Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6642605, 17 pages
https://doi.org/10.1155/2021/6642605

Research Article

A Lightweight Key Generation Scheme for Secure Device-to-Device (D2D) Communication

Chunwei Lou,[1] Mingsheng Cao ,[2] Rongchun Wu,[3] Dajiang Chen,[2,4] and Hua Xu[5]

[1]*University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China*
[2]*Network and Data Security Key Laboratory of Sichuan Province, UESTC, Chengdu, China*
[3]*Officers College of PAP, Chengdu, China*
[4]*Peng Cheng Laboratory, Shenzhen 518055, China*
[5]*School of Physics and Electronic Engineering, Yancheng Teachers University, Yancheng 224007, China*

Correspondence should be addressed to Mingsheng Cao; cms@uestc.edu.cn

Received 26 December 2020; Revised 24 January 2021; Accepted 8 February 2021; Published 9 March 2021

Academic Editor: Weizhi Meng

Key agreement is one the most essential steps when applying cryptographic techniques to secure device-to-device (D2D) communications. Recently, several PHY-based solutions have been proposed by leveraging the channel gains as a common randomness source for key extraction in wireless networks. However, these schemes usually suffer a low rate of key generation and low entropy of generated key and rely on the mobility of devices. In this paper, a novel secret key extraction protocol is proposed by using interference in wireless D2D fading channel. It establishes symmetrical keys for two wireless devices by measuring channel gains and utilizing artificial jamming sent by the third party to change the measured value of channel gains. We give a theoretically reachable key rate of the proposed scheme from the viewpoint of the information theory. It shows that the proposed scheme can make hundred times performance gain than the existing approaches theoretically. Experimental results also demonstrate that the proposed scheme can achieve a secure key distribution with a higher key rate and key entropy compared with the existing schemes.

1. Introduction

Because of the broadcast and open-air nature of a wireless channel, device-to-device (D2D) communications [1, 2] are vulnerable to message eavesdropping and node impersonation [3–6]. To resist these attacks, an effective method is to encrypt sensitive data with secret session keys and send encrypted data via wireless channels. However, it is necessary to agree on a common secret session key between two communicating parties beforehand. Most of traditional protocols (e.g., Diffie-Hellman method [7]) rely on the computing capability of adversary, which have high computational complexity. Since a lot of wireless devices (e.g., miniature sensors) have limited computing ability, the existing cryptographic methods need to overcome the contradictions between high computational complexity and limited computing ability [8].

Some popular research works leverage the channel randomness between two wireless devices. Many theoretical results (e.g., [9, 10]) show that multiple legitimate nodes can agree on a key unknown to an eavesdropper due to the high overhead of random coding. Recently, several radio channel features (i.e., temporal variations, spatial variations, and reciprocity of radio wave propagation) have been utilized for key extraction in wireless networks [11–13].

However, existing approaches still suffer from reliance on mobile environments, low key generation rate and key entropy [14]. To address these problems, a number of solutions have been proposed [15–19]. In [15], *iJam* is proposed to increase the channel change rate. Unfortunately, it decreases the throughout due to the retransmission-based self-protection procedure in the scheme. A key extraction scheme is proposed by exploiting multiantenna diversity [16]. However, it leads to an increase in the complexity of the transceivers. In [17], a key generation scheme is designed by using the randomness of channel phase. In [18], a secret key extraction protocol is proposed by leveraging the received signal strength (RSS). In [19], a secure key distribution scheme with artificial interference is designed. However, due to the inefficient bit extraction method and the low efficiency of artificial jamming, the key generation rate of the protocol is relatively low.

In this paper, a new secure key distribution approach is designed for key extraction in D2D communications. In our scenarios, a symmetrical key is aimed to be generated between two devices named Alice and Carol (Alice and Carol are called keying nodes) in the presence of an eavesdropper Eve. We also assume that there exists an assistance device Bob. The main contributions of the works are as follows:

(1) A new key generation scheme is designed for D2D communication by leveraging the artificial jamming to change the channel gains. Unlike existing approaches [8, 11], in the proposed scheme, the legitimate users can obtain multiple different channel measurements in each coherence time

(2) A new bit extraction method is proposed to improve the key generation rate and key entropy, which includes low entropy measurement elimination, random permutation, and adaptive multiple-bit extraction

(3) Extensive experiments are conducted to evaluate the performance of the proposed scheme with both theoretical analysis and simulation. Experimental results show that the proposed scheme can achieve a higher key generation rate and key entropy compared with existing schemes.

The reminder of this paper is organized as follows. Section 2 reviews the related work. In Section 3, the details of the proposed scheme and the theoretical analysis are presented. Section 4 details the experimental results and discussions. We finally conclude this work in Section 5.

2. The Literature Reviews

Recently, leveraging artificial jamming to improve the security of a wireless networking has drawn increasing attention [20–27]. In [20], Liu et al. proposed a secure communication scheme in a distributed relay networks, in which the destination transmits jamming signals to confuse the eavesdropper at first hop and the source and a particular relay jam eavesdropper cooperatively without jamming the destination at second hop. In [21], a two-stage cooperative scheme for secure communication with multiple helpers has been proposed. After that, Zheng et al. considered the secure communication scenario that the destination is with two antennas and only a single antenna is equipped in eavesdropper [22]. In this work, one antenna of destination receives the signals, and the other one transmits jamming to confuse the adversary. However, it requires a FD receiver and cannot guarantee the security when the adversary has multiple antennas. In [23], Li et al. studied the optimization problem for secrecy rate in a relay wiretap channel network, where the multiple multiantenna nodes act as the relaying nodes as well as the artificial jamming generation nodes. However, in a direct source-to-eavesdropper link case, it may be difficult to achieve a positive secrecy rate. In [24], an opportunistic relay-based secure communication scheme has been proposed to improve the secrecy rate for a relay network with two-hop. Specifically, a node (named opportunistic relay node) is used to forward the confidential signals and another node (named the jamming nodes) sends jamming signals to confuse the adversary. The multiantenna secure transmission by using beam-forming techniques to confuse multiple antenna eavesdroppers with limited feedback constraints has been studied in [25, 26]. However, these works only focused on optimizing the secrecy rate theoretically and could not be directly applied for secret key distribution in practice. For more information about improving secrecy rate with friendly jamming, please refer to the survey in [27]. The related work about jamming attack also includes [28].

Key generation with artificial interference has been analyzed in [19]. Different from [19], this paper has the following advantages: (1) The theoretical results about key rate are different. The lower bound of key rate in [19] is $(1/2T_c)[\ln\sqrt{b} + 3\ln 2\pi e - e^{-1}]$, while, in this paper, a lower bound of key rate is $(1/2T_c)[\ln(\pi(eb)^2) - e^{-1}]$. Thus, the new bound is at least L times over the bound in [19], where $L = \lfloor T_c f_s / 2M^* \rfloor$ is the number of rounds in the coherence time T_c, M is the length of probe vector for each measurement value, f_s is the sampling rate, and b^2 is the average power at keying node Alice and helper node Bob. In other words, the proposed scheme can measure L channel state information measurements for a secure key extraction in each coherence time. (2) The bit quantization method is different. Two-level bit quantization scheme is adopted in [19], while this paper presents an adaptive multiple-level bit extraction scheme. Moreover, the simulation results show that a larger jamming power may contribute to more bits extracted from each measurement (please refer to Section 4). (3) The approach to increasing the key bit entropy is different. In [19], there is no any added method to pretreat the measurements before bit quantization, while this paper proposed a low entropy measurement elimination algorithm and random permutation algorithm to eliminate the low entropy measurements and to increase the randomness of measurements, respectively.

3. The Proposed Solution

In this section, the network model and adversary model are first described. Then, we describe the proposed scheme. A random variable (RV) and its realization are denoted by an uppercase letter (e.g., X and Y) and a lowercase letter (e.g., x and y), respectively; a random vector is denoted by an hollow bold uppercase letter (e.g., $\mathbb{X}$ and $\mathbb{Y}$). Let H_{ij} be a RV of channel gains between device i and device j, T_c be the *coherence time* (i.e., the time interval over which the channel gain may be considered coherent), f_s be the sampling rate, M be the sample number by fully exploiting the coherence time interval, and M^* be the length of probe vector for each measurement at Alice and Carol.

In the system model, two devices, Alice and Carol, are aimed at building a common secret key for secure D2D communication by measuring the channel gains from the channel between them, and a trusted third party Bob (helper), who changes the state channel information of channel between Alice and Carol by broadcasting jamming signals. Alice and Carol can reconcile their measurements by sending some error-correcting information through a public channel, and a secure channel exists between Alice and Bob. Of course, there is an eavesdropper Eve who plans to break the secret key.

3.1. The Proposed Key Generation Protocol. The artificial-jamming-based secret key extraction consists of five components: (1) collection of random source, (2) low entropy measurements elimination, (3) random permutation, (4) adaptive multiple-bit extraction, and (5) information reconciliation and privacy amplification.

3.1.1. Collection of Random Source. Let Λ be a Gaussian distribution with mean of 0 and variance of b^2 and M^* be the probe vector length of measurement. The time is divided into slots $t_1, t_2, \cdots$.

Step (1) In t_1, Alice and Bob random choose $\lambda_A[1]$ and $\lambda_B[1]$ from $\Lambda \sim \mathbf{G}(0, b^2)$, respectively. Then, Alice transmits probe signals $\lambda_A[1]\vec{s}_A$ with length $|\vec{s}_A| = M^*$ to Carol, and Bob broadcasts jamming signals $\lambda_B[1]\vec{s}_B$ with length $|\vec{s}_B| = M^*$ simultaneously. The signal received by Carol is $\vec{y}_C[1] = \lambda_A[1]h_{AC}[1]\vec{s}_A + \lambda_B[1]h_{BC}[1]\vec{s}_B + \vec{n}_C[1]$, where $\vec{n}_C$ is the noise vector at Carol, and $\vec{s}_A$ and $\vec{s}_B$ are the known probe signals. In t_2, Carol transmits probe signals $\vec{s}_C$ with length $|\vec{s}_C|$ to Alice. The signals received by Alice and Bob are $\vec{y}_A[1] = h_{AC}[1]\vec{s}_C + \vec{n}_A[1]$ and $\vec{y}_B[1] = h_{BC}\vec{s}_C[1] + \vec{n}_B[1]$, respectively, where $\vec{s}_A = \vec{s}_B = \vec{s}_C = \vec{s}$.

Step (2) Repeat Step (1) N times. Then, Alice, Bob, and Carol have the N vectors as follows:

$$\vec{y}_A[i] = h_{AC}[i]\vec{s}_C + \vec{n}_A[i], \tag{1}$$

$$\vec{y}_B[i] = h_{BC}[i]\vec{s}_C + \vec{n}_B[i], \tag{2}$$

$$\vec{y}_C[i] = \lambda_A[i]h_{AC}[i]\,\vec{s}_A + \lambda_B[i]h_{BC}[i]\vec{s}_B + \vec{n}_C[i] \tag{3}$$

Step (3) Bob estimates $h_{BC}[i]$ by using the following equation:

$$\vec{h}_{BC}[i] \triangleq \vec{y}_B[i]\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} = h_{BC}[i] + \vec{n}_B[i]\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} \tag{4}$$

Step (4) Bob sends $\vec{h}_{BC}[i]$ and $\lambda_B[i]$ to Alice over the secure channel between them.

Step (5) Alice first computes

$$\begin{aligned}\widetilde{\vec{y}}_A[i] &\triangleq \lambda_A[i]\vec{y}_A[i] + \lambda_B[i]\vec{h}_{BC}[i]\vec{s} \\ &= \left(\lambda_A[i]h_{AC}[i] + \lambda_B[i]\vec{h}_{BC}[i]\vec{s} + \lambda_A[i]\vec{n}_A[i]\right).\end{aligned} \tag{5}$$

Then, Alice obtains the following equality:

$$\widehat{y}_A[i] \triangleq \widetilde{\vec{y}}_A[i]\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} = \lambda_A[i]h_{AC}[i] + \lambda_B[i]\tilde{h}_{BC}[i] + \lambda_A[i]\vec{n}_A[i]\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} \tag{6}$$

Step (6) Carol computes

$$\widehat{y}_A[i] \triangleq \vec{y}_A[i]\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} = \lambda_A[i]h_{AC}[i] + \lambda_B[i]h_{BC}[i] + \vec{n}_C[i]\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} \tag{7}$$

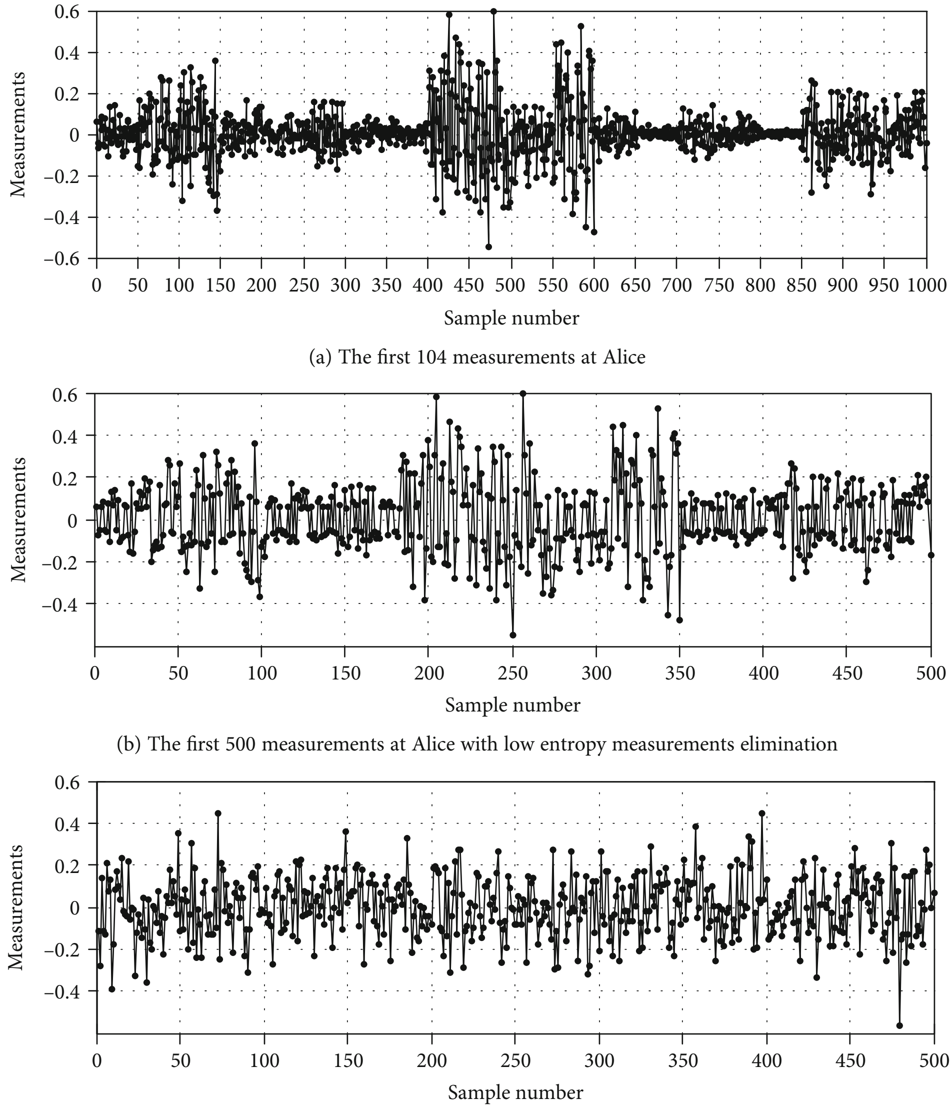
After the above steps, Alice and Carol have the N vectors $\overrightarrow{\widehat{y}_A} \triangleq <\{\widehat{y}_A[i]\}_{i=1}^{N}>$ and $\overrightarrow{\widehat{y}_C} \triangleq <\{\widehat{y}_C[i]\}_{i=1}^{N}>$, respectively.

3.1.2. Low Entropy Measurement Elimination. When the absolute values of h_{AC} and h_{BC} are small in a coherence time, the absolute values $\lambda_A h_{AC} + \lambda_B h_{BC}$ are also small. Thus, these measurements have low entropy during the coherence time. For example, Figure 1(a) plots the first 10^4 measurements at Alice, where there are 50 measurement values in each coherence time. We can see that the measurements with sample number between 800 and 850 have low entropy.

To obtain a high key entropy, we must eliminate the low entropy measurements. The elimination method is described as follows: Alice and Carol drop instances of their measurements if there are at least β successive measurements lied between $-\alpha$ and α. Then, they exchange index set of dropped measurements between them, and only keep the measurements that both two devices decide not to drop, where $\alpha \geq 0$ and $\beta \geq 0$ are the carefully chosen constants. We still denote the obtained vector after low entropy measurement elimination at Alice and Carol by $\langle\{\widehat{y}_A[i]\}_{i=1}^{N_1}\rangle$ and $\langle\{\widehat{y}_C[i]\}_{i=1}^{N_1}\rangle$, respectively.

Figure 1(b) shows the first two hundred measurements at Alice with low entropy measurement elimination.

3.1.3. Random Permutation. Since the values of channel gains are similar during each coherence time, the measurement values $\widehat{y}_A$ (and $\widehat{y}_C$) at Alice (and Carol) has a certain correlation in the coherence time (Figure 1(b)). In the proposed scheme, we break that correlation by using random permutation. In practical experiments, a simple algorithm Knuth shuffle [29] is applied to generate a permutation uniformly at random without retries, in the practical experiments. Specifically, after obtaining $\langle\{\widehat{y}_C[i]\}_{i=1}^{N_1}\rangle$, Alice runs the algorithm



(a) The first 104 measurements at Alice

(b) The first 500 measurements at Alice with low entropy measurements elimination

(c) The first 500 measurements at Alice with random permutation

Figure 1: Reprocessing of measurements before bit quantization.

Knuth shuffle to generate a permutation $g : \{1,\cdots,N1\} \rightarrow \{1,\cdots,N1\}$ and then transmits it to Carol. Finally, Alice and Carol compute $\vec{z}_A = \{\hat{y}_A[g(i)]\}_{i=1}^{N_1}$ and $\vec{z}_C = \{\hat{y}_C[g(i)]\}_{i=1}^{N_1}$, respectively.

For example, if $\overrightarrow{\hat{y}_A} = < -1, 0, 1 >$ and $g = [2, 1, 3]$, then $\vec{z}_A = <0, -1, 1>$. Figure 1(c) plots the measurements at Alice with random permutation.

3.1.4. Adaptive Multiple-Bit Extraction. In the implementation, we present *adaptive multiple-bit extraction scheme* (as shown in Figure 2) which is described as follows:

(1) Alice and Carol select a positive integer ω as the bit-number extracted for each channel measurement and choose two positive integers γ (named the valid zone width) and $\triangle\gamma$ (called the shield zone width)

(2) Let $\kappa = \gamma + \triangle\gamma$, where κ is called the block size. They divide $\vec{z}_A$ and $\vec{z}_C$ into small blocks with length κ, respectively

(3) For any block,

$$\vec{z}_\xi^{(i)} = <\vec{z}_\xi[(i-1)\kappa + 1], \cdots, \vec{z}_\xi[i\kappa]> \xi \in \{A, C\} \tag{8}$$

they (1) sort the elements of a sequence in ascending order; (2) for any $j \in \{1,\cdots,2^\omega\}$, map the rank from $(j-1)(\gamma + \triangle\gamma) + 1$ to $(j-1)(\gamma + \triangle\gamma) + \gamma$ elements (named level $j-1$) into $j-1$; (3) drop the remainder of channel measurements; and (4) exchange their dropped measurements list and keep the valid indices

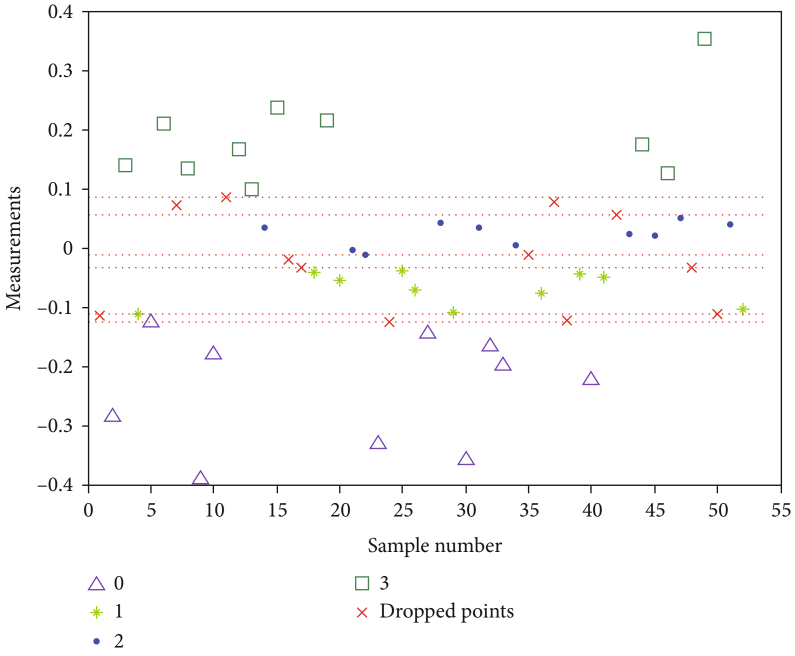


Figure 2: Adaptive multiple-bit extraction with $\omega = 2$, $\gamma = 10$, and $\Delta\gamma = 4$.

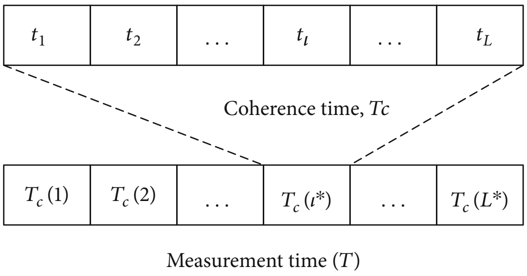


Figure 3: Time division, where **T** is the total measurement time (e.g., the sum of all of the probing time) and $T_c(l) = T_c(l = 1, \cdots, L^*)$.

(4) Alice and Carol obtain the corresponding bit streams by using the ω -bit Gary code $g : \{0, \cdots, 2^{\omega} - 1\} \rightarrow \{0, 1\}^{\omega}$, respectively. The bit streams after bit quantization is denoted as K_A^q and K_C^q

3.1.5. Information Reconciliation and Privacy Amplification. Because of the half-duplex beacon transmission and hardware variations, a small number of bit inconsistencies may exist between their bit streams. There are two ways to realize information reconciliation: interactive information reconciliation (IIR) scheme [30] or error-correcting codes (ECC) [31]. In the implementation, we use ECC-based information reconciliation (i.e., [127,85,13]-BCH code).

Moreover, as the reconciliation information is sent over a public and insecure channel, the adversary can leverage such information to obtain knowledge of the generated key. Privacy amplification protocols [32, 33] can be used to recover such entropy loss. In the proposed scheme, the keying hash function SHA_1 [32] is leveraged for privacy amplification.

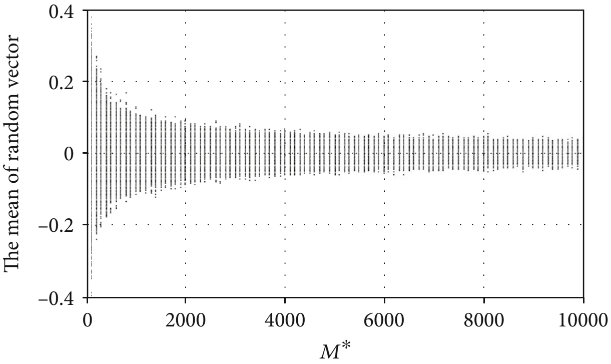


Figure 4: The mean of i.i.d. random variables $\mathbb{G}$ with standard normal distribution in 104 independent experiments under different length M^*.

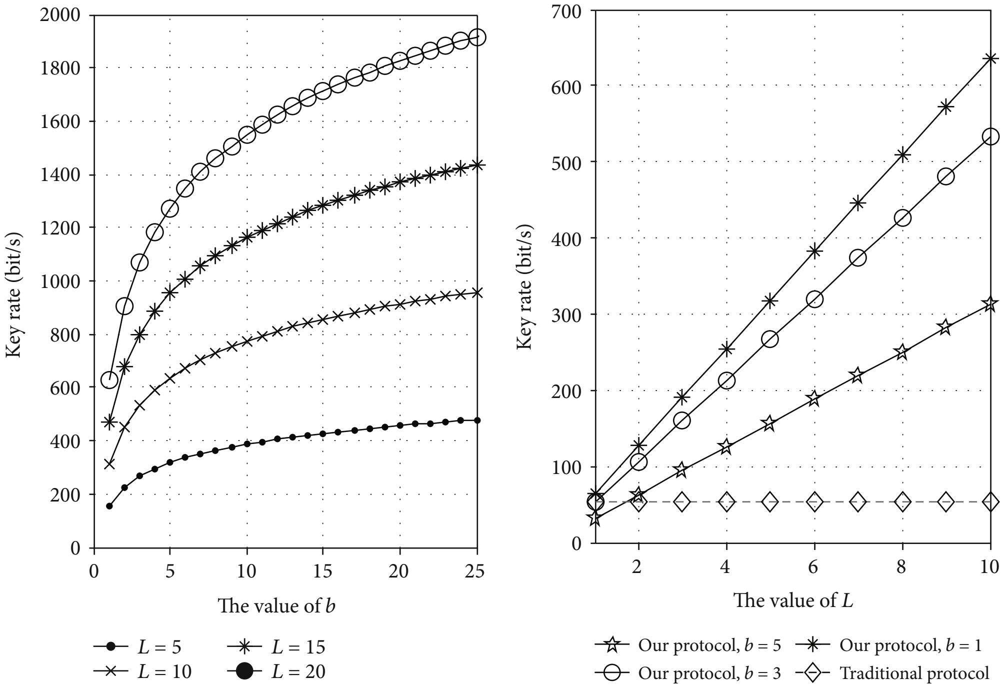
3.2. Theoretical Analysis

3.2.1. Theoretical Result. For mathematical simplicity, we denote the sample number M in T_c by

$$M = \lfloor f_s T_c \rfloor \; L = \left\lfloor \frac{M}{2M^*} \right\rfloor = \left\lfloor \frac{f_s T_c}{2M^*} \right\rfloor, \tag{9}$$

where L is the number of rounds in T_c and $\lfloor r \rfloor$ is the largest integer equal or less than to real number r.

Let **T** be the total measurement time (e.g., the sum of all of the probing time). As shown in Figure 3, we divide **T** as follows. First dividing **T** to L^* parts, where each part equals to coherence time T_c (i.e., $L^* = \lfloor \mathbf{T}/T_c \rfloor$). Then, splitting T_c into L parts: $t_1, \cdots, t_L$ equally. In time slot t_i, Alice, Bob, and Carol follow the first step of the presented protocol. All the RVs of obtained measurement values at Alice and Carol are



(a)

(b)

Figure 5: (a) The theoretical achievable key rate versus the upper bound b of Λ under different value of L. (b) The theoretical achievable key rate versus the upper bound b of Λ under different value of L.

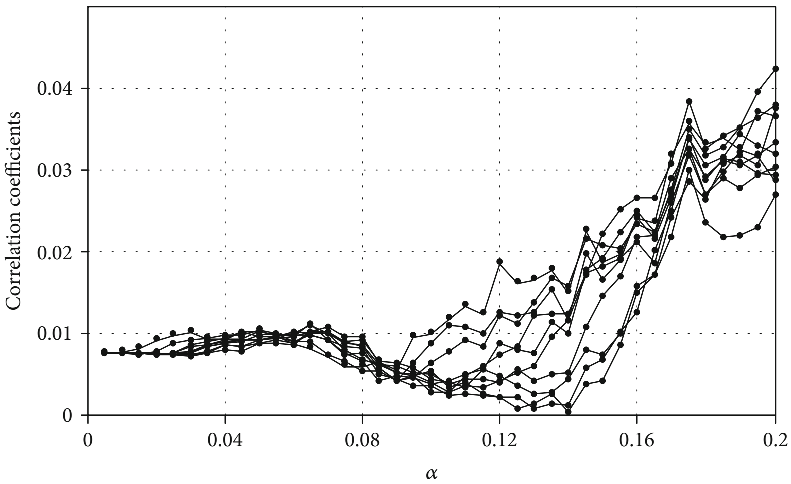


Figure 6: Correlation coefficients against α under different values of β, where $M^* = 2000$ and $b = 2$.

$$\widehat{Y}_A[i] \triangleq \Lambda_A[i]H_{AC} + \Lambda_B[i]\tilde{H}_{BC} + \Lambda_A[i]\mathbb{N}_A \frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2},$$
$$\widehat{Y}_C[i] \triangleq \Lambda_A[i]H_{AC} + \Lambda_B[i]H_{BC} + \mathbb{N}_C \frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2}, \tag{10}$$

where $i \in \{1, \cdots, L \times L^*\}$, $\tilde{H}_{BC} = H_{BC} + \mathbb{N}_B(\vec{s}^{\,T}/\|\vec{s}\|^2)$, $N_j(j \in \{A, B, C\})$ is the additive noise, and Nj is independent and identically distributed of random variable N_j $(j \in \{A, B, C\})$. In addition, the random vector of received signals at Eve are

$$\mathbb{Y}_{E\longleftarrow AB}[i] \triangleq \Lambda_A[i]H_{AE}\vec{s} + \Lambda_B[i]H_{BE}\vec{s} + \mathbb{N}_E,$$
$$\mathbb{Y}_{E\longleftarrow C}[i] \triangleq H_{CE}\vec{s} + \mathbb{N}_E, \tag{11}$$

where $i \in \{1,\cdots,L \times L^*\}$, $\mathbb{N}_E$ the additive noise vector.

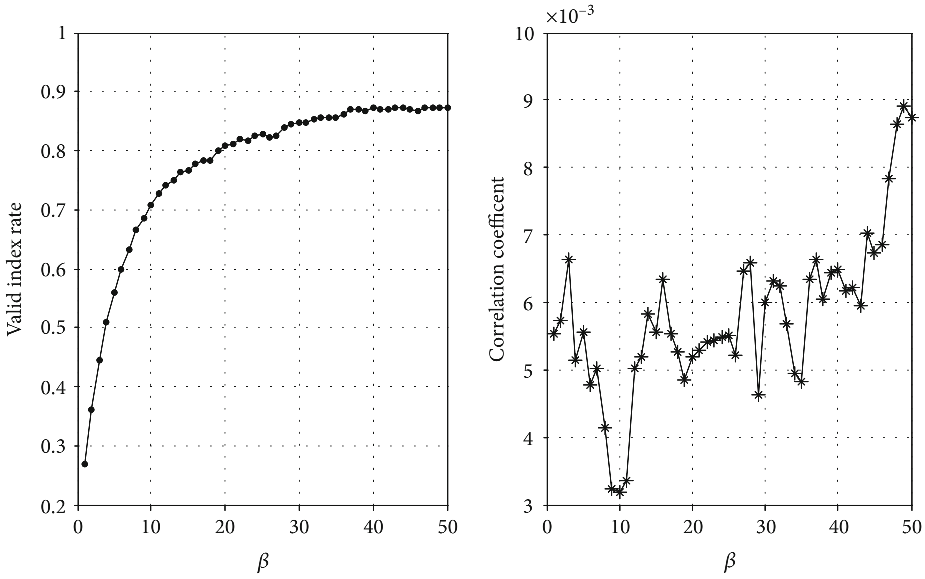


Figure 7: Valid index rate and correlation coefficients against β, where where SNR = 0 dB, $M^* = 2000$, $b = 2$, and $\alpha = 0.09$.

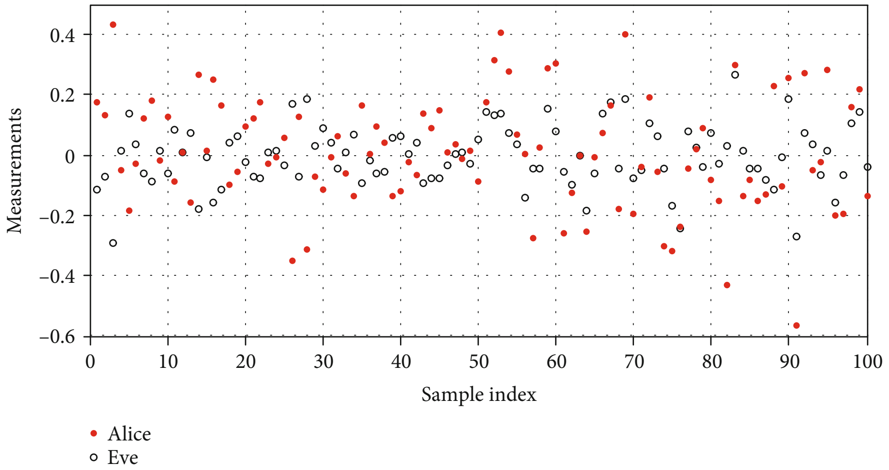


Figure 8: Measurements at Alice and Eve, where SNR = 0 dB, $M^* = 2000$, and $b = 2$.

After obtaining $\mathbb{Y}_{E\leftarrow AB}[i]$ and $\mathbb{Y}_{E\leftarrow C}[i]$, the optimal strategy of Eve is to compute

$$\widehat{Y}_{AE}[i] \triangleq \mathbb{Y}_{E\longleftarrow AB}[i]\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} = \Lambda_A[i]H_{AE} + \Lambda_B[i]H_{BE} + \mathbb{N}_C\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2},$$

$$\widehat{Y}_{CE}[i] \triangleq \mathbb{Y}_{E\longleftarrow C}[i]\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} = H_{CE} + \mathbb{N}_E\frac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2}, \tag{12}$$

where $i \in \{1,\cdots,L\times L^*\}$.

Based on the measurements at Alice, Carol, and Eve, the theorem is shown as follows.

Theorem 1. *Let $\delta_{AC}^2 = \delta_{BC}^2 = 1$. If the gains of channel between two devices is i.i.d. across coherence periods and the number of sampling M^* in $t_i (i = 1, 2,\cdots,N)$ is large enough, then the maximum key generation rate R_M of the presented protocol can be bounded by*

$$R_M \geq \frac{L}{2T_C}\left[\ln\left(\pi(eb)^2\right) - e^{-1}\right], \tag{13}$$

where T_c is the coherence time, M^* is the length of probe signals for each measurement value, f_s is the sampling rate, $L = \lfloor T_c f_s/2M^*\rfloor$ is the number of rounds in T_c, and b^2 is the average power at Alice and Bob.

Proof. Please refer to the Appendix.

3.2.2. Numerical Analysis. The impact of the parameter M^* on the key rate of the proposed scheme is first discussed. On the one hand, the larger the value of M^* means the more accurate measurement, the more accurate measurement represents the less information loss in information reconcile and hence the higher key rate. An experiment is conducted in MATLAB as follows. We generate a random vector $\mathbb{G} = \{G_i\}_{i=1}^{M^*}$ by using a random number generator with zero mean and variance 1. That is, $\mathbb{G}$ is the i.i.d. variable obeying standard normal distribution $\mathbf{G}(0, 1)$. Figure 4 plots the statistical average value of $\mathbb{G}$ in 10^4 independent experiments under different values of M^* (i.e., the length of $\mathbb{G}$). On the other hand, the smaller the value of M^* is, the more the number L of measurements of coherence time will be, yet the higher key rate.

Then, we discuss the impact of the value of b on the key rate. From Theorem 1, the key generation rate rises when the value of b increases. Furthermore, the key rate converges to infinite when b goes to infinite. As an example, for the parameters $T_c = 50$ ms, Figure 5(a) plots the achievable key rate when b increases under different values of L. Note that the jamming power of helper Bob is denoted by $P_I = b^2$. Thus, the key generation rate rises when the jamming P_I increases, and the key rate converges to infinite when P_I goes to infinite. However, due to the logarithmic relationship between the achievable key rate and the value of b, the key rate growth is slow with the value of b increase. It can also be obtained from Figure 5(a).

Lastly, we compared the proposed scheme with traditional schemes. By [34], the maximum key generation rate of traditional methods is $(1/T_c)\mathscr{H}(H_{AC}) = (1/2T_c) \ln (2\pi e \delta_{AC}^2)$. Take $T_c = 50$ ms, $f_s = 4$ GHz, $10^4 \leq M^* \leq 10^5$, and $\delta_{AC} = \delta_{BC} = 1$. Figure 5(b) plots the performance of traditional methods versus the proposed scheme. Moreover, if we fixed M^* and f_s, then, from $L = \lfloor T_c f_s / 2M^* \rfloor$, we have L is proportional to T_c. Specially, if we take $T_c = 200$ (the coherence time T_c can be up to 100-500 ms in static environment), $f_s = 4$ GHz (the sampling frequency of off-shelf-802.11 can achieve 20GHz) and $M^* = 10^4$, then $L = 100$. That is to say, the key generation rate of the proposed scheme is at least 100× better than that of traditional methods.

4. Experimental Results and Discussions

4.1. Experiment Setting. In the random source collection phase, it is assumed that both the artificial jamming and probes are *single-tone signals*. The probe signals are $s(\tau) = a_0 \cos (\omega_0 \tau + \theta_0)$ $(\tau \in [0, T])$, where a_0 is the amplitude, θ_0 is the initial phase, and ω_0 is the angular frequency. Specifically, the probing signals are based on λ_A (or λ_B) at jamming slots (i.e., Alice sends $\lambda_A s(\tau)$ and Bob sends $\lambda_B s(\tau), \tau \in [0, T]$, at time slot t_1). It is also assumed that the coherence time is $T_c = 80$ ms, the sampling rate is $f_s = 2.7$ GHz, and the single-tone signal's carrier frequency is 0.9 GHz.

In the information reconciliation phase, we assume that [127,85,13]-BCH code is used in our system. It is clear that the error tolerance of the code is $ET =^{\Delta} (6/127) \approx 0.047$ (i.e., *error threshold*). Specifically, Alice (resp., Carol) divides the quantized bits K_A^q (resp. K_C^q) into small blocks $K_A^q(1), \cdots, K_A^q(i), \cdots$ (resp. $K_C^q(1), \cdots, K_C^q(i), \cdots$) with block length 127, respectively. For each block $K_A^q(i)$ $(i = 1, 2, \cdots)$, Alice randomly chooses a codeword C_i from [127,85,13]-BCH codebook and sends $K_A^q \oplus C_i$ to Carol. After receiving $K_A^q(i) \oplus C_i$, Carol computes $C_i^* \triangleq K_C^q \oplus K_A^q \oplus C_i$ (note that the position of "1" in bits $K_C^q \oplus K_A^q$ means the mismatch between Alice and Carol happens in corresponding position). Thus, if the number of "1" in $K_C^q \oplus K_A^q$ is less than 6, Carol can obtain C_i from C_i^* with error-correcting code technical, and then, compute $K_A^q(i)$ by computing $C_i \oplus C_i^* \oplus K_C^q$. If we denote the bits after information reconciliation as K_A^r and K_C^r. Then, the common randomness $K_A (= K_A^r = K_C^r)$ between Alice and Carol is established when the mismatch bit number of each block is less than 6.

In the privacy amplification phase, we leverage the keying hash function SHA$_1$ [32]. Specifically, a keying hash function $F : \mathscr{K}_0 \times \mathscr{K}_1 \rightarrow \mathscr{K}$, where F is the well-known hash function SHA$_1$, $\mathscr{K}_0 = \mathscr{K}_1 = \{0, 1\}^L$, and $\mathscr{K} = \{0, 1\}^{L'}$. One of keying

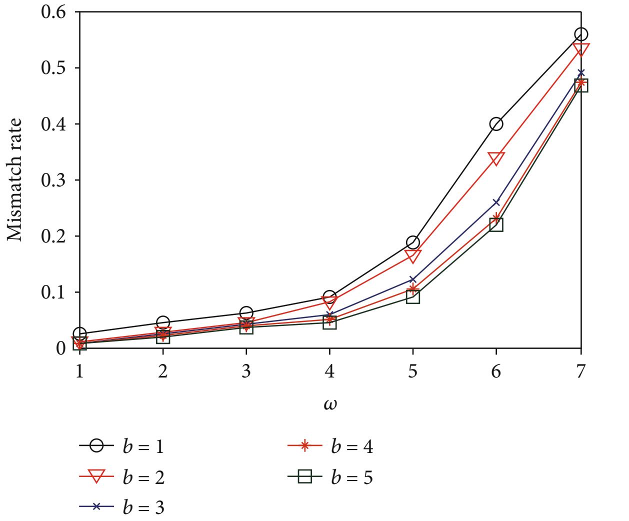


FIGURE 9: The mismatch rate versus ω under different values of b, where SNR = 0 dB and $M^* = 2000$.

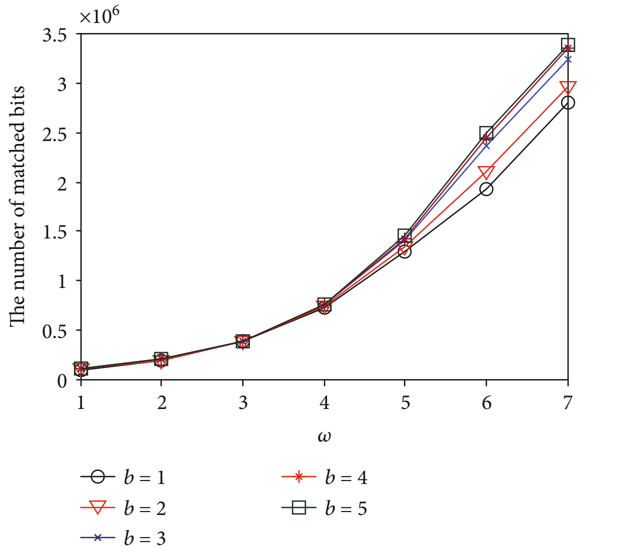


FIGURE 10: The number of matched bits versus ω under different values of b, where SNR = 0 dB and $M^* = 2000$.

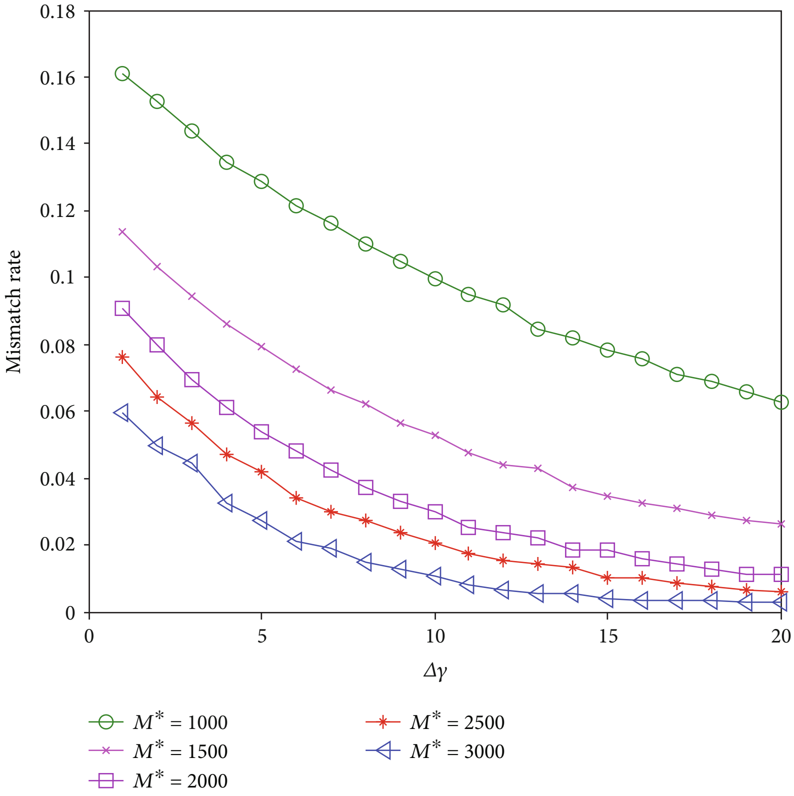


Figure 11: The mismatch rate versus $\Delta\gamma$ under different values of M^*.

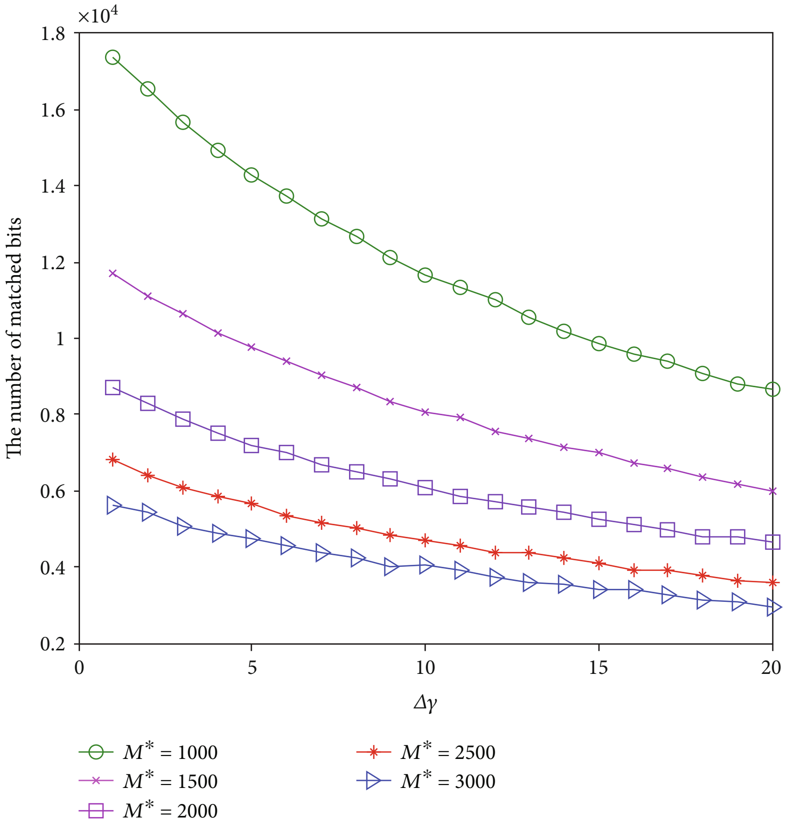


Figure 12: The number of matched bits versus $\Delta\gamma$ under different values of M^*.

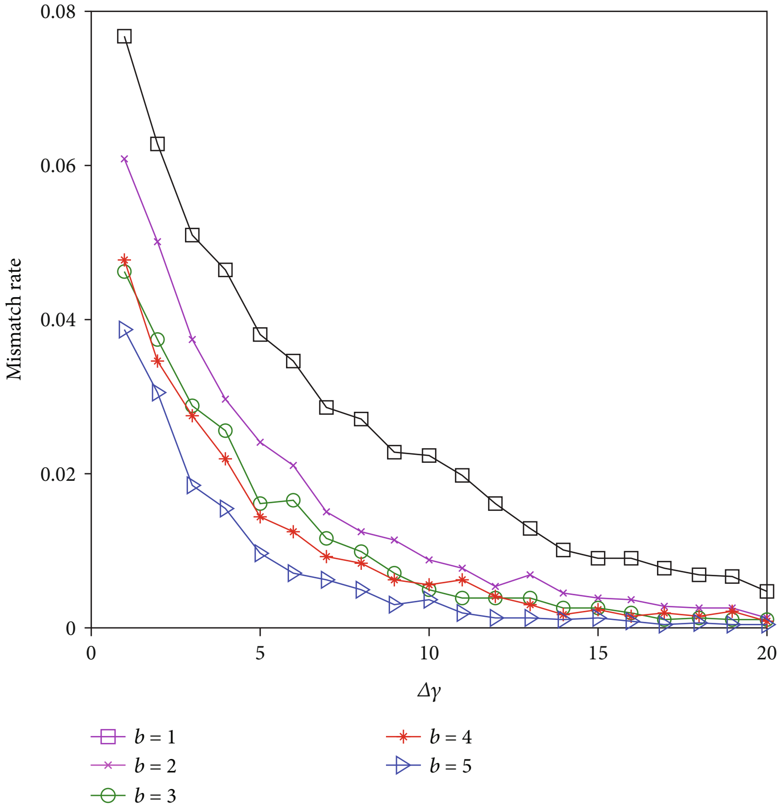


Figure 13: The mismatch rate versus $\Delta\gamma$ under different values of b.

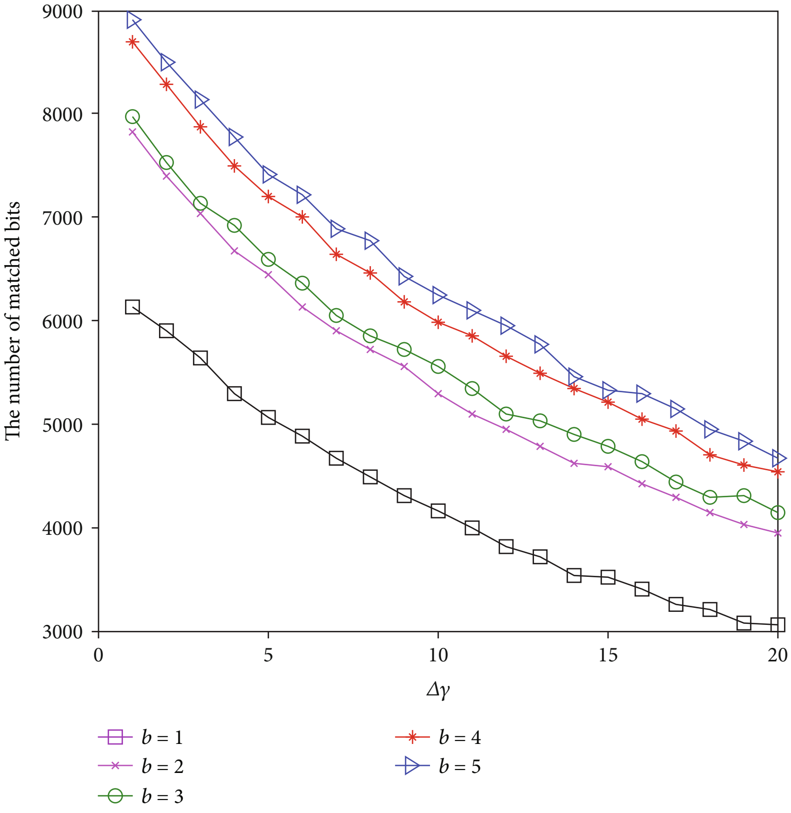


Figure 14: The number of matched bits versus $\Delta\gamma$ under different values of b.

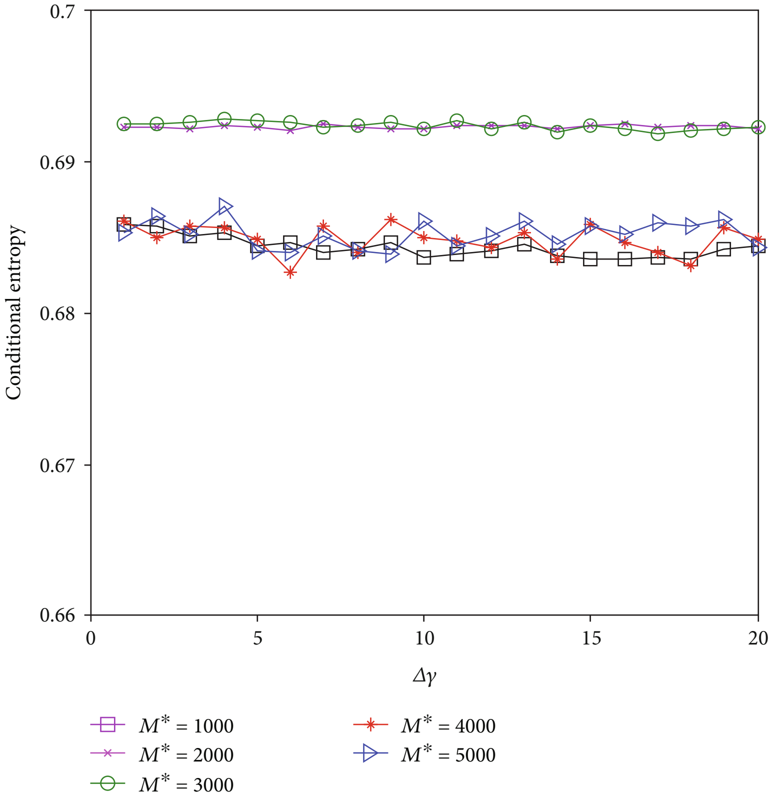


FIGURE 15: The correlation between conditional entropy and $\Delta\gamma$ under different values of M^*.

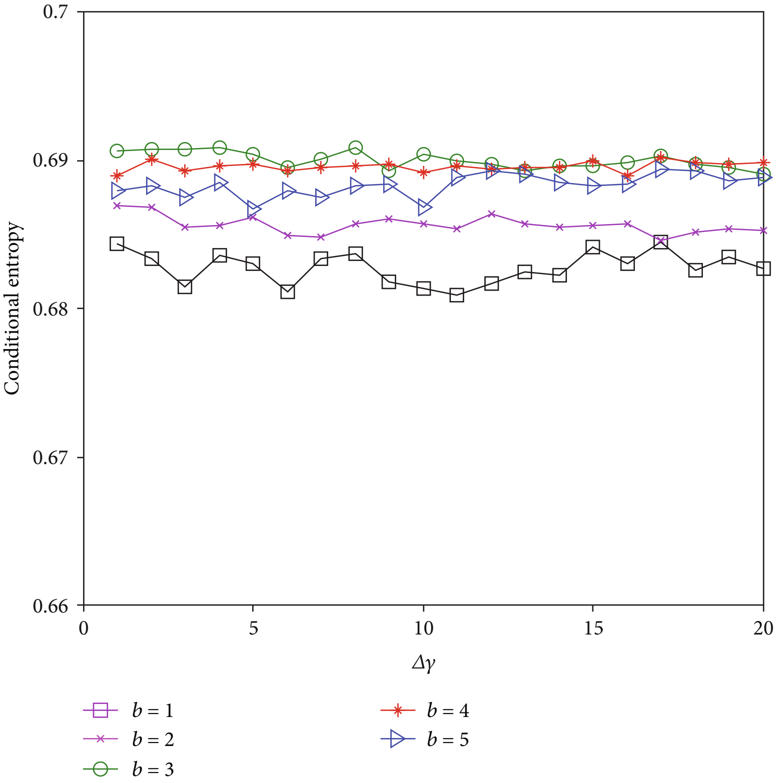


FIGURE 16: The correlation between conditional entropy and $\Delta\gamma$ under different values of b.

nodes (say Alice) uniformly chooses K_0 form $\mathscr{K}_0$ and public to the other node. Then, keying nodes compute the secret key by $K_\xi = F(K_0, K_\xi^r)(\xi \in \{A, C\})$. Moreover, in order to verify whether the two values K_A and K_C are equal, Alice and Carol can interact as follows. Alice first randomly chooses a bitstream R_A and then sends R_A and its tig $\mathrm{Tig}_A = \mathrm{SHA}_1(K_A, R_A)$ to Carol. After receiving R_A and Tig_A, Carol computes $\mathrm{Tig}_B = \mathrm{SHA}_1(K_B, R_A)$, and verify $\mathrm{Tig}_A = \mathrm{Tig}_B$ or not, if so, K_A and K_C are equal; if not, $K_A \neq K_C$.

4.2. Correlations between Keying Nodes and Eve. The statistic independence of the measurements of channel between Alice, Carol, and Eve is the hinge on the security of generated key. Figure 6 plots Pearson correlation coefficients of the measurements at the Alice and Eve against α under different values of β ($\beta = 5, 10, \cdots, 50$), where $b = 2$ and $M = 2000$. The result shows that, with a fixed $\alpha = 0.09$, the correlation coefficients is at a very low level. Take $\alpha = 0.09$, Figure 7 shows the valid index rate (i.e., the ratio of the number of valid index after the phase of *low entropy measurements elimination* to the number of measurements at Alice) and the correlation coefficients against β. We can see that, with a fixed $\beta = 10$, the valid index rate is greater than 0.7 and the correlation coefficients keep to a minimum. In the system, we set $\alpha = 0.09$ and $\beta = 10$. Figure 8 plots the measurments at Alice and Eve by taking SNR = 0 dB and $b = 2$. It is obvious that Eve measures significantly different values from Alice (i.e., *spatial variations* of wireless channel). The result shows that the proposed scheme can resist predictable channel attacks.

4.3. Mismatch Rate and Conditional Entropy. The impact of system parameter ω on the mismatch rate and the number of matched bits before the information reconciliation and privacy amplification phase is first considered. Figures 9 and 10 plot the mismatch rate and the number of matched bits versus $\Delta\gamma$ under different values of b, where $SNR = 0$ dB, $M = 2000$, $\gamma = 20$, and $\Delta\gamma = 10$. The results show that (1) a larger ω increases the number of matched bits but increases the mismatch rate; and (2) a larger b increases the number of matched bits and decreases the mismatch rate, in other words, a larger b can contribute to more bits extracted from each measurement. In particular, if $b = 2$, then the mismatch rate is less than the error threshold when $\omega = 2$ and is larger than error threshold when $\omega = 3$. Thus, if we take $b = 2$ in the system, then $\omega = 2$ is the optimal choice to maximize the key rate.

Then the impact of the parameters γ and $\Delta\gamma$ on mismatch rate and number of matched bits are discussed. Figures 11 and 12 plot the mismatch rate and the number of matched bits versus $\Delta\gamma$ under different values of M^*, where SNR = 0 dB, $b = 2$, $\omega = 2$, and $\gamma = 20$. Figures 13 and 14 show mismatch rate and match number versus $\Delta\gamma$ under different values of b, where SNR = 0 dB, $M^* = 2000$. The experimental results show that (i) the increase of M^* and $\Delta\gamma$ decrease the mismatch rate and the matched bits number. However, less mismatch rate means higher key rate, and fewer match number implies lower key generation rate. Thus, the value of M^* and $\Delta\gamma$ should be chosen carefully. (ii) The increase of b decreases the mismatch rate and increases the match rate, and hence, the higher key rate is guaranteed.

Table 1: The optimal value of $\Delta\gamma$ and M^*.

Index	SNR	$\Delta\gamma$	M^*	Mismatch rate	Bit rate
A	-10 dB	18	12000	0.0368	68
B	-5 dB	20	2000	0.0465	198
C	0 dB	12	1000	0.0439	970
D	5 dB	20	200	0.0461	1910
E	10 dB	11	100	0.0450	5640

Table 2: NIST statistical test suite results.

Test	A	B	C	D	E
Runs	0.92	0.89	0.86	0.77	0.65
FFT	0.87	0.82	0.82	0.78	0.71
Frequency	0.89	0.84	0.79	0.73	0.64
Approx. entropy	0.91	0.87	0.76	0.67	0.63
Longest run of ones	0.83	0.84	0.81	0.78	0.69

The next, the impact of the system parameters γ and $\Delta\gamma$ on the conditional entropy $\mathscr{H}(K_A^q \mid K_E^q)$ are discussed, where K_A^q and K_E^q are the bit streams at Alice and Eve after quantizing, respectively, and $\mathscr{H}(K_A^q \mid K_E^q) = \sum_{i,j} \mathrm{Pr}_{AE}(i, j) \log (1/\mathrm{Pr}_{A|E}(i \mid j))$ for $i, j \in \{0, 1\}$. Figure 15 plots the relationship between the value of $\Delta\gamma$, M^* and the conditional entropy. For instance, the conditional entropies are larger than 0.68 and less than 0.7. Figure 16 shows the conditional entropy against $\Delta\gamma$ under different values of b. In particular, all of the conditional entropies are larger than 0.68 and less than 0.7. The results show that $\Delta\gamma$, M^*, and b cause little impact to conditional entropy.

4.4. Key Rate and Randomness. Note that the bit streams after information reconciliation as K_A^r and K_C^r and denote the error-correcting information as Pub. Due to the fact that the conditional entropy $\mathscr{H}(K_A^q \mid K_E^q)$ is less than 0.7, the conditional entropies $\mathscr{H}(K_A^r \mid K_E^q, \mathrm{Pub}) \leq \mathscr{H}(K_A^q \mid K_E^q, \mathrm{Pub}) \leq \mathscr{H}(K_A^q \mid K_C^q) < 0.7$. To improve the key entropy, in *privacy amplification* phase of the simulation, we use $F : \mathscr{K}_0 \times \mathscr{K}_1 \rightarrow \mathscr{K}$, where F is the keying hash function SHA_1, $\mathscr{K}_0 = \mathscr{K}_1 = \{0, 1\}^L$, and $\mathscr{K} = \{0, 1\}^{L/2}$.

Taking $\alpha = 0.09$, $\beta = 10$, $\gamma = 20$, and $b = 2$, the simulation is conducted in a variety of M^* and $\Delta\gamma$ under different SNRs to find the optimal value of $\Delta\gamma$ and M^* to maximize the key rate (as shown in Table 1).

Moreover, the randomness of the generated key is the key for the proposed scheme to be widely used. To this end, a well-known randomness test suite NIST is used to verify the generated key's randomness. The p value from five kinds of tests is listed in Table 2. If the p value is greater than 0.01, then it means the bitstream passed the test. We conduct the simulation under different scenarios as shown in Table 1.

4.5. Comparison of Key Extraction Approaches. Some famous key extraction approaches are mentioned (i.e., RKG [8], CSKE [18], and SG [19]) in Section 1. Now, we compare their performance with the proposed scheme under different scenarios:

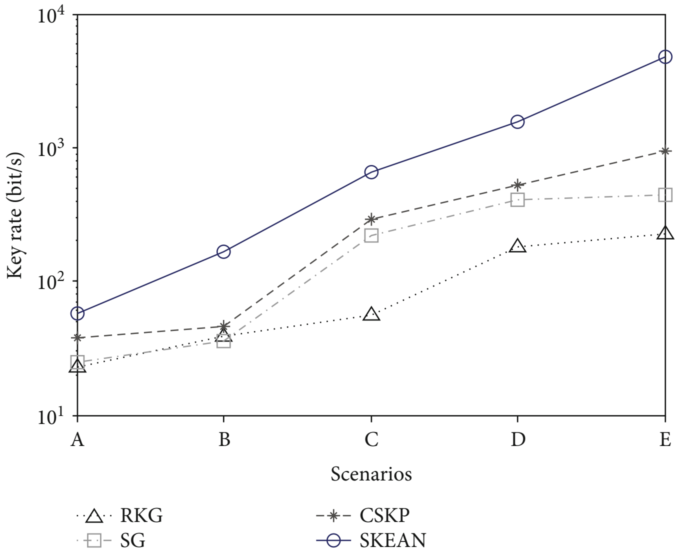
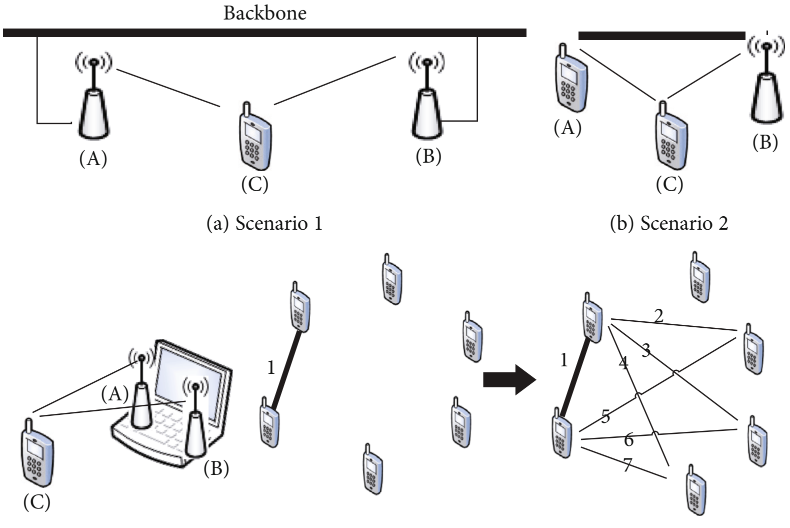


Figure 17: The key rate under different scenarios.



(a) Scenario 1

(b) Scenario 2

(c) Scenario 3

(d) Scenario 4

Figure 18: The application scenarios.

scenario A (SNR = −10 dB), scenario B (SNR = −10 dB), scenario C (SNR = 0 dB), scenario D (SNR = 5 dB), and scenario E (SNR = 10 dB). In SKEAN, the parameter selection is based on the parameter selection in Table 1. In RKG, the quantization threshold is selected so that at most 10% of the whole measurements are discarded. In CSKE, we set $m = 5$ (i.e., the measurements are quantized into 4 equally likely levels) and set the quantization threshold such that at most 30% of the measurements are dropped. In SG, we set the configurable parameters $\alpha = 0.3$, $P_B = 2$, and $\kappa = 30$.

The simulation results in Figure 17 shows that the protocol has a significantly higher secret bit generation rate compared with the existing methods. This is because (1) RKG only uses the measurements that above or below the threshold, which leads to low utilization of measurements; (2) both RKG and SG only extract 1 bit for each measurement, which lead to low efficiency of quantization; (3) the channel state information in each coherence time are coherent in CSKE, which leads measurements in a coherence time are similar; and (4) the help node only sends fixed jamming signals in each coherence time in SG, which also leads to the measurements in a coherence time are alike.

4.6. Discussions. The proposed scheme can be used in the typical application scenarios as follows.

Let us first consider the scenario with busy wireless channels (e.g., multiple access points and multiple users exist in a conference room, enterprise, hotel, etc.,), in which we try to solve the key generation problem between access points and users (case shown in Figure 18(a) where any two adjacent access points (A and B) are connected by Ethernet backbone). In this situation, we could assume that there exists a secure channel between A and B (e.g., Diffie-Hellman protocol can be used to produce a secure channel as the access points are not constrained by the energy and computing ability). Therefore, we can further generate the security key for access points and users by utilizing the proposed scheme with the secure channel.

Then we consider the key extraction between two users in the scenario of typical busy wireless environments (scenario (2) shown in Figure 18(b)). Based on the previous case, we can have a secure channel between the access points and users. With the secure channel, we can use the proposed scheme to extract a security key for two users.

Next, we consider another key generation problem in the scenario of MISO system (shown in Figure 18(c)). When Alice and Bob are the antennas of a device, the "secure channel" exists between them. We can further use the presented protocol to generate a security key for two devices.

In the case of group key generation, as shown in Figure 18(d), we can use the key extraction scheme (like work [16, 17] to set up a secure channel, then use the proposed scheme for the others. As shown in Figure 18(d), the secure channel 1 is built by traditional protocols and the secure channel 2, 3, 4, $\cdots$ can be set up by *KEI*. With no doubt, the efficiency of group key generation can be improved.

5. Conclusion

In this paper, a novel PHY-based approach has been designed for secret key extraction in wireless networks. The proposed scheme leverages jamming to changes the channel states such that two keying nodes can obtain a large number of channel measurements in each coherence time. To further improve the key generation rate and key entropy, a new bit extraction method has been presented to eliminate the low entropy measurement, to break the correlation of measurements in the coherence time with random permutation, and to transform the measurements into bit stream with an adaptive multiple-bit extraction scheme. Theoretical analysis and simulation have been presented to show the performance of the proposed scheme. The results show that the proposed scheme generates secret bits at low mismatch bit rate, high key rate, and high entropy.

Appendix

Proof of Theorem 1

Assumed that the sampling number M^* is sufficiently large and $\delta_{AC} = \delta_{BC} = 1$. Then, we have

$$\left(\begin{array}{l} \Lambda_A[i]\mathbb{N}_A \dfrac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} \rightarrow \Lambda_A[i]\mathscr{E}(N_A) = 0, \\ \mathbb{N}_C \dfrac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} \rightarrow \mathscr{E}(N_C) = 0, \\ \mathbb{N}_B \dfrac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} \rightarrow \mathscr{E}(N_B) = 0, \\ \mathbb{N}_E \dfrac{\vec{s}^{\,T}}{\left\|\vec{s}\right\|^2} \rightarrow \mathscr{E}(N_E) = 0. \end{array}\right. \tag{A.1}$$

Thus,

$$\widehat{Y}_A[i] = \widehat{Y}_C[i] = \Lambda_A[i]H_{AC} + \Lambda_B[i]H_{BC}, \tag{A.2}$$

$$\widehat{Y}_{AE}[i] = \Lambda_A[i]H_{AE} + \Lambda_B[i]H_{BE}, \tag{A.3}$$

$$\widehat{Y}_{CE}[i] = H_{CE}. \tag{A.4}$$

From [9], we obtain the maximum key rate R_M by

$$R_M = \frac{1}{T_c L^*} I\left(\widehat{Y}_A^{LL^*}; \widehat{Y}_C^{LL^*} \mid \widehat{Y}_{AE}^{LL^*}, \widehat{Y}_{CE}^{LL^*}\right). \tag{A.5}$$

From Equation (A.2), we can rewrite the above equality as

$$R_M = \frac{1}{T_c L^*} \mathscr{H}\left(\widehat{Y}_A^{LL^*} \mid \widehat{Y}_{AE}^{LL^*}, \widehat{Y}_{CE}^{LL^*}\right). \tag{A.6}$$

Denoted by $H_{ij}[l^*]$ as the channel gain between node i and j at l^*th coherence time and by $\Lambda_A^L[l^*]$ ($\Lambda_B^L[l^*]$) as the random vector selected by Alice (Bob) during in l^* th coherence time. We rewrite $\widehat{Y}_\zeta^{LL^*}$ as $<\widehat{Y}_\zeta^L[1], \cdots, \widehat{Y}_\zeta^L[l^*] \cdots, \widehat{Y}_\zeta^L[L^*]>$ for $\zeta \in \{A, C, AE, CE\}$, where $\widehat{Y}_\zeta^L[l^*]$ is the measured vector during in l^*th coherence time. Then, we have

$$\begin{aligned} &\widehat{Y}_A^L[l^*] = \widehat{Y}_C^L[l^*] = H_{AC}[l^*]\Lambda_A^L[l^*] + H_{BC}[l^*]\Lambda_B^L[l^*], \\ &\widehat{Y}_{AE}^L[l^*] = H_{AE}[l^*]\Lambda_A^L[l^*] + H_{BE}[l^*]\Lambda_B^L[l^*], \\ &\widehat{Y}_{CE}^L[l^*] = H_{CE}[l^*], \end{aligned} \tag{A.7}$$

where $l^* \in \{1,\cdots,L^*\}$. Due to the assumption that the RVs $\{\Lambda_A[i]\}_{i=1}^{LL^*}$, $\{\Lambda_B[i]\}_{i=1}^{LL^*}$ and the channel gains are i.i.d across coherence periods. Hence, by the chain rule of entropy [35], Equation (A.6) can be rewritten as

$$\begin{aligned} R_M = \frac{1}{T_c L^*} \sum_{l^*=1}^{L^*} H\left(\widehat{Y}_A^L[l^*] \middle| \widehat{Y}_A^L[1],\cdots,\widehat{Y}_A^L[l^*-1], \widehat{Y}_{AE}^{LL^*}, \widehat{Y}_{CE}^{LL^*}\right) =^{(a)} \\ \cdot \frac{1}{T_c L^*} \sum_{l^*=1}^{L^*} H\left(\widehat{Y}_A^L[l^*] \middle| \widehat{Y}_{AE}^L[l^*]\widehat{Y}_{CE}^L[l^*]\right), \end{aligned} \tag{A.8}$$

forms a *Markov chain* (RVs X, Y, and Z form a Markov chain in that order (denoted by $X \rightarrow Y \rightarrow Z$) if $P(x, z \mid y) = P(x \mid y) P(z \mid y)$.). Let J be a RV distributed over the integers $1, 2, \cdots, L^*$ uniformly and be independent of all the above RVs. Denoted by $\widehat{Y}_\zeta^L = \widehat{Y}_\zeta^L[J]$ for $\zeta \in \{A, AE, CE\}$. Then,

$$R_M = \frac{1}{T_c} H\left(\widehat{Y}_A^L \mid \widehat{Y}_{AE}^L, \widehat{Y}_{CE}^L\right). \tag{A.9}$$

Formally, variable H_{AC}, H_{BC}, H_{AE}, H_{BE}, H_{CE}, Λ_A, and Λ_B are pairwise independence. Then, the variables $\Lambda_A H_{AC} + \Lambda_B H_{BC}$, H_{AE}, H_{BE}, and H_{CE} are pairwise independence.

So,

$$\begin{aligned}\mathscr{H}\left(\widehat{Y}_A^L\middle|\widehat{Y}_{AE}^L, \widehat{Y}_{CE}^L\right) &=^{(b)}\mathscr{H}\left(\widehat{Y}_A^L\middle|\widehat{Y}_{AE}^L\right)\\ &=^{(c)}\sum_{i=1}^{L}\mathscr{H}\left(\widehat{Y}_A(i)\widehat{Y}_A[1],\cdots,\widehat{Y}_A[i-1], \widehat{Y}_{AE}^L\right)\\ &=^{(d)}\sum_{i=1}^{L}\mathscr{H}\left(\widehat{Y}_A[i]\widehat{Y}_{AE}[i]\right),\end{aligned}\tag{A.10}$$

where Equality (b) can be obtained by $\widehat{Y}_A^L \rightarrow \widehat{Y}_{AE}^L \rightarrow \widehat{Y}_{CE}^L$ forms a Markov chain; Equality (c) comes from the chain rule of entropy [35]. Equality (d) comes from the following claim.

Claim: For any $i \in \{1, 2,\cdots,L\}$, we have the result as follows:

$$\widehat{Y}_A[i] \rightarrow \widehat{Y}_{AE}[i] \rightarrow \left\langle \widehat{Y}_A^{i-1}, \widehat{Y}_{AE}^{i-1}, \widehat{Y}_{AE}[i+1],\cdots,\widehat{Y}_{AE}[L]\right\rangle,\tag{A.11}$$

forms a Markov chain.

Let $\Lambda_1^* = c_1\Lambda_A[1] + c_2\Lambda_B[1]$ and $\Lambda_2^* = c'_1\Lambda_A[2] + c'_2\Lambda_B[2]$ for any two pair of real number (c_1, c_2) (c'_1, c'_2), if Λ_A and Λ_B are i.i.d variables, then we have the RVs Λ_1^* and Λ_2^* are independent. Due to the fact that the channel gains are equal in T_c, we have $\{\widehat{Y}_A[i]\}_{i=1}^L$ are pairwise independence, and $\widehat{Y}_A[i]$ and $\widehat{Y}_{AE}[j]$ are independent for any $i, j, (i \neq j)$. Thus, the claim holds.

Now, we rewrite $\mathscr{H}(\widehat{Y}_A[i] \mid \widehat{Y}_{AE}[i])$ $(i = 1, 2, \cdots, L)$ as

$$\begin{aligned}\mathscr{H}\left(\widehat{Y}_A[i] \mid \widehat{Y}_{AE}[i]\right) &= \mathscr{H}(\Lambda_A[i]H_{AC} + \Lambda_B[i]H_{BC} \mid \Lambda_A[i]H_{AE} + \Lambda_B[i]H_{BE})\\ &\geq \mathscr{H}(\Lambda_A[i]H_{AC} + \Lambda_B[i]H_{BC} \mid \Lambda_A[i]H_{AE}\\ &\quad + \Lambda_B[i]H_{BE}H_{AC}, H_{BC}, H_{AE}, H_{BE})\\ &= \int\!\!\int\!\!\int\!\!\int f_1(x_1)f_2(x_2)f_3(x_3)f_4(x_4)\\ &\quad \times \{\mathscr{H}(\Lambda_A H_{AC} + \Lambda_B H_{BC} \mid \Lambda_A H_{AE} + \Lambda_B H_{BE}, H_{AC}\\ &= x_1, H_{BC} = x_2, H_{AE} = x_3, H_{BE} = x_4)\}dx_1dx_2dx_3dx_4,\end{aligned}\tag{A.12}$$

where f_i $(i = 1, 2, 3, 4)$ is the pdf of the corresponding Gaussian variables. By the following equality:

$$\begin{aligned}&\mathscr{H}(\Lambda_A H_{AC} + \Lambda_B H_{BC} \mid \Lambda_A H_{AE} + \Lambda_B H_{BE}, H_{AC} = x_1, H_{BC}\\ &\quad = x_2, H_{AE} = x_3, H_{BE} = x_4)\\ &\quad = \mathscr{H}(x_1\Lambda_A + x_2\Lambda_B \mid x_3\Lambda_A + x_4\Lambda_B, x_1, x_2, x_3, x_4)\\ &\quad = \mathscr{H}[x_4(x_1\Lambda_A + x_2\Lambda_B) - x_2(x_3\Lambda_A + x_4\Lambda_B)|x_3\Lambda_A + x_4\Lambda_B x_1, x_2, x_3, x_4]\\ &\quad = \mathscr{H}((x_4x_1 - x_2x_3)\Lambda_A \mid x_3\Lambda_A + x_4\Lambda_B, x_1, x_2, x_3, x_4)\\ &\quad = \mathscr{H}(\Lambda_A \mid x_3\Lambda_A + x_4\Lambda_B, x_1, x_2, x_3, x_4)\\ &\quad = \mathscr{H}(x_3\Lambda_A + x_4\Lambda_B \mid \Lambda_A, x_1, x_2, x_3, x_4)\\ &\qquad + \mathscr{H}(\Lambda_A \mid x_1, x_2, x_3, x_4) - \mathscr{H}(x_3\Lambda_A + x_4\Lambda_B \mid x_1, x_2, x_3, x_4)\\ &\quad = \mathscr{H}(\Lambda_B) + \mathscr{H}(\Lambda_A) - \mathscr{H}(x_3\Lambda_A + x_4\Lambda_B),\end{aligned}\tag{A.13}$$

we have

$$\begin{aligned}&\mathscr{H}\left(\widehat{Y}_A[i] \mid \widehat{Y}_{AE}[i]\right) \geq \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\mathscr{H}(\Lambda_A) + \mathscr{H}(\Lambda_B) - \mathscr{H}(x_3\Lambda_A + x_4\Lambda_B)\\ &\quad \times f_3(x_3)f_4(x_4)dx_3dx_4 =^{(e)} \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\frac{1}{2\pi}\\ &\quad \cdot \left[\ln\left(2\pi eb^2\right) - \frac{1}{2}\ln\left(2\pi eb^2\left(x_3^2 + x_4^2\right)\right)\right]\\ &\quad \times e^{-\left(x_3^2+x_4^2\right)/2}dx_3dx_4 \geq^{(f)} \frac{1}{2}\left[\ln\left(2\pi eb^2\right) + 1 - \ln 2 - e^{-1}\right],\end{aligned}\tag{A.14}$$

where Equality (e) comes from the fact that $\Lambda_A \sim \mathbf{G}(0, b^2)$, $\Lambda_B \sim \mathbf{G}(0, b^2)$, and $x_3\Lambda_A + x_4\Lambda_B \sim \mathbf{G}(0, b^2x_3^2 + b^2x_4^2)$; Equality (f) can be obtained by the following result: let $x_3 = r\cos\theta$ and $x_4 = r\sin\theta$, then, we have

$$\begin{aligned}&\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\frac{1}{4\pi}e^{-\left(x_3^2+x_4^2\right)/2}\ln\left(2\pi eb^2\left(x_3^2 + x_4^2\right)\right)dx_3dx_4\\ &\quad = \int_0^{2\pi}\int_0^{+\infty}\frac{1}{4\pi}e^{-\frac{r^2}{2}}\ln\left(2\pi eb^2r^2\right)rdrd\theta\\ &\quad = \frac{1}{2}\ln 4\pi eb^2 + \frac{1}{2}\int_0^{+\infty}e^{-t}\ln tdt\left(\text{Take}t = \frac{1}{2}r^2\right)\\ &\quad = \frac{1}{2}\ln 4\pi eb^2 + \frac{1}{2}\left[\int_0^1 e^{-t}\ln tdt + \int_1^{+\infty}e^{-t}\ln tdt\right]\\ &\quad \leq \frac{1}{2}\ln 4\pi eb^2 + \frac{1}{2}\left[\int_0^1 \ln tdt + \int_1^{+\infty}e^{-t}\ln tdt\right]\\ &\quad = \frac{1}{2}\ln 4\pi eb^2 + \frac{1}{2}\left[-1 + \int_1^{+\infty}\frac{1}{t}e^{-t}dt\right] \leq \frac{1}{2}\ln 4\pi eb^2\\ &\qquad + \frac{1}{2}\left[-1 + \int_1^{+\infty}e^{-t}dt\right] = \frac{1}{2}\ln 4\pi eb^2 + \frac{1}{2}\left[e^{-1} - 1\right].\end{aligned}\tag{A.15}$$

Combine with Equations (A.9), (A.10), and (A.14), we have

$$R_M \geq \frac{L}{2T_c}\left[\ln\left(2\pi eb^2\right) + 1 - \ln 2 - e^{-1}\right] = \frac{L}{2T_c}\left[\ln\left(\pi(eb)^2\right) - e^{-1}\right].\tag{A.16}$$

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is jointly supported by NSFC (Nos. 61771417, 61872059, and 61502085) and the project "The Verification Platform of Multi-tier Coverage Communication Network for oceans" (No. LZC0020).

References

[1] A. Paramonov, O. Hussain, K. Samouylov, A. Koucheryavy, R. Kirichek, and Y. Koucheryavy, "Clustering optimization for out-of-band D2D communications," *Wireless Communications and Mobile Computing*, vol. 2017, Article ID 6747052, 11 pages, 2017.

[2] N. Zhang, P. Yang, J. Ren, D. Chen, L. Yu, and X. Shen, "Synergy of big data and 5g wireless networks: opportunities, approaches, and challenges," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 12–18, 2018.

[3] A. P. G. Lopes and P. R. L. Gondim, "Low-cost authentication protocol for D2D communication in m-Health with trust evaluation," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8876807, 16 pages, 2020.

[4] D. Chen, Z. Zhao, X. Qin et al., "MAGLeak: a learning-based side-channel attack for password recognition with multiple sensors in IIoT environment," *IEEE Transactions on Industrial Informatics*, p. 1, 2020.

[5] M. Cao, L. Wang, Z. Qin, and C. Lou, "A lightweight fine-grained search scheme over encrypted data in cloud-assisted wireless body area networks," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 9340808, 12 pages, 2019.

[6] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. Shen, "Physical layer based message authentication with secure channel codes," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1079–1093, 2020.

[7] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[8] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM conference on Computer and communications security - CCS '07*, pp. 401–410, New York, NY, USA, October 2007.

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

[10] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005*, pp. 2152–2155, Adelaide, SA, Australia, September 2005.

[11] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom '08*, pp. 128–139, New York, NY, USA, September 2008.

[12] S. Jana, S. 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 international conference on Mobile computing and networking*, pp. 321–332, New York, NY, USA, September 2009.

[13] 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.

[14] J. Croft, N. Patwari, and S. K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, pp. 70–81, New York, NY, USA, April 2010.

[15] S. Gollskota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *2011 Proceedings IEEE INFOCOM*, pp. 1125–1133, Shanghai, China, April 2011.

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

[17] 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, April 2011.

[18] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *2012 Proceedings IEEE INFOCOM*, pp. 927–935, Orlando, FL, USA, March 2012.

[19] 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.

[20] Y. Liu, J. Li, and A. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 682–694, 2013.

[21] B. Yang, W. Wang, B. Yao, and Q. Yin, "Destination assisted secret wireless communication with cooperative helpers," *IEEE Signal Processing Letters*, vol. 20, no. 11, pp. 1030–1033, 2013.

[22] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2015.

[23] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beam-forming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Transactions on Signal Processing*, vol. 63, no. 1, pp. 206–220, 2016.

[24] C. Wang, H. Wang, and X. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 589–605, 2015.

[25] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Transactions Wireless Communications*, vol. 14, no. 5, pp. 2742–2754, 2015.

[26] H. Wang, C. Wang, and D. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Transactions on Signal Processing*, vol. 63, no. 23, pp. 6285–6298, 2015.

[27] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. Lee Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[28] Z. Yang, P. Cheng, and J. Chen, "Learning-based jamming attack against low-duty-cycle networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 6, pp. 650–663, 2015.

[29] R. Durstenfeld, "Algorithm 235: random permutation," *Communications of the ACM*, vol. 7, no. 7, p. 420, 1964.

[30] G. Brassard and L. Salvail, "Secret key reconciliation by public discussion," in *Advances in Cryptology — EUROCRYPT '93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol 765*, T. Helleseth, Ed., pp. 410–423, Springer, Berlin, Heidelberg, 1993.

[31] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology - EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027*pp. 523–540, Springer, Berlin, Heidelberg.

[32] D. Eastlake and P. Jones, "US secure hash algorithm 1 (SHA1)," *RFC*, vol. 3174, 2001.

[33] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part I: definitions and a completeness result," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 822–831, 2003.

[34] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," in *2009 IEEE International Conference on Communications*, pp. 1–5, Dresden, Germany, June 2009.

[35] T. M. Cover and J. Thomas, *Elements of Information Theory*, Wiley, New York, NY, USA, 1991.