random sources with random and great fluctuations. The minimum weight-based matching method helps legitimate users to obtain an agreement on the permutation order of CSI without revealing it. The random perturbation generation method based on the permutation order improves the randomness and reduces the correlation of secret keys. Simulation results show that the proposed RPP-WKG scheme can efficiently improve the randomness and KGR of the generated secret keys in a quasistatic environment.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the National Key R&D Program of China (2020YFE0200600).

References

[1] B. Mao, Y. Kawamoto, and N. Kato, "Ai-based joint optimization of qos and security for 6G energy harvesting internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7032–7042, 2020.

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

[3] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5g and beyond wireless

networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 55–61, 2019.

[4] A. Bunin, Z. Goldfeld, H. H. Permuter, S. S. Shitz, P. Cuff, and P. Piantanida, "Key and message semantic-security over state-dependent channels," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1541–1556, 2018.

[5] H. Mack and T. Schroer, "Security midlife crisis: building security in a new world," *IEEE Security & Privacy*, vol. 18, no. 4, pp. 72–74, 2020.

[6] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2011, https://www.amazon.com/Cryptography-Network-Security-Principles-Practice/dp/0133354695.

[7] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.

[8] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pp. 128–139, San Francisco, California USA, 2008.

[9] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.

[10] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *2010 Proceedings IEEE INFOCOM*, pp. 1–9, San Diego, CA, USA, 2010.

[11] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: a review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[12] A. Salam, M. C. Vuran, and S. Irmak, "A statistical impulse response model based on empirical characterization of wireless underground channels," *IEEE Transactions on Wireless Communications*, vol. 19, no. 9, pp. 5966–5981, 2020.

[13] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Transmit beamforming for layered physical layer security," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 9747–9760, 2019.

[14] R. Chopra, C. R. Murthy, and R. Annavajjala, "Physical layer security in wireless sensor networks using distributed co-phasing," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2662–2675, 2019.

[15] Á. Vázquez-Castro and M. Hayashi, "Physical layer security for rf satellite channels in the finite-length regime," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 981–993, 2018.

[16] Z. Li, Q. Pei, I. Markwood, Y. Liu, and H. Zhu, "Secret key establishment via rss trajectory matching between wearable devices," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 802–817, 2017.

[17] H. Zhao, Y. Zhang, X. Huang, Y. Xiang, and C. Su, "A physical-layer key generation approach based on received signal strength in smart homes," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 4917–4927, 2021.

[18] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, and P. Thomas, "Physical layer secret-key generation with discreet cosine transform for the internet of things," in *2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, Paris, France, 2017.

[19] H. Liu, Y. Wang, Y. Ren, and Y. Chen, "Bipartite graph matching based secret key generation," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*, pp. 1–10, Vancouver, BC, Canada, 2021.

[20] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, "Quasi-static multiple-antenna fading channels at finite blocklength," *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 4232–4265, 2014.

[21] Y. Xi, A. Burr, J. Wei, and D. Grace, "A general upper bound to evaluate packet error rate over quasi-static fading channels," *IEEE Transactions on Wireless Communications*, vol. 10, no. 5, pp. 1373–1377, 2011.

[22] T. Lu, L. Chen, J. Zhang, K. Cao, and A. Hu, "Reconfigurable intelligent surface assisted secret key generation in quasi-static environments," *IEEE Communications Letters*, vol. 26, no. 2, pp. 244–248, 2021.

[23] M. He, J. Xu, W. Xu, H. Shen, N. Wang, and C. Zhao, "RIS-assisted quasi-static broad coverage for wideband mmwave massive MIMO systems," 2022, https://arxiv.org/abs/2203.00400.

[24] Y. Huang, L. Jin, H. Wei, Z. Zhong, and S. Zhang, "Fast secret key generation based on dynamic private pilot from static wireless channels," *China Communications*, vol. 15, no. 11, pp. 171–183, 2018.

[25] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.

[26] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Transactions on Communications*, vol. 66, no. 7, pp. 3022–3034, 2018.

[27] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on pid controller," *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1842–1852, 2012.

[28] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for tdd-ofdm systems over fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5176–5186, 2017.

[29] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 205–215, 2010.

[30] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "Smokegrenade: an efficient key generation protocol with artificial interference," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1731–1745, 2013.

[31] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1484–1497, 2012.

[32] S. Wang and C. Li, "Discrete double-bit hashing," *IEEE Transactions on Big Data*, vol. 8, pp. 482–494, 2019.

[33] R.-C. Tu, X.-L. Mao, B. Ma et al., "Deep cross-modal hashing with hashing functions and unified hash codes jointly learning," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, pp. 560–572, 2020.

[34] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *2011 Proceedings IEEE INFOCOM*, pp. 1422–1430, Shanghai, China, 2011.

[35] T. Peng, W. Dai, and M. Z. Win, "Efficient and robust physical layer key generation," in *MILCOM 2019-2019 IEEE Military*

Communications Conference (MILCOM), pp. 1–6, Norfolk, VA, USA, 2019.

[36] Z. Ji, Z. He, Y. Zhang, and X. Chen, "A two-step decorrelation method on time-frequency correlated channel for secret key generation," in *2018 IEEE wireless communications and networking conference (WCNC)*, pp. 1–6, Barcelona, Spain, 2018.

[37] F. Passerini and A. M. Tonello, "Secure phy layer key generation in the asymmetric power line communication channel," *Electronics*, vol. 9, no. 4, p. 605, 2020.

[38] H. Tan, D. Ostry, and S. Jha, "Exploiting multiple side channels for secret key agreement in wireless networks," in *Proceedings of the 19th International Conference on Distributed Computing and Networking*, pp. 1–10, Varanasi, India, 2018.

[39] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Booz-Allen and Hamilton Inc Mclean Va, Tech. Rep, 2001.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5328007, 9 pages
https://doi.org/10.1155/2022/5328007

Research Article

Differentiated Reception Modes Based Multiple Access

Z. Chang,[1] **P. Lyu**,[2] **and B. Peng**[2]

[1]*School of Communications and Information Engineering & School of Artificial Intelligence, Xi'an University of Posts & Telecommunications, China*
[2]*School of Cyber Engineering, Xidian University, China*

Correspondence should be addressed to Z. Chang; changzhixian@xupt.edu.cn

Received 18 July 2022; Accepted 22 September 2022; Published 11 October 2022

Academic Editor: Xiaoying Liu

In recent years, the continuous increase in wireless data services and users' traffic demand has been imposing great challenges on traditional multiple access control (MAC) methods. Some existing MAC techniques improve the communication system's spectral efficiency (SE) via signal processing based cochannel interference (CCI) management. However, no interference management (IM) is free, i.e., its realization is based on the consumption of some communication resources, such as power and degree-of-freedom (DoF), which can also be used for the user's desired data transmission. To lessen the resource cost for IM-based MAC, we exploit interactions among multiple wireless signals to propose a new MAC method, namely, Differentiated Reception Modes based Multiple Access (DRM-MA), in this paper. Under DRM-MA, a central control unit (CCU) is adopted to manage and pair multiple transmitting antennas with their serving receivers (Rxs). The CCU first calculates the phase difference of signals sent from each candidate antenna and perceived by the two receiving antennas of an Rx based on the locations of the transmitting antenna and Rx. Then, the CCU selects and pairs a proper transmitting antenna with each Rx, so that various Rxs can adopt either additive or subtractive reception mode to postprocess the signals received by its two antennas to realize in-phase desired signal construction and inverse-phase interference destruction. DRM-MA can avoid transmission performance loss incurred by signal processing-based IM. Our theoretical analysis and simulation results have shown that DRM-MA can enable concurrent data transmissions of multiple antenna-receiver pairs and output a high system's SE.

1. Introduction

With the continuous growth of users' demand for mobile data services, wireless communication technology has been developing rapidly. Compared to previous communication systems, 5G (the fifth generation) is expected to provide a larger system capacity, higher data rate, lower latency, and more transmission reliability [1]. The Internet of Things (IoT) is a typical application scenario in the 5G era and has been under fast development in recent years, yielding explosive growth of various IoT terminals. It is estimated that by the year 2025 there will be more than 41.6 billion IoT devices connected to the network [2]. The increase of IoT devices and the massive connections of IoT networks impose higher requirements on future wireless communication systems. Due to limited communication resources, efficiently supporting more users with high data transmission quality simultaneously has become a hot topic that is worthy of a thorough investigation.

Traditional orthogonal multiple access (OMA) technologies, including frequency division multiple access (FDMA), time division multiple access (TDMA), code division multiple access (CDMA), and space division multiple access (SDMA), allocate various types of communication resources, such as frequencies, time slots, code-words, and spatial subchannels, to multiple users in an orthogonal way to avoid cochannel interference (CCI) among concurrent data transmissions, hence, realizing resource sharing among multiple users [3]. However, the above OMA methods are featured as fixed resource allocation and have low resource utilization. Therefore, due to the limitation of communication resources (especially the spectrum resource) and the rapid increase in the number of wireless users, OMA is facing a great challenge. By dynamically sharing frequency resources

to multiple users, ALOHA, carrier sense multiple access (CSMA) [4, 5], and cognitive radio (CR) [6] have been proposed successively, with which the spectrum utilization can be effectively improved. However, such random/opportunistic MACs have collision and transmission failure problems, hence incurring resource waste, to remedy this deficiency, additional cost, and resource consumption (e.g., retransmission and reservation overhead) result.

In recent years, nonorthogonal multiple access (NOMA), which is regarded as a promising MAC method that can be applied in 5G, has been invented and attracted a lot of attention. Uplink NOMA [7] allows multiple transmitters (Txs) to transmit to their common receiver (Rx) via the same frequency channel in a non-orthogonal way. The Rx can employ successive interference cancellation (SIC) [8] to mitigate CCI. However, SIC has an error propagation problem [9] which incurs a high bit-error rate (BER) of the subsequently decoded user data, thus limiting its application. By noting that increasing the number of receiving antennas can strengthen Rx's spatial signal processing capability, and the data carried in multiple concurrent signals can be distinguished and recovered in the spatial domain [10], some researchers incorporate multiantenna with SIC to balance the complexity and BER performance of communication systems [11, 12]. However, due to equipment constraints such as hardware size and complexity, it is impractical to increase the number of receiving antennas without limit, especially for mobile devices. Therefore, some researchers exploit interactions among multiple wireless signals to design multiuser communication schemes. The authors of [13, 14] proposed interference neutralization (IN) in which the desired Tx constructs and sends a neutralizing signal of the same amplitude and opposite phase with respect to the interference perceived by its serving Rx so that the neutralizing signal can counteract the interference at the Rx. Since the power cost for generating the neutralizing signal is high, [15] designed interference steering (IS). By constructing a steering signal at the serving Tx, only the projection of the interference on the desired transmission at the interfered Rx is mitigated, hence, yielding the steered disturbance to be orthogonal to the desired signal.

Based on the above discussion, we will propose a novel MAC method, called Differentiated Reception Modes based Multiple Access (DRM-MA) in this paper. By exploiting interactions among wireless signals, DRM-MA lets mobile users adopt either additive or subtractive reception mode based on the phase difference of the signals sent from their serving and interfering antennas and perceived by their two receiving antennas so that the desired signals and the interferences can be constructively and destructively combined at each Rx. In this way, concurrent data transmissions of multiple antenna-receiver pairs are realized. Compared to traditional signal processing-based MAC methods discussed in the previous paragraph, our method does not incur a signal processing burden at either side of the communication link. However, to realize the method, the central control unit (CCU) needs to determine the serving antenna for each Rx, hence incurring some computational complexity.

The main contributions of this paper are two-fold:

(i) *Proposal of DRM-MA*. By exploiting interactions among two wireless signals, an Rx can select the appropriate reception mode according to the phase difference of the signals sent from the antennas of serving Tx and interfering Tx and observed by its receiving antennas, respectively. Then, the desired signal components can be constructively combined while the interferences are neutralized with each other at the Rx

(ii) *Development of Antenna Selection Criterion*. Aiming at strengthening the desired signal and suppressing the CCI as much as possible, various candidate transmitting antenna sets are calculated, from which the serving antenna for each Rx is then selected, and accordingly, each Rx determines its reception mode

The rest of the paper is organized as follows. Section 2 describes the system model while Section 3 details the design of DRM-MA. In Section 4, we evaluate the performance of DRM-MA. Finally, we conclude the paper in Section 5.

Throughout this paper, we use the following notations. Let $|\cdot|$ denote the absolute value of a scalar. argmax$\{\cdot\}$ indicates an operation finding the argument that gives the maximum value from a target function.

2. System Model

We consider a downlink communication scenario consisting of a central control unit (CCU) and multiple distributedly located transmitting antennas under CCU's control. The antennas are uniformly deployed in the area of $V \times H$. As Figure 1 shows, the antenna whose y- and x-coordinates are v and h, respectively, is denoted as Tx_{vh} ($v \in \{1, 2, \cdots, V\}, h \in \{1, 2, \cdots, H\}$). Tx_{vh} can also be regarded as a single-antenna transmitter. The transmit power of each antenna is P_T. For simplicity, we plot two Rxs, say Rx_m and Rx_k, in the communication environment. Each Rx is equipped with $N_R = 2$ antennas. The two antennas of Rx_m are denoted as m_1 and m_2, while Rx_k's antennas are k_1 and k_2. Let $g_{m_1}^{vh}$ and $g_{m_2}^{vh}$ represent the channel fading coefficients between Tx_{vh} and Rx_m's two antennas. Similarly, $g_{k_1}^{vh}$ and $g_{k_2}^{vh}$ are the fading coefficients between Tx_{vh} and Rx_k's antennas, respectively. We adopt free-space propagation model [16], hence, the power of received signal at antenna κ ($\kappa \in \{m_1, m_2, k_1, k_2\}$) from Tx_{vh} can be computed as $P_\kappa^{vh} = P_T G_{vh} G_\kappa \lambda^2 / \Gamma (4\pi l_\kappa^{vh})^2$ where λ represents the signal's wavelength. G_{vh} and G_κ are the gains of the transmitting antenna Tx_{vh} and receiving antenna κ. Γ is the path-loss factor. l_κ^{vh} denotes the distance from Tx_{vh} to κ. We assume that CCU can accurately obtain the channel coefficients from all transmitting antennas to each receiving antenna of an Rx. By exploiting channel reciprocity [17], the uplink and downlink can have the same channel coefficients.

We employ φ_κ^{vh} to represent the phase of the signal sent from Tx_{vh} and perceived by receiving antenna κ. To reduce signaling overhead, we let Rx_ℓ ($\ell \in \{m, k\}$) only feed back to CCU the midpoint coordinate, i.e., C_ℓ, of the line segment

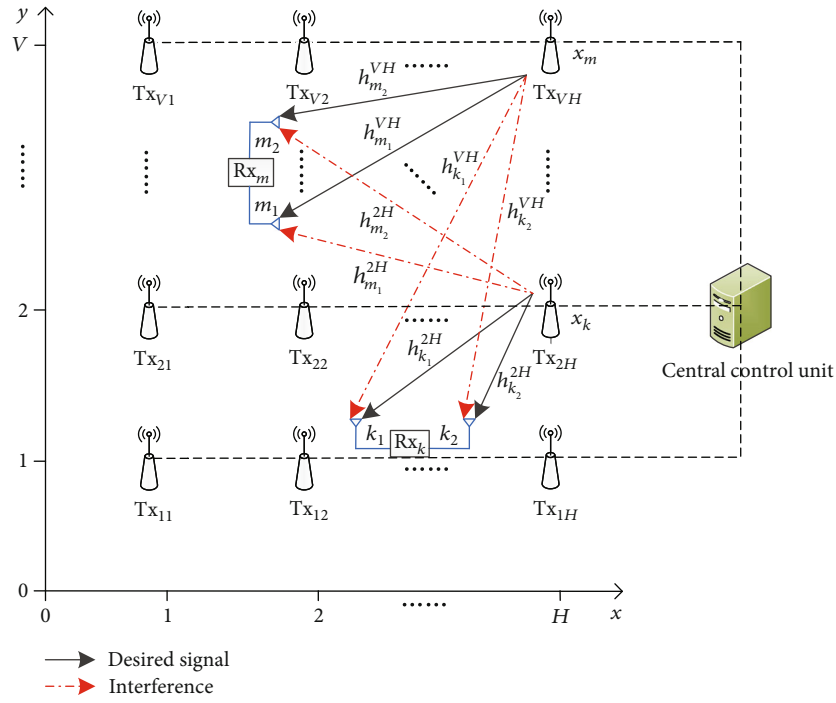


Figure 1: System model.

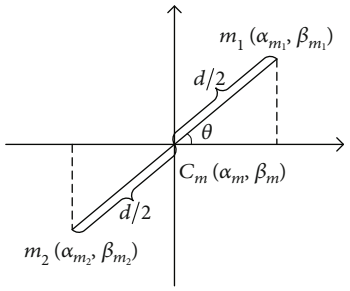


Figure 2: Geometrical illustration of Rx_m's two receiving antennas, and $m_1\bar{m}_2$'s midpoint C_m and phase angle θ.

$\ell_1\bar{\ell}_2$ between Rx_ℓ's two receiving antennas, and the phase angle θ of $\ell_1\bar{\ell}_2$ with respect to the horizontal axis. In Figure 2, taking Rx_m as an example, CCU can calculate the coordinates of Rx_m's two receiving antennas, i.e., m_1 and m_2, according to C_m, θ, and antenna spacing d (we assume the distance between Rx's two antennas is available to CCU). As Figure 2 shows, we denote the coordinate of the midpoint of line segment $m_1\bar{m}_2$ as $C_m(\alpha_m, \beta_m)$, then, the x - and y-coordinates of m_1 can be calculated as $\alpha_{m_1} = \alpha_m + 1/2d \cos\theta$ and $\beta_{m_1} = \beta_m + 1/2d \sin\theta$, respectively. Similarly, the coordinates of receiving antenna m_2 are $\alpha_{m_2} = \alpha_m - 1/2\, d \cos\theta$ and $\beta_{m_2} = \beta_m - 1/2d \sin\theta$.

3. Design of DRM-MA

This section details the design of Differentiated Receive Mode-based Multiple Access (DRM-MA). We will first present the basic principle of DRM-MA and then give the criterion based on which the transmitting antennas serving multiple Rxs are selected and paired with the Rxs; accordingly, and each Rx determines its reception mode.

3.1. Basic Design of DRM-MA. For clarity, we take two Rxs as an example to present the principle of DRM-MA. As Figure 1 shows, we assume that the serving antennas for R x_m and Rx_k have been determined (the antenna selection method will be given in the next subsection). Without loss of generality, we let antennas $Tx_{v_m h_m}$ and $Tx_{v_k h_k}$ send desired signals to Rx_m and Rx_k, respectively. It should be noticed that $Tx_{v_m h_m}$ causes interference to Rx_k and vice versa. Therefore, we also call $Tx_{v_m h_m}$ and $Tx_{v_k h_k}$ permissive interfering antennas of Rx_k and Rx_m, respectively.

We use x_m and x_k to denote the desired data symbols of Rx_m and Rx_k. Both $Tx_{v_m h_m}$ and $Tx_{v_k h_k}$ send one desired signal to their intended Rx. Then, the mixed signals perceived by antennas m_1 and m_2 of Rx_m, denoted as y_{m_1} and y_{m_2}, respectively, can be expressed as

$$\begin{cases} y_{m_1} = g_{m_1}^{v_m h_m} x_m + g_{m_1}^{v_k h_k} x_k + n_{m_1}, \\ y_{m_2} = g_{m_2}^{v_m h_m} x_m + g_{m_2}^{v_k h_k} x_k + n_{m_2}, \end{cases} \tag{1}$$

where g_κ^τ ($\tau \in \{v_m h_m, v_k h_k\}$ and $\kappa \in \{m_1, m_2\}$) denote the fading coefficient of the channel from Tx_τ to Rx_m's antenna κ. The first term on the right-hand side (RHS) of each subequation in Eq. (1) represents for the desired signal from T $x_{v_m h_m}$, while the second term denotes the interference from $Tx_{v_k h_k}$. The third term is Additive White Gaussian Noise (AWGN) whose element has zero-mean and variance σ_n^2.

The complex channel coefficient g_κ^τ can be expressed as [18]

$$g_\kappa^\tau = |g_\kappa^\tau| e^{j\varphi_\kappa^\tau}, \tag{2}$$

where $|g_\kappa^\tau|$ denotes the amplitude fading, and $\varphi_\kappa^\tau \in [0, 2\pi]$ is the phase offset yielded by the channel.

Substituting Eq. (2) into Eq. (1), we can get

$$\begin{cases} y_{m_1} = \left|g_{m_1}^{v_m h_m}\right| x_m e^{j\varphi_{m_1}^{v_m h_m}} + \left|g_{m_1}^{v_k h_k}\right| x_k e^{j\varphi_{m_1}^{v_k h_k}} + n_{m_1}, \\ y_{m_2} = \left|g_{m_2}^{v_m h_m}\right| x_m e^{j\varphi_{m_2}^{v_m h_m}} + \left|g_{m_2}^{v_k h_k}\right| x_k e^{j\varphi_{m_2}^{v_k h_k}} + n_{m_2}. \end{cases} \tag{3}$$

From Eq. (3), we can obtain the phase difference of the desired signal components perceived by Rx_m's two antennas as $\Delta\varphi_m^{v_m h_m} = |\varphi_{m_1}^{v_m h_m} - \varphi_{m_2}^{v_m h_m}|$. If $(\Delta\varphi_m^{v_m h_m}) \bmod (2\pi) = \pi$ (mod $(\cdot)$ represents modulo operation) holds, Rx_m can simply subtract one antenna's received signal from the other, so that the in-phase superposition of the desired signal is realized. Otherwise, if $(\Delta\varphi_m^{v_m h_m}) \bmod (2\pi) = 0$ holds, Rx_m can add the received signals of its two antennas to achieve the in-phase desired signal combination. Meanwhile, m_1 and m_2 also receive interference from $Tx_{v_k h_k}$ (see the second terms on the RHS of Eq. (3)). If the phase difference of the two interfering components satisfies $(\Delta\varphi_m^{v_k h_k}) \bmod (2\pi) = \pi$, Rx_m should add up the two interferences to mitigate their influence. Otherwise, if $(\Delta\varphi_m^{v_k h_k}) \bmod (2\pi) = 0$ holds, Rx_m should subtract one disturbance from the other to realize interference cancellation. Likewise, Rx_k can realize desired signal construction and interference destruction based on the phase difference of two desired/interfering signal components at its antennas. Therefore, in the use of DRM-MA, CCU first calculates the phase difference of signals sent from each candidate antenna and perceived by the two receiving antennas of an Rx based on the locations of the transmitting antenna and Rx, then determines the Rx's reception mode according to the phase difference.

Upon employing various reception modes, i.e., additive or subtractive, each Rx realizes both desired signal strengthening and interference cancellation. Without loss of generality, we take $(\Delta\varphi_m^{v_m h_m}) \bmod (2\pi) = \pi$ and $(\Delta\varphi_m^{v_k h_k}) \bmod (2\pi) = 0$ as an example, then, Rx_m can adopt subtractive mode to get the following equation.

$$\begin{aligned} y_m = & \underbrace{\left(\left|g_{m_1}^{v_m h_m}\right| e^{j\varphi_{m_1}^{v_m h_m}} - \left|g_{m_2}^{v_m h_m}\right| e^{j\varphi_{m_2}^{v_m h_m}}\right) x_m}_{\text{In-phase desired signal construction.}} \\ & + \underbrace{\left(\left|g_{m_1}^{v_k h_k}\right| e^{j\varphi_{m_1}^{v_k h_k}} - \left|g_{m_2}^{v_k h_k}\right| e^{j\varphi_{m_2}^{v_k h_k}}\right) x_k}_{\text{Inverse-phase interference destruction.}} + n_m. \end{aligned} \tag{4}$$

Since $|g_{m_1}^{v_m h_m}| e^{j\varphi_{m_1}^{v_m h_m}}$ and $|g_{m_2}^{v_m h_m}| e^{j\varphi_{m_2}^{v_m h_m}}$ are known to Rx_m, Rx_m can adopt coefficient $(|g_{m_1}^{v_m h_m}| e^{j\varphi_{m_1}^{v_m h_m}} - |g_{m_2}^{v_m h_m}| e^{j\varphi_{m_2}^{v_m h_m}})^{-1}$ to postprocess y_m to obtain the estimated desired signal as

$$\widehat{y}_m = \left(\left|g_{m_1}^{v_m h_m}\right| e^{j\varphi_{m_1}^{v_m h_m}} - \left|g_{m_2}^{v_m h_m}\right| e^{j\varphi_{m_2}^{v_m h_m}}\right)^{-1} y_m. \tag{5}$$

Meanwhile, the phase difference of the desired and interfering signal sent from $Tx_{v_m h_m}$ and $Tx_{v_k h_k}$, respectively, and received by Rx_k's two antennas k_1 and k_2 should satisfy $(\Delta\varphi_k^{v_k h_k}) \bmod (2\pi) = 0$ and $(\Delta\varphi_k^{v_m h_m}) \bmod (2\pi) = \pi$. In such a case, Rx_k can employ additive mode to get the following equation.

$$\begin{aligned} y_k = & \underbrace{\left(\left|g_{k_1}^{v_k h_k}\right| e^{j\varphi_{k_1}^{v_k h_k}} + \left|g_{k_2}^{v_k h_k}\right| e^{j\varphi_{k_2}^{v_k h_k}}\right) x_k}_{\text{In-phase desired signal construction.}} \\ & + \underbrace{\left(\left|g_{k_1}^{v_m h_m}\right| e^{j\varphi_{k_1}^{v_m h_m}} + \left|g_{k_2}^{v_m h_m}\right| e^{j\varphi_{k_2}^{v_m h_m}}\right) x_m}_{\text{Inverse-phase interference destruction.}} + n_k. \end{aligned} \tag{6}$$

Then, by adopting $(|g_{k_1}^{v_k h_k}| e^{j\varphi_{k_1}^{v_k h_k}} + |g_{k_2}^{v_k h_k}| e^{j\varphi_{k_2}^{v_k h_k}})^{-1}$ to postprocess y_k, Rx_k can get the estimated signal as

$$\widehat{y}_k = \left(\left|g_{k_1}^{v_k h_k}\right| e^{j\varphi_{k_1}^{v_k h_k}} + \left|g_{k_2}^{v_k h_k}\right| e^{j\varphi_{k_2}^{v_k h_k}}\right)^{-1} y_k. \tag{7}$$

We can see from Eqs. (4) and (6) that employing additive and subtractive mode, respectively, Rx_m and Rx_k can postprocess the received signals of their antennas. In this way, the desired signal is strengthened while the disturbance is suppressed, thus realizing DRM-MA.

3.2. Design of Antenna Selection Criterion. In the previous subsection, we have presented the basic idea of DRM-MA under the assumption that serving antennas for Rxs have been determined. In this subsection, we will still take two Rxs as an example to design the serving antenna selection criterion.

To select the proper antenna to serve an Rx, say Rx_m, CCU needs to calculate the coordinates of m_1 and m_2 based on the information of C_m, d, and θ and then compute the phase of the signal sent from each candidate antenna Tx_{vh} $(v \in \{1, 2, \cdots, V\}, h \in \{1, 2, \cdots, H\})$ and perceived by Rx_m's receiving antenna κ $(\kappa \in \{m_1, m_2\})$ as

$$\varphi_\kappa^{vh} = \frac{2l_\kappa^{vh}\pi}{\lambda} = \frac{2l_\kappa^{vh}\pi f}{c}, \tag{8}$$

where f denotes the frequency of the transmitted signal and λ is the signal's wavelength. c represents the speed of light. l_κ^{vh} is the distance from Tx_{vh} to Rx_m's antenna κ.

Table 1: Determining candidate serving antenna set (SAS) and Rx's reception mode (RM) under $K = 2$.

Case	SAS for Rx_m	SAS for Rx_k	Rx_m's RM	Rx_k's RM
I	$\mathfrak{R}_{oo}^{mk}$	$\mathfrak{R}_{ee}^{mk}$	Subtractive	Additive
II	$\mathfrak{R}_{oe}^{mk}$	$\mathfrak{R}_{eo}^{mk}$	Subtractive	Subtractive
III	$\mathfrak{R}_{eo}^{mk}$	$\mathfrak{R}_{oe}^{mk}$	Additive	Additive
IV	$\mathfrak{R}_{ee}^{mk}$	$\mathfrak{R}_{oo}^{mk}$	Additive	Subtractive

Then, we can get the phase difference $\Delta\varphi_m^{vh}$ of the signals sent from Tx_{vh} and received by Rx_m's two antennas as

$$\Delta\varphi_m^{vh} = \left|\varphi_{m_1}^{vh} - \varphi_{m_2}^{vh}\right| = \frac{2\pi f\left|l_{m_1}^{vh} - l_{m_2}^{vh}\right|}{c}. \tag{9}$$

Since we employ the free-space propagation model, in what follows, we only consider the influence of the signal's propagation on φ_κ^{vh} and $\Delta\varphi_m^{vh}$. Without loss of generality, we take Rx_m as an example. If $(\Delta\varphi_m^{vh}) \bmod (2\pi) = \pi$ holds, we store Tx_{vh} in a transmitting antenna set Ω_o^m. Otherwise, if $(\Delta\varphi_m^{vh}) \bmod (2\pi) = 0$ holds, Tx_{vh} is added to transmitting antenna set Ω_e^m. When an antenna in sets Ω_o^m and Ω_e^m is selected to serve Rx_m, Rx_m needs to adopt additive and subtractive reception modes accordingly. Similarly, transmitting antenna sets Ω_o^k and Ω_e^k for Rx_k can be obtained.

Next, we calculate intersections of Rx_m's sets Ω_o^m and Ω_e^m and Rx_k's Ω_o^k and Ω_e^k, respectively, to obtain four candidate transmitting antenna sets, i.e., $\mathfrak{R}_{oo}^{mk} = \Omega_o^m \bigcap \Omega_o^k$, $\mathfrak{R}_{oe}^{mk} = \Omega_o^m \bigcap \Omega_e^k$, $\mathfrak{R}_{eo}^{mk} = \Omega_e^m \bigcap \Omega_o^k$, and $\mathfrak{R}_{ee}^{mk} = \Omega_e^m \bigcap \Omega_e^k$, as given in Table 1. Accordingly, four differentiated reception modes of the two Rxs can be determined. Taking candidate antenna set $\mathfrak{R}_{oo}^{mk}$ as an example, the subscript oo indicates that the phase difference of signals sent from each antenna in set $\mathfrak{R}_{oo}^{mk}$ and perceived by the two receiving antennas of both Rx_m and Rx_k is odd times of π. That is, when an antenna in $\mathfrak{R}_{oo}^{mk}$ serves Rx_m or Rx_k, either Rx_m or Rx_k should adopt the subtractive reception mode to strengthen its desired signal. As for $\mathfrak{R}_{eo}^{mk}$, its subscript eo indicates that the phase difference of the signals sent from $\mathfrak{R}_{eo}^{mk}$'s antenna and observed by Rx_m's and Rx_k's two antennas is even and odd times of π, respectively. Therefore, when an antenna in $\mathfrak{R}_{eo}^{mk}$ is selected to serve Rx_m or Rx_k, Rx_m should adopt additive mode, while Rx_k should use subtractive, to strengthen their desired signal. As Table 1 shows, Rx_m and Rx_k can adopt either identical reception modes (cases II and III) or different modes (cases I and IV) in terms of their serving transmitting antenna sets.

In practice, when selecting a serving antenna for an Rx, not only does the desired signal at the intended Rx need to be strong but also the interference to other unintended Rxs should be as small as possible. In what follows, we will present the serving antenna selection criterion on the premise that the candidate serving antenna sets have been determined.

Without loss of generality, we take the case I in Table 1 as an example. When a candidate $Tx_{vh} \in \mathfrak{R}_{oo}^{mk}$ serves Rx_m and interferes with Rx_k, Rx_m adopts subtractive mode to subtract the desired signal perceived by one antenna from the other. Then, we can have•

$$\Delta A_m^{vh} = \left|g_{m_1}^{vh}\right| e^{j\varphi_{m_1}^{vh}} - \left|g_{m_2}^{vh}\right| e^{j\varphi_{m_2}^{vh}}. \tag{10}$$

As for Rx_k, it employs additive reception mode to alleviate the interference sent from Tx_{vh} and received by its two antennas. We can get

$$\Sigma A_k^{vh} = \left|g_{k_1}^{vh}\right| e^{j\varphi_{k_1}^{vh}} + \left|g_{k_2}^{vh}\right| e^{j\varphi_{k_2}^{vh}}. \tag{11}$$

Then, we should select the Tx_{vh} that can maximize ΔA_m^{vh}, denoted as $Tx_{v_m h_m}$, as Rx_m's serving antenna; that is, ($Tx_{v_m h_m} = \arg\max_{Tx_{vh} \in \mathfrak{R}_{oo}^{mk}} \{\Delta A_m^{vh}\}$). However, by taking the interference from Tx_{vh} to Rx_k into account, we should employ $(\Sigma A_k^{vh})^{-1}$ as another factor affecting Rx_m's serving antenna selection. That is, since ΣA_k^{vh} indicates residual interference at Rx_k, we should use an antenna yielding as small ΣA_k^{vh} as possible to serve Rx_m. Based on the above discussion, to take both desired signal strengthening at Rx_m and interference cancellation at Rx_k into consideration, an antenna outputting the largest $\mu_{mk}^{vh} = \xi\Delta A_m^{vh} + (1-\xi)(\Sigma A_k^{vh})^{-1}$ where $\xi \in [0, 1]$ is a weight coefficient and should be selected to serve Rx_m. Specifically, in this example, we determine Rx_m's serving antenna according to ($Tx_{v_m h_m} = \arg\max_{Tx_{vh} \in \mathfrak{R}_{oo}^{mk}} \{\mu_{mk}^{vh}\}$). If one prefers a better performance of Rx_m, a larger ξ should be adopted; otherwise, if one wants the interference at Rx_k to be small, a smaller ξ should be used.

In the previous design, we simply assume that the phase difference of signal components perceived by an Rx's two antennas is either odd or even times of π, based on which the candidate serving antenna sets can be determined. However, in practice, the phase difference is usually not exactly the odd or even times of π. In such a situation, we need to introduce a tolerance coefficient ε to relax the requirement of the phase difference of signals at Rx's two antennas. Otherwise, too strict a phase difference requirement may yield an empty candidate serving antenna set, hence incurring the unavailability of DRM-MA.

Based on the above discussion, we adopt $(\Delta\varphi_m^{vh}) \bmod (2\pi) = \pi \pm \varepsilon$ and $(\Delta\varphi_m^{vh}) \bmod (2\pi) = \pm\varepsilon$ instead of $(\Delta\varphi_m^{vh}) \bmod (2\pi) = \pi$ and $(\Delta\varphi_m^{vh}) \bmod (2\pi) = 0$, respectively, as the criterion to determine the candidate serving antenna sets. In this way, we can ensure that the candidate serving antenna set is not empty by using a proper ε. However, this will incur nonideal in-phase construction of desired signal and inverse-phase interference destruction at Rx. To solve this problem, Rx can perform phase compensation according to the phase difference of the signals perceived by its two antennas [19],

and then accurate in-phase desired signal superposition and inverse-phase interference cancellation can be realized. The stronger the phase compensation capability of the Rx is, the larger ε can be used.

It should be noticed that although phase compensation can yield the phase difference of the signal components perceived by Rx's two antennas to be exactly odd times or even times of π, the signal components' amplitudes may not be the same, hence incurring residual interference at Rx. Fortunately, since the size of Rx and its antenna spacing are small, the difference in propagation distance from the interfering antenna to Rx's two receiving antennas is limited. Therefore, the influence of residual interference is negligible. For space limit, we omit the detailed discussion about the residual interference in this paper.

3.3. Extended Design of DRM-MA. In previous subsections, we simply assume two Rxs for clarity. In this subsection, we will extend DRM-MA to a multi-Rx situation to show its scalability.

We let the number of Rxs be three, i.e., Rx_m, Rx_k, and Rx_s are in the communication scenario. First, CCU calculates the phase difference of the signals sent from each T x_{vh} and perceived by the Rxs' receiving antennas. Then, an antenna set suitable for serving each Rx under additive and subtractive reception modes can be obtained. We denote the set of serving antennas for Rx_ϖ under additive and subtractive modes as Ω_e^ϖ and Ω_o^ϖ, respectively, where $\varpi \in \{m, k, s\}$. Then, we select one set from the serving antenna sets of Rx_m, Rx_k, and Rx_s in turn and calculate the intersection of the three selected sets, so that eight cases of candidate serving antenna sets can be obtained as $\mathfrak{R}_{ooo}^{mks} = \Omega_o^m \bigcap \Omega_o^k \bigcap \Omega_o^s$, $\mathfrak{R}_{ooe}^{mks} = \Omega_o^m \bigcap \Omega_o^k \bigcap \Omega_e^s$, $\mathfrak{R}_{oeo}^{mks} = \Omega_o^m \bigcap \Omega_e^k \bigcap \Omega_o^s$, $\mathfrak{R}_{oee}^{mks} = \Omega_o^m \bigcap \Omega_e^k \bigcap \Omega_e^s$, $\mathfrak{R}_{eoo}^{mks} = \Omega_e^m \bigcap \Omega_o^k \bigcap \Omega_o^s$, $\mathfrak{R}_{eoe}^{mks} = \Omega_e^m \bigcap \Omega_o^k \bigcap \Omega_e^s$, $\mathfrak{R}_{eeo}^{mks} = \Omega_e^m \bigcap \Omega_e^k \bigcap \Omega_o^s$, and $\mathfrak{R}_{eee}^{mks} = \Omega_e^m \bigcap \Omega_e^k \bigcap \Omega_e^s$. As Table 2 shows, the above eight sets correspond to eight combinations of the three Rxs' reception modes. Taking $\mathfrak{R}_{eee}^{mks}$ as an example, its subscript is *eee*, this indicates that when an antenna in set $\mathfrak{R}_{eee}^{mks}$ serves Rx_ϖ ($\varpi \in \{m, k, s\}$), the phase difference of the signals perceived by Rx_ϖ's two antennas is even times of π, thus Rx_ϖ should adopt subtractive reception mode.

Based on the various combinations of the serving antenna sets, the reception modes of multiple Rxs can be determined. Since there is always no cooperation among multiple Rxs, Rxs' reception modes should be determined by the CCU and then informed to each Rx. We further present the extension of DRM-MA to the case of K ($K > 2$) Rx. First, we index all Rxs from 1 to K. For simplicity, we replace the subscripts o and e of the candidate serving antenna sets with binary numbers 0 and 1, respectively. In this way, the string composed of o and e can be equivalent to a binary code. Provided with K Rxs, DRM-MA first calculates Ω_e^ϖ and Ω_o^ϖ where $\varpi \in \{1, 2, \cdots, K\}$ for each Rx, based on which 2^K cases of candidate serving antenna sets, denoted as $\mathfrak{R}_{b_1 \cdots b_K}^{1 \cdots K}$ where $b_1 \cdots b_K$ can be either $o(0)$ or $e(1)$, can be obtained. Next, we can select any one of the 2^K candidate antenna sets (e.g., case I in Table 2) and mark it as the serving antenna set for Rx_1 (e.g., as for case I in Table 2, $\mathfrak{R}_{ooo}^{mks}$ whose subscript is 000 serves Rx_m). Then, we select the serving antenna set for Rx_2 (e.g., as for case I in Table 2, $\mathfrak{R}_{eeo}^{mks}$ whose subscript is 110 serves Rx_k); the 1st and 2nd bits of R x_2's serving antenna set's subscript should be opposite to those of Rx_1's, while the rest bits of the two Rxs' serving antenna sets' subscripts are the same. As for Rx_3 (under $K = 3$, according to Table 2, $\mathfrak{R}_{eoe}^{mks}$ whose subscript is 101 serves Rx_s); the 1st and 3rd bits of Rx_3's serving antenna set's subscript should be opposite to those of Rx_1's, while the remaining bits of the two Rxs' sets' subscripts are the same. As for Rx_K, the 1st and K^{th} bits of its serving antenna set need to be opposite to those Rx_1's, while the remaining bits of the two Rxs's sets' subscripts are the same.

Table 2: Determining candidate serving antenna set (SAS) and Rx 's reception mode (RM) under $K = 3$.

Case	SAS for R x_m	SAS for R x_k	SAS for R x_s	Rx_m's RM	Rx_k's RM	Rx_s's RM
I	$\mathfrak{R}_{ooo}^{mks}$	$\mathfrak{R}_{eeo}^{mks}$	$\mathfrak{R}_{eoe}^{mks}$	Subtractive	Additive	Additive
II	$\mathfrak{R}_{ooe}^{mks}$	$\mathfrak{R}_{eee}^{mks}$	$\mathfrak{R}_{eoo}^{mks}$	Subtractive	Additive	Subtractive
III	$\mathfrak{R}_{oeo}^{mks}$	$\mathfrak{R}_{eoo}^{mks}$	$\mathfrak{R}_{eee}^{mks}$	Subtractive	Subtractive	Additive
IV	$\mathfrak{R}_{oee}^{mks}$	$\mathfrak{R}_{eoe}^{mks}$	$\mathfrak{R}_{eeo}^{mks}$	Subtractive	Subtractive	Subtractive
V	$\mathfrak{R}_{eoo}^{mks}$	$\mathfrak{R}_{oeo}^{mks}$	$\mathfrak{R}_{ooe}^{mks}$	Additive	Additive	Additive
VI	$\mathfrak{R}_{eoe}^{mks}$	$\mathfrak{R}_{oee}^{mks}$	$\mathfrak{R}_{ooo}^{mks}$	Additive	Additive	Subtractive
VII	$\mathfrak{R}_{eeo}^{mks}$	$\mathfrak{R}_{ooo}^{mks}$	$\mathfrak{R}_{oee}^{mks}$	Additive	Subtractive	Additive
VIII	$\mathfrak{R}_{eee}^{mks}$	$\mathfrak{R}_{ooo}^{mks}$	$\mathfrak{R}_{oeo}^{mks}$	Additive	Subtractive	Subtractive

Based on the above process, 2^K combinations of serving antenna sets for K Rxs can be obtained. Then, an Rx, say $Rx_{\hat{k}}$ ($\hat{k} \in \{1, \cdots, K\}$) can determine its reception mode in terms of the $\hat{k}^{th}$ bit of its serving antenna set's subscript. Specifically, if the $\hat{k}^{\text{th}}$ bit is $o(0)$, $Rx_{\hat{k}}$ should adopt subtractive mode; otherwise, for $e(1)$, additive reception mode should be used. We take case I in Table 2 as an example, the first user Rx_m adopts subtractive mode according to the 1st bit of $\mathfrak{R}_{ooo}^{mks}$'s subscript. Similarly, the second user Rx_k employs additive mode based on the 2nd bit of $\mathfrak{R}_{eeo}^{mks}$'s subscript. As for the last user Rx_s, its uses additive mode according to the 3rd bit of $\mathfrak{R}_{eoe}^{mks}$)'s subscript.

Based on the above descriptions, DRM-MA can be applied to the communication scenario with K Rxs.

4. Evaluations

In this section, we use MATLAB to evaluate the performance of the proposed DRM-MA. We consider a communication scenario of 10m × 10m, in which multiple antennas, denoted as Tx_{vh} ($v \in \{1, 2, \cdots, V\}, h \in \{1, 2, \cdots, H\}$), are uniformly distributed. The transmit power of Tx_{vh} is P_T. The

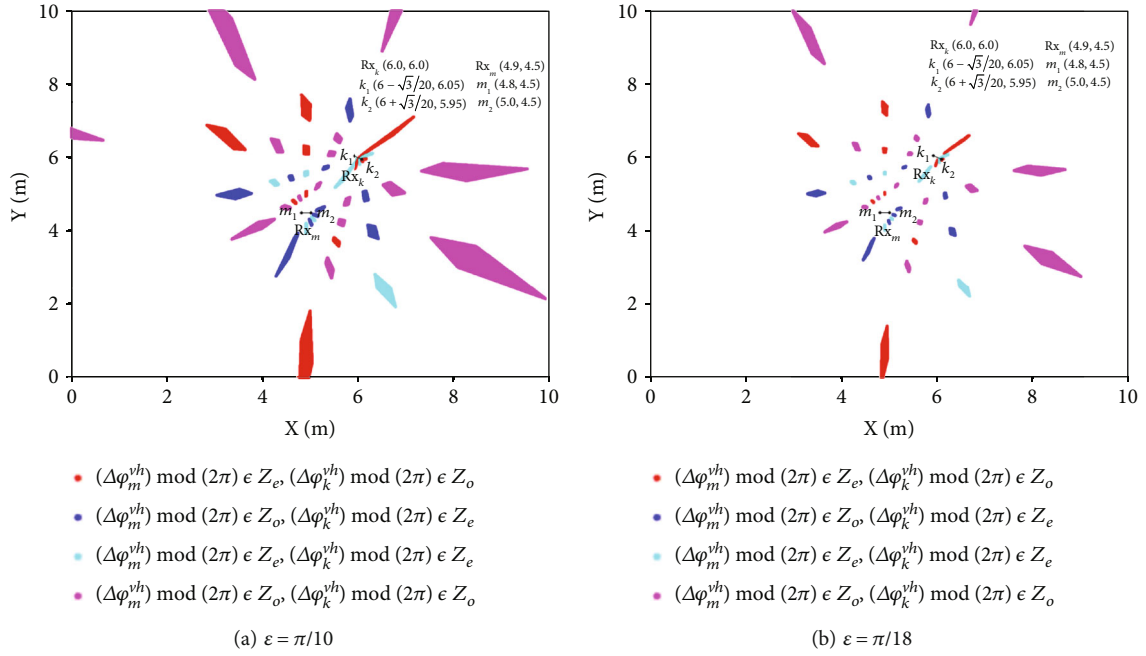


FIGURE 3: Distribution of candidate serving antennas for Rx_m and Rx_k under various εs.

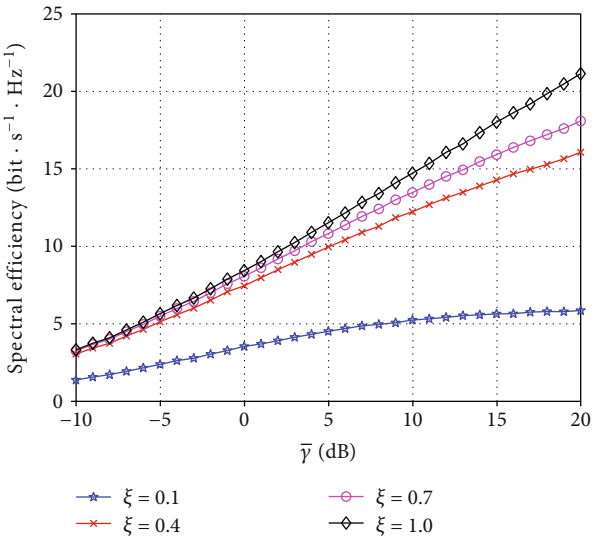


FIGURE 4: Variation of system's average SE with $\bar{\gamma}$ under various ξs.

carrier frequency is 2.4 GHz. Two Rxs, denoted as Rx_m and Rx_k, are arbitrarily located in the communication area and equipped with two antennas. The distance between Rx's two receiving antennas, d, is 0.2 m. We employ the free space propagation model as given in Section 2. The signal power sent from Tx_{vh} and received by antenna κ ($\kappa \in \{m_1, m_2, k_1, k_2\}$) is $P_\kappa^{vh} = P_T G_{vh} G_\kappa \lambda^2 / \Gamma (4\pi l_\kappa^{vh})^2$ where $G_{vh} = 1$, $G_\kappa = 1$, and $\Gamma = 1$. l_κ^{vh} (measured in meter) is the distance from Tx_{vh} to antenna κ. We adopt the serving antenna selection weight $\xi \in [0, 1]$ and define the signal-to-noise ratio (SNR) as $\bar{\gamma} = 10 \lg(\gamma) dB$ where $\gamma = P_T/\sigma_n^2$ and σ_n^2 represents for the noise power. In determining transmitting antenna sets Ω_o^m and Ω_e^m, we take Tx_{vh} in the range of $\pm\varepsilon$ near odd and even times of π into account. To be specific, we define two phase intervals, $\mathbb{Z}_o = [\pi - \varepsilon, \pi + \varepsilon]$ and $\mathbb{Z}_e = [0, \varepsilon] \bigcup [2\pi - \varepsilon, 2\pi]$. Then, for example, if $(\Delta\varphi_m^{vh})$ mod $(2\pi) \in \mathbb{Z}_e$ (or $(\Delta\varphi_m^{vh})$ mod $(2\pi) \in \mathbb{Z}_o$) holds, Tx_{vh} can serve Rx_m and Rx_m should employ additive (or subtractive) reception mode.

Figure 3 simulates the distribution of candidate serving antennas for Rx_m and Rx_k in the communication scenario under various εs. As the figure shows, the coordinates of the midpoints of $m_1\bar{m}_2$ and $k_1\bar{k}_2$ are set to be $C_m(4.9,4.5)$ and $C_k(6, 6)$; and accordingly, the antennas' coordinates are $m_1(4.8,4.5)$, $m_2(5,4.5)$, $k_1(6 - \sqrt{3}/20,6.05)$, and $k_2(6 + \sqrt{3}/20,5.95)$, respectively. As for Tx_{vh} in the red area, on one hand, it yields signals' phase difference at Rx_m satisfying $(\Delta\varphi_m^{vh})$ mod $(2\pi) \in \mathbb{Z}_e$, thus is added to set Ω_e^m; on the other hand, the signals' phase difference at Rx_k satisfies $(\Delta\varphi_k^{vh})$ mod $(2\pi) \in \mathbb{Z}_o$, and hence Tx_{vh} belongs to set Ω_o^k. Therefore, we add Tx_{vh} to the candidate serving antenna set $\mathfrak{R}_{eo}^{mk} = \Omega_e^m \bigcap \Omega_o^k$. Then, if Tx_{vh} in $\mathfrak{R}_{eo}^{mk}$ transmits to Rx_m, Rx_m should employ additive reception mode; if Tx_{vh} in $\mathfrak{R}_{eo}^{mk}$ serves Rx_k, Rx_k should adopt subtractive mode. Similarly, as for Tx_{vh} in the dark blue area, on one hand, it yields signals' phase difference at Rx_m satisfying $(\Delta\varphi_m^{vh})$ mod $(2\pi) \in \mathbb{Z}_o$, thus is added to set Ω_o^m; on the other hand, the signals' phase difference at Rx_k satisfies $(\Delta\varphi_k^{vh})$ mod $(2\pi) \in \mathbb{Z}_e$, and hence, Tx_{vh} belongs to set Ω_e^k. Therefore, we add Tx_{vh} to the candidate serving antenna set $\mathfrak{R}_{oe}^{mk} = \Omega_o^m \bigcap \Omega_e^k$. Accordingly, if Tx_{vh} in $\mathfrak{R}_{oe}^{mk}$ transmits to Rx_m, Rx_m should employ subtractive reception mode; if Tx_{vh} in $\mathfrak{R}_{oe}^{mk}$ serves Rx_k, Rx_k should adopt additive mode.

As for Tx_{vh} in the light blue area, it yields signals' phase difference at Rx_m's and Rx_k's two receiving antennas

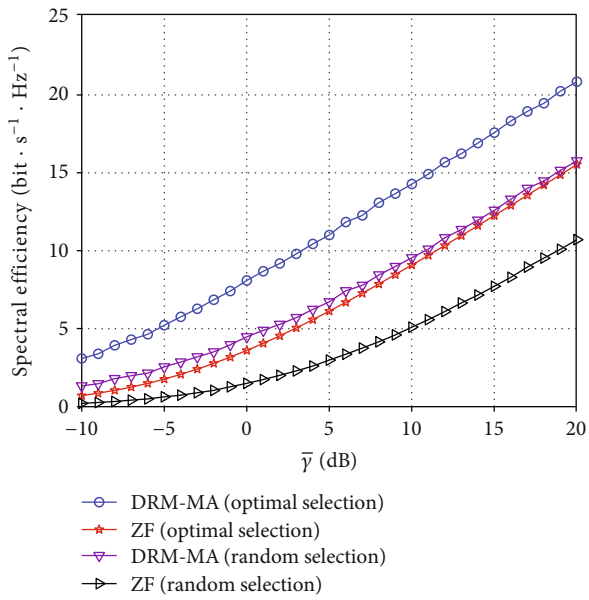


Figure 5: Comparison of DRM-MA and ZF reception.

satisfying $(\Delta\varphi_m^{vh}) \bmod (2\pi) \in \mathbb{Z}_e$ and $(\Delta\varphi_k^{vh}) \bmod (2\pi) \in \mathbb{Z}_e$, respectively. Thus, Tx_{vh} belongs to Ω_e^m and Ω_e^k, yielding candidate serving antenna set $\mathfrak{R}_{ee}^{mk} = \Omega_e^m \bigcap \Omega_e^k$. Accordingly, if Tx_{vh} in $\mathfrak{R}_{ee}^{mk}$ serves Rx_m or Rx_k, either Rx should employ additive reception mode. Similarly, as for Tx_{vh} in the magenta area, it yields signals' phase difference at Rx_m's and Rx_k's two receiving antennas satisfying $(\Delta\varphi_m^{vh}) \bmod (2\pi) \in \mathbb{Z}_o$ and $(\Delta\varphi_k^{vh}) \bmod (2\pi) \in \mathbb{Z}_o$, respectively. Thus, Tx_{vh} belongs to Ω_o^m and Ω_o^k, yielding candidate serving antenna set $\mathfrak{R}_{oo}^{mk} = \Omega_o^m \bigcap \Omega_o^k$. Accordingly, if Tx_{vh} in $\mathfrak{R}_{oo}^{mk}$ serves Rx_m or Rx_k, either Rx should employ subtractive reception mode.

As Figure 3 shows, under a small ε, the ranges of phase intervals $\mathbb{Z}_o$ and $\mathbb{Z}_e$ become small too, hence yielding reduced areas and decreased the number of candidate serving antennas for Rx_m and Rx_k. Given the strong enough phase compensation capability of the Rx, a large ε can be adopted, then, the ranges of phase intervals $\mathbb{Z}_o$ and $\mathbb{Z}_e$ are enlarged, yielding more candidate serving antennas for Rx_m and Rx_k. In what follows, we will evaluate DRM-MA's SE performance and compare it with zero-forcing (ZF) reception. Since DRM-MA employs a single transmitting antenna for each Rx's data transmission, Tx-side array signal processing methods cannot be used in our communication scenario. However, as the Rx is equipped with 2 antennas, the Rx-side array processing such as ZF is taken into account. In the following simulation, we assume 2 Rxs in the communication area and 16 candidate serving antennas are involved in sets $\mathfrak{R}_{oo}^{mk}$ and $\mathfrak{R}_{ee}^{mk}$, respectively. We let $Tx_{v_m h_m}$ in $\mathfrak{R}_{oo}^{mk}$ and $Tx_{v_k h_k}$ in $\mathfrak{R}_{ee}^{mk}$ serve Rx_m and Rx_k. Accordingly, Rx_m and Rx_k adopt subtractive and additive reception mode, respectively. Without loss of generality, we assume that $Tx_{v_m h_m}$ in $\mathfrak{R}_{oo}^{mk}$ serves Rx_m, and $Tx_{v_k h_k}$ in $\mathfrak{R}_{ee}^{mk}$ serves Rx_k. Then, according to Eqs. (10) and (11), we can compute SE of Rx_m and Rx_k as $r_m = \log_2(1 + \|\sqrt{P_T}\Delta A_m^{v_m h_m}\|^2 / \|\sqrt{P_T}\Delta A_m^{v_k h_k}\|^2 + \sigma_n^2)$ and $r_k = \log_2(1 + \|\sqrt{P_T}\Sigma A_k^{v_k h_k}\|^2 / \|\sqrt{P_T}\Sigma A_k^{v_m h_m}\|^2 + \sigma_n^2)$, respectively.

Figure 4 plots the variation of two Rxs' sum SE with $\bar{\gamma}$ under card $(\mathfrak{R}_{oo}^{mk})$ = card $(\mathfrak{R}_{ee}^{mk}) = 16$ where card $(\cdot)$ denotes the number of elements in a set, and $\xi \in \{0.1, 0.4, 0.7, 1.0\}$. As the figure shows, the system's average SE grows with the increase of $\bar{\gamma}$. Under fixed $\bar{\gamma}$, DRM-MA's system SE increases as ξ grows. This is because when ξ is large, a serving transmitting antenna that can yield a high desired data transmission rate is preferred (see Section 3.2). Moreover, since the residual interference is negligible in our system settings when applying DRM-MA, it is better to focus on selecting a good serving antenna for each Rx rather than avoiding residual interference to unintended Rxs. Therefore, we can see from the figure that under $\xi = 1$, DRM-MA outputs the highest system's SE.

Figure 5 plots the variation of two Rxs' sum SE with $\bar{\gamma}$ under DRM-MA and ZF reception. We set card $(\mathfrak{R}_{oo}^{mk})$ = card $(\mathfrak{R}_{ee}^{mk}) = 16$ and $\xi = 1$. To make the simulation results more convincing, both DRM-MA and ZF are divided into two versions for comparison. The method that employs antenna selection given in Section 3.2 is called optimal selection. As its counterpart, method that randomly chooses a serving antenna from $\mathfrak{R}_{oo}^{mk}$ and $\mathfrak{R}_{ee}^{mk}$ for Rx_m and Rx_k is called random selection.

As Figure 5 shows, the SE of DRM-MA (Optimal selection) outputs the highest system's SE. DRM-MA (random selection) ranks second. Then comes ZF (optimal selection). ZF (random selection) yields the lowest system's SE. This is because the optimal selection chooses the best serving antenna that yields the strongest desired signal at its intended Rx; as a comparison, random selection randomly selects an antenna from sets $\mathfrak{R}_{oo}^{mk}$ and $\mathfrak{R}_{ee}^{mk}$ to serve Rx_m and Rx_k, respectively. Moreover, as abovementioned, the residual interference is so small that can be neglected. Therefore, optimal selection excels random selection in the system's SE. Given the fixed antenna selection strategy, DRM-MA outputs higher SE than ZF. This is because, under DRM-MA, each Rx can realize desired signal construction and interference destruction simultaneously via serving antenna selection and reception mode adaptation; and there is no desired signal power loss in the use of DRM-MA. However, as a comparison, ZF causes desired signal's power loss while suppressing the interference [24]. Therefore, DRM-MA is advantageous over ZF in SE.

5. Conclusion

In this paper, we have proposed a novel MAC method called DRM-MA. Based on the phase difference of signals sent from each candidate transmitting antenna and perceived by the two receiving antennas of multiple Rxs, proper serving antennas are selected and paired with the Rxs. Then, each Rx adopts either additive or subtractive reception mode to postprocess the signals received by its two antennas, to realize in-phase desired signal construction and inverse-

phase interference destruction simultaneously. In this way, multiple concurrent data transmissions are realized. Our simulation results have shown that DRM-MA can effectively strengthen the desired signal and suppress CCI among coexisting antenna-receiver pairs, hence outputting a high system's SE.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the project of Key Laboratory of Science and Technology on Communication Network under Grant 6142104200412, in part by the China University Industry-University-Research Innovation Fund under Grant 2021FNA03001, and in part by Communication Soft Science Research Project under Grant 2022-R-41.

References

[1] A. Osseiran, F. Boccardi, V. Braun et al., "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, 2014.

[2] *Future Networks*, 2020, http://www.gsma.com/futurenetworks/ip_services/understanding-5g/.

[3] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, Dresden, Germany, 2013.

[4] C. Namislo, "Analysis of mobile radio slotted ALOHA networks," *IEEE Journal on Selected Areas in Communications*, vol. 2, no. 4, pp. 583–588, 1984.

[5] G. Bianchi, L. Fratta, and M. Oliveri, "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs," in *Proceedings of PIMRC '96 - 7th International Symposium on Personal, Indoor, and Mobile Communications*, vol. 2, pp. 392–396, Taipei, Taiwan, 1996.

[6] J. Zhu, Z. Xu, F. Wang et al., "Double threshold energy detection of cooperative spectrum sensing in cognitive radio," in *Proc. of International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, pp. 1–5, 2008.

[7] Z. Wei, J. Guo, D. W. Ng, and J. Yuan, "Fairness comparison of uplink NOMA and OMA," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–6, Sydney, NSW, Australia, 2017.

[8] K. Jamal and E. Dahlman, "Multi-stage serial interference cancellation for DS-CDMA," in *Proceedings of Vehicular Technology Conference - VTC*, vol. 2, pp. 671–675, Atlanta, GA, USA, 1996.

[9] B. Ling, C. Dong, J. Dai, and J. Lin, "Multiple decision aided successive interference cancellation receiver for NOMA systems," *IEEE Wireless Communications Letters*, vol. 6, no. 4, pp. 498–501, 2017.

[10] D. Halperin, M. J. Ammer, T. E. Anderson, and D. Wetherall, "Interference cancellation: better receivers for a new wireless MAC," *Hotnets*, pp. 1–6, 2007.

[11] Z. Li, X. Dai, and K. G. Shin, "Decoding interfering signals with fewer receiving antennas," in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9, San Francisco, CA, USA, 2016.

[12] Z. Li, J. Ding, X. Dai, K. G. Shin, and J. Liu, "Exploiting interactions among signals to decode interfering transmissions with fewer receiving antennas," *Computer Communications*, vol. 136, pp. 63–75, 2019.

[13] Z. Li, K. G. Shin, and L. Zhen, "When and how much to neutralize interference?," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, 2017.

[14] D. Wu, C. Yang, T. Liu, and Z. Xiong, "Feasibility conditions for interference neutralization in relay-aided interference channel," *IEEE Transactions on Signal Processing*, vol. 62, no. 6, pp. 1408–1423, 2014.

[15] Z. Li, Y. Liu, K. G. Shin, J. Liu, and Z. Yan, "Interference steering to manage interference in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10458–10471, 2019.

[16] J. Xu, W. Liu, F. Lang, Y. Zhang, and C. Wang, "Distance measurement model based on RSSI in WSN," *Wireless Sensor Network*, vol. 2, no. 8, pp. 606–611, 2010.

[17] J. Guey and L. Larsson, "Modeling and evaluation of MIMO systems exploiting channel reciprocity in TDD mode," in *IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004*, pp. 4265–4269, Los Angeles, CA, 2004.

[18] S. Althunibat, V. Sucasas, and J. Rodriguez, "A physical-layer security scheme by phase-based adaptive modulation," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 9931–9942, 2017.

[19] E. Simon, L. Ros, and K. Raoof, "Synchronization over rapidly time-varying multipath channel for CDMA downlink RAKE receivers in time-division mode," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 4, pp. 2216–2225, 2007.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8768928, 14 pages
https://doi.org/10.1155/2022/8768928

Research Article

LAAP: Lightweight Anonymous Authentication Protocol for IoT Edge Devices Based on Elliptic Curve

Xinghui Zhu,[1,2] Zhong Ren,[1] Ji He,[1,2,3,4] Baoquan Ren,[4] Shuangrui Zhao,[1,2] and Pinchang Zhang[5]

[1]*School of Computer Science and Technology, Xidian University, Xi'an 710071, China*
[2]*Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an 710071, China*
[3]*Guangzhou Institute of Technology, Xidian University, 510555 Guangzhou, China*
[4]*Institute of Systems General, Academy of Systems Engineering, Academy of Military Sciences, Beijing 100101, China*
[5]*School of Computer, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210023, China*

Correspondence should be addressed to Ji He; garyhej1991@gmail.com

Received 24 June 2022; Revised 17 August 2022; Accepted 5 September 2022; Published 22 September 2022

Academic Editor: Kechen Zheng

The massive heterogeneous devices and open channels of the Internet of Things (IoT) lead to low efficiency and privacy leakage in the authentication process, which brings great challenges to identity authentication. This paper focuses on the anonymous authentication between the IoT edge device and the cloud server. In this work, we first propose a novel lightweight anonymous authentication protocol (LAAP) to meet security and efficiency requirements. Especially, the proposed protocol uses dynamic pseudonyms to prevent the traceable attacks caused by fixed identity identification and also uses symmetric encryption to optimize the server's search for anonymous device information, and the time complexity is reduced from $O(n)$ to $O(1)$. Then, the formal security analysis and informal security analysis are provided to prove the security of the proposed protocol. Finally, extensive numerical results indicate that the proposed LAAP protocol is superior to the benchmarks in terms of computing overhead and communication overhead, while the storage overhead is consistent with the lowest level among other protocols.

1. Introduction

The Internet of Things (IoT) aims to connect massive sensing devices through wireless networks to realize information interaction between the physical world and the virtual world. With the wide application of IoT, it has been involved in all walks of life, such as the Internet of Vehicles, Internet of Medical Things, and Smart City. According to GSMA forecast, the number of IoT devices worldwide will reach about 23.3 billion in 2025 [1]. Due to the limited storage, computing, communication, and power capabilities of IoT sensing devices, combining edge-embedded devices with cloud computing creates a new paradigm called CloudIoT [2]. Under this paradigm, embedded devices can rely on the processing power of cloud computing and use various services provided by cloud computing. However, when an embedded device establishes a communication connection with a cloud server, security is the primary concern.

In recent years, privacy and data security issues caused by IoT terminal devices have frequently occurred. On June 8, 2020, security experts disclosed a new UPnP vulnerability named "Call Stranger" [3], which affects the security of billions of devices, including the TV and network equipment of ASUS, Belkin, Dell, Samsung, TP-Link, and other companies. The vulnerability could be exploited by a remote, unauthenticated attacker. In September 2021, researchers discovered a high-level security vulnerability CVE-2021-36260 in Hikvision IP camera/NVR device firmware. The attack can fully control the device through the shell and obtain any information of the owner and further laterally attack the internal network without leaving any daily login information [4]. The report released by the Unit 42 team

[5] shows that 98% of IoT devices leak user privacy due to unencrypted traffic, 57% of devices are vulnerable to moderate or severe attacks, and devices have become the preferred target for attackers.

Authentication can guarantee the identity legitimacy of communication parties in the IoT and is a key technology to solve security problems. The authentication process usually involves two parts, i.e., identity authentication and key negotiation. Identity authentication is to ensure the legitimacy of the identities of both communication parties. Key negotiation is used to establish a session key for subsequent security access and secure data transmission. Note that security authentication protocols need to consider the following principles: (1) for lightweight, most IoT devices cannot support complex authentication protocols because of their limited computing resource [6]; (2) for privacy protection, during the interaction of the device, the advanced techniques (e.g., anonymity and blockchain) need to be adopted to prevent malicious attackers from obtaining the private information of the devices and users [7].

1.1. Related Work. To implement the security authentication of IoT devices, various protocols and methods were studied. Kalra and Sood in [8] proposed a two-way authentication scheme to realize mutual authentication and meet essential security requirements. Considering the security defects and structural problems of the protocol [8], the improved protocols in [9, 10] were proposed to defend against server emulation attacks. Rostampour et al. then proposed a privacy-preserving anonymous authentication protocol named ECC-bAP in [11]; the results indicated that the proposed protocol can achieve the untraceable purpose by traversing the registry. Then, the authors in [12] proposed an authentication protocol based on bilinear pairing to solve the problems of privacy protection and authentication table theft. Subsequently, the enhanced IoT mutual authentication protocol and improved ECC-based authentication protocol were proposed in [13, 14], respectively. To defend against more types of attacks including known temporary information attacks, DoS attacks, Panda and Chattopadhyay proposed an anonymous authentication scheme integrating a password validator in [15]. Further, Bhuarya et al. in [16] proposed an enhanced authentication scheme to defend known session-specific temporary information attack, where the hypertext transfer protocol (HTTP) cookies were used to authenticate clients. However, the large exponential powers employed by these protocols leads to a large amount of computation.

The dynamic pseudonym is an effective method to solve traceable problems. A pseudonym ID is used to conduct authentication between client and server and is dynamically updated after completion of authentication. Das et al. first proposed an authentication protocol [17] where dynamic ID technology was used to avoid the risk of ID theft. However, the protocol suffers from smart card theft attacks. Then, Jiang and Das et al. devoted to solving the problem in [18, 19], respectively. Notice when the above schemes are attacked asynchronously, i.e., the attacker blocks the exchange messages of the authentication protocol, and the interaction between the authentication parties is out of sync, such that the protocol cannot work. Thus, Gope et al. in [20–23] studied the authentication scheme based on emergency ID and secret key technology to solve the problem of asynchronous attack. In such schemes, clients and servers share a set of emergency IDs and keys in addition to dynamic pseudonyms. Once the dynamic pseudonyms are out of sync, emergency IDs and keys are used to interact. However, the emergency IDs and keys occupy a large amount of storage space, and once the emergency ID and emergency key are used up, the device must be reregistered. Recently, some researchers devoted to designing grant-free access scheme for M2M communications [24] and used the advanced methods to realize the authentication, e.g., deep learning [25, 26] and blockchain [27, 28]. However, they are not suitable for IoT devices with limited computing overhead.

1.2. Motivation and Contribution. To sum up, it can be found that the mentioned authentication protocols based on identity and pseudonym do not consider the privacy protection and cannot resist traceable attacks. For example, if the long-term key is leaked, the attacker can simulate the session key negotiation between the terminal and the server and occupy the position of the legitimate device. As a result, the legitimate device cannot carry out normal session key negotiation. Furthermore, during authentication process, the server needs to traverse the password verifier table to find the relevant registration information, and the search time increases linearly with the number of devices. The protocols with privacy protection cannot take into account both authentication efficiency and security while realizing anonymity. Dynamic pseudonym schemes are vulnerable to asynchronous attacks. Therefore, this paper focuses on the authentication between the edge server and device in the IoT and designs a new authentication protocol to realize the privacy protection and improve the efficiency of authentication. Our main contributions can be summarized as follows:

(i) We propose a lightweight anonymous authentication protocol (LAAP) based on elliptic curve cryptography (ECC) to implement security authentication between the servers and devices. Dynamic pseudonym is used to defend against traceable attacks caused by fixed identity identification. Besides, symmetric encryption is used to optimize the server's search for anonymous device information, and the time complexity is reduced from $O(n)$ to $O(1)$

(ii) We provide the formal analysis and informal analysis to validate the security of the proposed protocol. The analysis shows that the proposed protocol can satisfy the anonymity and defend against asynchronous attacks. We also perform random oracle models and AVISPA Tool to prove the security of the certification process

(iii) We provide extensive simulation results to testify the authentication efficiency of the proposed

protocol. The results indicate that the proposed scheme outperforms the benchmarks in terms of computation overhead, communication overhead, and storage overhead

Organization of this paper is as follows: In Section 2, we introduce the preliminaries. In Section 3, we present details of our proposed authentication protocol. Security analysis and performance evaluation are given in Sections 4 and 5, respectively. At last, Section 6 offers our conclusions and potential future works.

2. Preliminaries

In this section, we first introduce the system model and then introduce the related elliptic curve cryptography and the corresponding mathematical problems.

2.1. System Model. In this work, we focus on the authentication between cloud server (S) and embedded devices (D) in the IoT shown as Figure 1. The embedded device can be small devices (e.g., environmental sensors, cameras, and smart meters) or large-scale devices (e.g., intelligent vehicles and smart charging piles). The cloud server has powerful computing resources and storage resources, so that it can provide various services for embedded devices. For example, in mobile edge computing networks [29], the device first uploads data to the cloud server and then uses the computing resources to process its data. The cloud server also provides a bootstrap program for the system, enabling authentication to be performed smoothly. Before providing these services, they authenticate between the device and server to ensure legitimate access via wireless channels.

2.2. Elliptic Curve Cryptography. The security properties of ECC are mainly based on the intractable problem of discrete logarithms in elliptic curves. Given a prime field $\mathbb{F}_p$, the elliptic curve point is set $E_p(a, b)$ on the finite field can be expressed as

$$E_y(a,b): \{(a,b)|y^2 = x^3 + ax + b \mod p, x, y \in \mathbb{F}_y, 4a^3 + 27b^2 \mod p \neq 0\} \cup \{O\}, \tag{1}$$

where $a, b \in \mathbb{F}_p$, the prime number $p(p > 3)$ is the order of the finite field, and O represents the infinity point. The Ellipse Curve Discrete Logarithm Problem (ECDLP) can be described as follows:

Definition 1. ECDLP: let $\mathbb{G}$ denote the cyclic group generated by the base point G and the operation rules of Abelian groups on the elliptic curve $E_y(a, b)$. For a given $P, Q \in \mathbb{G}$, if $Q = kP$, where $k \in Z_p^*$, k cannot be solved in polynomial time, which is usually used as the private key.

Based on the ellipse curve and the ECDLP, the security if the ECC can be described as the Ellipse Curve Computation Diffie-Hellman Problem (ECCDHP), which is defined as follows.

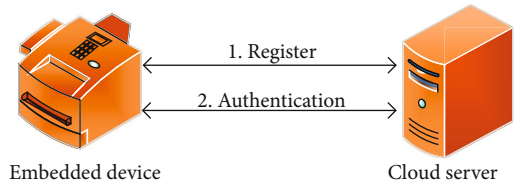


Figure 1: System model.

Definition 2. ECCDHP: let $\mathbb{G}$ be the cyclic group generated by the base point G and the operation rules of Abelian groups on the elliptic curve $E_y(a, b)$. For $P, Q, R \in \mathbb{G}$, if $Q = xP$ and $R = yP$, where $x, y \in Z$, we have that computing xyP in polynomial time is a hard problem.

2.3. Random Oracle Model. Random oracle model (ROM) is proposed by Bellare and Rogaway [30], which made the provable security methodology that was purely theoretical research in the past make significant progress in practical applications. When applying the ROM, the necessary work is to establish a security model that treats different subjects as random oracles (RO). The RO has the following three characteristics: (1) consistency: for the same query, RO will always return the same output; (2) computability: for different queries, RO can obtain results and return them in polynomial time; and (3) uniform distribution: for different queries, the output of RO is evenly distributed in the value space without collision that the output obtained by different queries is always different.

To prove the security of the model, it is necessary to establish an attacker $\mathcal{A}$ for the model and to provide the attacker with a simulated environment indistinguishable from the actual environment. For $\mathcal{A}$, the complexity and safety of the model boil down to mathematical computational difficulties (e.g., large factorization, ECDLP, and ECCDHP). In ROM, the convention judgement appears as

(1) Formally define the security of the scheme, assuming that the attacker can destroy the security of the protocol with a nonnegligible probability in polynomial time

(2) The attacker simulates the real environment by querying different random oracles

(3) The way of attacking the attacker and the result boils down to solving a mathematical problem

Although the ROM methodology cannot be used as absolute proof that the actual solution is safe, it can still be a necessary basic safety test. Thus, this paper adopts it to validate the security of the proposed protocol.

3. Design of the Authentication Protocol

In this section, we introduce the proposed LAAP protocol including three phases, i.e., initialization phase, registration phase, and authentication phase. A summary of the notations used in this article is provided in Table 1.

Table 1: List of the related notations.

Notation	Description
D_i, ID_i	The i device and its device ID
S	Cloud server
x	Cloud server symmetric key
PK_S, K	Server public key, private key
NID	Device pseudonym identification
NID'	Updated pseudonym identification
DID	Device real identity
DID'	Device updated real identity
$Sync$	Server sync value
N_1, N_2, R_i	Random number
$\mathbb{G}$	Cyclic additive group of order q
S_i	Device-side hash chain value
S_{ii}	Server-side hash chain value
$h()$	One-way hash function
$\|\|$	Connect operation
SK	Session key

3.1. Initialization Phase. Before authentication, the server needs to perform necessary parameter initialization operations. Initialization parameters are divided into public parameters and private parameters. The server selects an elliptic curve E based on the finite prime field $\mathbb{F}_p$ and selects the additive group of curve E of the order q. Then, the public key of the server PK_S can be calculated as $PK_S = K \times G$, where $K(K \in Z_q^*)$ is the private key and G is the generator of the group $\mathbb{G}$. The server also needs to select a suitable one-way hash function $h : \{0,1\}^* \longrightarrow \{0,1\}^{l_h}$, where the input is any length binary string and the output is a binary string of fixed length l_h. The server generates a random key x as a symmetric encryption key and selects an appropriate symmetric encryption algorithm as the basic algorithm for device identification update. The server publishes the parameters $\langle \mathbb{G}, PK_S, G, h \rangle$ as public parameters and stores $\langle x, K \rangle$ as private parameters.

3.2. Registration Phase. Before starting key negotiation, the device first needs to complete the registration. The LAAP protocol can ensure that the registration is completed by the public channel, and check whether the message responded by the server is legal. The registration process can be divided into three steps described as Figure 2. In the following, we will detail the three steps.

Step 1. The device D first selects an unique ID, which is only known by the device. Then, the device generates a random number N_1 to randomize its ID and calculates PID, Z_1, Z_2 and $PPID$ as $PID = h(ID\|N_1), Z_1 = N_1 \times G, Z_2 = N_1 \times PK_S$ and $PPID = PID \oplus Z_2$, respectively. Finally, the device sends the message $\langle Z_1, PPID \rangle$ to the server through the public channel.

Step 2. After receiving the registration information $\langle Z_1, PPID \rangle$ from D, server S uses the key K to restore the data, where Z_2^* and PID are calculated according to $Z_2^* = Z_1 \times K, PID = PPID \oplus Z_2^*$, respectively. After restoring PID, T_i is generated based on the device registration identity as $T_i = h(R_i\|PID\|h(K))$, which is used to calculate the identity information for each authentication of the device. Otherwise, the server also generates a new identity $PID_{\text{new}} = h(PID\|R_i)$ for the device as the identity of the authentication stage. The server will save two IDs for each device, i.e., PID_{new} and PID_{old}, where PID_{new} is the new device ID and PID_{old} is the old ID of the previous session. Then, the hash value of PID is used as the initial value of the hash chain, which will be updated during each session key negotiation process.

Subsequently, the server uses the hash value of the key K to encrypt T_i and S_i and stores the results in its database. After that, the server calculates the message of the response device as $Z_3 = (NID\|PID) \oplus S_i$ and $Z_4 = (T_i\|PID) \oplus S_i$. Finally, the server sends $\langle Z_3, Z_4 \rangle$ to the device through the public channel and stores $\langle PID_{\text{new}}, PID_{\text{old}}, U_i, X_i, \text{Sync} \rangle$ as the registration information corresponding to the device.

Step 3. After receiving the message $\langle Z_3, Z_4 \rangle$ from the server, the device uses the initial value of the hash chain to restore and verify the data as $(NID\|PID') = Z_3 \oplus S_i, (T_i\|PID') = Z_4 \oplus S_i$. By splitting the data, the device verifies whether the decrypted PID' is the same as the PID saved by itself. If they are the same, the device confirms that the message was sent by the server and stores $\langle NID, T_i \rangle$ as the registration information for subsequent identity authentication and key negotiation.

3.3. Authentication Phase. When the device wants to upload data or access the server, the device and server need to complete identity authentication and key negotiation. The authentication process can be divided into four steps described as Figure 3. In the following, we will introduce the four steps for details.

Step 1. Device D first generates a random number N_1 and calculates $P_1 = N_1 \times G$, $CK_i' = h(T_i\|S_i) \times G$, and $A_i = CK_i' \times N_1$, where CK_i' and A_i are temporary values generated by the synchronization hash chain and the identity information in the registration phase. Then, the verification message P_2 is generated as $P_2 = h(A_i\|S_i\|P_1)$. On the one hand, it can prevent message tampering, and on the other hand, it can verify whether the identity is legitimate. Finally, the device sends the message $\langle P_1, P_2, NID \rangle$ to the server for authentication.

Step 2. After receiving the message $\langle P_1, P_2, NID \rangle$, S restores the identity information DID based on the symmetric key x. If the recovery is successful, S can judge the recovery based on the matching information of the database; otherwise, terminate the session. When $DID = PID_{\text{new}}$, the server updates the synchronization hash value as $S_{ii} = h(S_{ii}\|\text{Sync})$ and reconstructs the authentication temporary value for this session as $CK_i = h(T_i\|S_{ii}), A_i' = CK_i \times P_1$. Then, S calculates the verification message P_2' as $P_2' = h(A_i'\|S_{ii}\|P_1)$. If $P_2 \neq P_2'$, it

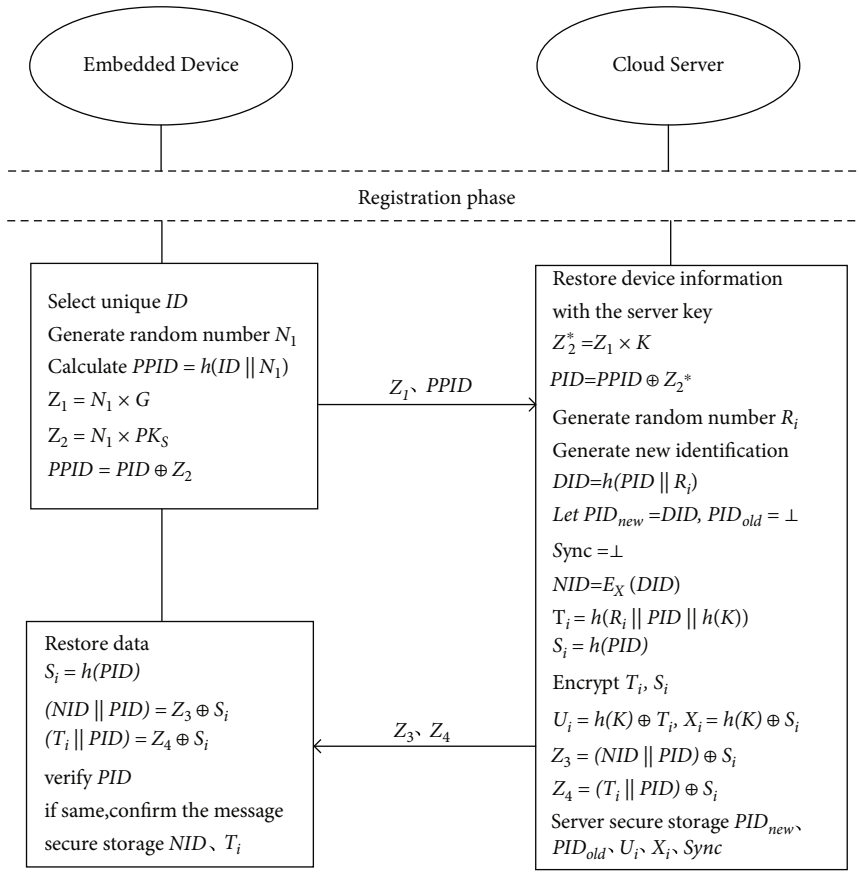


Figure 2: Illustration of registration phase of LAAP.

means that the message has been tampered with and the session is terminated. Otherwise, S generates a random number N_2 and a new identity for D as $DID' = h(DID \| N_2)$. Finally, S calculates the verification messages as $P_3 = NID' \oplus S_{ii}$, $P_4 = h(NID' \| S_{ii} \| A_i')$ and sends them to D.

Step 3. After receiving the message $\langle P_3, P_4 \rangle$, D decrypts and verifies the new ID $P_4' = h(NID' \| S_i \| A_i)$ where $NID' = S_i \oplus P_3$. If $P_4 \neq P_4'$, the message verification fails, and the session is terminated; otherwise, D calculates the negotiated session key and the verification message as $SK = h(A_i \| NID' \| NID)$, $P_5 = h(SK \| NID' \| NID)$. Finally, the device sends the message $\langle P_5 \rangle$ to the server.

Step 4. After receiving the message $\langle P_5 \rangle$, S can calculate the negotiated session key and verify the message as $SK = h(A_i' \| PID_{\text{new}} \| PID_{\text{old}})$ and $P_5' = h(SK \| PID_{\text{new}} \| PID_{\text{old}})$, respectively. If $P_5 \neq P_5'$,the server terminate the session, otherwise, the session key negotiation is successful.

4. Security Analysis

In this section, we provide the formal analysis and informal analysis to validate the security of the proposed protocol.

4.1. Formal Security Proof. For the formal analysis, we first adopts the widely accepted ROM [30] to verify the security of the proposed protocol.

4.1.1. Formal Security Proof with ROM. The extended RO is described as follows: $TestID(D_i, NID_i, OID_i)$ is used to query the real identity information of the device, where NID_i and OID_i represent the identity after session key negotiation and the identity before session key negotiation, respectively. $Corrupt(D_i, a)$ is used to query the secret information of the device and simulate the attack of the device being stolen.

There are two participants Π in this work, i.e., server S and the embedded device D. Each participant has multiple instances (i.e., ROs). Let D_i and S_i represent the i-th instance of them, respectively; DID_i and SID_i represent the identity of D_i and S_i that are used to negotiate the session key, respectively; NID_i and OID_i indicate the updated ID and the pre-updated ID of D, respectively; H_D^i and H_S^i, respectively, represent the hash chain status of D and S; SK_i^j represents the negotiated key for the j-th time.

If the instance S_i receives all the expected messages according to the predetermined steps, the instance enters the accepting state denoted as $Acc_{\Pi}^i = 1$. In this protocol, the parties negotiating the secure session key should meet the following conditions: (1) both S and D enter the

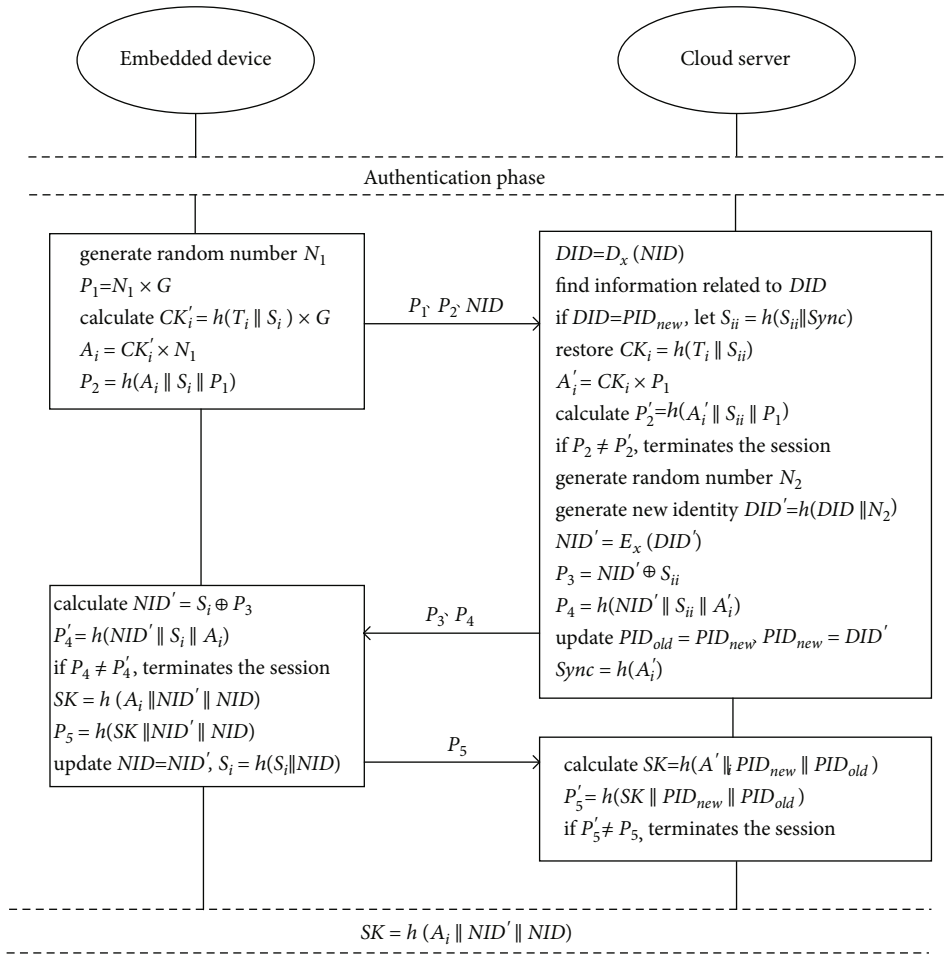


Figure 3: Illustration of authentication phase of LAAP.

receiving state, i.e., $Acc_D^i = Acc_S^i = 1$; (2) D updates the identity, $DID_i = NID_i$; (3) the identities of S and D are not empty, i.e., $DID_i \neq null$, $SID_i \neq null$

In the ROM, an attacker can simulate the attack by querying the RO. The included query is defined as follows:

Passive attack $Execute(D_i, S_i)$: the attacker can query the oracle to obtain the messages exchanged between D_i and S_i, giving the attacker the ability to eavesdrop on the channel.

Active attack $Send(\Pi, m)$: the attacker can interact with any participant by querying the oracle machine, and the oracle machine processes the message. If the message is valid, the oracle machine returns the processing result of message m; if the message is invalid, the oracle machine ignores the message.

$Reveal(\Pi)$: the attacker can obtain the session key of any participant by querying the oracle, and this query will only return the held key if the participant actually holds the session key. When an attacker queries the random oracle, the correct session key will be returned only if Π is accepted; otherwise, a random element in the state space will be returned.

$Corrupt(D_i, a)$: when $a = 1$, the hash chain value of D_i is fed back during the query. If the hash chain value is invalid, the random element in the state space is returned. When $a = 2$, the query information is the registration information T_i of D_i. If the registration information T_i is invalid, the random element in the state space is returned.

$TestID(D_i, NID_i, OID_i)$: the attacker can obtain the real identity of the device by querying the oracle. If the sent message D_i is accepted, it will return the real identity of the device; otherwise, it will return a random element in the state space. This oracle is used to test the anonymity of the protocol.

$TestSK(\Pi)$: when the attacker queries the oracle, the RO throws an unbiased coin b, and the result is used to determine whether the query returns the correct result. If $b = 0$, it returns a random element in the state space; if $b = 1$, and the participant holds the session key, return the correct session key; otherwise return it. The oracle tests the security of the negotiated session key, where the query can only be executed once.

Semantic security for session keys. In the defined ROM, attacker $\mathcal{A}$ can query the session key through $Reveal(\Pi)$ or $TestSK(\Pi)$, and random elements in the state space will be returned during the query process; query through $TestID(D_i, NID_i, OID_i)$ The real identity of the device. $\mathcal{A}$ needs to distinguish between random elements and real information. The goal of $\mathcal{A}$ is to guess the real information. At the end of

the experiment, the attacker returns a guess bit c^*. If $c^* = c$, then $\mathcal{A}$ wins the game event, which destroys the security of the protocol. $Succ_i$ denotes that $\mathcal{A}$ wins the ith experiment, and P denotes the constructed LAAP protocol. More precisely, the advantage of $\mathcal{A}$ overcoming the semantic security of the protocol is $\mathrm{Adv}_p = |2 \cdot \Pr[\mathrm{Succ}_0]| - 1$, if the experiment ends, the probability of obtaining $\mathcal{A}$ attack success is negligible, indicating that the protocol is semantically secure.

Based on the above definitions, we have the following theorem which proves the security of the proposed protocol.

Theorem 3. *Let Adv_P denote the advantage of an adversary $\mathcal{A}$ to break through the semantic security of the proposed protocol P, and let $Adv_{E_x}^{SE}$ denote the advantage of $\mathcal{A}$ in cracking the ciphertext symmetric encrypted with the server key pair within a probability polynomial, and let $Adv_{E_p}^{ECDLP}$ denote the advantage of solving the ECDLP problem of E_p in any polynomial time*

$$Adv_P \le \frac{2(q_s + q_e)^2 + 2q_t^2}{2^{l_h}} + 2Adv_{E_p}^{ECDLP}(t) + 2Adv_{E_x}^{SE}(t), \quad (2)$$

where E_p and E_x are the elliptic curve group and the symmetric encryption algorithm, respectively, and q_s, q_e, and q_t denote the times that attacker $\mathcal{A}$ executes the queries Send(Π, m), Execute(D_i, S_i), and TestID(D_i, a), respectively

Proof. Let $\Pr[\mathrm{Succ}_i]$ denote the probability that $\mathcal{A}$ wins in the i-th experiment. The contribution of the $(i+1)$-th experiment to the probability of $\mathcal{A}$ winning can be expressed $|\Pr[\mathrm{Succ}_i] - \Pr[\mathrm{Succ}_{i+1}]|$. The proof process can be described as the following five different experiments.

Experiment 1. This experiment corresponds to a real attack in the ROM. When $\mathcal{A}$ implements a real attack on the protocol P under the ROM model, we have

$$\mathrm{Adv}_P = |2 \cdot \Pr[\mathrm{Succ}_0]| - 1. \quad (3)$$

Experiment 2. This experiment is used to simulate an eavesdropping attack of an adversary $\mathcal{A}$. We know $SK = h(A_i \| NID' \| NID)$ in the protocol, where A_i is calculated by the embedded device through CK_i and random number N_1, and NID' is encrypted by the server with the secret key x. Even if intercepting all parameters transmitted during the authentication phase, $\mathcal{A}$ still cannot get it any information. Therefore implementing an eavesdropping attack cannot increase the probability of $\mathcal{A}$ winning, and we can obtain

$$\Pr[\mathrm{Succ}_0] = \Pr[\mathrm{Succ}_1]. \quad (4)$$

Experiment 3. This experiment is used to simulate all possible hash collisions in the authentication phase based on Experiment 2. $\mathcal{A}$ tries to find hash collisions, and if the same output is produced for different inputs, the game ends. According to the birthday paradox (the number of collision tests for a hash table of N bit length is not $2N$ but only N), we have

$$|\Pr[\mathrm{Succ}_2] - \Pr[\mathrm{Succ}_1]| \le \frac{(q_s + q_e)^2}{2^{l_h}}, \quad (5)$$

where q_s and q_e represent the times that attacker $\mathcal{A}$ queries $Send(\Pi, m)$ and $Execute(D_i, S_i)$, respectively.

Experiment 4. Based on Experiment 3, attacker $\mathcal{A}$ queries the device's secret information T_i and hash chain value S_i by adding $TestID(D_i, NID_i, OID_i)$. If $\mathcal{A}$ successfully obtains the information, the probability that $\mathcal{A}$ wins the experiment is

$$|\Pr[\mathrm{Succ}_2] - \Pr[\mathrm{Succ}_1]| \le \frac{q_t^2}{2^{l_h}}, \quad (6)$$

where q_t represents the times that the attacker $\mathcal{A}$ queries $TestID(D_i, a)$.

Experiment 5. Based on Experiment 4, the experiment adds that $\mathcal{A}$ can tamper with the authentication information and make legitimate participants believe the tampered message, i.e., $\mathcal{A}$ can eavesdrop on the message and can make Hash collision. The following two cases will occur: (1) $\mathcal{A}$ tampers with message P_1, and (2) $\mathcal{A}$ tampers with message P_3.

Case 1. In this case, after tampering with P_1, the adversary needs to solve how to correspond to the verification message P_2. For this reason, the adversary needs to solve the ECDLP problem, and guess N_1 and CK_i, (i.e., $2\mathrm{Adv}_P^{\mathrm{ECDLP}}(t)$), so that it can guess CK_i. Besides, $\mathcal{A}$ still needs to solve a symmetric key problem to generate legal P_5, i.e., $\mathrm{ADV}_{E_x}^{SE}(t)$. Overall, we have

$$\Pr[\mathrm{Succ}_4|\mathrm{Case1}] \le 2\mathrm{Adv}_{E_p}^{\mathrm{ECDLP}}(t) + \mathrm{Adv}_{E_x}^{SE}(t). \quad (7)$$

Case 2. In this case, $\mathcal{A}$ tampers with P_3 to impersonate the server. Assuming that $\mathcal{A}$ has obtained the synchronization value S_i shared by the device and the server, $\mathcal{A}$ still needs to solve the symmetric key decryption problem, i.e., $\mathrm{Adv}_{E_x}^{SE(t)}$. Similarly, if $\mathcal{A}$ has decrypted the current symmetric key problem, $\mathcal{A}$ still needs to solve the ECDLP problem to obtain the legal A_i, i.e., $\mathrm{Adv}_{E_p}^{\mathrm{ECDLP}}(t)$. Thus, we have

$$\Pr[\mathrm{Succ}_4|\mathrm{Case2}] \le \mathrm{Adv}_{E_p}^{\mathrm{ECDLP}}(t) + \mathrm{Adv}_{E_x}^{SE}(t). \quad (8)$$

In summary, the probability that the adversary $\mathcal{A}$ wins in Experiment 5 is

$$|\Pr[\mathrm{Succ}_4] - \Pr[\mathrm{Succ}_3]| \le \mathrm{Adv}_{F_p}^{\mathrm{ECDLP}}(t) + \mathrm{Adv}_{E_x}^{SE}(t). \quad (9)$$

All random predictions are simulated in the above four experiments. The results indicate that $\mathcal{A}$ has no advantage in guessing the bit c, and the only way to pass the test is to

perform $TestSK(\Pi)$ query guessing, i.e.,

$$\Pr[\mathrm{Succ}_4] = \frac{1}{2}. \tag{10}$$

Using the triangle inequality, we can obtain

$$\frac{1}{2}\mathrm{Adv}_P = |\Pr[\mathrm{Succ}_0] - \Pr[\mathrm{Succ}_4]|. \tag{11}$$

Based on (3)–(8), we have

$$|\Pr[\mathrm{Succ}_0] - \Pr[\mathrm{Succ}_4]| \le \frac{(q_s + q_e)^2}{2^{l_h}} + \frac{q_t^2}{2^{l_h}} + \mathrm{Adv}_P^{\mathrm{ECDLP}}(t) + \mathrm{Adv}_{E_x}^{SE}(t). \tag{12}$$

Submitting (12) into (11), we can obtain (2). □

Remark 4. This result indicates that the adversary $\mathscr{A}$ has no extra advantage to win the experiment and the proposed scheme is secure.

4.1.2. Formal Security Proof with AVISPA Tool. In this part, the AVISPA verification tool is used to verify the security of the LAAP protocol. The experimental environment is Oracle VM VirtualBox, SPAN-Ubuntu10.10-light. The HLPSL language description of the protocol is divided into the following five dimensions.

Role attributes: D and S are two agents, Hash and Mutli are two hash functions, Kab is a symmetric key, and Snd and RCV are the communication channels between the client and the outside world. The local variables defined are the same as the protocol description, as shown in Figure 4(a). The modeling of the server is similar to that of the client, as shown in Figure 4(b).

Role conversion process: the conversion process of D in LAAP is divided into three stages: register1 means that D starts to register and sends registration information to S; register2 means that D receives the response from S, conducts authentication calculation, and initiates an authentication request; authentication1 indicates that D receives the response from S and completes the final authentication process, as shown in Figure 5(a). Similarly, the conversion process of S is also divided into three stages: register indicates that S requests the registration information of D; authentication1 means that S receives the authentication request of D and performs verification and response; authentication2 means that S receives the response of D and completes the final authentication process, as shown in Figure 5(b).

Session attributes: the modeling of LAAP session attributes defines the rules that the communicating entities follow. The definition of basic attributes includes the role agents D and S, hash functions Hash and Multi, symmetric key Qi, and communication channels SND and RCV as shown in Figure 5(c).

Environmental attributes: the definition content of LAAP environment includes the communication channel of the communication entity, communication entity (including d, s, and i), security target constant, and session combination, as shown in Figure 5(d).

Safety goals: the security goal describes the secret information "secrecy_of" and the authentication quantity "authentication_o" of the communication entity defined in the protocol shown in Figure 6.

The OFMC simulation results are shown in Figure 6, and the ATSE simulation results are shown in Figure 6. From Figure 7, we can see that the LAAP realizes two-way authentication while resisting man-in-the-middle attacks and replay attacks, which proves the security of the protocol.

4.2. Informal Security Analysis. Informal security analysis mainly consists of two parts, i.e., basic function security and common attack defense. Basic functional security includes mutual authentication and device anonymity. Common attacks resistance mainly includes traceable attack defense, asynchronous attack defense, DoS attack defense, replay attack defense, and simulation attack defense.

Mutual authentication. In the LAAP protocol, server S authenticates the legal identity of device D based on the message $\langle P_1, P_2, NID\rangle$ and then restores the identity of the device with NID. This precess is performed through symmetric encryption. If S gets a string of garbled characters after decrypting NID or cannot find matching information in the verification table, S will discard the authentication message. After successfully decrypting NID and obtaining the device's identity DID, S verifies the authenticity of the device with $CK_i = h(T_i \| S_{ii}), P_2' = h(A_i' \| S_{ii} \| P_1)$. If $P_2 = P_2'$, the verification is passed. In the response message $\langle P_3, P_4\rangle$, P_3 contains the new identity of the device, which is encrypted by the hash chain value synchronized by both parties, and P_4 contains the authentication information A_i. Notice that only valid S can calculate A_i'. Thus, if the P_4' calculated by the device is the same as the received P_4, D can confirm the legal identity of S

Device anonymity. Device anonymity means that attacker $\mathscr{A}$ cannot obtain any identifying information about the participants by listening to the messages in the channel. In the LAAP, the method of dynamic pseudonym and synchronous hash chain are used to solve the anonymity of the device. Notice that the identity identification NID is dynamically updated in the second phase of device authentication so that the identity identifications are different at different session stages. Under the Deolv-Yao attack model [31], $\mathscr{A}$ is completely unable to distinguish the attribution of different sessions. Therefore, the proposed protocol satisfies the anonymity requirement of the device.

Traceable attack defense. Traceable attack means that attacker $\mathscr{A}$ can identify the belonging of messages by listening to the information in the channel, so as to carry out specific analysis to undermine the security of the protocol. Recall that the LAAP protocol used the dynamic pseudonym. Thus, after each successful session key negotiation, the device identity is updated. That is, the NID^i sent in the i-th session is completely different from the NID^{i+1} sent in the $(i+1)$-th session. Therefore, $\mathscr{A}$ cannot determine which communication entity the session message belongs to and

```
role client(
    D, S: agent,
    Hash, Multi:hash_func,
    Kab : symmetric_key,
    SND,RCA : channels(dy))
played_by D def=
    local
        State : nat,
        PID, DID, Ga,N1, PIDi : text,
        Si, Ti, Ck, Ui, Vi, Cki : message,
        SK, Viii, P1, Ai : message,
        P2, Vii, Yi, NID, Yii: message
    init
        State := 0
    transition
        …
end role
```

(a) Role attribute of D

```
role server(
    D, S: agent,
    Hash, Multi: hash_func,
    Kab : symmetric_key,
    SND,RCA : channels(dy))
played_by D def=
    local
        State : nat,
        PID, Xs, Ra, DID, SS, Ga : text,
        Sii, PKs,PIDi, PPID, N2 : text,
        Ti, Ui, VI,P1, P2, Vii, Yi, Cki, Ckii: message,
        P22, NID, Viii, Sk, SViii, Ai : message
    init
        State := 1
    transition
        …
end role
```

(b) Role attribute of S

Figure 4: Role attributes of the client D and the serve S.

```
register1. State = 0 /\ RCV(start) =|>
    State′ := 2 /\ Si′ := Hash(PID)/\ SND(PID_Kab)
        /\secret(PID,secret_of_pid, D, S)/\ secret(Si′, secret_of_si, D)
register2. State = 2 /\ RCV(Ui′.Vi′_Kab)=|>
    State′ := 4 /\ DID′ := xor(Vi′, PID)
        /\ Ti′ := xor(Ui′, PID) /\ Ck′ := Hash(Ti′.Si) /\ Cki′ := exp(Ga, Ck′)
        /\ Ck′ := exp(Ga, Ck′) /\ N1′ := new()
        /\ P1′ := exp(Ga, N1′) /\ Ai′ := exp(Cki′, N1′)
        /\ P2′ := Hash(Ai′.Si) /\ PIDi′:= xor(PID, Si)
        /\SND(exp(Ga, N1′).Hash(Ai′.Si). xor(PID, Si))
        /\SND(exp(Ga, N1′).Hash(Ai′.Si). xor(PID, Si))
        /\ secret(Cki′, secret_of_cki, D) /\ secret(DID′, secret_of_did, D)
        /\ secret(Ai′, secrecy_of_ai, D, S) /\ secret(N1′, secrecy_of_n1, D)
authentication1. State = 4 /\ RCV(Vii′.Yi′)=|>
    State′ := 6 /\ NID′ := xor(Vii′, Si) /\ Yii′ := Hash(NIS′.Si.Ai)
        /\ SK′ := Hash(Ai.NID′) /\ Viii′ := Hash(SK′.NID′)
        /\ SND(Viii) /\ witness(S, D, auth_d2s_nid, NID′)
        /\ request(D, S, auth_s2d_pid, PID)
```

(a) Role change process of D

```
register. State = 1 /\ RCV(PID_Kab) =|>
    State′:= 3/\ Xs′ := new() /\ Ra′:=new()
        /\ DID′ := ncw() /\ PKs′:= cxp(Ga, SS)
        /\ Ti′ := Hash(Ra′.Hash(DID′).Hash(Xs′))
        /\ Ui′ := xor(Ti′, PID) /\ Vi′ := xor(PID, DID′)
        /\ Sii′:= Hash(PID) /\ SND(Ui′.Vi′_Kab)
        /\ secret(Sii′, secret_of_sii, S) /\ secret(Ui′, secret_of_ui, S)
        /\ secret(Vi′, secret_of_vi, S) /\ secret(Ti′,secret_of_ti, D, S)
authentication1. State = 3 /\ RCV(P1′.P2′.P1Di′)=|>
    State′ := 5 /\ PPID′:= xor(PIDi′, Sii) /\ witness(D, S, auth_s2s_pid, PPID′)
        /\ Cki′ := Hash(Ti,Sii)/\Ckii′ := exp(Ga, Cki′)
        /\ Ai′ := exp(P1′, Ckii′) /\ P22′ := Hash(Ai′, Sii)
        /\ N2′:= new( )/\ NID′ := Hash(PPID′.Cki′.N2′)
        /\ Vii′:= xor(NID′, Sii) /\ Yi′:= Hash(NID′.Sii.Ai′) /\ SND(Vii′.Yi′)
        /\ secret(N2′, secrecy_of_n2, S) /\ secret(NID′, secret_of_nid, D, S)
authentication2. State = 5 /\ RCV(Viii′) =|>
    State′ := 7 /\ Sk′:= Hash(Ai.NID) /\SViii′:= Hash(SK′.NID)
        /\ request(S, D, auth_d2s_nid, NID)
```

(b) Role change process of S

```
role session(
    D, S : agent,
    Hash, Multi: hash_func,
    Qi: symmetric_key,
    SND, RCV: channel(dy))
def=
    local
        SA,SB:channel(dy),
        RA,RB:channel(dy)

    composition
        device(D, S, Hash, Multi, Qi, SA, RA)
        /\ server(D, S, Hash, Multi, Oi, SB, RB)
end role
```

(c) Session attributes

```
role environment() def=
    local
        SND, RCV: channel(dy)
    const
        d, s, i: agent,
        h1, mu1: hash_func,
        ds, di, is: symmetric_key,
        secret_of_pid,secret_of_si : protocol_id,
        secret_of_cki, secret_of_did : protocol_id,
        secret_of_sii,secret_of_ui : protocol_id,
        secret_of_vi, secret_of_ti : protocol_id,
        secrecy_of_ai, secrecy_of_n1: protocol_id,
        secrecy_of_n2, secrecy_of_nid : protocol_id,
        auth_s2d_pid, auth_d2s_nid : protocol_id
        intruder_knowledge = {d, s, h1, mul}

    composition
        session(d, s, h1, mu1, ds, SND, RCV)
        /\ session(d, s, h1, mu1, ds, SND, RCV)
        /\ session(d, i, h1, mu1, di, SND, RCV)
        /\ session(i, s, h1, mu1, is, SND, RCV)
end role
```

(d) Environmental attributes

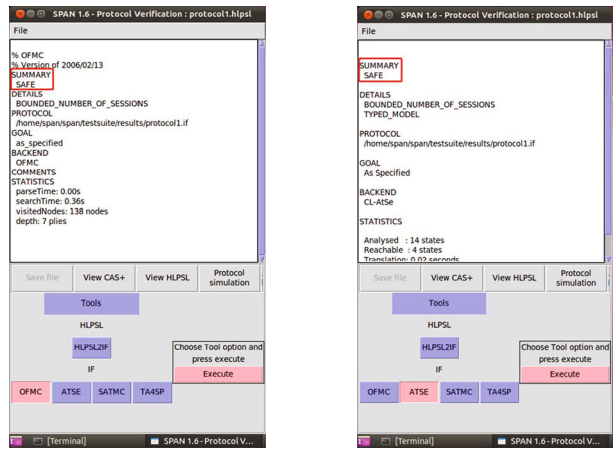
Figure 5: Role change process, session attributes, and environmental attributes.

```
goal
    % device register
    secrecy_of secret_of_pid,secret_of_si
    secrecy_of secret_of_cki,secret_of_did
    % device register
    secrecy_of secret_of_sii,secret_of_ui
    secrecy_of secret_of_vi,secret_of_ti
    secrecy_of secret_of_n2,secret_of_nid
    secrecy_of secret_of_ai,secret_of_n1
    authentication_on auth_s2d_pid
    authentication_on auth_d2s_nid
end goal
```

Figure 6: Description of the safety goals.

also cannot track the session information of specific equipment.

Asynchronous attack defense. An asynchronous attack intercepts message transmission to make protocol participants lose synchronization. As a result, the protocol cannot be executed correctly, thus destroying the protocol. According to the LAAP, the messages transmitted on the public channel includes $\langle P_1, P_2, NID\rangle$, $\langle P_3, P_4\rangle$, and $\langle P_5\rangle$. There are two messages related to synchronization information, i.e., the initial authentication message $\langle P_1, P_2, NID\rangle$ and the response message $\langle P_3, P_4\rangle$ sent by S and D, respectively. For attacker $\mathcal{A}$, intercepting message $\langle P_1, P_2, NID\rangle$ has no



(a) OFMC backend simulation results (b) ATSE backend simulation results

Figure 7: Verification results of security with AVISPA.

effect on the synchronization of the protocol. Thus, we only consider the following two cases.

Case 1 ($\mathscr{A}$ intercepts the message). S has updated the device ID as $PID_{\text{new}} = DID^{i+1}$, $PID_{\text{old}} = DID^{i}$ because S has already processed the message i. At this time, due to the information interception, the identity identifier DID^{i} of D is the corresponding NID^{i}. When the timer of D expires, D will regenerate the random number to reauthenticate and send the message $\langle P_1^i, P_2^i, NID^i \rangle$ to S. We can see that $PID_{\text{old}} = DID^{i}$, and S will determine that D is out of synchronization, and the current hash value is directly used for authentication.

Case 2 ($\mathscr{A}$ intercepts the message $\langle P_5 \rangle$). The system status is that S updated the device ID, and D updated the device ID and hash chain value. After $\langle P_5 \rangle$ is intercepted, the hash chain value of the protocol participant S is synchronously behind D. When the timer of device D expires, D resends the authentication message $\langle P_1^{i+1}, P_2^{i+1}, NID^{i+1} \rangle$, and $PID_{\text{new}} = DID^{i+1}$. the hash chain value will be updated, and $Sync$ will be used in the update process. Therefore, D and S will resume synchronization.

DoS attacks defense. DoS attack means that attacker $\mathscr{A}$ sends a large amount of invalid authentication information to the server, which consumes the computing resources of the server and makes the server unable to provide services normally. In the protocols in [11, 15], there is a way to find information about related devices by traversing the password check table or the local registry. Thus, their time complexity is $O(n)$. When there are enough registrations, even if most of the devices are offline, the server will go through all the devices during the authentication process. The proposed LAAP protocol combine the dynamic pseudonym with symmetric encryption, and the time complexity is reduced from $O(n)$ to $O(1)$. So, the proposed protocol has a high authentication efficiency and can resist DoS attacks.

Replay attacks defense. Replay attack means that the attacker resends the message sent in the history negotiation stage to the server, thus achieving the purpose of spoofing. In LAAP, the messages transmitted by the public channel consist $\langle P_1, P_2, NID \rangle$,$\langle P_3, P_4 \rangle$, and $\langle P_5 \rangle$. Let the message sent by the device in the i-th session be $\langle P_1^i, P_2^i, NID^i \rangle$, the message sent by the server be $\langle P_3^i, P_4^i \rangle$, and the response message from the device be $\langle P_5^i \rangle$. Thus, there would be the following three cases.

Case 1 ($\mathscr{A}$ replays the message $\langle P_1^i, P_2^i, NID^i \rangle$). We will analyze it from two subcases. In subcase 1, the attacker launches a replay attack in the middle of the i-th and $(i+1)$-th key negotiation at the device side. Note that the device has not performed the $(i+1)$-th key negotiation. Because the server will store the ith device identity, the server will find $PID_{\text{old}} = D_x(NID^i)$ in the authentication table and will consider that device is out of asynchrony. So in the next step of message verification, the server will calculate $\text{Sync} = h(A_i')$ and classify the message as a replay attack and discard the session. In subcase 2, $\mathscr{A}$ uses the device history negotiation information $\langle P_1^{i-n}, P_2^{i-n}, NID^{i-n} \rangle$, where $n \in [0, i-1)$): After receiving $\langle P_1^{i-n}, P_2^{i-n}, NID^{i-n} \rangle$, the server uses key symmetric decryption to get the $(i-n-1)$-th device identity based on NID^{i-n}. But the server cannot find the relevant information in the database, and it will discard the session.

Case 2 ($\mathscr{A}$ replay the message $\langle P_3^i, P_4^i \rangle$). Similarly, we will analyze it from two subcases. Subcase 1 is similar to the above subcase. After receiving $\langle P_3^i, P_4^i \rangle$, the device will decrypt P_3^i to obtain the new device identifier $NID^{i'}$. At this time, the hash chain value at the device has been updated, and $P_4^{i'}$ computed by the device is different from the received P_4. So, the device will terminate the session. For subcase 2, after receiving the history information $\langle P_3^{i-n}, P_4^{i-n} \rangle$ (where $n \in [0, i-1)$), the device will decrypt P_3^{i-n} to get the identity NID^{i-n+1}. However, because the hash chain value has been updated several times, $NID^{i-n+1'}$ obtained by decrypting

$P_4^{i-n'}$ is different from P_4^{i-n}. Thus, the device will terminate the session.

Case 3 ($\mathscr{A}$ replay the historical message $\langle P_5^i \rangle$). The server will use the new authentication information and message to calculate as follows:

$$SK = h\left(A'_{i\_\text{new}} \| NID'_{\text{new}} \| NID_{\text{new}}\right),$$
$$P'_{5\_\text{new}} = h(SK_{\text{new}} \| SK_{\text{new}}). \tag{13}$$

We can find that P'_{5_new} is different from P_5^i. Thus, the session key negotiation cannot be successful, and the server will discard the session.

Based on the analysis of the above three cases, we proof that the proposed protocol can resist the replay attacks.

Simulation attack defense. An emulation attack means that the attacker tampers authentication information to establish session keys on the simulated device or server. An attacker $\mathscr{A}$ can tamper with or send historical authentication messages to spoof the device or the server based on the intercepted authentication messages.

For messages $\langle P_1, P_2, NID \rangle$, $\mathscr{A}$ has no access to the registration information T_i and the synchronization hash value of the device, so it cannot obtain the legitimate P_2 to spoof S. If $\mathscr{A}$ replays the historical messages, see the above analysis for details. For messages $\langle P_3, P_4 \rangle$, $\mathscr{A}$ cannot know symmetric encryption key x of S and the authentication message A'_i generated in this session, so it cannot compute the legitimate P_3 and P_4. If $\mathscr{A}$ replays the historical message, the session is terminated due to authentication failure. For message $\langle P_5 \rangle$, $\mathscr{A}$ cannot know the authentication message A'_i of this session, so that it cannot compute P_5. If $\mathscr{A}$ replays the history message, the authentication will fail, and S terminates the session. In summary, the proposed protocol can resist the simulation attacks.

We provide Table 2 to show the comparison of security performance between LAAP and the benchmarks. The dimension of comparison is based on the basic functional security and common attack resistance described in the above. In Table 2, where "Yes" (resp. "No") indicate that the protocol can (cannot) support the security feature, and "—" indicates that the protocol does not involve this security feature. From Table 2, we can see that the proposed LAAP protocol can resist more security attacks.

Table 2: Comparison of security performance.

Index Bench	S1	S2	S3	S4	S5	S6	S7
Cws	No	No	No	No	Yes	No	—
Wang	Yes	No	Yes	No	Yes	No	—
Panda	Yes	Yes	Yes	Yes	Yes	No	—
Rostampour	Yes	Yes	Yes	Yes	No	Yes	—
Bhuarya	Yes	Yes	Yes	Yes	Yes	No	—
LAAP	Yes	Yes	Yes	Yes	Yes	Yes	Yes

S1-S7 are the index of the mutual authentication, device anonymity, traceable attack defense, asynchronous attack defense, DoS attacks defense, replay attacks defense, and simulation attack defense, respectively.

5. Performance Evaluation

In this section, we provide the performance comparisons between the prosed LAAP protocol with several related protocols [9–11, 15] in terms of computational overhead, storage overhead, and communication overhead. For a fair comparison, all experiments use the http://golang.org/x/crypto/bn256 curve and the hash function SHA-256.

5.1. Computational Cost Analysis. We first provide the comparison of a computational overhead between the proposed protocol and the benchmarks. The computational cost is divided into the time-consuming of the device in the registration phase and the authentication phase. The calculation overhead is shown in Table 3. From Table 3, we can see that in the registration stage, the proposed protocol increases the computational overhead of the device but reduces the overhead of the server. We also can observe that in the authentication stage, we reduce the computational overhead of both the device and server. Finally, the results of total overhead indicate that the proposed scheme outperforms the benchmarks.

In order to show the total computation cost under different numbers of devices, we plot Figure 8. We can observe that compared with the benchmarks, the proposed protocol can bring a lower computation cost. Furthermore, as the number of devices increases, the performance improvement of our protocol becomes more obvious. Therefore, the proposed protocol is more suitable for deployment in the IoT with a large number of devices.

5.2. Storage Cost Analysis. Here, we provide the comparison of the store overhead between the proposed protocol and the benchmarks. The store cost consists the space-consuming of the device in the registration phase and the authentication phase. In the analysis process, SHA-256 and bn256 are used as the hash function and elliptic curve, respectively.

According to Figure 2, the storage information at the device includes NID_i, T_i, and S_i. So the storage space required at the device side is $256 + 256 + 256 = 768$ bits in the registration phase. As Figure 3 shown, the storage space required by the server is $256 + 256 + 256 + 256 + 256 = 1280$ bits in the authentication phase. The storage overhead of the benchmarks is calculated in the same way, and the detailed data is shown in Table 4. To show the comparison results more visually, we provide Figure 9. We can observe that the storage space required by the LAAP protocol at the device is consistent with the minimum storage required by the benchmarks, and the store overhead at the server only be higher than the protocol in [11]. Thus, our protocol requires higher storage overhead than the protocol in [11] but lower than other protocols in [9, 10, 15].

5.3. Communication Cost Analysis. Finally, we provide the comparison of the communication cost between the proposed protocol and the benchmarks. Similarly, the

Table 3: The comparison of calculation overhead (ms).

		Regist.	Authen.	Total
[9]	Device	0	71.0163	206.4185
	Server	53.4174	81.9848	
[10]	Device	0	66.0148	183.1098
	Server	54.8872	62.2078	
[11]	Device	9.8241	93.9545	318.3577
	Server	52.4631	162.116	
[15]	Device	0.5751	94.8175	328.901
	Server	12.0247	221.4837	
LAAP	Device	45.1705	46.3724	149.3163
	Server	12.998	44.7754	

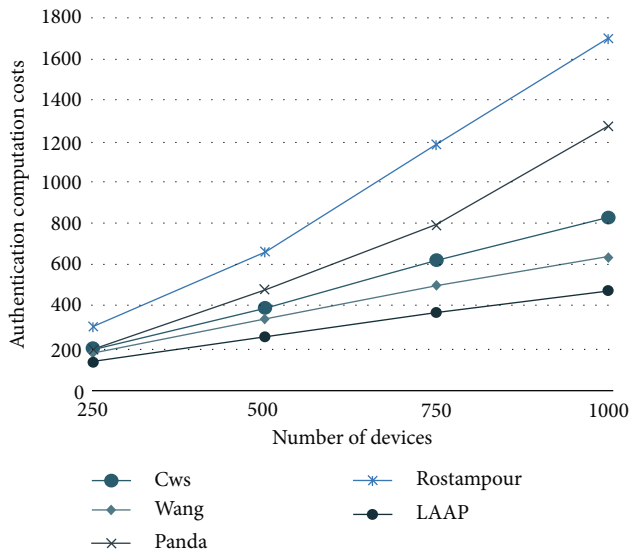


Figure 8: Total computation cost vs. various number of devices.

Table 4: The comparison of store overhead (bits).

	Registration	Authentication	Total
[9]	1024	1280	2304
[10]	768	1280	2048
[11]	768	768	1536
[15]	1536	1793	3329
LAAP	768	1280	2048

communication cost consists the consumption of the device in the registration phase and the authentication phase.

According to Figure 2, the information transmitted by the device includes Z_1, $PPID_i$, Z_3, and P_4. So the communication cost in the registration phase is $256 + 512 + 256 + 256 = 1280$ bits. As Figure 3 shown for the proposed protocol, the communication overhead at the server is $512 + 256 + 256 + 256 + 256 + 256 = 1792$ bits in the authentication phase. The communication overhead of the benchmarks is calculated in the same way and the detailed data is shown in Table 5..

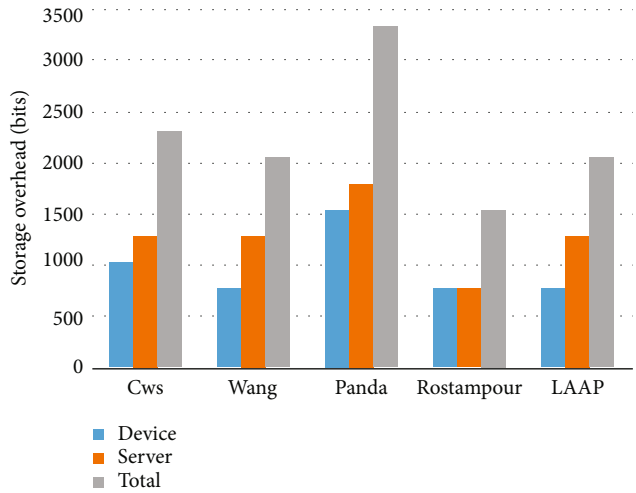


Figure 9: Storage cost comparison.

We further provide Figure 10 to show the detailed comparison. We can see from Figure 10 that the communication overhead of the proposed protocol in the registration phase is slightly higher than the benchmarks. That is due to the fact that the proposed protocol takes necessary encryption measures to ensure public channel registration. However, the proposed protocol takes the lowest communication overhead. Considering that in practical applications, the number of registration stages is much less than the number of authentication stages, it is acceptable to increase the overhead of registration stage slightly. We can also find that the proposed protocol has the lowest total communication overhead and an average of 12.73% reduction in terms of communication overhead compared to other protocols.

5.4. Performance Analysis under Different Number of Devices. To verify the performance of the proposed protocol under a large number of devices, the stress testing tool GO-WRK and custom scripts are used in this subsection to analyze the performance of the device registration module, server registration module, and identity authentication module of the system.

We first analyze the average response time for different numbers of the devices in the registration phase in Table 6. We can see that when the number of registered devices is less than 1400, the server has a relatively fast response rate, and the average response time is 48.57 ms. When the number of registered devices is greater than 1400, the response time increases proportionally as the number of devices increases. It indicates that when the number of registrations is higher than 1400, the system performance is saturated and all resources are fully utilized.

Then, we provide Table 7 to show the average cost under the different number of devices in the certificate phase. As shown in Table 7, under the LAAP protocol, the average time consumption of the devices is 58.15 ms, and as the number of concurrent devices increases, the device time consumption is basically stable. When the server does not reach saturation, the server takes an average of 64.1 ms. After the server reaches saturation, the response time of

Table 5: The comparison of communication overhead (bits).

	Registration	Authentication	Total
[9]	1024	2560	3584
[10]	768	2304	3072
[11]	768	3072	3840
[15]	1280	2304	3584
LAAP	1280	1792	3072

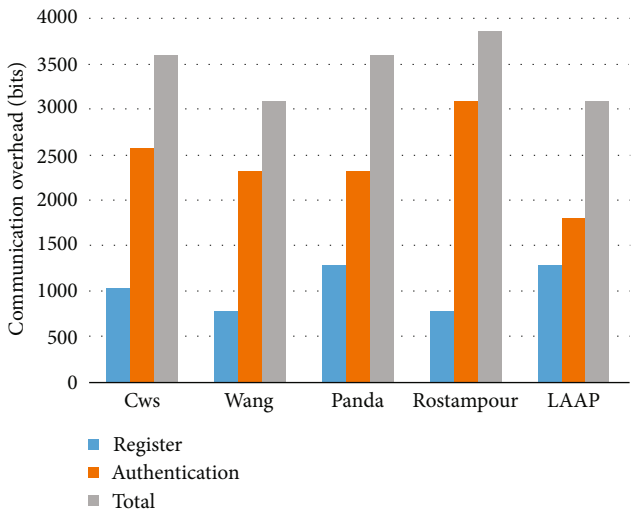


Figure 10: Communication cost comparison.

Table 6: Average response time of devices in the registration phase (ms).

Num.	Ave-time	Suc. rate	Num.	Ave-time	Suc. rate
200	48.31	100%	1800	93.23	100%
600	47.32	100%	2000	122.76	100%
1000	48.03	100%	2200	157.72	100%
1400	50.61	100%	2400	189.31	100%
1600	60.87	100%	2600	225.12	100%

Num.: number of devices; Ave. time: average response time; Suc. rate: success rate.

Table 7: Average cost in the certification phase.

Num.	D-Cost (ms)	S-Cost (ms)	Aut-efficiency
200	58.11	63.21	100%
400	56.98	65.79	100%
600	56.43	64.33	100%
800	57.21	63.31	100%
1000	56.45	62.75	100%
1200	58.97	65.21	100%

Num.: number of devices; D-Cost and S-Cost: average cost at device and serve, respectively.

the server increases with the number of concurrent authentication devices. The saturation threshold of the server is 1200 devices. In the case of a single server, the server can quickly complete the authentication and key negotiation of 1200 devices.

6. Conclusion

In this work, we proposed a lightweight anonymous authentication protocol named LAAP against asynchronous attacks to realize the anonymous authentication between device and server in the IoT. Through informal security analysis and formal security analysis, we found that the proposed protocol has the following advantages: (1) it can solve the problem that the device identification is fixed and easy to be tracked by dynamically updating the identification; (2) the hashing chain value of communication devices can be adaptively synchronized to resist asynchronization attack; (3) the time complexity of finding the registration information of the device through the anonymous identity of the device is $O(1)$. Besides, extensive results were provided to indicate that the total overhead is lower than the benchmarks.

Note that this work only considers identity authentication within a single network domain. Therefore, the lightweight anonymous authentication of the IoT across network domains will be the future research direction. In addition, using the intelligent algorithms [32] to optimize our methods and solve the authentication of large-scale heterogeneous devices are also the future research.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported in part by the National Key R&D Program of China (Grant No. 2018YFE0207600), the National Natural Science Foundation of China (NSFC) under Grant 61972308, the Basic and Applied Basic Research Fund of Guangdong Province (Grant No. 2021A1515111017), and the Natural Science Basic Research Program of Shaanxi (Program No. 2019JC-17).

References

[1] GSMA, "The mobile economy 2022," 2022, https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf.

[2] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: opportunities and challenges," in *2014 IEEE World Forum on Internet of Things*, pp. 375-376, Seoul, Korea, 2014.

[3] M. R. Simpson, *Assessment of the Impact of Cyberattacks on Power System Stability-Manipulation of Controllable Loads in Smart Homes, M.S. Thesis*, High Voltage Equipment and Grids, Digitalization and Energy Economics, 2021.

[4] NSFOCUS, "Cybersecurity in the context of building a cyber power," 2022, http://blog.nsfocus.net/wp-content/uploads/

2022/03/Cybersecurityin-the-Context-of-Building-a-Cyber-Power.pdf.

[5] Unit 42, *2020 Unit 42 IoT Threat Report*, Technical Representative, 2020.

[6] C. Wu, "An overview on the security techniques and challenges of the internet of things," *Journal of Cryptologic Research*, vol. 2, no. 1, pp. 40–53, 2015.

[7] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IOT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606–1616, 2019.

[8] S. Kalra and S. K. Sood, "Secure authentication scheme for IOT and cloud servers," *Pervasive and Mobile Computing*, vol. 24, pp. 210–223, 2015.

[9] C.-C. Chang, H.-L. Wu, and C.-Y. Sun, "Notes on "secure authentication scheme for IoT and cloud servers"," *Pervasive and Mobile Computing*, vol. 38, pp. 275–278, 2017.

[10] K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, "A secure authentication scheme for internet of things," *Pervasive and Mobile Computing*, vol. 42, pp. 15–26, 2017.

[11] S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, "ECCbAP: a secure ECC-based authentication protocol for IoT edge devices," *Pervasive and Mobile Computing*, vol. 67, article 101194, 2020.

[12] H.-L. Wu, C.-C. Chang, and L.-S. Chen, "Secure and anonymous authentication scheme for the internet of things with pairing," *Pervasive and Mobile Computing*, vol. 67, article 101177, 2020.

[13] S. Bhubaneswari and N. Ananth, "Enhanced mutual authentication scheme for cloud of things," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 15, pp. 1571–1583, 2018.

[14] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IOT and cloud servers," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, 2018.

[15] P. K. Panda and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment," *Journal of Reliable Intelligent Environments*, vol. 6, no. 2, pp. 79–94, 2020.

[16] P. Bhuarya, P. Chandrakar, R. Ali, and A. Sharaff, "An enhanced authentication scheme for internet of things and cloud based on elliptic curve cryptography," *International Journal of Communication Systems*, vol. 34, no. 10, 2021.

[17] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[18] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-to-peer Networking and Applications*, vol. 8, no. 6, pp. 1070–1081, 2015.

[19] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-to-peer Networking and Applications*, vol. 9, no. 1, pp. 223–244, 2016.

[20] P. Gope, J. Lee, and T. Q. Quek, "Resilience of dos attacks in designing anonymous user authentication protocol for wireless sensor networks," *IEEE Sensors Journal*, vol. 17, no. 2, pp. 498–503, 2017.

[21] P. Gope and B. Sikdar, "An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3126–3135, 2018.

[22] P. Gope, J. Lee, and T. Q. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.

[23] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3953–3962, 2019.

[24] H. Han, L. Fang, W. Lu, W. Zhai, Y. Li, and J. Zhao, "A GCICA grant-free random access scheme for M2M communications in crowded massive MIMO systems," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6032–6046, 2022.

[25] A. K. Sahu, S. Sharma, and R. Raja, "Deep learning-based continuous authentication for an IoT-enabled healthcare service," *Computers and Electrical Engineering*, vol. 99, article 107817, 2022.

[26] S. Zeng, Y. Chen, X. Li, J. Zhu, Y. Shen, and N. Shiratori, "Visibility graph entropy based radiometric feature for physical layer identification," *Ad Hoc Networks*, vol. 127, article 102780, 2022.

[27] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.

[28] C. Zhang, L. Zhu, and C. Xu, "BPAF: blockchain-enabled reliable and privacy-preserving authentication for fog-based IOT devices," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 88–96, 2022.

[29] L. Liu, M. Zhao, M. Yu, M. A. Jan, D. Lan, and A. Taherkordi, "Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–14, 2022.

[30] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," in *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 62–73, Fairfax, Virginia, USA, 1993.

[31] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[32] J. Feng, L. Liu, Q. Pei, and K. Li, "Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 11, pp. 2687–2700, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3657706, 14 pages
https://doi.org/10.1155/2022/3657706

Research Article

On the Performance Supremum of CFO Based Physical Layer Identification

Shuiguang Zeng,[1,2,3,4,5] **Yin Chen**,[6,7] **Xufei Li**,[1,2] **Yulong Shen**,[1,2] **Dongmei Zhao**,[3,4,5] **Jinxiao Zhu**,[8] **and Norio Shiratori**[9]

[1]*School of Computer Science and Technology, Xidian University, Xi'an 710071, China*
[2]*Shaanxi Key Laboratory of Network and System Security, Xi'an 710071, China*
[3]*College of Computer and Cyber Security, Hebei Normal University, Shijiazhuang 050024, China*
[4]*Hebei Key Laboratory of Network and Information Security, Shijiazhuang 050024, China*
[5]*Hebei Provincial Engineering Research Center for Supply Chain Big Data Analytics & Data Security, Shijiazhuang 050024, China*
[6]*Graduate School of Media and Governance, Keio University, Fujisawa 252-0882, Japan*
[7]*Reitaku University, 2-1-1, Hikarigaoka, Kashiwa City, Chiba Prefecture 277-8686, Japan*
[8]*Faculty of Information Networking for Innovation and Design (INIAD), Toyo University, Tokyo 115-0053, Japan*
[9]*Research and Development Initiative, Chuo University, Tokyo 112-8551, Japan*

Correspondence should be addressed to Jinxiao Zhu; zhu@iniad.org

Received 18 June 2022; Revised 1 July 2022; Accepted 20 July 2022; Published 8 August 2022

Academic Editor: A.H. Alamoodi

Physical layer identification is an emerging technique that exploits physical layer features to identify wireless devices. The identification accuracy and the device quantity that can be identified at most are significant for the identification scheme. Existing works primarily focus on the feature correlation analysis for multifeature selection without investigating the least upper bound (supremum) of the performance of a single feature. The supremum indicates the limit of the performance, which is another sight for evaluating the quality of features and improving the performance of the identification scheme. Therefore, this paper first investigates the supremum of the performance of the most commonly used physical layer feature, i.e., carrier frequency offset (CFO). Specifically, we offer a rigorous mathematical analysis and derive the closed-form expression of the supremum of identification accuracy based on the max-min distance analysis (MMDA) criterion. And then, the supremum of the number of distinguishable devices is also analyzed. Finally, we conducted a simulation study to verify the theoretical analysis result.

1. Introduction

Device identification plays a vital role in wireless networks, conventionally realized with pre-distributed information such as IP addresses, MAC addresses, and international mobile station equipment identity (IMEI) numbers. With this information, basic access control [1] and location tracking [2] can be implemented. However, the mentioned addresses and numbers can easily be spoofed, exposing wireless devices and infrastructures to security threats [3]. Furthermore, it is often restricted to collect identity information due to business, privacy, and legal reasons, while identity is necessary for some applications. Therefore, there is an urgent need to find a more reliable or complementary way to identify devices.

Recently, the rich characteristics of the physical layer have been intensively investigated to implement device identification in wireless networks [4–6], also known as physical layer identification. Various physical layer features can be extracted and performed as the device's identity. These features stem from the small-scale hardware impairment in the transceivers or the location-specific characteristics of the wireless channel between the transmitter and receiver. According to the signal types collected for feature extraction, there are two categories of identification schemes, i.e.,

transient and steady-state signal-based ones [7]. Since the steady-state signal is easier to capture than the transient one and has attracted more attention from researchers, we concentrate on this type. Two approaches are reported in the literature for physical layer identification based on steady-state signals according to different classifier types.

The first approach, called shallow classifier-based device identification, implements the identification with hand-crafted features calculated from the received signals by carefully designed feature extraction algorithms. These features, usually relying on expert feature knowledge, will then be exploited with traditional shallow classifiers such as support vector machine (SVM) and K-nearest neighbor (KNN) or binary hypothesis testing to identify and authenticate transmitters [7–11].

The second approach takes advantage of the powerful learning ability of deep learning to identify wireless devices with the collected raw in-phase and quadrature (IQ) signal or its transformed information [6, 12–19]. Hence, it is known as deep learning-based physical layer identification. In this approach, hidden features can be automatically extracted from wireless frames with the aid of the representation learning ability of deep learning methods without using explicit feature calculation algorithms.

Both approaches are regarded as multiclass classification problems when using machine learning classifiers to discriminate multiple devices. It is intuitive that the identification accuracy will decrease as the quantity of devices increases. In other words, if we want to achieve the desired accuracy, the quantity of devices that can be identified will be limited. Recent work supports such a claim from the view of experiments, where the accuracies drop for both WiFi and ADS-B datasets using two deep learning models when the quantity of devices increases to 10,000 from 100 [19]. And there exist works focusing on the combination of multiple features to improve identification performance [8]. Their work is based on the view that a single feature leads to limited identification accuracy or limited number of distinguishable devices. User capacity of the physical layer identification system is investigated in [20, 21], where the authors consider the frequency characteristics from fast Fourier transform (FFT) as the radio frequency fingerprints.

Except for the mentioned related works, we still lack detailed analysis on the supremum of the identification accuracy and distinguishable devices for specific hand-crafted features, i.e., what is the highest identification accuracy and how many devices could identify at most under given conditions? This is important for investigating the performance and quality of a specific physical layer feature in an identification scheme and gives insight into finding approaches to improve the performance, such as identification with multiple features. Therefore, this paper focuses on issues not touched upon in existing works with the following contributions:

(1) Firstly, with the max-min distance analysis (MMDA) criterion and other mathematical analyses, we derive the closed-form expression of the supremum of the identification accuracy of the shallow classifier-based scheme given specific conditions

(2) Secondly, we also analyze the supremum of the number of distinguishable devices (device quantity supremum) of the shallow classifier-based scheme given the accuracy constraint

(3) Finally, through comprehensive simulations, we confirm the theoretical analysis and provide some interesting insights. The results indicate that the feature range (the value range of the physical layer features such as CFO specified in the standard protocol) and the SNR are the main factors affecting the identification performance, consistent with the theoretical analysis. We compare the accuracy of the shallow classifier– and deep learning–based identification schemes with the accuracy supremum. We also investigate the device quantity supremum with simulation with different CFO ranges and accuracy constraints at various SNRs

The rest of this paper is organized as follows. Section 2 reviews related works and introduces basic knowledge. Section 3 describes the system and communication models. Section 4 focuses on the supremum analysis of the shallow classifier-based identification scheme. Section 5 presents the simulation settings and results. Finally, Section 6 concludes this paper.

2. Related Work and Background

In this section, we first present related works, and further introduce certain basic knowledge regarding machine learning.

2.1. Related Work. There is no difference between shallow classifier– and deep learning–based device identification in terms of essential processes, including feature extraction and device identification. However, steady-state radiometric features such as carrier frequency offset (CFO) [22] and in-phase and quadrature imbalance (IQI) [23] rely on the expert knowledge of signal processing. Therefore, the feature extraction is explicit and protocol-specific. On the other hand, deep learning methods [17, 24] can automatically extract implicit features rather than expert feature engineering based on the raw IQ samples of the signal. However, this process usually requires dedicated hardware, such as graphics processing units (GPUs), to accelerate the computation.

For the first type of identification approaches, the estimation method and the number of independent features are the key factors that affect the performance. It is acknowledged that employing multiple features can improve identification accuracy. Therefore, some existing works focus on exploring new features and integrating with other features [8]. Peng et al. smartly combine differential constellation trace figure, CFO, modulation offset, and IQI to identify 54 ZigBee devices and achieve classification error rates of 4.48% and 9.42% under the line of sight (LOS) and none-line of sight (NLOS) scenarios [25].

While recently, deep learning-based identification approaches have attracted considerable research attention, which apply various deep neural network models to implement the feature extraction and identification processes, raw IQ samples or their transformed information, such

as power spectrum and FFT sequence, can be used directly as the inputs of the models.

However, the upper bounds or the supremum of identification accuracy and the number of distinguishable devices for hand-crafted features are unclear for device identification. The supremum of a single feature in terms of accuracy and device number indicates the ultimate performance, with which we can design a better identification scheme and implement a more appropriate feature selection and combination. Although Wang et al. [20] [21] explore the user capacity of the physical identification system, they consider the frequency characteristics from FFT as the radio frequency fingerprints without analyzing hand-crafted features.

2.2. Machine Learning. From the view of model structure, machine learning can be categorized as shallow classifiers and deep learning. Shallow classifiers, which usually adopt statistical models with only a few layers of composition, are mainstream research before the breakthrough of deep learning. These classifiers include naive Bayes, support vector machine (SVM), AdaBoost, random forest, and KNN and are still adopted in many commercial classification systems. Deep learning technologies are neural networks with many layers of nonlinear information processing. In recent years, they have been widely studied in many fields such as computer vision, speech recognition, and cybersecurity.

2.2.1. Shallow Classifiers. Shallow classifiers always have a very efficient and effective performance on high-quality samples [26]. This paper adopts KNN as a shallow classifier for device identification based on hand-crafted features. KNN is a simple but efficient machine learning algorithm, usually used for classification and regression. Usually, the new sample/case will be assigned to the class that is most common among its K-nearest neighbors measured by a distance function, i.e., the majority voting of the new case's neighbors according to the distance such as Euclidean distance [27].

2.2.2. Deep Learning. There are different deep learning models, such as recurrent neural network (RNN), convolutional neural network (CNN), and generative adversarial network (GAN). This paper focuses on CNN since it has been investigated in much recent literature and has shown great potential in device identification. A general CNN comprises one or more convolutional layers, pooling layers, and fully connected (FC) layers [28]. The convolutional layers aim to promote important hidden features of the input data through the specially designed structures called "filters" having different dimensions, also known as feature extractors. Also, different types of CNN have been investigated for device identification. 1D and 2D CNNs with one/two-dimensional convolutional layers are exploited to identify wireless devices [19, 29]. Complex-valued neural networks are explored in [30] to improve the wireless identification performance.

3. System Model

In this section, we first describe the considered identification and communication model. Then, we formulate the concerning problem about the least upper bound analysis.

Table 1: List of variables and notations.

Notation	Definition
M	Class (transmitter) number
U_ε	CFO range
L	Number of multipath components
γ/η	Signal-to-noise ratio (SNR)
L_s	The length of training sequence
$(\cdot)^*$	Complex conjugate operator
$\mathfrak{I}(\cdot)$	Imaginary part of complex number
$\mathfrak{R}(\cdot)$	Real part of complex number
$Q(\cdot)$	Q-function
$\sup A$	Supremum of set A
$f'(\cdot)$	First-order derivative
$f''(\cdot)$	Second-order derivative
$f^{-1}(\cdot)$	Inverse function
$\lfloor\cdot\rfloor$	Floor function

Table 1 summarizes the main variables and notations used in this paper.

3.1. Identification Model. As shown in Figure 1, the model comprises a wireless receiver (RX) and M wireless transmitters (TX). The receiver attempts to identify each transmitter using the received wireless frames. The receiver first collects the raw IQ samples of the concerned field, e.g., baseband preamble, via frame detection and synchronization from the received wireless signals subject to the concerned channels. The receiver can calculate the hand-crafted features using the raw IQ samples for identification. Also, it can directly use the raw IQ samples to identify transmitters with deep learning. Then, the transmitter identification will be formulated as a multiclass classification problem based on hand-crafted features or raw IQ samples, depending on the adopted classifier.

3.2. Communication Model. At the receiver, the passband signal is down-converted to the baseband. Then, the received baseband signal is sampled by the analog-to-digital converter (ADC) to obtain the discrete complex-valued preamble signal, i.e., the raw IQ samples. The baseband signal with CFO is given as [31]:

$$r(n) = e^{j2\pi n\Delta f} s(n) + w(n), \tag{1}$$

where $\Delta f = \varepsilon T_s$ is the normalized CFO with ε being the CFO in the corresponding range $[-U_\varepsilon, U_\varepsilon]$ parts per million (ppm) to the carrier frequency f_c. The range is usually specified in the communication standard concerned. Here, $T_s \triangleq 1/B_w$ is the sampling interval with B_w being the total communication bandwidth, and $w(n) \sim \mathcal{CN}(0, \sigma_n^2)$ is the circular symmetric additive white Gaussian noise (AWGN) with zero mean and variance σ_n^2. Let $a(n)$ denotes the long training symbols with length of $2 \times L_s$, which usually contains

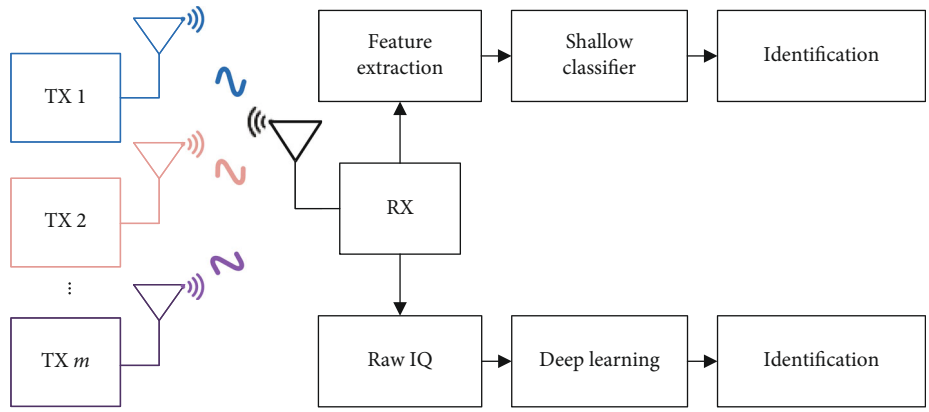


Figure 1: System model of typical physical layer identification.

two L_s-length repetitive sequences. And it is a classical preamble structure in many wireless protocols such as most specifications in the IEEE 802.11 family. When the baseband signal is only subject to the AWGN channel, $s(n)$ is the same as $a(n)$, and the received signal is denoted as (1). When the baseband signal is subject to multipath channel, $s(n)$ is given by

$$s(n) = \sum_{l=0}^{L-1} h(l) a_{n-l}, \tag{2}$$

where $h(l) 0 \le l \le (L-1)$ represents the channel coefficients of the multipath fading channel. Notably, we assume the locations of transmitters and receiver are fixed. Hence, the Doppler offset is zero, and the channel profile is static during the operation time, which can be considered a quasi-static channel similar to [32]. This is reasonable for many wireless networks such as wireless sensor networks (WSN) and wireless local area networks (WLAN) where fixed sink nodes or routers create a static channel profile when the receiver location is also fixed. We then denote the concerned preamble containing the two repetitive long training sequences as $\mathbf{r} = [r(0), r(1), \cdots, r(2L_s - 1)]$ after synchronization and denote the SNR of the received signal as γ with the unit of dB, which is calculated as follows:

$$\gamma = 10 \log(\eta) = 10 \log\left(\frac{1}{2L_s} \frac{\sum_{n=0}^{2L_s-1} |s(n)|^2}{\sigma_n^2}\right), \tag{3}$$

where $\eta = \sigma_s^2/\sigma_n^2$ and σ_s^2 and σ_n^2 represent the power of signal and noise, respectively.

3.3. Problem Formulation. For the shallow classifier-based identification scheme with CFO, the CFO will be first estimated from raw IQ samples of the preamble field of the received signal. Then with the collected feature of each frame, we can train a shallow classifier for device identification.

We are interested in how the identification accuracy will vary with the range of a single feature and other conditions. And are there any supremum or upper bound of identification accuracy and the number of distinguishable devices with the considered feature? In a word, our primary aim is to investigate the performance limits of each specific feature adopted in physical layer identification by answering the above questions.

4. Identification Performance and the Supremum

At the receiver, the raw IQ samples of the long training sequence are adopted to implement hand-crafted feature estimation for identification. We then analyze the supremum of identification accuracy and the device quantity supremum considering CFO.

4.1. CFO Estimation. Similar to [33–35], when the length of the long training sequence is larger than the maximum channel delay L in (2), i.e., $L_s \ge L$, the CFO can be estimated by the two repetitive long training sequences. We first calculate the phase difference ϕ between the frequency responses of two identical and consecutive long training sequences as

$$\phi = \arctan\left\{\frac{\Im\left(\sum_{n=0}^{L_s-1} r^*[n] r[n+L_s]\right)}{\Re\left(\sum_{n=0}^{L_s-1} r^*[n] r[n+L_s]\right)}\right\}, \tag{4}$$

where $r[n]$ is the complex I and Q samples of the frequency response of a training sequence and n is the time index in a window of $2L_s$ samples. Then, we achieve the estimated CFO as

$$\widehat{\varepsilon}_h = \frac{\phi}{2\pi L_s}, \tag{5}$$

and according to [35], the standard deviation of the CFO

estimation is

$$\sigma_{\widehat{\varepsilon_h}} = \frac{1}{2\pi L_s \sqrt{L_s \eta}}, \tag{6}$$

which can be considered as the lower bound of the CFO estimation error in the receiver. Usually, there exists more than one method for estimating the same feature with different estimating errors, i.e., variance, which results in different performances for the shallow classifier-based identification.

4.2. The Supremum of the Identification Accuracy. Since the true CFOs of the transmitters are independent uniform random variables in the concerned range $[-U_\varepsilon, U_\varepsilon]$ [35] [36], we denote it as $\varepsilon_m \in [-U_\varepsilon, U_\varepsilon], m = 1, 2, \cdots, M$. And we define the spacing between two adjacent true CFOs as the distance of $d_m = \varepsilon_{m+1} - \varepsilon_m, m = 1, 2, \cdots, M-1$; then, we have $\sum_{m=1}^{M-1} d_m \le 2U_\varepsilon$. Assuming the mean distance of the CFO $\bar{d} = \sum_{m=1}^{M-1} d_m / M - 1$, then we have

$$0 \le \bar{d} \le \frac{2U_\varepsilon}{M-1}. \tag{7}$$

The overall accuracy is widely used for multiclass classification problems, whose definition is as

$$ACC = \frac{TP_m}{S}, \tag{8}$$

where S is the total number of predictions and TP_m is the true positive predictions when considering the classification as a binary classification regarding the m-th class and other classes. We can also denote the classification error rate and accuracy as $p_e = 1 - p_a$ and p_a as (9) according to [37], where $Q(x) = 1/\sqrt{2\pi}\int_x^\infty e^{-t^2/2}dt$ is the Q-function:

$$p_a = \frac{\left(\left(1 - Q\left(d_1/2\sigma_{\widehat{\varepsilon_h}}\right)\right) + \sum_{m=1}^{M-2}\left(1 - Q\left(d_m/2\sigma_{\widehat{\varepsilon_h}}\right) - Q\left(d_{m+1}/2\sigma_{\widehat{\varepsilon_h}}\right)\right) + \left(1 - Q\left(d_{M-1}/2\sigma_{\widehat{\varepsilon_h}}\right)\right)\right)}{M} = 1 - \frac{2}{M}\sum_{m=1}^{M-1} Q\left(\frac{d_m}{2\sigma_{\widehat{\varepsilon_h}}}\right). \tag{9}$$

As we assume that the variances of the estimated CFO of all devices are the same at a specific SNR, which means all the CFO samples are from homoscedastic Gaussians as the same standard deviation of (6). We can adopt the MMDA criterion to achieve the maximum separation of all devices concerning CFO [38]. According to this criterion, to achieve a maximum classification accuracy, we have to maximize the minimum distance of each class pair (two devices) to guarantee the separation as best as possible of any class pairs as

$$\max \min_{1 \le m \le M-1} d_m, \tag{10}$$

where the inner minimization chooses the minimum CFO distance $d' \in D'$ of all class pairs, while the outer maximization maximizes this minimum distance [38]. Here, D' is the set of minimum CFO distance.

Theorem 1. *For M devices, the supremum of the minimum distance of the CFO $\sup D'$ in the range U_ε is $\bar{\mathfrak{d}} = 2U_\varepsilon/(M-1)$.*

Proof. According to the definition of supremum, we first adopt proof by contradiction to prove that $2U_\varepsilon/(M-1)$ is an upper bound of the minimum distance set D', i.e., $2U_\varepsilon/(M-1) \ge d'$, where $2U_\varepsilon/(M-1) = \max(\bar{d})$ as in (7). If $\max(\bar{d}) < d'$, then we have $2U_\varepsilon = (M-1)\max(\bar{d}) < (M-1)d' \le d_1 + d_2 + \cdots + d_{M-1} \le 2U_\varepsilon$, which is a contradiction.Therefore, $2U_\varepsilon/(M-1) \ge d'$ holds. Second, we prove $2U_\varepsilon/(M-1)$ is the minimum of the upper bounds. $\forall 0 < \xi < 2U_\varepsilon/(M-1)$; we find $d_0' = 1/2((2U_\varepsilon/(M-1)) - \xi + (2U_\varepsilon/(M-1))) = (2U_\varepsilon/(M-1)) - (\xi/2)$, and $d_0' \in D'$ fulfills $d_0' > (2U_\varepsilon/(M-1)) - \xi$, which completes the proof. □

Proposition 2. *When the true CFOs of all devices are distributed with equal distance in the concerned range, i.e., the minimum distance of the CFO equals to its supremum, the separation of all devices will be the best. Thus, in this case, $d_1, d_2, \cdots, d_{M-1} = \sup D' = 2U_\varepsilon/(M-1)$, we have the least upper bound, i.e., the supremum of accuracy p_a as*

$$\begin{aligned}\bar{p}_a &= 1 - 2\left(\frac{M-1}{M}\right)Q(Y) = 1 - 2\left(\frac{M-1}{M}\right)Q\left(\frac{U_\varepsilon}{(M-1)\sigma_{\widehat{\varepsilon_h}}}\right) \\ &= 1 - 2\left(\frac{M-1}{M}\right)Q\left(\frac{U_\varepsilon}{2(M-1)\pi L_s\sqrt{L_s\eta}}\right),\end{aligned} \tag{11}$$

where $Y = \bar{\mathfrak{d}}/2\sigma_{\widehat{\varepsilon_h}}$ and $\bar{\mathfrak{d}} = 2U_\varepsilon/(M-1)$.

Proof. First, we prove $\bar{p}_a$ is an upper bound of the accuracy p_a. Since $Q(x) = 1 - \Phi(x)$, where $\Phi(x) = 1/\sqrt{2\pi}\int_{-\infty}^x e^{-1/2t^2}dt$ is the cumulative distribution function (CDF) for the standard Gaussian distribution. We have $Q'(x) = -\Phi'(x) = -P(x) < 0$, where $P(x) = 1/\sqrt{2\pi}e^{-1/2x^2}$ is the probability density function (PDF). And when $x > 0$, $Q''(x) = -P'(x) = x(1/$

$\sqrt{2\pi})e^{-1/2x^2} > 0$, which means the Q-function is a monotone decreasing convex function when $x > 0$. Using Jensenâ€™s inequality, we have

$$\frac{1}{M-1}\sum_{m=1}^{M-1} Q\left(\frac{d_m}{2\sigma_{\widehat{\varepsilon_h}}}\right) \geq Q\left(\frac{\sum_{m=1}^{M-1} d_m}{2\sigma_{\widehat{\varepsilon_h}}(M-1)}\right) = Q(Y), \quad (12)$$

$$1 - \frac{2}{M}\sum_{m=1}^{M-1} Q\left(\frac{d_m}{2\sigma_{\widehat{\varepsilon_h}}}\right) \leq 1 - 2\left(\frac{M-1}{M}\right)Q(Y). \quad (13)$$

Combining Equation (11) and the expressions of p_a and $\bar{p}_a$ in Equations (9) and (12), we have $p_a \leq \bar{p}_a$, and thus, $\bar{p}_a$ is an upper bound of p_a.

Second, we prove $\bar{p}_a$ is the minimum of the upper bounds of p_a. With $\forall 0 < \xi < 2U_\varepsilon/(M-1)$, we construct a function as

$$f(\xi) = \frac{2}{M}(Q(Y-\xi) + Q(Y+\xi) - 2Q(Y)). \quad (14)$$

Given that the Q-function is a monotone decreasing convex function when $x > 0$, we have $f(\xi) > 0$, and when $\xi \longrightarrow 0$, $f(\xi) \longrightarrow 0$.

With (12) and (15), then we have

$$\bar{p}_a - f(\xi) = 1 - \frac{2}{M}((M-3)Q(Y) - Q(Y-\xi) - Q(Y+\xi)), \quad (15)$$

and we can find

$$p_0 = 1 - \frac{2}{M}\left((M-3)Q(Y) + Q\left(Y-\frac{\xi}{2}\right) + Q\left(Y+\frac{\xi}{2}\right)\right), \quad (16)$$

with $p_0 \in \mathbb{P}_a$ fulfills $p_0 > \bar{p}_a - f(\xi)$, where $\mathbb{P}_a$ is the set of identification accuracy. Because combined with (16) and (17) and applying the Lagrange mean value theorem, we have $p_0 - (\bar{p}_a - f(\xi)) > 0$, i.e., $p_0 > \bar{p}_a - f(\xi)$ as in (17), where $Y - \xi < x_1 < Y - (\xi/2)$, $Y + (\xi/2) < x_2 < Y + \xi$, and $x_2 > x_1$. Finally, according to the definition of supremum, the proof completes.

$$\begin{aligned} p_0 - (\bar{p}_a - f(\xi)) &= \frac{2}{M}\left(\left(Q(Y-\xi) - Q\left(Y-\frac{\xi}{2}\right)\right)\right. \\ &\quad \left. - \left(Q\left(Y+\frac{\xi}{2}\right) - Q(Y+\xi)\right)\right) \\ &= \frac{\xi}{M}\left(Q'(x_2) - Q'(x_1)\right) > 0. \end{aligned} \quad (17)$$

□

We can observe from (11) that the accuracy supremum is determined by the feature range, the number of transmitters to be identified, and the precision of the feature estimation method (i.e., the standard deviation of the estimate).

4.3. The Device Quantity Supremum. We define the supremum of the number of distinguishable devices or the device quantity supremum of an identification scheme as the device number under which the accuracy of the identification scheme will not exceed the given constraint. And then, with this supremum, we can evaluate the performance limit of the adopted feature for device identification. Intuitively, the supremum is related to the identification accuracy as shown in (11). However, it is difficult to deduce a closed-form expression of the inverse function of (11) concerning M and $\bar{p}_a$, then we denote (11) as $\bar{p}_a = f(M)$ for simplicity. And given the monotone decreasing property of $\bar{p}_a = f(M)$, we have the following proposition.

Proposition 3. *For a specific feature range U_ε and feature estimation, given the target accuracy, the device quantity supremum is $\bar{M} = \lfloor f^{-1}(\bar{p}_a) \rfloor, \bar{M} \geq 2, \bar{M} \in \mathbb{N}^+$, where $\bar{p}_a = f(M)$ is as shown in (11).*

Proof. We define two functions $g(m) = (m-1)/m$ and $h(m) = Q(U_\varepsilon/((m-1)\sigma_{\widehat{\varepsilon_h}}))$, then we can denote (11) as $\bar{p}_a = 1 - 2g(m)h(m)$. Since both $g(m)$ and $h(m)$ are strictly monotone decreasing with $0.5 \leq g(m) < 1, m \in \mathbb{R}, m \geq 2$ and $0 < h(m) < 0.5$, $-2g(m)h(m)$ will be strictly monotone increasing. Thus, $f(m)$ will be a strictly monotone decreasing function too. According to the properties of the inverse of strictly monotone function, $f^{-1}(\bar{p}_a)$ also will be a monotone decreasing function. The device number is an integer set, denoting as $\mathbb{M} = \{M \subset \mathbb{N}^+ | M \leq \lfloor f^{-1}(\bar{p}_a) \rfloor\}$, and $\bar{M} = \lfloor f^{-1}(\bar{p}_a) \rfloor$ is the supremum of the number set $\mathbb{M}$. We prove it by contradiction as follows. Suppose that $\bar{M}$ is not the supremum of $\mathbb{M}$, which means there is at least an integer $M' \in \mathbb{M}$ that fullfils $M' > \bar{M}$. Obviously, this is a contradiction because M' should be $\leq \bar{M}$ according to its definition, which means the premise cannot be true. Thus, the device number supremum is $\bar{M}$. □

It indicates that the maximum number of transmitters can be identified, i.e., device quantity supremum under the constraint of the desired accuracy is determined by the feature's range and the precision of the estimation method. Although it is difficult to give the closed-form expression of $f^{-1}(\bar{p}_a)$, we can depict the relationship between M and $\bar{p}_a$ by simulation and observe the variation of the device quantity supremum.

5. Simulation Study

5.1. Simulation Settings. We simulated a typical wireless communication processing of 802.11a based on OFDM. Similar to [16], we also generated the beacon frames for transmitter identification where the (legacy) long training field (L-LTF) was adopted to estimate the CFO. We implemented data generation and processing, machine learning, and deep learning methods on a platform with MATLAB R2021a. The platform is a Dell Precision 3640 tower workstation (https://dl.dell.com/topicspdf/precision-3640-workstation_owners-manual2_en-

us.pdf) with an Intel(R) Core(TM) i9-10900K CPU and 32GB RAM running the Ubuntu 18.04 operating system. Further, we used an NVIDIA GeForce RTX 3080 GPU configured on the workstation to train and test the deep learning-based models. The main simulation parameters, including the communication system and the Rayleigh channel, are shown in Table 2.

As the system model shows in Section 3, the receiver collects signals from the transmitters and then uses L-LTF to extract the features and identify the devices. Following the specification, the transmitted L-LTF sequences are configured as the same for all transmitters, enabling the algorithm to avoid any data dependency. Since we assume the transmitters and receiver are static, the multipath channel profile and RF impairments do not vary in time.

After comparing several shallow classifiers in common use, we selected KNN for the shallow classifier-based identification. We tuned parameters of "100" as the number of neighbors, "Euclidean" as the distance metric, and "Equal" as the distance weight.

We adopted the same CNN architecture in [16] as the deep learning identification method. The detailed CNN architecture's parameters, including convolutional layers (Conv2D), pooling layers (MaxPooling2D), and fully connected layers (FC, also known as the dense layer), is shown in Table 3.

To minimize the sampling bias (when selecting data from the dataset) and ensuring statistical confidence, we adopted a 5-fold cross-validation (CV) in the classification evaluation. We split the dataset into five blocks, ensuring that each block has 200 random frames from each device since we collected 1000 frames per transmitter. Then, we performed five rounds of training and testing for each shallow classifier- and deep learning-based model. One block was selected as the test dataset, and the rest were used for training in each round. We considered the averaged overall test accuracy of the five-round CV as the final metric to evaluate the identification performance, i.e., $\bar{A}CC = ACC_k/5$, where ACC_k is the overall test accuracy of the k-th round of CV.

Table 2: Simulation parameters of the communication system.

Parameter	Value
Transmitter number (M)	50,400
Frames per transmitter (F_d)	1000
Carrier frequency (f_c)	5.765 GHz
CFO ranges (U_ε)	2.5,5, 10, 20 ppm
Bandwidth (B_w)	20 MHz
Sampling frequency (f_s)	20 MHz
Length of L-LTF (L_s)	64
Rayleigh path number	3
Discrete path delay in seconds	$[0,1.8,3.4]/f_s$ s
Average path gains	[0,−2,−10]
Maximum Doppler shift	0

Table 3: Architecture of the CNN Model [16].

Layer	Type	Kernel size	Stride	#kernel	Input size
L1	Input				$128 \times 2 \times 1$
L2	Conv2D	7×1		50	$128 \times 2 \times 1$
L3	MaxPool	[2, 1]	[2, 1]		$122 \times 2 \times 50$
L4	Conv2D	7×2		50	$61 \times 2 \times 50$
L5	MaxPool	[2, 1]	[2, 1]		$55 \times 1 \times 50$
L6	FC			256	$27 \times 1 \times 50$
L7	FC			80	$27 \times 1 \times 256$
L8	Out			M	$27 \times 1 \times 80$

5.2. Identification Accuracy and the Supremum

5.2.1. Identification Under AWGN Channel. As shown in Figure 2, in each CFO range (2.5CFO means $U_\varepsilon = 2.5$ ppm), the identification accuracy of the shallow classifier-based scheme (i.e., with the classifier of KNN and hand-crafted feature CFO, denoted as HC) is always under the supremum (SUP). As the SNR increases, the accuracy first exceeds that of deep learning and then to the supremum. When the SNR is between −20 and 0 dB, the gap between the accuracy of the shallow classifier-based scheme and the supremum is small. When the SNR increases from 0 to 50 dB, the gap first widens and then closes. When SNR ≥45 dB, the accuracy reaches the supremum of 100% in the range of 20 ppm. It is reasonable because the error of the estimated CFO will be smaller at higher SNR, as discussed in Section 4. Moreover, the accuracy of the deep learning-based scheme (denoted as DP) in all CFO ranges converges to approximately 95% except for 20 ppm where the accuracy converges to 98%. It indicates that deep learning has limited discriminative capabilities for CFO at higher SNR compared with hand-crafted feature estimation. On the other hand, the deep learning-based scheme can achieve better performance at lower SNR. It means that the influence of SNR on the deep learning scheme is not as significant as that of hand-crafted feature estimation since the former performs better under low SNR.

5.2.2. Identification on More Transmitters. To observe the supremum and identification accuracy with a larger device scale, we implemented the simulation with 400 transmitters. Figure 3 shows the results considering 400 transmitters with the same CFO ranges as in Figure 2. It also presents the identification accuracy of the two shallow classifier-based and deep learning-based schemes with the same CFO ranges and the same transmitter quantity under the AWGN channel. Comparing Figures 3(a)–3(d)with Figures 2(a)–2(d), it is evident that the accuracy of both schemes with 400 transmitters is lower than those with 50 transmitters, respectively. Also, the supremum decreases too. Combined with Figure 2, we find that at the SNR of about 45 dB, no matter how the quantity of devices changes, the shallow classifier-based scheme consistently exceeds the deep learning-based one.

5.2.3. Identification Under Static Rayleigh Channel. In Figure 4, we also compare the identification accuracy under the static Rayleigh channel with the supremum. Comparing the performance of the deep learning-based scheme in

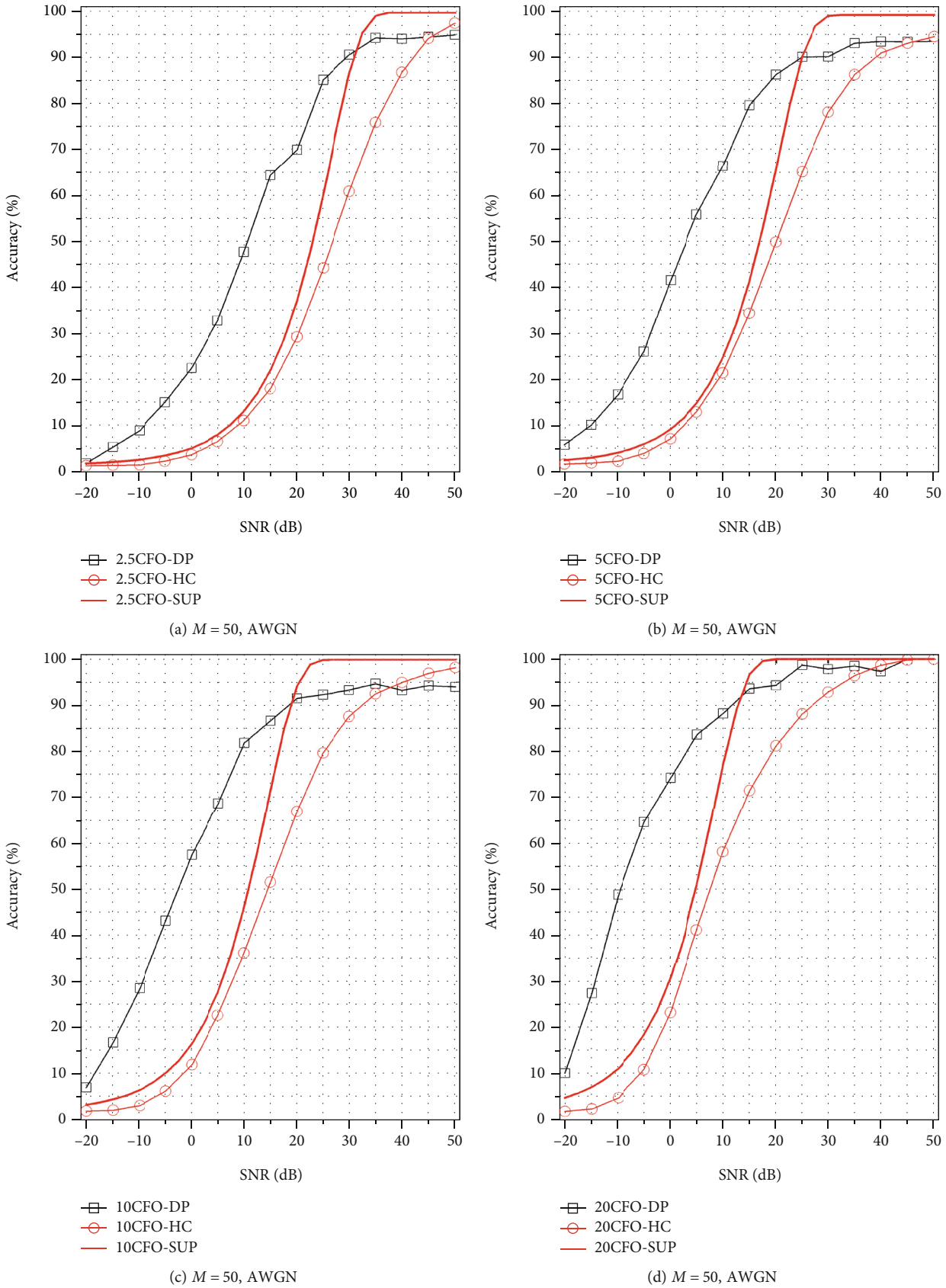
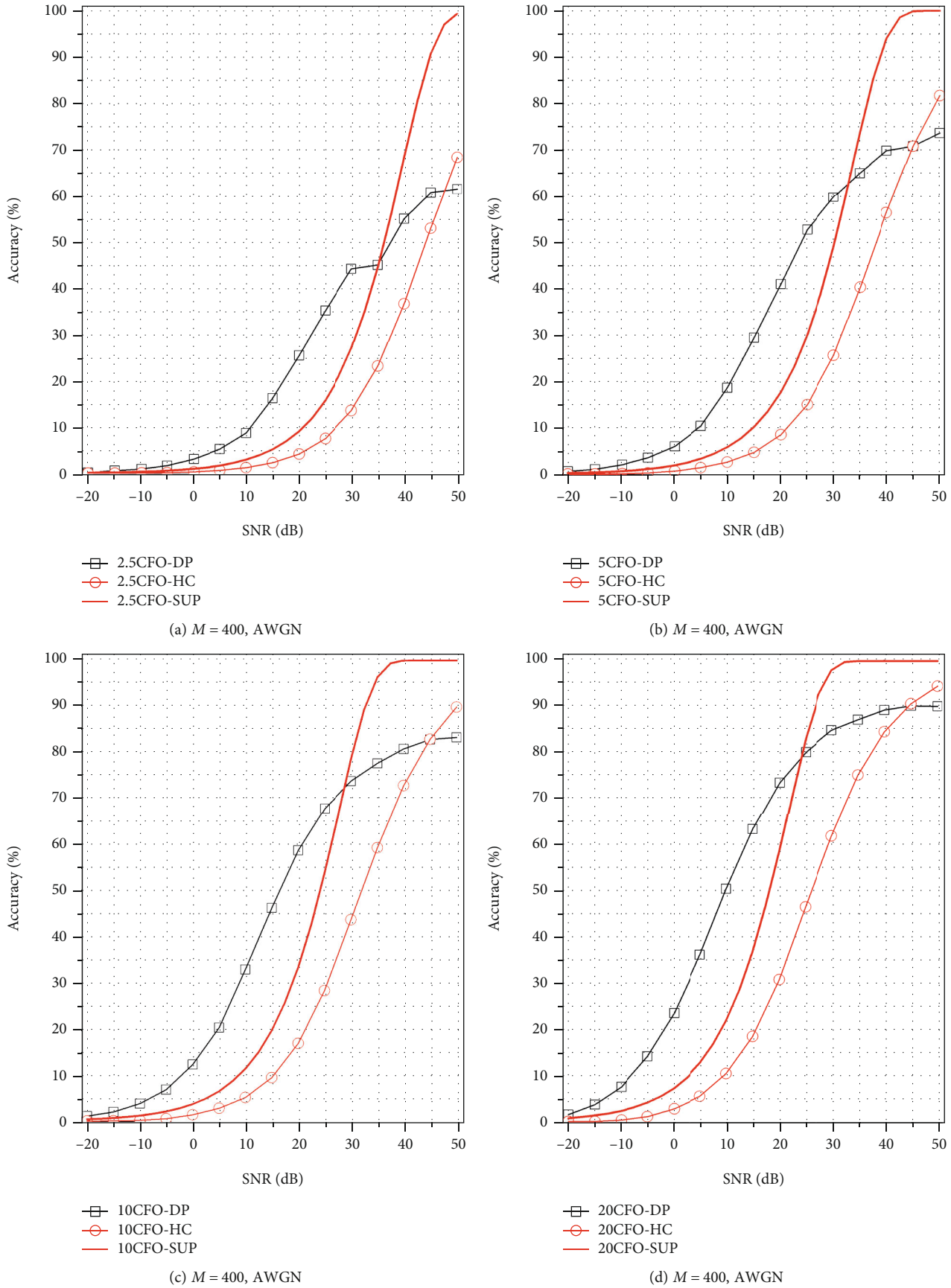


FIGURE 2: Identification accuracy of schemes using KNN with CFO (HC) and deep learning with raw IQ samples (DP) under different CFO ranges (e.g., 2.5CFO means $U_\varepsilon = 2.5$ ppm) and AWGN channel vs. the accuracy supremum (SUP).



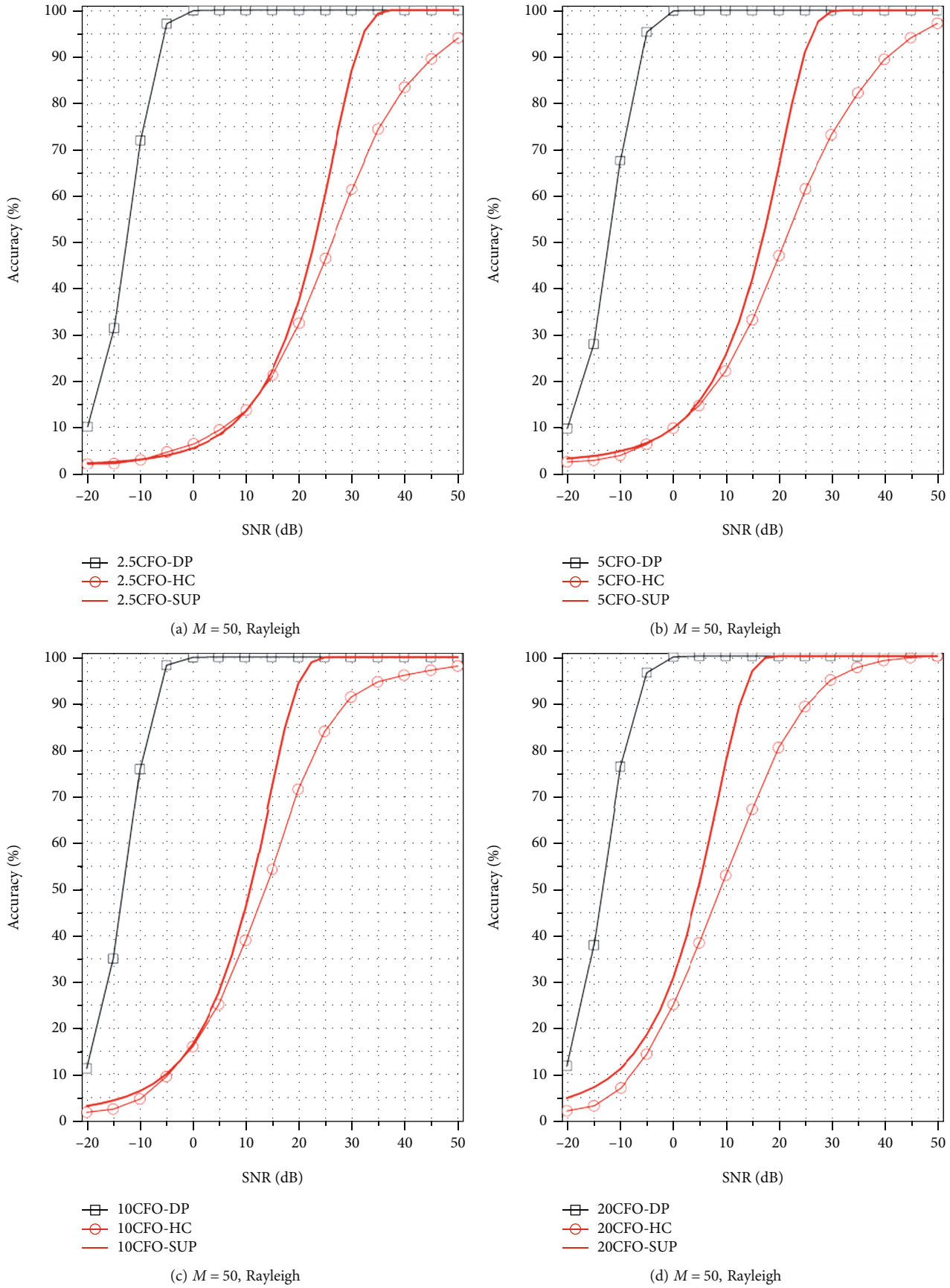
(a) $M = 400$, AWGN

(b) $M = 400$, AWGN

(c) $M = 400$, AWGN

(d) $M = 400$, AWGN

Figure 3: Identification accuracy under AWGN channel vs. the accuracy supremum.



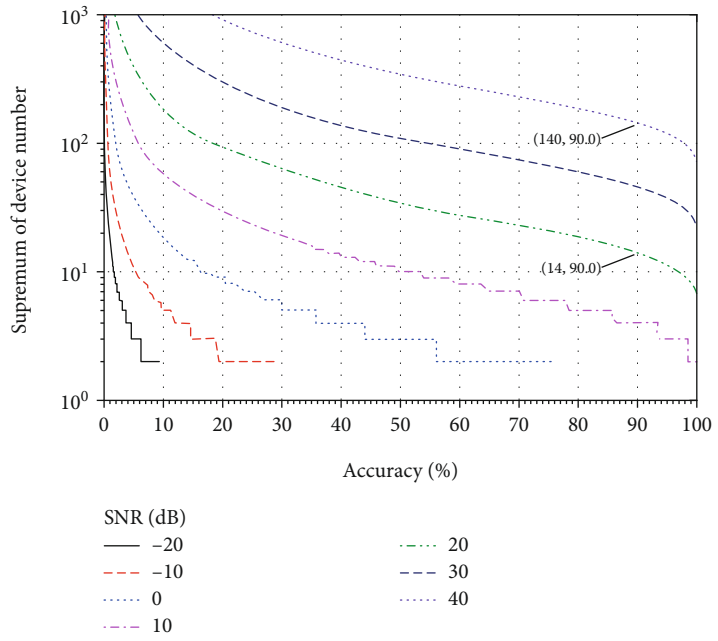
(a) $M = 50$, Rayleigh

(b) $M = 50$, Rayleigh

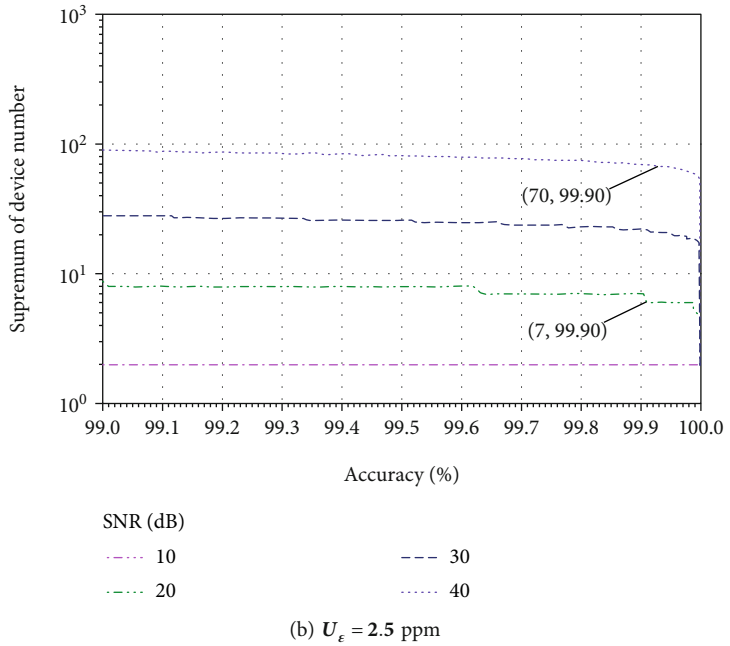
(c) $M = 50$, Rayleigh

(d) $M = 50$, Rayleigh

Figure 4: Identification accuracy under Rayleigh channel vs. the accuracy supremum.

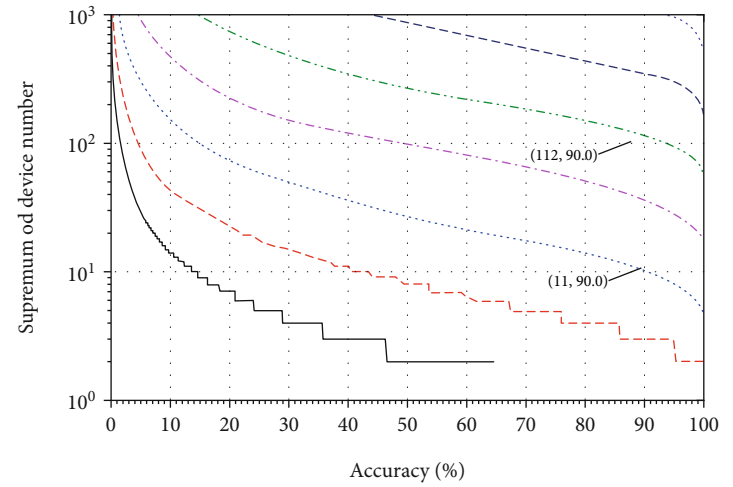


(a) $U_\varepsilon = 2.5$ ppm

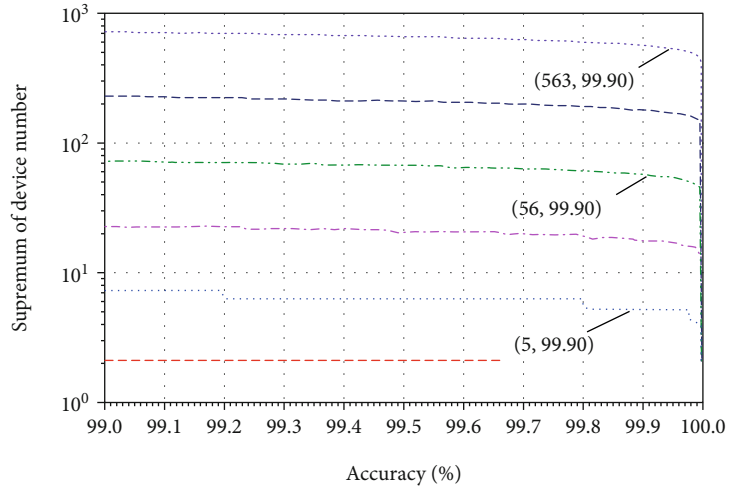


(b) $U_\varepsilon = 2.5$ ppm

Figure 5: Continued.



(c) $\boldsymbol{U_\epsilon = 20}$ ppm



(d) $\boldsymbol{U_\epsilon = 20}$ ppm

Figure 5: The device quantity supremum using KNN with hand-crafted feature (i.e., CFO) under different identification accuracy and SNR with different CFO range.

Figure 2 with that of Figure 4, we can observe that the accuracy is improved obviously under the static Rayleigh channel in each CFO range. However, when looking into the three subfigures in Figure 4, we can find that expanding the CFO range has little effect on the accuracy improvement for the deep learning-based scheme. This result validates that deep learning can learn more information from the multipath channel than from the device's feature, which is consistent with the study of [32]. In other words, the identification accuracy of the deep learning-based scheme will be affected more by the channel than device features. On the other hand, the shallow classifier-based scheme is less affected by the channel than the deep learning one since the accuracy under the Rayleigh channel is only improved slightly in each CFO range. Especially at low SNRs, the gap between the accuracy of the shallow classifier-based scheme and the supremum under the Rayleigh channel is slightly smaller than that of the AWGN channel.

5.3. The Device Quantity Supremum. Figure 5 presents the device quantity supremum under different SNRs considering CFO as the physical layer feature. Figures 5(b) and 5(d)

show the details of Figures 5(a) and 5(c), respectively, when the accuracy constraint ≥99%. As shown in Figures 5(a) and 5(c), the supremum will decrease with the increasing of the desired identification accuracy while also increases with the SNR. With the feature range of 2.5 ppm, the results in Figures 5(a) and 5(b) show that when the SNR<20 dB, the receiver can identify no more than 15 transmitters under the required accuracy of 90%. Even at a high SNR of 40 dB, if a 90% accuracy is required, there should be no more than 140 transmitters. Moreover, when higher accuracy is required, the supremum will be smaller. For example, with the accuracy requirement reaching 99.9%, the device quantity supremum even decreased to 7 and 70 at the SNR of 20 and 40 dB, respectively. However, a small CFO range is quite common for some off-the-shelf wireless devices operating under rigorous synchronization requirements, such as mobile phones and high-end laptops [39].

In Figures 5(c) and 5(d), losing the feature range to 20 ppm, then we can see the supremum increases too. For the same accuracy requirement of 90%, the device quantity supremum can reach 112 at the SNR of 20 dB, more than seven times that in the CFO range of 2.5 ppm. But the supremum is only 11 when the SNR is 0 dB. With the high accuracy requirement of 99.9%, the supremum is 5, 56, and 563 at the SNRs of 0, 20, and 40 dB, respectively. Thus, it is evident that only considering one feature such as CFO, the device identification capability, i.e., the device number supremum, is small, especially when the range is small. Combined with the analysis of the supremum and the simulation results, we can find that a larger feature range, more precise feature estimation, and higher SNR of the signal can improve the accuracy and the device quantity supremum.

6. Conclusion

This paper analyzed the accuracy supremum and the device quantity supremum of the shallow classifier-based physical layer identification scheme based on the hand-crafted feature. Specifically, we mathematically analyzed and deduced the closed-form expression of the accuracy supremum of the identification scheme based on CFO. We also investigated the device quantity supremum, i.e., the supremum of the number of distinguishable devices. The simulation results are consistent with the theoretical analysis. According to the analysis and simulation, there is insufficient fingerprinting space only considering one feature, such as CFO. Thus, if we want to identify more devices, a larger feature range or higher SNR of the signal can help.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported in part by the National Key R&D Program of China (Grant No. 2018YFE0207600), the Natural Science Foundation of China (NSFC) under Grant 61972308, the Natural Science Basic Research Program of Shaanxi (Program No. 2019JC-17), the Hebei Science Supported Planning Projects Under Grant 20310701D, the JSPS A3 Foresight Program (Grant No. JPJSA3F20200001), and the Grants-in-Aid for Scientific Research (JSPS KAKENHI, Grant Number 20K19801).

References

[1] A. C. V. Gummalla and J. O. Limb, "Wireless medium access control protocols," *IEEE Communications Surveys & Tutorials*, vol. 3, no. 2, pp. 2–15, 2000.

[2] D. J. Leith and S. Farrell, "Contact tracing app privacy: What data is shared by Europe's GAEN contact tracing apps," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, pp. 1–10, Vancouver, BC, Canada, 2021.

[3] Y. Mirsky and M. Guri, "DDoS attacks on 9-1-1 emergency services," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2767–2786, 2020.

[4] P. Zhang, J. Liu, Y. Shen, and X. Jiang, "Exploiting channel gain and phase noise for PHYlayer authentication in massive MIMO systems," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4265–4279, 2021.

[5] P. Zhang, Y. Shen, X. Jiang, and W. Bin, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Transactions on Communications*, vol. 68, no. 4, pp. 2446–2458, 2020.

[6] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for LoRa using deep learning," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 8, pp. 2604–2616, 2021.

[7] Y. Lin, J. Jia, S. Wang, B. Ge, and S. Mao, "Wireless device identification based on radio frequency fingerprint features," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, 2020.

[8] S. Zeng, Y. Chen, X. Li, J. Zhu, Y. Shen, and N. Shiratori, "Visibility graph entropy based radiometric feature for physical layer identification," *Ad Hoc Networks*, vol. 127, p. 102780, 2022.

[9] J. Chang, Y. Xiao, and Z. Zhang, "Wireless physical-layer identification assisted 5g network security," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1–5, Paris, France, 2019.

[10] Y. Liu, J. Wang, J. Li, S. Niu, and H. Song, "Machine learning for the detection and identification of internet of things (IOT) devices: A survey," *IEEE Internet Things J*, vol. 9, 2021.

[11] S. Chen, Z. Pang, H. Wen, K. Yu, T. Zhang, and Y. Lu, "Automated labeling and learning for physical layer authentication against clone node and Sybil attacks in industrial wireless edge networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2041–2051, 2020.

[12] B. Li and E. Cetin, "Design and evaluation of a graphical deep learning approach for RF fingerprinting," *IEEE Sensors Journal*, vol. 21, no. 17, pp. 19462–19468, 2021.

[13] M. Ramasubramanian, C. Banerjee, D. Roy, E. Pasiliao, and T. Mukherjee, "Exploiting spatio-temporal properties of I/Q

signal data using 3d convolution for RF transmitter identification," *IEEE Journal of Radio Frequency Identification*, vol. 5, no. 2, pp. 113–127, 2021.

[14] J. M. McGinthy, L. J. Wong, and A. J. Michaels, "Groundwork for neural network-based specific emitter identification authentication for iot," *IEEE Internet Things Journal*, vol. 6, no. 4, pp. 6429–6440, 2019.

[15] T. Jian, B. C. Rendon, E. Ojuba et al., "Deep learning for rf fingerprinting: a massive experimental study," *IEEE Internet Things Magazine*, vol. 3, no. 1, pp. 50–57, 2020.

[16] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "Oracle: optimized radio classification through convolutional neural networks," in *Proceedings of The 38th IEEE International Conference on Computer Communications (INFOCOM 2019)*, pp. 370–378, Paris, France, 2019.

[17] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 160–167, 2018.

[18] S. Balakrishnan, S. Gupta, A. Bhuyan, P. Wang, D. Koutsonikolas, and Z. Sun, "Physical layer identification based on spatial–temporal beam features for millimeter-wave wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1831–1845, 2019.

[19] A. Al-Shawabka, F. Restuccia, S. D'Oro et al., "Exposing the fingerprint: dissecting the impact of the wireless channel on radio fingerprinting," in *Proceedings of The 39th IEEE International Conference on Computer Communications (INFOCOM 2020)*, pp. 646–655, Toronto, ON, Canada, 2020.

[20] Z. S. WenhaoWang, K. Ren, and B. Zhu, "User capacity of wireless physical-layer identification: an information-theoretic perspective," in *2016 IEEE International Conference on Communications (ICC)*, pp. 1–6, Kuala Lumpur, Malaysia, 2016.

[21] W. Wang, Z. Sun, K. Ren, and B. Zhu, "User capacity of wireless physical-layer identification," *IEEE Access*, vol. 5, pp. 3353–3368, 2017.

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

[23] P. Hao, X. Wang, and A. Behnad, "Performance enhancement of I/Q imbalance based wireless device authentication through collaboration of multiple receivers," in *2014 IEEE International Conference on Communications (ICC)*, pp. 939–944, Sydney, Australia, 2014.

[24] F. Restuccia, S. D'Oro, A. Al-Shawabka et al., "Deepradioid: real-time channel resilient optimization of deep learning-based radio fingerprinting algorithms," in *Proceedings of the 20th International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 51–60, Hawaii, USA, 2019.

[25] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, and Y. Yan, "Design of a hybrid RF fingerprint extraction and device classification scheme," *IEEE Internet Things Journal*, vol. 6, no. 1, pp. 349–360, 2019.

[26] X.-C. Yin, C. Yang, W.-Y. Pei, and H.-W. Hao, "Shallow classification or deep learning: an experimental study," in *2014 22nd International Conference on Pattern Recognition*, pp. 1904–1909, Stockholm, Sweden, 2014.

[27] M. Kantardzic, *Data mining: concepts, models, methods, and algorithms*, John Wiley & Sons, 2011.

[28] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," 2015, https://arxiv.org/abs/1511.08458.

[29] Q. Wu, C. Feres, D. Kuzmenko et al., "Deep learning based rf fingerprinting for device identification and wireless security," *Electronics Letters*, vol. 54, no. 24, pp. 1405–1407, 2018.

[30] Y. Wang, G. Gui, H. Gacanin, T. Ohtsuki, O. A. Dobre, and H. V. Poor, "An efficient specific emitter identification method based on complex-valued neural networks and network compression," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 8, pp. 2305–2317, 2021.

[31] M. Morelli and U. Mengali, "Carrier-frequency estimation for transmissions over selective channels," *IEEE Transactions on Communications*, vol. 48, no. 9, pp. 1580–1589, 2000.

[32] K. Sankhe, M. Belgiovine, F. Zhou et al., "No radio left behind: radio fingerprinting through deep learning of physical-layer hardware impairments," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 165–178, 2019.

[33] J. Li, G. Liu, and G. B. Giannakis, "Carrier frequency offset estimation for OFDM-based WLANs," *IEEE Signal Processing Letters*, vol. 8, no. 3, pp. 80–82, 2001.

[34] D. Huang and K. B. Letaief, "Carrier frequency offset estimation for OFDM systems using null subcarriers," *IEEE Transactions on Communications*, vol. 54, no. 5, pp. 813–823, 2006.

[35] W. Hou, X. Wang, and J.-Y. Chouinard, "Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates," in *2012 IEEE International Conference on Communications (ICC)*, pp. 3559–3563, Ottawa, Canada, 2012.

[36] M. M. U. Rahman, A. Yasmeen, and J. Gross, "Phy layer authentication via drifting oscillators," in *2014 IEEE Global Communications Conference*, pp. 716–721, Sydney, Australia, 2014.

[37] L. Yang, S. Song, Y. Gong, H. Gao, and W. Cheng, "Nonparametric dimension reduction via maximizing pairwise separation probability," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 10, pp. 3205–3210, 2019.

[38] W. Bian and D. Tao, "Max-min distance analysis by using sequential sdp relaxation for dimension reduction," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 5, pp. 1037–1050, 2010.

[39] J.-C. Lin, "Synchronization requirements for 5g: an overview of standards and specifications for cellular networks," *IEEE Vehicular Technology Magazine*, vol. 13, no. 3, pp. 91–99, 2018.