Hindawi
Mobile Information Systems
Volume 2017, Article ID 7393526, 13 pages
https://doi.org/10.1155/2017/7393526

Research Article

Efficient Physical-Layer Secret Key Generation and Authentication Schemes Based on Wireless Channel-Phase

Longwang Cheng,[1] Li Zhou,[1,2] Boon-Chong Seet,[3] Wei Li,[1] Dongtang Ma,[1] and Jibo Wei[1]

[1] *School of Electronic Science and Engineering, National University of Defense Technology, Changsha, China*
[2] *Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory, Shijiazhuang, China*
[3] *Department of Electrical and Electronic Engineering, Auckland University of Technology, Auckland, New Zealand*

Correspondence should be addressed to Li Zhou; zhouli2035@nudt.edu.cn

Received 3 February 2017; Accepted 30 April 2017; Published 10 July 2017

Academic Editor: Wei Tan

Copyright © 2017 Longwang Cheng et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Exploiting the inherent physical properties of wireless channels to complement or enhance the traditional security mechanisms has attracted prominent attention recently. However, the existing secret key generation schemes suffer from miscellaneous extracting procedure. Many PHY-layer authentication schemes assume that the knowledge of the shared key is preknown. In this paper, we propose PHY-layer secret key generation and authentication schemes for orthogonal frequency-division multiplexing (OFDM) systems. In the secret key generation scheme, to simplify the extracting procedure, only one legitimate party is chosen to probe the channel and quantize the measurements to obtain the preliminary key. The preliminary key is masked by the channel-phase after the mapping and before equalization and distributed to the other party. The final shared key is used for the PHY-layer authentication scheme in which random signals and the shared key masked by the channel-phase are exchanged at the PHY-layer. Then, a binary hypothesis test is formulated for authentication. Simulation results show that the proposed secret key generation scheme outperforms the existing schemes. For the PHY-layer authentication scheme, it is immune to various passive and active attacks and a high successful authentication rate is acquired even at low signal-to-noise ratio region.

1. Introduction

With the continuous development of the wireless communications, people pay more and more attention to the security issue. The security mechanisms of traditional communications networks mainly rely on symmetric or asymmetrical encryption algorithms to achieve confidentiality and authentication. However, due to the lack of key management infrastructures and limited resources of the devices, the conventional security mechanisms may be inapplicable in wireless communications. In addition, the broadcasting nature of the wireless channels causes the wireless communication channel easily to be eavesdropped on or intercepted by an adversary [1, 2]. Therefore, the interest in exploiting the characteristics of the wireless channels at the PHY-layer to enhance and complement the conventional security mechanisms is growing, such as the secret key extraction from the characteristics of wireless channels [3–19] and PHY-layer authentication [20–27].

From an information-theoretic perspective, the authors of [3, 4] demonstrated that it is possible to extract secret key bits from the correlated random sources. Fortunately, with the properties of randomness, location-specific, and reciprocity, the wireless channels can be seen as natural correlated random sources. In [5], Hassan et al. firstly introduced the idea of generating secret keys from the characteristics of the wireless channels. Since then, many investigators pay attention to extract secret keys from received signal strength (RSS) [6–9], since the RSS is easy to acquire from the off-the-shelf wireless cards. However, these methods suffer from scalability and low secret key generation rate (KGR) which is defined as the average amount of secret key bits produced in one measurement/second [10–12]. To resolve these issues, researchers exploit the channel state information (CSI) to extract secret keys [13–15]. Besides, to increase the KGR, the orthogonal frequency-division multiplexing (OFDM) [18, 19] and multi-input-multi-output (MIMO) techniques in the PHY-layer are adopted.

Various efforts also have been made towards PHY-layer authentication, which can be recognized as a complement or an enhancement to the higher layer authentication mechanisms. In general, according to whether a shared secret key between the legitimate parties is utilized to authenticate each other or not, the existing PHY-layer authentication schemes can be divided into key based or keyless [20]. In some practical cases, it might be difficult to implement the keyless authentication schemes [21–23]. This is because the features of either the transmitting device or the specific channel between the legitimate users, which are exploited to authenticate the transmission, are required to be identified. Instead, the authentication schemes based on the shared key between two legitimate users [25–27] are closer to the conventional challenge-response authentication protocols. In [25], the specific spatial and temporal multipath fading channel between the transmitter and the receiver was exploited for an authentication algorithm. The authors of [26] proposed a PHY-layer challenge-response authentication mechanism (PHY-CRAM) where the randomness and reciprocity of the wireless signal amplitude are exploited for authentication. In [27], a PHY-layer phase challenge-response authentication scheme (PHY-PCRAS) was proposed. It exploited the randomness and reciprocity of the channel-phase response to protect shared key from possible eavesdropping and achieve authentication.

However, the existing secret key generation schemes suffer from miscellaneous extracting procedure which may lead to a high secret key bits mismatched rate (BMR, defined as the ratio of the number of bits unmatched between Alice and Bob's preliminary keys to the number of the preliminary key [7]) and an inefficiency in secret key generation. The key based authentication schemes assume that the knowledge of the shared key is preknown between the authenticated parties, but how to implement the secret key distribution is not given. In this paper, we propose PHY-layer secret key generation and authentication schemes for OFDM systems. Both schemes exploit the randomness and reciprocity of the channel-phase response that is very sensitive to the distance between the legitimate parties. In the secret key generation scheme, to simplify the extracting procedure, only one legitimate party is chosen to probe the channel and quantize the measurements to obtain the preliminary key. After mapping and before equalizing, the preliminary key is masked in the channel-phase and then distributed to the other legitimate party. The final shared key is used for the PHY-layer authentication scheme in which random signals and the generated shared key masked by the channel-phase through mapping and before equalizing are exchanged at the physical layer. Then, a binary hypothesis test is formulated for the authentication procedure.

The security strength of our proposed schemes relies heavily on the randomness of the fading channel and the relative geographic location of the attacker and legitimate users, because the channel-phase response is sensitive to the distance between the legitimate parties. That is, even when the attacker's computational power is increased, the security of our schemes is guaranteed.

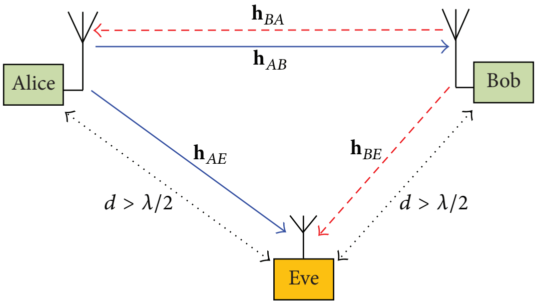


Figure 1: The system model.

The major contributions of this paper are summarized as follows:

(i) To simplify the secret key extraction procedure, we propose a secret key generation scheme based on the channel-phase response in which only one node is chosen to generate the preliminary key and further the preliminary key is masked by the channel-phase after mapping and before equalizing and distributed to the other node.

(ii) Extensive simulations are conducted to compare the secret key generation performance of the prior works with the proposed scheme and the security of the keys is evaluated under passive attack.

(iii) With the aid of the secret keys extracted in the proposed secret key generation scheme, we propose a PHY-layer authentication scheme based on the channel-phase response in which the shared key masked by the channel-phase is exchanged at the PHY-layer.

(iv) The judgement of the authentication is transformed into a binary hypothesis test and the security strength is analyzed under various types of attacks.

The remainder of this paper is organized as follows. In Section 2, we introduce the system model for the two proposed schemes. The procedure and performance of the proposed secret key generation scheme are analyzed in detail in Section 3. In Section 4, the proposed PHY-layer authentication is presented and the security and performance of the scheme are evaluated. Finally, concluding remarks are made in Section 5.

2. System Model

2.1. System Model Description. As shown in Figure 1, an OFDM network with three nodes, in which Alice and Bob are legitimate nodes and Eve is an adversary, is considered. Each node is equipped with a single antenna. All nodes work in half-duplex mode and a time-division duplex (TDD) system is employed. The forward and reverse propagation channels are identical during coherence time by reciprocity.

The distance from Eve to both Alice and Bob is more than $\lambda/2$, where λ is the wavelength of the radio waves; thus the wiretap channels and the legitimate channel are uncorrelated [28].

2.2. The Assumptions. It is assumed that the subcarriers are well separated for ensuring independent fading, which ensures the randomness of the extracted secret keys and the independence of the subchannels.

For the secret key generation case, Alice and Bob want to build a shared secret key. Eve, a passive adversary who tries to obtain the key by eavesdropping, can monitor all the communications during the secret key extraction and neither modify any messages exchanged between Alice and Bob nor jam the legitimate channel. For the PHY-layer authentication case, Alice and Bob try to authenticate each other. Eve is an active attacker who not only can listen to the communications for authentication but also perform various active attacks.

The procedures and parameters of the secret key generation scheme and the PHY-layer authentication scheme adopted by Alice and Bob are assumed to be open to Eve.

2.3. Channel Reciprocity. The principle of the short-term reciprocity of the radio channel is the basis of the two proposed schemes. As discussed in [29], this is guaranteed because, in the real environments compared to channel coherence time T_C, the processing time of channel probing or authentication can be much smaller. For example, we consider the 2.4 GHz radio frequency carrier. For a mobile scenario, the channel variation is mainly due to Doppler effects and when the relative speed between the transmitter and receiver is $v = 60\,\text{km/h}$, the Doppler frequency is $f_d = vf/c = 16.67 \times 2.4 \times 10^9/(3 \times 10^8) = 133.3\,\text{Hz}$. Empirically, the channel coherence time T_C which is related to the maximum Doppler frequency shift can be calculated as $T_C = 9/16\pi f_d = 9/(16\pi \times 133.3) = 1.3\,\text{ms}$. In our proposed schemes, the processing time, which demands for channel coherence, includes double propagation time T_p and transmitting time T_t and one operation delay T_d. For 5 MHz sampling rate, it takes about $T_t = 16$ us to transmit an OFDM symbol with 64 subcarriers and 16 cyclic prefix samples. When the distance is 3000 m, the propagation time $T_P = 10$ us. In general, the transmitting time is in the same order of the operation delay. Then the total processing time $2T_t + 2T_P + T_d$ is much smaller than the coherence time T_c in our two proposed schemes.

3. Secret Key Generation and Performance Analysis

3.1. The Proposed Secret Key Generation Scheme. Compared to single carrier systems, OFDM systems can provide extra randomness in view of the use of multiple subchannels. In this paper, we propose a secret key generation scheme based on the channel-phase response of OFDM systems in frequency domain.

In general, a secret key generation scheme consists of the following four steps:

(1) Channel probing: Alice and Bob alternately and periodically send the probe signals to each other to obtain the characteristics of channel between them.

(2) Measurement quantization: Alice and Bob separately quantize the collected channel characteristics into bit vector to obtain a preliminary secret key bits.

(3) Information reconciliation: due to the nature of half-duplex and noise, a small number of Alice and Bob's preliminary keys may be mismatched. They exchange messages to agree on a synchronized key.

(4) Privacy amplification: since the messages exchanged in the information reconciliation phase are open to Eve, they may be exploited by Eve to infer the generated keys. To address this issue, Alice and Bob apply privacy amplification method to eliminate Eve's partial information about the key and obtain a shared key.

We can find that, for half-duplex mode, the legitimate nodes have to transmit probe signals alternately to characterize the channel, which means they cannot probe the channel simultaneously. After collecting sufficient measurements, they quantize the measurements into preliminary keys separately. These phases may bring estimation error and quantization error, which may lead to many mismatched bits between the preliminary keys generated by the legitimate parties. Thus, the cost to reconcile the mismatched bits is high.

In this paper, to address this problem, we propose a scheme in which only one of the legitimate nodes is chosen to perform the channel probing and measurement quantization. This simplifies the procedure of secret key generation and eliminates the estimation error and quantization error.

Under the principle of reciprocity, we set $\mathbf{h}_{AB} = \mathbf{h}_{BA} = \mathbf{h}$. To maintain the reciprocity requirement, for each of Alice to Bob's channel probes, the corresponding Bob to Alice's channel probe event must be conducted within the coherence time of the channel. The process of the proposed secret key generation scheme is depicted in Figure 2 and the detailed steps are as follows. (Note that throughout this paper, the signals and equations are in frequency domain.)

Step 1 (channel probing). The experiments in [7] revealed that, in certain environments, due to lack of variations in the wireless channel, the extracted bits have very low entropy making these bits unsuitable for a secret key, which can cause predictable key generation by an adversary in these static environments. To prevent this, during channel probing, we utilize random signals to probe the channel. Suppose that Bob is chosen to probe the channel and quantize the channel measurements. Thus, Alice transmits the random probe signal $\mathbf{s}_a = [s_{a,1}, s_{a,2}, \ldots, s_{a,N}]$ to Bob, where $s_{a,i} = \exp(j\theta_{a,i})$, $\theta_{a,i} \sim U[0, 2\pi]$ for $i = 1, 2, \ldots, N$, and N is the number of the subcarriers of the OFDM system. The random signal $\mathbf{s}_a$ is unknown to Bob and Eve.

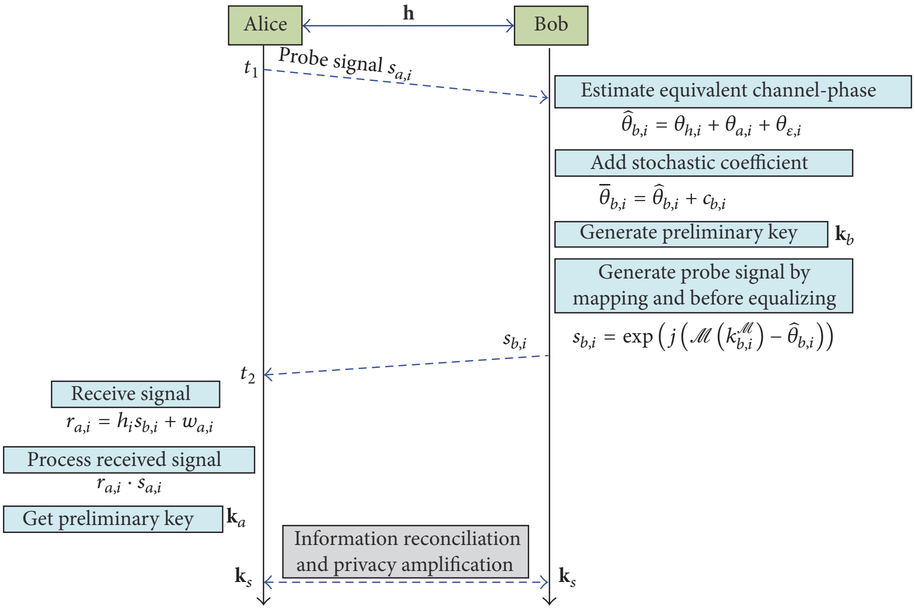

Alice
h
Bob
Probe signal $s_{a,i}$
t_1
Estimate equivalent channel-phase
$\hat{\theta}_{b,i} = \theta_{h,i} + \theta_{a,i} + \theta_{\varepsilon,i}$
Add stochastic coefficient
$\bar{\theta}_{b,i} = \hat{\theta}_{b,i} + c_{b,i}$
Generate preliminary key
$\mathbf{k}_b$
Generate probe signal by mapping and before equalizing
$s_{b,i}$
$s_{b,i} = \exp\left(j\left(\mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) - \hat{\theta}_{b,i}\right)\right)$
t_2
Receive signal
$r_{a,i} = h_i s_{b,i} + w_{a,i}$
Process received signal
$r_{a,i} \cdot s_{a,i}$
Get preliminary key
$\mathbf{k}_a$
Information reconciliation and privacy amplification
$\mathbf{k}_s$
$\mathbf{k}_s$

Figure 2: The process of the secret key generation.

Without loss of generality, we only take the ith $(1 \le i \le N)$ subcarrier, for example. Thus, the received signal at Bob can be expressed as

$$\begin{aligned} r_{b,i} &= h_i s_{a,i} + w_{b,i} = \left|h_i\right| \exp\left(j\theta_{h,i}\right) s_{a,i} + w_{b,i} \\ &= \left|h_i\right| \exp\left(j\theta_{h,i} + j\theta_{a,i}\right) + w_{b,i}, \end{aligned} \tag{1}$$

where h_i denotes the ith subchannel response of the legitimate channel in frequency domain and $\theta_{h,i}$ is the underlying subchannel-phase response. The subchannels are independent and identically distributed (i.i.d.) and $h_i \sim \mathscr{CN}(0, \sigma_h^2)$. $w_{b,i}$ is the i.i.d. complex Gaussian noise with zero mean and variance σ_n^2.

Based on the received signal, Bob gets the subchannel-phase response estimation as

$$\hat{\theta}_{b,i} = \tan^{-1}\left(\frac{\operatorname{imag}\left(r_{b,i}\right)}{\operatorname{real}\left(r_{b,i}\right)}\right) = \theta_{h,i} + \theta_{a,i} + \varepsilon_{b,i}, \tag{2}$$

where $\varepsilon_{b,i}$ is the phase estimation error. Note that the phase of the random probe signal $\theta_{a,i}$ is contained in the subchannel-phase response estimation, so we treat $\hat{\theta}_{b,i}$ as equivalent subchannel-phase response estimation.

If Eve is in close proximity to Bob (here the "close" means that the distance between Eve and Bob is much smaller than $\lambda/2$, which may lead to highly correlated $\mathbf{h}_{AB}$ and $\mathbf{h}_{AE}$), she may infer the preliminary key easily based on her observations. To reduce the risk, Bob adds a stochastic coefficient to $\hat{\theta}_{b,i}$ as

$$\bar{\theta}_{b,i} = \hat{\theta}_{b,i} + c_{b,i}, \tag{3}$$

where $c_{b,i}$ is uniformly distributed over $[0, 2\pi]$ and $\mathbf{c}_b = [c_{b,1}, c_{b,2}, \ldots, c_{b,N}]$. Bob obtains the vector records as $\bar{\boldsymbol{\theta}}_b = [\bar{\theta}_{b,1}, \bar{\theta}_{b,2}, \ldots, \bar{\theta}_{b,N}]$.

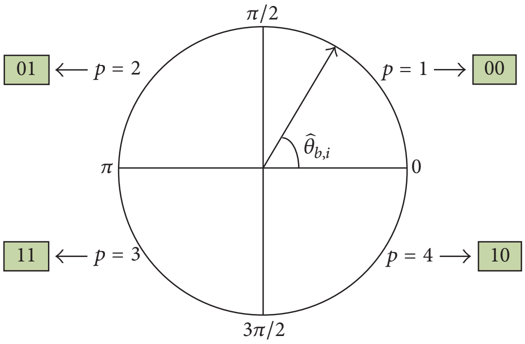


Figure 3: A quantization example with $M = 2$.

Step 2 (measurement quantization and preliminary key distribution). Bob quantizes the vector records $\bar{\theta}_b$ into bit vector to obtain the preliminary key. Firstly, Bob divides the interval $[0, 2\pi)$ into 2^M subintervals, where 2^M is the number of quantization levels, which is bounded by the mutual information between Alice and Bob [30]. Thus each $\bar{\theta}_{b,i}$ can be quantized to M binary bits. The pth $(1 \le p \le 2^M)$ subinterval is $[2\pi(p-1)/2^M, 2\pi p/2^M)$. Secondly, gray code is used to assign a binary code word with M bits to each subinterval. A quantization example with $M = 2$ is illustrated in Figure 3.

The ith record can be quantized as

$$\begin{aligned} &Q\left(\bar{\theta}_{b,i}\right) = p_i, \\ &\qquad \text{if } \operatorname{mod}\left(\bar{\theta}_{b,i}, 2\pi\right) \in \left[\frac{2\pi\left(p_i - 1\right)}{2^M}, \frac{2\pi p_i}{2^M}\right). \end{aligned} \tag{4}$$

After quantization, Bob obtains the preliminary key as $\mathbf{k}_b = [k_{b,1}, k_{b,2}, \ldots, k_{b,NM}]$.

Then, Bob sends "probe signal" to Alice. Different from the constant probe signal and $\mathbf{s}_a$, this probe signal, in fact, is the preliminary key after mapping and before equalizing. Thus, the probe signal can be expressed as

$$s_{b,i} = \exp\left(j\mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) - j\widehat{\theta}_{b,i}\right), \tag{5}$$

where $\mathscr{M}(\cdot)$ denotes the mapping operation on the preliminary key and $k_{b,i}^{\mathscr{M}} = [k_{b,(i-1)l+1}, \dots, k_{b,(i-1)l+l}]$ is the ith input secret key sequence with length l ($Nl \leq NM$). When $l = 2$, a mapping function can be designed as

$$\mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) = \begin{cases} 0, & k_{b,i}^{\mathscr{M}} = \begin{bmatrix} 0 & 0 \end{bmatrix} \\ \dfrac{\pi}{2}, & k_{b,i}^{\mathscr{M}} = \begin{bmatrix} 0 & 1 \end{bmatrix} \\ \pi, & k_{b,i}^{\mathscr{M}} = \begin{bmatrix} 1 & 1 \end{bmatrix} \\ \dfrac{3\pi}{2}, & k_{b,i}^{\mathscr{M}} = \begin{bmatrix} 1 & 0 \end{bmatrix}. \end{cases} \tag{6}$$

The mapping function is known to Alice. The subtraction term in (5) denotes the preequalization process using the equivalent subchannel-phase response estimation. In fact, the preequalization process can be seen as an encryption operation; thus the preliminary key is masked by the subchannel-phase response estimation.

Alice's received signal can be expressed as

$$\begin{aligned} r_{a,i} &= h_i s_{b,i} + w_{a,i} \\ &= \left|h_i\right| \exp\left(j\left(\theta_{h,i} + \mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) - \widehat{\theta}_{b,i}\right)\right) + w_{a,i}, \end{aligned} \tag{7}$$

where $w_{a,i} \sim \mathscr{CN}(0, \sigma_n^2)$ is the i.i.d. complex Gaussian noise. Based on the reciprocity between the forward and reverse links and substituting $\widehat{\theta}_{b,i}$ with (2), (7) can be simplified as

$$r_{a,i} = \left|h_i\right| \exp\left(j\left(\mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) - \theta_{a,i} - \varepsilon_{b,i}\right)\right) + w_{a,i}. \tag{8}$$

As observed in (8), during the receiving, Alice completes the subchannel-phase equalization and eliminates the encryption based on the channel reciprocity. Alice further multiplies (8) by the random probe signal $s_{a,i}$ and gets

$$s_{a,i} r_{a,i} = \left|h_i\right| \exp\left(j\left(\mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) - \varepsilon_{b,i}\right)\right) + s_{a,i} w_{a,i}. \tag{9}$$

Then, Alice performs unmapping on the phase of $s_{a,i} r_{a,i}$ to acquire the preliminary key transmitted by Bob.

In conclusion, in this step, Bob firstly obtains the preliminary key by quantizing the vector records and randomly chooses Nl key bits from the preliminary key as the input key sequences of the mapping function. Secondly, these key sequences are mapped, preequalized, and transmitted to Alice. Lastly, Alice acquires these key sequences based on the channel reciprocity. So the preliminary key is distributed from Bob to Alice.

Step 3 (information reconciliation and privacy amplification). Note that, in our scheme, we assume that the length of the preliminary key is NM. In practical systems, this length may be much longer, which in turn may require more rounds of channel probing and secret key distribution. Alice and Bob need to update the random probe signal vector $\mathbf{s}_a$ and the stochastic coefficient vector $\mathbf{c}_b$, respectively, after each round.

Due to the noise, a small number of mismatched bits may exist in the preliminary keys of Alice and Bob. Then, the mismatched bits are reconciled by using BCH codes to get synchronized keys. The privacy of the synchronized keys is subsequently enhanced by using a hash function to obtain a secure and common key.

During the secret key generation process, Alice and Bob should do Steps 1 and 2 fast enough to ensure that $t_2 - t_1$ is not more than the coherence time. We can observe that due to the random probe signal, the randomness of the channel is ensured even if the environments are static. So it also can address the highly correlated and unsecure key bits problem in stationary environments [7].

3.2. Performance Analysis

3.2. Performance Analysis. In this subsection, we will analyze the proposed secret key generation scheme and evaluate its performance in terms of the secret key capacity, bits mismatched, and key generation rates.

3.2.1. Security Analysis. Eve is a passive attacker and only can listen to the communications during secret key generation. For ease of analysis, we neglect the effect of noise in Step 1 so that Eve's received signal from Alice is

$$r_{ea,i} = h_{AE,i} s_{a,i} = \left|h_{AE,i}\right| \exp\left(j\theta_{hAE,i} + j\theta_{a,i}\right), \tag{10}$$

where $h_{AE,i} = |h_{AE,i}| e^{j\theta_{hAE,i}}$ is the ith subchannel from Alice to Eve. In Step 2, Eve's received signal from Bob can be expressed as

$$\begin{aligned} r_{eb,i} &= h_{BE,i} s_{b,i} = \left|h_{BE,i}\right| \\ &\quad \cdot \exp\left(j\left(\theta_{hBE,i} + \mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) - \widehat{\theta}_{b,i}\right)\right) = \left|h_{BE,i}\right| \\ &\quad \cdot \exp\left(j\left(\theta_{hBE,i} + \mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) - \theta_{h,i} - \theta_{a,i} - \varepsilon_{b,i}\right)\right), \end{aligned} \tag{11}$$

where $h_{BE,i} = |h_{BE,i}| e^{j\theta_{hBE,i}}$ is the ith subchannel from Bob to Eve. We can find that the factors which influence Eve to derive the key bits are the phases of h_i, $h_{AE,i}$, $h_{BE,i}$, and $s_{a,i}$, that is, $\theta_{h,i}$, $\theta_{hAE,i}$, $\theta_{hBE,i}$, and $\theta_{a,i}$. Besides, the stochastic coefficient $c_{b,i}$ also impairs Eve's inference to some extent.

To reduce the factors, Eve can multiply (10) by (11) and obtains

$$\begin{aligned} r_{eb,i} r_{ea,i} &= \left|h_{BE,i} h_{AE,i}\right| \\ &\quad \cdot \exp\left(j\left(\theta_{hBE,i} + \theta_{hAE,i} + \mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) - \theta_{h,i} - \varepsilon_{b,i}\right)\right). \end{aligned} \tag{12}$$

Then, the factors are reduced to $\theta_{h,i}$, $\theta_{hAE,i}$, and $\theta_{hBE,i}$. Note that since the phase of the signals transmitted by Alice and Bob in Steps 1 and 2 is random, it is hard for Eve to estimate the phases of $\theta_{hAE,i}$ and $\theta_{hBE,i}$. Thus, it is difficult for Eve to derive the generated keys and we will analyze various cases in the following.

Firstly, both Alice and Bob are far away from Eve, so that the wiretap channels (i.e., h_{AE} and h_{BE}) and the legitimate channel (i.e., h) are uncorrelated, along with the random signal $\mathbf{s}_a$ and stochastic coefficient $\mathbf{c}_b$; for Eve, it is almost impossible to obtain the generated secret keys from her measurements.

Then, an aggressive case, where Eve is close to Bob, is considered. In this case, $h_{AE,i} \approx h_{AB,i} = h_i$. Then (10) can be approximately simplified as

$$r_{ea,i} = |h_i| \exp\left(j\theta_{h,i} + j\theta_{a,i}\right). \tag{13}$$

Then the phase of $r_{ea,i}$ is approximately equal to Bob's equivalent subchannel-phase response estimation $\widehat{\theta}_{b,i}$. So for Eve it is possible to infer the preliminary key by the same quantization approach. However, due to the random coefficient $\mathbf{c}_b$, which is unknown to Eve, the probability of obtaining the key based on $r_{ea,i}$ is low. In (11) and (12), since $h_{BE,i}$ is uncorrelated with $h_{BA,i}$, for Eve it is improbable to derive the distributed preliminary key.

Lastly, we consider that Eve is close to Alice. Under this circumstance, $h_{BE,i} \approx h_{BA,i} = h_i$, so (11) becomes

$$r_{eb,i} = |h_{BE,i}| \exp\left(j\left(\mathscr{M}\left(k_{b,i}^{\mathscr{M}}\right) - \theta_{a,i} - \varepsilon_{b,i}\right)\right). \tag{14}$$

Since $\theta_{a,i}$ is random and unknown to Eve, she cannot infer the key based on $r_{eb,i}$. In this situation, $h_{AE,i}$ is uncorrelated with $h_{AB,i}$, so it is obvious that Eve cannot obtain the key based on (10) and (12).

In conclusion, when Eve is a passive attacker, the secret key cannot be derived only by her observations and Alice and Bob can still establish a secure key. In fact, the channel-phase response is sensitive to the distance between Alice and Bob, so for Eve it is more difficult to infer the secret key bits from her measurements of the channel-phase. In addition, in [31], the authors pointed out that applying error-correcting codes on the preliminary key with reasonable rate can ensure the correct preliminary key for Alice in theory, while ensuring useless information for Eve. It means that we can design an error-correcting code with proper rate to further ensure the security of the proposed scheme.

3.2.2. The Secret Key Generation Performance. Firstly, the secret key capacity which is defined as the maximum available key generation rate [3] is considered. Since the subchannels are independent, for ease of analysis, we only take one of the subchannels, for example. Our proposed scheme can be approximatively modeled as Bob generating a random source $X = h$ and Alice observing the random source as $Y = X + W_a = h + W_a$, where $h \sim \mathscr{CN}(0, \sigma_h^2)$ is one of the subchannel responses and $W_a \sim \mathscr{CN}(0, \sigma_w^2)$ is the observed noise. Alice and Bob extract secret keys from the phases of X and Y, that is, θ_X and θ_Y, respectively. Assuming that Eve's observations are uncorrelated with Alice's, the secret key capacity can be expressed as [3]

$$C_P = I\left(\theta_X; \theta_Y\right), \tag{15}$$

where symbol $I(\cdot;\cdot)$ denotes the mutual information between two random variables. Since the joint probability density function of θ_X and θ_Y is difficult to calculate, we adopt the information theoretical estimators (ITE) toolbox to estimate the secret key capacity [32]. The input of the ITE is $(\boldsymbol{\theta}_X; \boldsymbol{\theta}_Y)$, where $\boldsymbol{\theta}_X = [\theta_{X,1}, \theta_{X,2}, \ldots, \theta_{X,k}]$, $\boldsymbol{\theta}_Y = [\theta_{Y,1}, \theta_{Y,2}, \ldots, \theta_{Y,k}]$, and k is the length of the input. In the simulations, the signal-to-noise ratio (SNR) is defined as σ_h^2/σ_w^2.

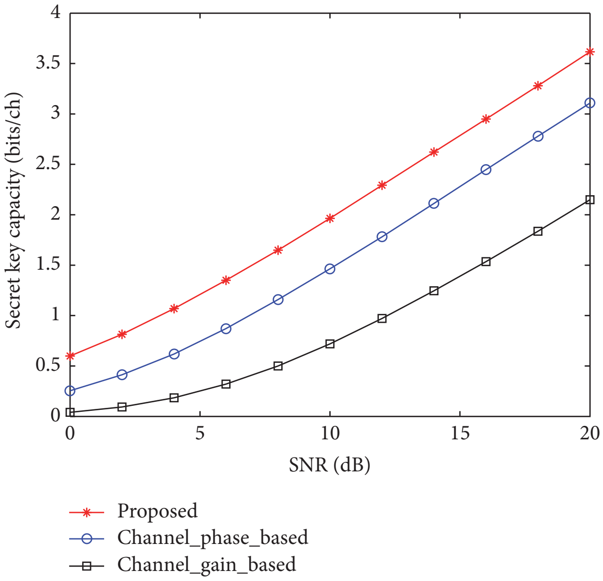


FIGURE 4: The secret key capacity of different schemes.

The secret key capacity of the proposed secret key generation scheme is compared with the existing channel-phase based secret key generation scheme [15] and channel-gain based secret key generation scheme [14] in Figure 4. During channel probing, the channel condition of these three schemes is identical. We can clearly observe that, in contrast to the channel-phase based and channel-gain based schemes, our proposed scheme achieves a greater secret key capacity. For example, when SNR is 10 dB, the secret key capacity of the proposed scheme is 34% and 170% greater than the channel-phase based scheme and channel-gain based scheme, respectively. Note that the secret key capacity of the discussed OFDM systems is N times of those shown in Figure 4.

Secondly, we analyze the secret key bits mismatched and key generation rates. The BMR and KGR of the proposed scheme are evaluated through Monte-Carlo simulations under multipath channels and further are compared with the channel-phase based and channel-gain based schemes. Since it does not need to estimate the CSI during channel probing, in the simulations, the probe signal contains two OFDM symbols, that is, one pilot symbol for synchronization and one symbol for signal phase estimation. The carrier frequency of the OFDM system is 2.4 GHz and the number of the subcarriers is $N = 64$. We consider the multipath Rayleigh fading channel with 2 us constant delay time and the maximum Doppler frequency is 0 Hz (suppose that Alice and Bob remain static in the simulations). The sample interval is 0.25 us.

These three schemes adopt the same quantization method, that is, equal interval quantization method, in

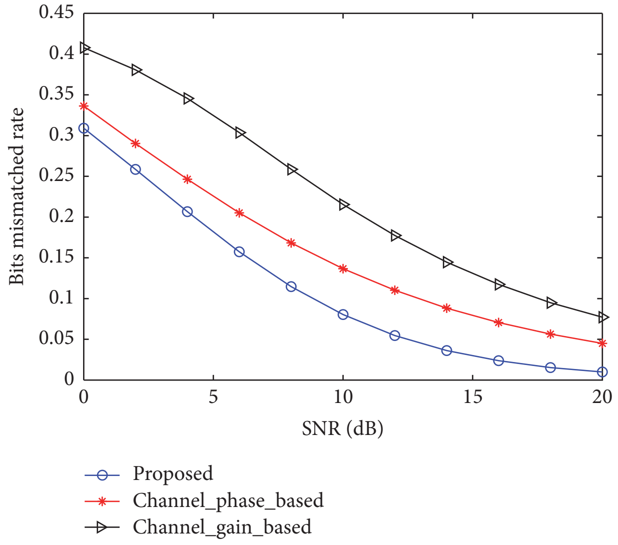


Figure 5: The BMR performance of different schemes.

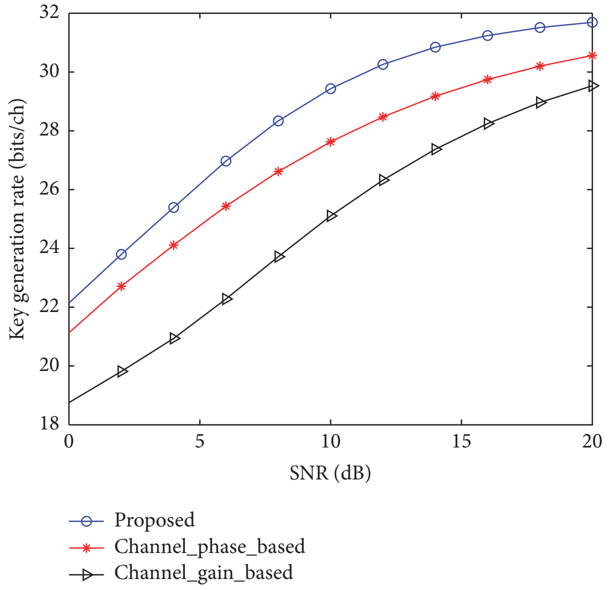


Figure 6: The KGR performance of different schemes.

Table 1: The evaluation of randomness test.

Test	P value
Frequency	0.65
Block Frequency	0.55
Cumulative sum (Rev)	0.30
Cumulative sum (Fwd)	0.64
Approximate entropy	0.69
Runs	0.48
Longest run	0.54
Serial	0.72 0.55

which the characteristics space is divided on average into $2^M = 4$ subspaces. The same information is reconciled and privacy amplification approaches are employed. Note that, theoretically, the bit length of the resulting quantization should be bounded by the mutual information between Alice and Bob [33]. In other words, the quantization level 2^M should not be higher than the secret key capacity, that is, $2^M \leq 2^{C_P}$. However, for ease of analysis, the quantization levels for the three schemes are all set as $2^M = 4$.

Figures 5 and 6 show the BMR and KGR performance of these schemes, respectively. From these two figures, we can observe that the BMRs of these schemes decrease, while the KGRs increase as SNR increases. The primary reason is that the accuracy of the channel estimates obtained in the channel probing phase increases as SNR increases. The BMR and KGR performances of the proposed scheme exhibit apparent superiority to the other schemes. For example, when SNR = 10 dB, the BMR and KGR of the proposed scheme decreases by 41% and increases 6.6%, respectively, compared to the channel-phase based scheme.

Lastly, the randomness of the secret key is analyzed. A cryptographic key should be substantially random; otherwise, an adversary can crack the key with low cost. A widely used randomness test suite NIST [34] is employed to verify the randomness of our generated secret key bits. The NIST test suite is a statistical package consisting of 16 tests which were developed to test the randomness of binary sequences. To pass the test, all the P values of the 16 tests should be at least greater than 0.01. We randomly select 10-bit sequences generated from our simulations at SNR = 10 dB. Due to the limitation of bit length, we run eight typical tests. The results in Table 1 shows that our generated bit sequences pass the NIST test and their average entropy is close to that of a truly random sequence.

4. PHY-Layer Authentication Scheme and Performance Analysis

4.1. PHY-Authentication Scheme. In the proposed secret key generation scheme, the legitimate parties establish a shared key which can be used for the encryption and authentication. The existing key based authentication schemes assume that the knowledge of the shared key is preknown between the authenticated parties, but how to achieve the secret key distribution is not given. Consider that the shared key between the authenticated parties is generated by our proposed secret key generation scheme.

After establishing a shared key and a period of time without communication, if Alice and Bob want to establish a communication, they need to authenticate each other. In this section, we propose a challenge-response PHY-layer authentication scheme for OFDM systems, which exploits the short-term reciprocity and randomness of the channel-phase response in TDD mode. Generally, Alice and Bob need a two-way authentication process to achieve the mutual authentication. However, the one-way authentication process is enough to describe the process, since both directions of the two-way authentication employ the same regulation. We assume that Alice wants to communicate with Bob, who in turn needs to verify the identity of "Alice" based on the proposed challenge-response PHY-layer authentication scheme (here Bob is assumed to be legitimate, while, for the illegitimate Bob, it will be analyzed later). The process of the proposed PHY-layer authentication scheme is shown in Figure 7 and the detailed stages are as follows.

Stage 1. Alice transmits an authentication request signal to Bob. The authentication request signal contains the frame type, time stamp information, media access control address, and so forth.

Stage 2. After receiving the authentication request, Bob contemplates that "Alice" wants to communicate with himself. Then Bob generates a response signal vector $\mathbf{s}_b = [s_{b,1}, s_{b,2}, \ldots, s_{b,N}]$ and sends to "Alice," where $s_{b,i} = \exp(j\theta_{b,i})$ and $\theta_{b,i} \sim U[0, 2\pi]$ for $i = 1, 2, \ldots, N$. N is the number of the subcarriers. The random response signal vector $\mathbf{s}_b$ is unknown to Alice and Eve.

Stage 3. The received signal of the ith subcarrier in frequency domain at Alice is

$$\begin{aligned} r_{a,i} &= h_{BA,i} s_{b,i} + w_{b,i} \\ &= \left|h_{BA,i}\right| \exp\left(j\theta_{hBA,i} + j\theta_{b,i}\right) + w_{a,i}, \end{aligned} \tag{16}$$

where $h_{BA,i}$ denotes the ith subchannel response from Bob to Alice and $\theta_{hBA,i}$ is the underlying subchannel-phase response. The subchannels are i.i.d. and $h_{BA,i} \sim \mathscr{CN}(0, \sigma_h^2)$. $w_{a,i}$ is the i.i.d. complex Gaussian noise with zero mean and variance σ_n^2. Alice is not concerned with what Bob transmits but only estimates the phase of the received signal. The estimation can be expressed as

$$\widehat{\theta}_{a,i} = \tan^{-1}\left(\frac{\operatorname{imag}\left(r_{a,i}\right)}{\operatorname{real}\left(r_{a,i}\right)}\right) = \theta_{hBA,i} + \theta_{b,i} + \varepsilon_{a,i}, \tag{17}$$

where $\varepsilon_{a,i}$ is the phase estimation error.

Then, to generate a tagged signal vector $\mathbf{s}_a$ for authentication, Alice processes her shared secret key by using the mapping function and preequalizes the mapped key by subtracting the phase estimation vector $\widehat{\boldsymbol{\theta}}_a$ (here the length of the shared key is assumed to be long enough). The tagged signal at the ith subcarrier is

$$s_{a,i} = \exp\left(j\mathscr{M}\left(k_{a,i}^{\mathscr{M}}\right) - j\widehat{\theta}_{a,i}\right). \tag{18}$$

Alice sends the tagged signal to Bob. As processed in (18), the secret key for authentication is masked by phase estimation and it is difficult for a passive attacker to crack the authenticated secret key.

Stage 4. Bob's received signal is

$$\begin{aligned} r_{b,i} &= h_{AB,i} s_{a,i} + w_{b,i} \\ &= \left|h_{AB,i}\right| \exp\left(j\left(\theta_{hAB,i} + \mathscr{M}\left(k_{a,i}^{\mathscr{M}}\right) - \widehat{\theta}_{a,i}\right)\right) + w_{b,i}, \end{aligned} \tag{19}$$

where $h_{AB,i}$ denotes the ith subchannel response from Alice to Bob, and $\theta_{hAB,i}$ is the underlying subchannel-phase response. $w_{b,i} \sim \mathscr{CN}(0, \sigma_n^2)$ is the i.i.d. complex Gaussian noise. Alice and Bob perform these steps fast enough to ensure the time interval from Stages 2–4 is smaller than the coherence time; thus $h_{AB,i} = h_{BA,i} = h_i$. Then (19) can be simplified as

$$r_{b,i} = \left|h_i\right| \exp\left(j\left(\mathscr{M}\left(k_{a,i}^{\mathscr{M}}\right) - \theta_{b,i} - \varepsilon_{a,i}\right)\right) + w_{b,i}. \tag{20}$$

We can find that the channel-phase equalization has been completed during the receiving. Bob multiplies $s_{b,i}$ by his response signal $r_{b,i}$ and gets $\mathbf{y} = \mathbf{r}_b \odot \mathbf{s}_b$, where $\odot$ denotes element-wise multiplication.

The ith element of $\mathbf{y}$ can be expressed as

$$y_i = r_{b,i} s_{b,i} = \left|h_i\right| \exp\left(j\left(\mathscr{M}\left(k_{a,i}^{\mathscr{M}}\right) - \varepsilon_{a,i}\right)\right) + w_{b,i} s_{b,i}. \tag{21}$$

Then Bob obtains the signal y_i which only contains the mapped secret key from Alice and estimation error. Based on y_i, combining his shared key, Bob needs to judge whether the other party is Alice or not. There are two solutions for this judgement. A straightforward solution is to check the difference between the obtained authenticated key $\mathbf{k}_a^{\mathscr{M}}$ from "Alice" and his own secret key $\mathbf{k}_b^{\mathscr{M}}$, where $\mathbf{k}_a^{\mathscr{M}} = \mathscr{M}^{-1}(\angle\mathbf{y})$. The difference is defined as $D = \operatorname{sum}(\mathbf{k}_a^{\mathscr{M}} \oplus \mathbf{k}_b^{\mathscr{M}})$, where $\oplus$ is the XOR operation. If $D < D_0$, Bob determines that the other party is Alice; otherwise it is not, where D_0 is a constant real number. However, it is hard to determine D_0 in practical systems. Thus, we provide another solution in which the authentication judgement is formulated as a binary hypothesis test.

From (21), we can find that the phase of y_i is mainly affected by the mapped authenticated key. In order to eliminate the influence of the authenticated key, similar to [27], we generate a variable with the expression as

$$C = \left|e^{-j\mathscr{M}(\mathbf{k}_b^{\mathscr{M}})} \mathbf{y}^T\right|, \tag{22}$$

where $()^T$ denotes transpose operation. Thus, the binary hypothesis test can be expressed as

$$\begin{aligned} &\mathscr{H}0\colon \mathbf{k}_x^{\mathscr{M}} = \mathbf{k}_e^{\mathscr{M}}, \\ &\mathscr{H}1\colon \mathbf{k}_x^{\mathscr{M}} = \mathbf{k}_b^{\mathscr{M}}, \end{aligned} \tag{23}$$

where $\mathbf{k}_x^{\mathscr{M}}$ denotes the authenticated key possessed by "Alice." For $\mathscr{H}0$ and $\mathscr{H}1$, the corresponded $C_{\mathscr{H}0}$ and $C_{\mathscr{H}1}$ are

$$\begin{aligned} &C_{\mathscr{H}0} \\ &\quad = \left|\sum_{i=1}^{N}\left(\left|h_i\right| e^{j(\mathscr{M}(k_{e,i}^{\mathscr{M}}) - \mathscr{M}(k_{b,i}^{\mathscr{M}}) - \varepsilon_{a,i})} + e^{-j\mathscr{M}(k_{b,i}^{\mathscr{M}})} w_{b,i} s_{b,i}\right)\right|, \\ &C_{\mathscr{H}1} = \left|\sum_{i=1}^{N}\left(\left|h_i\right| e^{j(-\varepsilon_{a,i})} + e^{-j\mathscr{M}(k_{b,i}^{\mathscr{M}})} w_{b,i} s_{b,i}\right)\right|. \end{aligned} \tag{24}$$

Based on (24), Bob makes a final decision by comparing with a threshold T.

$$C \underset{\mathscr{H}0}{\overset{\mathscr{H}1}{\gtrless}} T. \tag{25}$$

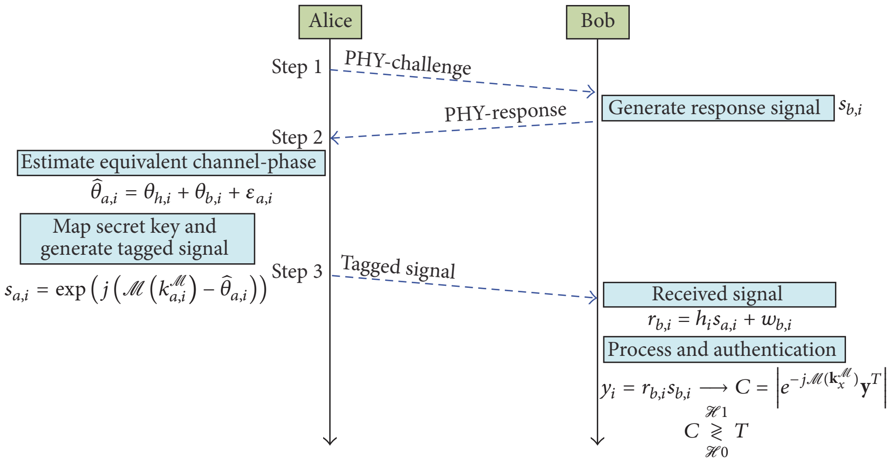

Alice
Bob
Step 1
PHY-challenge
Generate response signal
$s_{b,i}$
PHY-response
Step 2
Estimate equivalent channel-phase
$\hat{\theta}_{a,i} = \theta_{h,i} + \theta_{b,i} + \varepsilon_{a,i}$
Map secret key and generate tagged signal
Step 3
Tagged signal
$s_{a,i} = \exp\left(j\left(\mathscr{M}\left(k_{a,i}^{\mathscr{M}}\right) - \hat{\theta}_{a,i}\right)\right)$
Received signal
$r_{b,i} = h_i s_{a,i} + w_{b,i}$
Process and authentication
$y_i = r_{b,i} s_{b,i} \longrightarrow C = \left|e^{-j\mathscr{M}(\mathbf{k}_x^{\mathscr{M}})}\mathbf{y}^T\right|$
$C \underset{\mathscr{H}0}{\overset{\mathscr{H}1}{\gtrless}} T$

Figure 7: The process of the PHY-layer authentication.

If $\mathscr{H}1$ is true, then Bob judges that the other party is Alice; otherwise, it is not.

Now, it is essential to find the threshold T. We can see that, in both hypotheses, $e^{-j\mathscr{M}(\mathbf{k}_b^{\mathscr{M}})}\mathbf{y}^T$ is the sum of N dependent normally distributed random variables. The resulting sum is still normally distributed [27]; thus its amplitude C obeys Rice distribution. The probability density function of C is

$$f_{C_{\mathscr{H}i}}(x) = \frac{x}{\sigma_{\mathscr{H}i}^2}\exp\left(-\frac{x^2+\overline{C}_{\mathscr{H}i}^2}{2\sigma_{\mathscr{H}i}^2}\right) I_0\left(\frac{x\overline{C}_{\mathscr{H}i}}{\sigma_{\mathscr{H}i}^2}\right), \tag{26}$$

where $x \geq 0$, $i = 0, 1$. $\overline{C}_{\mathscr{H}i}$ and $\sigma_{\mathscr{H}i}^2$ denote the mean and variance of $C_{\mathscr{H}i}$, respectively. $I_0(\cdot)$ is the zero-order modified Bessel function of the first kind. Based on $f_{C_{\mathscr{H}i}}(x)$, we can calculate the false acceptance rate (the rate that the attacker passes the authentication) as

$$\begin{aligned} P_f &= \int_T^{+\infty} f_{C_{\mathscr{H}0}}(x)\,dx \\ &= \int_T^{+\infty} \frac{x}{\sigma_{\mathscr{H}0}^2}\exp\left(-\frac{x^2+\overline{C}_{\mathscr{H}0}^2}{2\sigma_{\mathscr{H}0}^2}\right) I_0\left(\frac{x\overline{C}_{\mathscr{H}0}}{\sigma_{\mathscr{H}0}^2}\right)dx \\ &= \int_{T/\sigma_{\mathscr{H}0}}^{+\infty} \frac{x}{\sigma_{\mathscr{H}0}}\exp\left(-\frac{\left(x/\sigma_{\mathscr{H}0}\right)^2+\left(\overline{C}_{\mathscr{H}0}/\sigma_{\mathscr{H}0}\right)^2}{2}\right) \\ &\quad \cdot I_0\left(\frac{x}{\sigma_{\mathscr{H}0}}\frac{\overline{C}_{\mathscr{H}0}}{\sigma_{\mathscr{H}0}}\right) d\left(\frac{x}{\sigma_{\mathscr{H}0}}\right) = Q\left(\frac{\overline{C}_{\mathscr{H}0}}{\sigma_{\mathscr{H}0}}, \frac{T}{\sigma_{\mathscr{H}0}}\right), \end{aligned} \tag{27}$$

where $Q(a,b) = \int_b^{+\infty} x\exp(-(x^2+a^2)/2)I_0(ax)dx$. $Q(\cdot,\cdot)$ is Marcum Q function. Thus, for a given false acceptance rate P_f, the threshold value T can be calculated by (27). Furthermore, we can get the successful authenticate rate (the rate that the legitimate user passes the authentication) as

$$P_d = \int_T^{+\infty} f_{C_{\mathscr{H}1}}(x)\,dx = Q\left(\frac{\overline{C}_{\mathscr{H}1}}{\sigma_{\mathscr{H}1}}, \frac{T}{\sigma_{\mathscr{H}1}}\right). \tag{28}$$

4.2. *Security Analysis.*

To evaluate the security of the proposed scheme, in this section, we analyze various types of attackers.

Eve, as the adversary, knows Alice and Bob's PHY-layer authentication scheme. When Eve is a passive attacker, she only can listen to all the communications inside the network and attempts to learn the shared key from the information that she eavesdropped. In Section 3.2, we have analyzed that it is almost impossible for Eve to crack and infer the shared key during the secret key generation. Thus, during the authentication, it is also difficult for Eve to derive the shared key and pass the authentication as a passive attacker, and the analysis process is similar. Therefore, we mainly consider the case that Eve is an active attacker. When Eve is an active attacker, she can perform three types of attacks, namely, impersonation attacks, jamming attacks, and replay attacks.

4.2.1. *Impersonation Attacks.*

Eve can impersonate Alice or Bob under impersonation attacks. If Eve initiates Stage 1 (sends authentication request to Bob), she can hardly succeed. The reason is that Bob's response contains no information about the shared key in Stage 2. If Eve impersonates Alice in Stage 3 and sends a tagged signal to Bob, she will not be authenticated by Bob as she has no information about the authenticated key. Compared to the other two stages, Stage 2 is more vulnerable, since, during Stage 1, Alice does not know the legitimacy of its counterpart. In this case, Eve impersonates Bob and may steal the authenticated key from the tagged signal of Alice. To solve this problem, the authors in [26] proposed a mutual authentication approach by sharing two distinguished keys, K_A and K_B, between Alice and Bob. However, the keys of Alice and Bob generated by the secret key generation scheme are identical in our scheme, which means that the mutual authentication approach cannot be applied directly. To solve this problem in our scheme, after Alice has been authenticated by Bob, they drop the authenticated key. When Alice authenticates Bob, they choose new authenticated key from the remaining shared key. If Bob cannot provide a valid tagged signal, Alice would consider that this “Bob” is impersonated. Thus, Eve cannot actively steal the shared key and pass the authentication under impersonation attacks.

4.2.2. Jamming Attacks. As discussed in [35], Eve can attempt to disrupt the authentication procedure by jamming attacks. When she performs jamming in Stage 2, it may make Bob unable to authenticate Alice, which means the denial of service. However, the frequent jamming in Stage 2 is apt to be detectable. When Eve jams Stages 1 and 3, the jamming signal may be viewed as interference, and, if the jamming signal is not AWGN-like, it can be suppressed through conventional interference rejection techniques.

4.2.3. Replay Attacks. In Stages 2 and 3, Eve’s received signals in the noiseless setting are, respectively, given by

$$r_{eb,i} = h_{BE,i}s_{b,i} = \left|h_{BE,i}\right| \exp\left(j\theta_{hBE,i} + j\theta_{b,i}\right), \tag{29}$$

$$\begin{aligned} r_{ea,i} &= h_{AE,i}s_{a,i} \\ &= \left|h_{AE,i}\right| \exp\left(j\left(\theta_{hAE,i} + \mathscr{M}\left(k_{a,i}^{\mathscr{M}}\right) - \widehat{\theta}_{a,i}\right)\right), \end{aligned} \tag{30}$$

where $h_{BE,i} = |h_{BE,i}|e^{j\theta_{hBE,i}}$ and $h_{AE,i} = |h_{AE,i}|e^{j\theta_{hAE,i}}$ are the ith subchannel from Bob to Eve and Alice to Eve, respectively. In a signal replay attack, Eve can store the waveforms as shown in (29) and (30) and simply replay the waveforms (since the signal in Step 1 contains no information about the shared key, we ignore Eve’s replay of this signal). If the waveform in (29) is replayed, Alice will send the tagged signal since Alice does not know the legitimacy of its counterpart. Then Eve can get the authenticated key from the tagged signal. This case is similar to the impersonation attack in which Bob is impersonated by Eve, so we can employ the mutual authentication approach to address this problem. If the waveform in (30) is replayed, since the channel-phase response between two legitimate users is unique and cannot be revealed to Eve, the signal received by Bob will be

$$\begin{aligned} r_{b,i}^{e} &= h_{EB,i}r_{ea,i} = \left|h_{EB,i}h_{AE,i}\right| \\ &\quad \cdot \exp\left(j\left(\theta_{hEB,i} + \theta_{hAE,i} + \mathscr{M}\left(k_{a,i}^{\mathscr{M}}\right) - \widehat{\theta}_{a,i}\right)\right). \end{aligned} \tag{31}$$

It is obvious that Bob will not accept it.

From the analysis above, we can find that, under various active attacks, it is nearly impossible for Eve to obtain the authenticated secret key or be authenticated by Alice or Bob.

4.3. Performance Evaluation. In this subsection, we present extensive simulations to demonstrate the effectiveness of the proposed scheme.

In the simulations, assuming that the receiver achieves ideal synchronization, so that the response message and tagged message contain only one OFDM symbol, respectively. The carrier frequency of the OFDM system is 2.4 GHz. The propagation environment is simulated by Rayleigh fading with 2 us constant delay time and the maximum Doppler frequency is 10 Hz. The sample interval is 0.25 us. The length of the mapping function input bits is set to be 2, so $2N$ key bits are needed for the simulations.

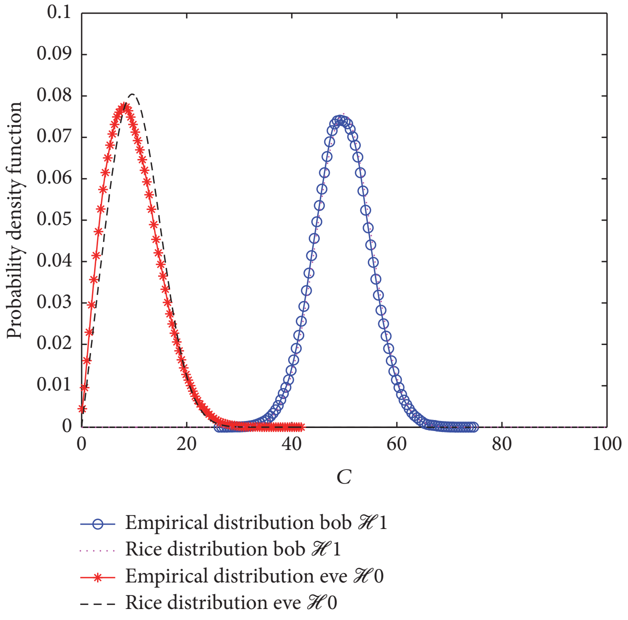


FIGURE 8: PDFs of $C_{\mathscr{H}0}$ and $C_{\mathscr{H}1}$ at SNR = 5 dB for $N = 64$.

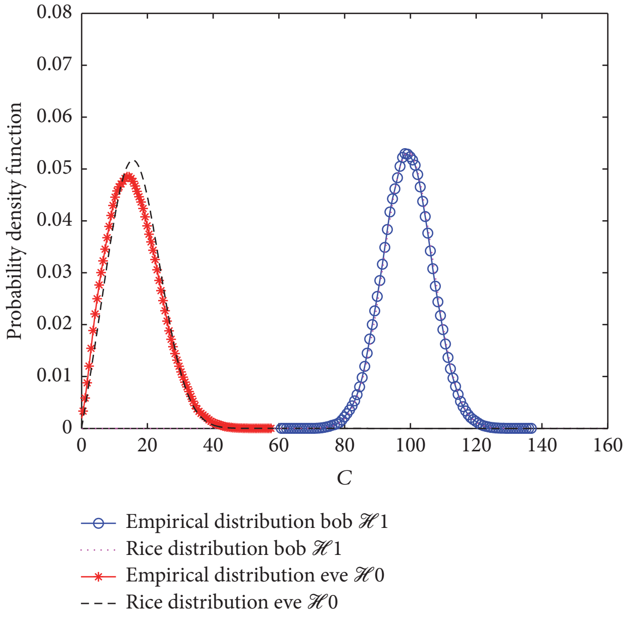
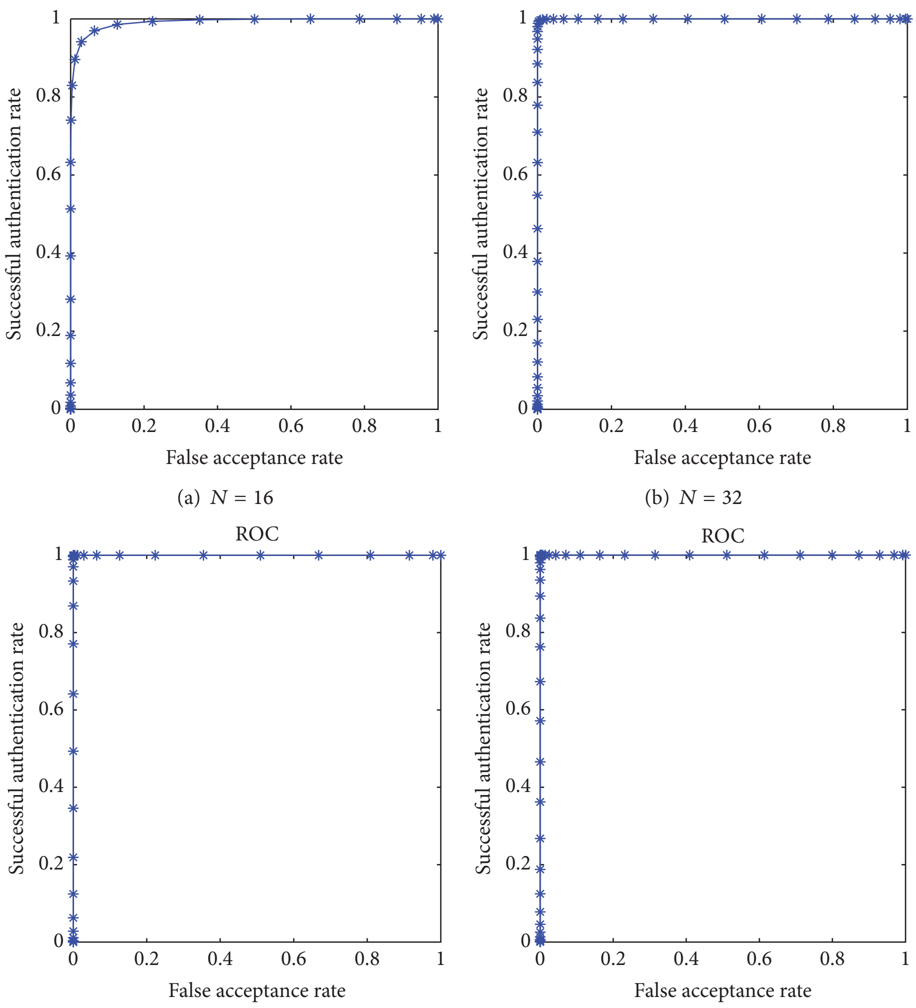


FIGURE 9: PDFs of $C_{\mathscr{H}0}$ and $C_{\mathscr{H}1}$ at SNR = 5 dB for $N = 128$.

Extensive Monte-Carlo simulations are conducted to investigate the PDFs of C under two hypothesis $\mathscr{H}0$ and $\mathscr{H}1$, which can be utilized to evaluate false acceptance rate and successful authentication rate. Furthermore, the appropriate choice of the threshold T also can be determined by these PDFs.

Figures 8 and 9 show the empirical PDFs of $C_{\mathscr{H}0}$ and $C_{\mathscr{H}1}$ at SNR = 5 dB for $N = 64$ and $N = 128$, respectively. As claimed in Section 4.1, $C_{\mathscr{H}0}$ and $C_{\mathscr{H}1}$ obey Rice distribution. Hence, Rice distributions according to (26) are also given in both figures, where the mean and variance are directly



(a) $N = 16$

(b) $N = 32$

(c) $N = 64$

(d) $N = 128$

Figure 10: Successful authentication rate versus false acceptance rate for different N when SNR = 5 dB.

estimated through Monte-Carlo simulations [36]. From these two figures, we can find that the empirical distributions are coincided well with the theoretical Rice distributions. We also note that the PDFs of $C_{\mathscr{H}0}$ and $C_{\mathscr{H}1}$ are distinguished clearly in Figure 8 and in Figure 9 and the PDF of $C_{\mathscr{H}1}$ is far apart from that of $C_{\mathscr{H}0}$ even at SNR = 5 dB. Thus, it is easy to calculate threshold T if the successful authentication rate and false acceptance rate are given.

The receiver operating characteristic (ROC) describes the correlation between the false acceptance rate and the successful authentication rate. Figure 10 plots the ROC performance for different N when SNR = 5 dB. From these four subfigures, we can find that the ROC performance becomes better as N increases. Furthermore, when $N = 32$, the ROC are nearly ideal even at SNR = 5 dB.

4.4. Comparison with PHY-CRAM and PHY-PCRAS. The PHY-layer authentication schemes PHY-CRAM [26] and PHY-PCRAS [27] were shown to be simple and feasible. In the following, we will compare our proposed scheme with these two schemes.

As illustrated in Figure 11, for ROC performance, our scheme is better than PHY-CRAM and very similar to PHY-PCRAS. The reason is that our proposed scheme and PHY-PCRAS employ the channel-phase response, while amplitude modulation is employed in PHY-CRAM, which in performance is usually worse than phase modulation. Since the amplitude of all the subcarriers are not the same, the received performance may be impacted due to different SNR at each subchannel. Furthermore, in PHY-CRAM, high-peak fluctuations may occur, and in practice it is required to suppress the high peak with additional complexity. However, since OFDM technique is employed, compared to PHY-CRAM, our proposed scheme and PHY-PCRAS are more sensitive to the frequency offset.

As discussed in [26, 27], for impersonation attacks, our proposed scheme and PHY-PCRAS are more secure than PHY-CRAM. This can be explained by the better ROC performance and the fact that the channel-phase response

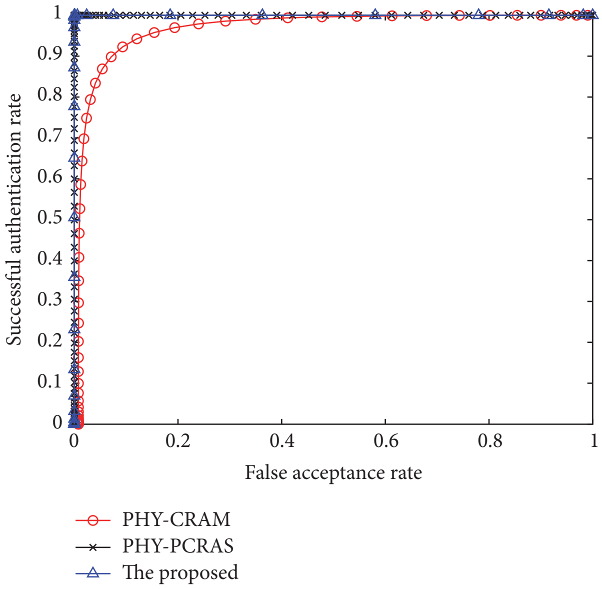


Figure 11: The ROC performance comparisons of the proposed authentication scheme, PHY-CRAM, and PHY-PCRAS at SNR = 5 dB with $N = 64$.

is more sensitive than channel-amplitude response to the distance between Alice and Bob.

The shared key of our proposed scheme is obtained from the proposed secret key generation scheme, while the other two schemes suppose that the shared key is preknown.

5. Conclusion

In this paper, to simplify the secret key extracting procedure based on the characteristics of the wireless channels and reduce the secret key bits mismatched rate, we propose a secret key generation scheme based on the channel-phase response. In the scheme, only one node is chosen to probe the channel and perform the quantization phase. Then the preliminary key is distributed after mapping and before equalizing. Further a PHY-layer authentication scheme is proposed utilizing the extracted secret key. This scheme exploits the short-term reciprocity of the channel-phase response and the sensitivity to the distance between the legitimate parties. The simulation results reveal that the proposed secret key generation scheme achieves a better performance compared to the existing scheme in terms of KGR, BMR, and secret key capacity. Besides, the extracted key passes the NIST randomness test. For the PHY-layer authentication scheme, the numerical results show that it performs better than existing work even at SNR = 5 dB when the shared key is obtained from the proposed secret key generation scheme, ensuring the randomness and security.

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 (Grants nos. 61601482, 61601516, 61601480, and 61502518) and sponsored by the Foundation of Science and Technology on Information Transmission and Dissemination in Comm. Networks Lab, National Key Laboratory of Anti-Jamming Communication Technology.

References

[1] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, 2012.

[2] W. Li, Y. Tang, M. Ghogho, J. Wei, and C. Xiong, "Secure communications via sending artificial noise by both transmitter and receiver: optimum power allocation to minimise the insecure region," *IET Communications*, vol. 8, no. 16, pp. 2858–2862, 2014.

[3] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE. Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[4] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE. Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[5] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 4, pp. 207–212, 1996.

[6] 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 Annual International Conference on Mobile Computing and Networking (MobiCom '08)*, pp. 128–139, San Francisco, Calif, USA, September 2008.

[7] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '09)*, pp. 321–332, Beijing, China, September 2009.

[8] X. Hu, X. Li, E. C.-H. Ngai, V. C. M. Leung, and P. Kruchten, "Multidimensional context-aware social network architecture for mobile crowdsensing," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 78–87, 2014.

[9] X. Hu, J. Zhao, B.-C. Seet, V. C. M. Leung, T. H. S. Chu, and H. Chan, "S-aframe: agent-based multilayer framework with context-aware semantic service for vehicular social networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 1, pp. 44–63, 2015.

[10] L. Cheng, W. Li, D. Ma, J. Wei, and X. Liu, "Moving window scheme for extracting secret keys in stationary environments," *IET Communications*, vol. 10, no. 16, pp. 2206–2214, 2016.

[11] L. Cheng, W. Li, L. Zhou, C. Zhu, J. Wei, and Y. Guo, "Increasing secret key capacity of OFDM systems: a geometric program approach," *Concurrency and Computation: Practice and Experience*, 2016.

[12] L. Zhou, Z. Sheng, L. Wei et al., "Green cell planning and deployment for small cell networks in smart cities," *Ad Hoc Networks*, vol. 43, pp. 30–42, 2016.

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

[14] E. Zhang, P. Yuan, and J. Du, "Verifiable rational secret sharing scheme in mobile networks," *Mobile Information Systems*, vol. 2015, Article ID 462345, 7 pages, 2015.

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

[16] X. Hu, T. H. S. Chu, V. C. M. Leung, E. C.-H. Ngai, P. Kruchten, and H. C. B. Chan, "A survey on mobile social networks: applications, platforms, system architectures, and future research directions," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1557–1581, 2014.

[17] L. Zhou, X. Hu, E. C.-H. Ngai et al., "A dynamic graph-based scheduling and interference coordination approach in heterogeneous cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 3735–3748, 2016.

[18] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proceedings of the 32nd IEEE Conference on Computer Communications (INFOCOM '13)*, pp. 3048–3056, April 2013.

[19] X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, "A secret key generation method based on CSI in OFDM-FDD system," in *Proceedings of the IEEE Globecom Workshops (GC Wkshps '13)*, pp. 1297–1302, December 2013.

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

[21] 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.

[22] X. Hu, T. H. S. Chu, H. C. B. Chan, and V. C. M. Leung, "Vita: a crowdsensing-oriented mobile cyber-physical system," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 148–165, 2013.

[23] A. Ferrante, N. Laurenti, C. Masiero, M. Pavon, and S. Tomasin, "On the error region for channel estimation-based physical layer authentication over rayleigh fading," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 941–952, 2015.

[24] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2010.

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

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

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

[28] W. C. Jakes Jr., *Microwave Mobile Communications*, Wiley-IEEE Press, Piscataway, NJ, USA, 1994.

[29] X. Du, D. Shan, K. Zeng, and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *Proceedings of the 33rd IEEE Conference on Computer Communications (INFOCOM '14)*, pp. 1276–1284, IEEE, Ontario, Canada, May 2014.

[30] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: secret sharing using reciprocity in ultrawideband channels," in *Proceedings of the IEEE International Conference on Ultra-Wideband (ICUWB '07)*, pp. 270–275, September 2007.

[31] Q. Dai, H. Song, L. Jin, and K. Huang, "Physical layer authentication and secret key distribution mechanism based on euivalent channel," *Science China*, vol. 44, no. 12, pp. 1580–1592, 2014.

[32] Z. Szabó, "Information theoretical estimators toolbox," *Journal of Machine Learning Research*, vol. 15, pp. 283–287, 2014.

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

[34] A. Rukhin, J. Sota, J. Nechvatal et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Special Publication NIST 800-22, National Institute of Standards and Technology, 2010.

[35] X. Wu, Z. Yang, C. Ling, and X. G. Xia, "A Physical-Layer Authentication Assisted Scheme for Enhancing 3GPP Authentication," 2015, http://arxiv.org/abs/1502.07565v1.

[36] T. R. Benedict and T. T. Soong, "The joint estimation of signal and noise from the sum envelope," *IEEE Transactions on Information Theory*, vol. 13, no. 3, pp. 447–454, 1967.

Hindawi

Submit your manuscripts at
https://www.hindawi.com

Advances in Multimedia
The Scientific World Journal
International Journal of Distributed Sensor Networks
Journal of Industrial Engineering
Applied Computational Intelligence and Soft Computing
Advances in Fuzzy Systems
Modelling & Simulation in Engineering
Journal of Computer Networks and Communications
Advances in Artificial Intelligence
Advances in Computer Engineering
International Journal of Computer Games Technology
International Journal of Biomedical Imaging
Advances in Artificial Neural Systems
Advances in Software Engineering
Journal of Robotics
Advances in Human-Computer Interaction
Computational Intelligence and Neuroscience
International Journal of Reconfigurable Computing
Journal of Electrical and Computer Engineering