Efficient secret key generation scheme of physical layer security communication in ubiquitous wireless networks

Hailiang Xiong1,2,3 | Guangyuan Wang1 | Jian Ding2 | Weihong Zhu1 | Hongji Xu1 | Changwu Hu1 | Zhenzhen Mai1 | Ruochen Bian1

1 The School of Information Science and Engineering, Shandong University, Qingdao 266237, China
2 The National Key Laboratory of Electromagnetic Environment, China Research Institute of Radiowave Propagation, Qingdao 266107, China
3 The State Key Laboratory of Integrated Services Networks, Xidian University, Xi’an 710071, China

Correspondence
Weihong Zhu and Hongji Xu, The School of Information Science and Engineering, Shandong University, Qingdao, 266237, China.
Email: zhuwh@sdu.edu.cn, hongjixu@sdu.edu.cn

Funding information
Natural Science Foundation of Shandong Province, Grant/Award Number: ZR2019MF038; Open Fund of the National Key Laboratory of Electromagnetic Environment, Grant/Award Number: 202003006, Qingdao Science and Technology Project, Grant/Award Number: 2022XHL; Open Fund of State Key Laboratory of Integrated Services Networks, Grant/Award Number: ISN22-06

Abstract
This paper focuses on high efficiency secret key generation mechanism of physical-layer communication over fading channels in ubiquitous wireless networks. The secret key rate via traditional physical-layer approach could be limited when the wireless propagation channels connecting two sensors change slowly. To generate a high-rate secret key and improve the communication efficiency over quasi-static block fading channels, a novel multi-randomness device-to-device secret key generation strategy and a cooperative communication mechanism aided by relay nodes are proposed. In the proposed schemes, the legitimate members to send random signals rotationally in every coherent time $T$ are set; thus, two legitimate ubiquitous wireless network members, Alice and Bob, can obtain the potential correlated information by exploiting the randomness and the reciprocity of the wireless propagation channels. Considering the reciprocity of wireless channels is variable while the forward channel gain and backward channel gain are correlated in coherent time, a modified secret key generation scheme is proposed via layered coding with theoretical secret key rates derived. The simulation results show that the proposed scheme outperforms traditional approaches with favourable application prospects in ubiquitous wireless communications networks and internet of things.

1 | INTRODUCTION

Wireless sensor networks (WSNs) are distributed intelligent networks composed of a large number of tiny sensor nodes with wireless communication and computing capabilities deployed in a specific area. In recent years, with the information science industry rapidly developing, WSNs is becoming one of the most important role of ubiquitous wireless networks (UWNs). As a foundation of the internet of things technology, low-cost UWNs have been widely used due to them being flexible, powerful and low-cost in data collection and short distance wireless communication. However, UWNs are highly susceptible to attacks due to their unique characteristics: large-scale, self-organization, dynamic topology, and constrained resources [1]. Naturally, security policies are urgently needed to ensure the safe transmission of information between two legitimate nodes. While designing security policies, a general structure is aimed at eliminating some or all attacks. In recent years, sorts of protocols based on information security principles such as confidentiality, integrity, authentication, and availability are developed for security vulnerabilities [2, 3].

Key management is one of the most important issues in many secure communications, and it is also a kernel mechanism to ensure the security of network services and various applications [4]. With the ever-increasing demands for transmission security in UWNs, there is an urgent need to introduce secure and reliable key management schemes into UWNs. The resources of UWNs are seriously limited; public key cryptography algorithm such as Rivest–Shamir–Adleman

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.
© 2021 The Authors. IET Communications published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology
(RSA) is computationally intensive, so it was unsuitable for UWNs. Recently, a series of research indicate that if one chooses appropriate algorithm and parameters, optimize and reduce power consumption, public key cryptography algorithms can also be used in UWNs [5]. For public key cryptography algorithms in UWNs applications, most of the existing literatures focus on the research and improvement of RSA or error correcting code (ECC) algorithms. There are also many researchers devoting themselves to the application of symmetric cryptographic mechanisms in UWNs due to its advantages in computing speed and energy consumption [6–8]. In the symmetric encryption mechanism, two communicating parties use the same key for encryption and decryption. Therefore, key distribution has always been a challenge in symmetric encryption.

Fortunately, physical layer communication is found to be robust when the security performance is considered [9–13]. Physical layer security technique is becoming an alternative approach to prevent attacks in UWNs since it takes the following advantages: (1) less computational power needed; (2) the communication can still be secure in the case where there are eavesdroppers. Recently, physical layer secret key generation (SKG) by exploiting the randomness and the reciprocity of the wireless channels to extract secret keys over public channels has attracted considerable attention [14–21]. If the eavesdroppers are located far enough from the legitimate users, for example, more than half of the wavelength, the legitimate members experience independent channels to eavesdroppers, which enables them to generate a secret key at legitimate members. By separately measuring their common channel, the two legitimate members, often namely Alice and Bob, can obtain highly correlated channel measurements. After a series of follow-up steps including quantization, information reconciliation, and privacy amplification, Alice and Bob can extract a common secret key through the noisy channel measurements. In a nutshell, the common wireless channel connecting two communication nodes provides a valuable common random source required for generating secret keys using the method proposed in [22] and [23]. Since the generated secret bits are stored for further use with one-time-pad scheme, it will not affect the real-time data communication, even if there is a loss or delay in some block. Hence, in SKG, we are more interested in the rate of secret key.

Commonly, the rate of traditional secret key generated by physical-layer approach could be limited when the wireless channels connecting two sensors change slowly. To improve the key generation rate, [15] proposed a relay-assisted method, in which the random channels associated with relay nodes in the network topology are exploited as added stochastic sources for secret key generation. When the direct link channel is not sufficient to generate a key, the cooperative scheme has also been considered [16, 24, 25]. In [16], a three-time-slot secret key generation scheme for two single-antenna legitimate users with the help of a relay has been proposed, the transmission schemes are described and the simulation results are presented using information estimation based on k-nearest neighbor distance. In [24], a secret key generation scheme using a two-way relay channel has been proposed and a k-nearest relay distance mutual information estimation is also used to present a secret key rate.

This paper, to generate a high-rate secret key and improve the security of the ubiquitous wireless networks, proposes a novel multi-randomness (MR) device-to-device secret key generation strategy and develops a novel cooperative communication mechanism aided by relay nodes over quasi-static block fading channels. In the proposed schemes, we set the legitimate members to send random signals rotationally during the coherent time $T$; thus two legitimate UWNs members Alice and Bob can obtain the potential correlated information by exploiting the randomness and the reciprocity of the wireless channels. After quantization, information reconciliation, and privacy amplification, Alice and Bob can extract a common secret key through the noisy channel measurements. Furthermore, we also consider the scenario that the reciprocity of wireless channels is variable while the forward channel gain and the backward channel gain are correlated in the coherent time. In this case, we present a modified secret key generation scheme via layered coding, which is proved to be theoretically optimal. The simulation results demonstrate that the proposed scheme outperforms traditional approaches with favourable application prospect in ubiquitous wireless networks.

The remaining parts of the paper are organized as follows: Section 2 describes the system model and summarizes some important definitions with the conclusions of secret key rate. In Section 3, we propose a novel device-to-device secret key generation scheme over quasi-static block fading channels in detail. In Section 4, we propose a cooperative secret key generation scheme with assistance of relay nodes. We further extend the study to the scenario in which the forward gain and backward gain of wireless channels are not equal but correlated in Section 5. Simulation results of the proposed scheme and the modified secret key generation scheme are presented in Section 6. Section 7 draws the conclusions.

2 | SYSTEM MODEL AND SECRET KEY DEFINITION

In this section, we first introduce the system model and summarize some important definition and conclusions of the secret key rate.
2.1 System model

The secret key generation system considered in this paper is a simple device-to-device model with two legitimate UWNs members Alice and Bob, as shown in Figure 1. Alice and Bob are equipped with a single antenna. They communicate with an identical frequency and can transmit signals over the wireless channels and send helper information over the public channel. As generally assumed in most research literature, there is a passive eavesdropper Eve, which does not interfere with legitimate members. The fading channels are independent quasi-static fading channels, where the fading channels remain constant for a certain coherent time but vary independently from one coherent time to another. It is also assumed that the channel gain $h_0 \sim \mathcal{N}(0, \sigma_0^2)$, and the noise in each channel also obeys Gaussian distribution with zero mean and variance $\sigma^2$. In this place, we should note that the proposed method still works if the distribution of wireless channel gain changes.

For practical reasons, we consider the model as half-duplex, in which Alice and Bob can not transmit or receive signals at the same time.

2.2 Secret key capacity

We suppose the legitimate members Alice, Bob and the eavesdropper Eve obtain $n$ sequences $X = (X_1, X_2, ..., X_n)$, $Y = (Y_1, Y_2, ..., Y_n)$, and $Z = (Z_1, Z_2, ..., Z_n)$, respectively. Alice and Bob calculate a common key represented as $K_A$ and $K_B$, respectively, based on their observations. Hence, the generated secret key rate $r_K(X; Y | Z)$ can be upper and lower bounded as [14, 16, 24]

$$r_K(X; Y | Z) \leq \min[I(X; Y), I(X; Y | Z)],$$

$$r_K(X; Y | Z) \geq \max[I(Y; X) - I(Y; Z), I(Y; X) - I(Y; Z)],$$

where $I(A; B)$ denotes the mutual information of $A$ and $B$, and the conditional mutual information can be calculated by

$$I(X; Y | Z) = H(X, Z) + H(Y, Z) - H(Z) - H(X, Y, Z),$$

where $H(A, B)$ denotes the joint entropy of $A$ and $B$.

3 DEVICE-TO-DEVICE SECRET KEY GENERATION SCHEME VIA WIRELESS CHANNEL RECIPROCITY

In this section, we present a device-to-device secret key generation scheme over quasi-static block fading channels. The proposed method can be summarized as two steps: (1) randomness sending: Alice and Bob send random signals alternately in coherent time $T$, then they can obtain the correlated information by exploiting the randomness and the reciprocity of the wireless channels; (2) key agreement: Alice and Bob agree on a common randomness secret key according to their obtained information by using Slepian–Wolf code.

Firstly, Alice transmits a Gaussian random signal $x_{A_1} \sim \mathcal{N}(0, \sigma_{A_1}^2)$ with power $P_A$ over wireless fading channel; then the received signal of Bob and Eve can be expressed as

$$Y_{B_1} = h_0 x_{A_1} + N_{B_1},$$

$$Y_{E_1} = h_1 x_{A_1} + N_{E_1},$$

respectively, where $h_0$ and $h_1$ are the wireless channel gains from Alice to Bob and Eve, $N_{B_1}$ and $N_{E_1}$ are channel noises. Then, Bob transmits a Gaussian random signal $x_{B_1} \sim \mathcal{N}(0, \sigma_{B_1}^2)$ with power $P_B$ over wireless fading channel, the received signal of Alice and Eve can be expressed as

$$Y_{A_1} = h_0 x_{B_1} + N_{A_1},$$

$$Y_{E_2} = h_2 x_{B_1} + N_{E_2},$$

respectively. Repeat the above process until the coherent time ends. Consequently, Alice and Bob obtain correlated information

$$X_A^T Y_A = \left( x_{A_1} Y_{A_1}, x_{A_2} Y_{A_2}, ..., x_{A_{T_0}} Y_{A_{T_0}} \right),$$

$$X_B^T Y_B = \left( x_{B_1} Y_{B_1}, x_{B_2} Y_{B_2}, ..., x_{B_{T_0}} Y_{B_{T_0}} \right),$$

respectively, where $T_0$ represents the time required to complete a transmission, and $\lfloor . \rfloor$ denotes the largest integer that is smaller than its argument. Since the channel gain $h_1$ and $h_2$ are independent of $h_0$, the observations obtained by Eve are independent of that obtained by Alice and Bob, and Eve learns nothing about $X_A^T Y_A$ and $X_B^T Y_B$. 

![FIGURE 1 Device-to-device secret key generation model](image-url)
From $(x_A^T Y_A, x_B^T Y_B)$, Alice and Bob can agree on a secret key with the rate

$$R = \frac{1}{T} I(x_A, Y_A; \mathbf{x}_B, Y_B)$$

$$= \frac{1}{T} I(x_A, Y_A; \mathbf{x}_B, Y_B)$$

$$= \frac{1}{T} I(Y_A; Y_B | x_A, x_B) + I(x_A; Y_B | x_A) + I(x_B; Y_A | x_B)$$

$$= \frac{1}{T} I(Y_A; Y_B | x_A, x_B) + I(x_A; Y_B | x_A) + I(x_B; Y_A | x_B)$$

$$= \frac{1}{T} I(Y_A; Y_B | x_A, x_B) + I(x_A; Y_B | x_A) + I(x_B; Y_A | x_B)$$

$$= \frac{1}{T} I(Y_A; Y_B | x_A, x_B) + I(x_A; Y_B | x_A) + I(x_B; Y_A | x_B),$$

where the last step follows the fact that $x_A$ and $x_B$ are independent. Obviously, the first term of (7) comes from the randomness of wireless channel which equals to the secret key rate of conventional method [15, 24],

$$I(x_A; Y_B | x_A, x_B)$$

$$= -\frac{1}{2T} \log \left( 1 - \frac{1}{(1 + \frac{\sigma^2}{\sigma^2_{\mathbf{x}_A, \mathbf{x}_B}}) (1 + \frac{\sigma^2}{\sigma^2_{\mathbf{x}_B, \mathbf{x}_A}}) - \rho_{\mathbf{x}_A, \mathbf{x}_B}^2 \right),$$

and the second term of (7),

$$I(x_A; Y_B) = I(x_A; Y_B | h_0) - I(x_A; h_0 | Y_B)$$

$$= I(x_A; Y_B | h_0) + I(x_A; h_0) - I(x_A; h_0 | Y_B)$$

$$= I(x_A; Y_B | h_0),$$

where the last step follows the fact that $x_A$ and $h_0$ are independent.

In this place, we introduce the following multivariate normal distribution [28]. Let $X_1, X_2, ..., X_n$ have a multivariate normal distribution with mean $\mu$ and covariance matrix $K$. The probability density function of $X_1, X_2, ..., X_n$ is given by

$$f(x) = \frac{1}{(2\pi)^{\frac{n}{2}} |K|^\frac{1}{2}} e^{-\frac{1}{2} (x - \mu)^T K^{-1} (x - \mu)}. \quad (10)$$

So the entropy can be expressed as

$$b(f) = -\int f(x) \left[ -\frac{1}{2} (x - \mu)^T K^{-1} (x - \mu) - \ln(2\pi)^2 |K|^\frac{1}{2} \right] dx$$

$$= \frac{1}{2} E \left[ \sum_{i,j} (X_i - \mu_i) K^{-1}_{ij} (X_j - \mu_j) \right] + \frac{1}{2} \ln(2\pi)^2 |K|$$

$$= \frac{1}{2} \sum_{i,j} E \left[ (X_i - \mu_i) (X_j - \mu_j) (K^{-1})_{ij} \right] + \frac{1}{2} \ln(2\pi)^2 |K|$$

$$= \frac{1}{2} \sum_{i,j} K_{ij} (K^{-1})_{ij} + \frac{1}{2} \ln(2\pi)^2 |K|$$

$$= \frac{1}{2} \sum_{i,j} I_{ij} + \frac{1}{2} \ln(2\pi)^2 |K|$$

$$= \frac{n}{2} + \frac{1}{2} \ln(2\pi)^2 |K|$$

$$= \frac{1}{2} \log(2\pi e)^2 |K|. \quad (11)$$

Consider the conditional mutual information $I(x_A; Y_B | h_0)$ above, when $h_0$ is given, $h_0$ could be regarded as a constant. Hence, $Y_{B_i} = h_0 x_{A_i} + N_{B_i}$ can be considered as a Gaussian random variable. Therefore, we have

$$b(x_{A_i}; Y_{B_i} | h_0) = \frac{1}{2} \log(2\pi e)^2 |K|$$

$$= \frac{1}{2} \log(2\pi e)^2 \sigma^2_{A_i} (1 - \rho_i^2). \quad (12)$$

Hence,

$$I(x_A; Y_B | h_0) = \sum_{i=1}^{\frac{1}{2}} I(x_{A_i}; Y_{B_i} | h_0)$$

$$= b(Y_{B_i}) + b(x_{A_i}) - b(x_{A_i}, Y_{B_i})$$

$$= -\frac{1}{2} \log(1 - \rho_i^2), \quad (13)$$

where $\rho_i$ is the correlation coefficient of $x_{A_i}$ and $Y_{B_i}$.

The covariance of $x_{A_i}$ and $Y_{B_i}$ can be calculated as

$$\sigma_{x_{A_i}, Y_{B_i}} = E[(x_{A_i} - E(x_{A_i}))(Y_{B_i} - E(Y_{B_i}))]$$

$$= h_0 \sigma^2_{A_i}. \quad (14)$$
It is easy to check that the variances $\text{var}(x_A) = \sigma_A^2$, $\text{var}(y_B) = \frac{b^2_i \sigma_A^2}{\sigma_A^2 + \sigma^2}$, thus

$$\rho_i^2 = \frac{\text{cov}(x_A, y_B)}{\text{var}(x_A) \text{var}(y_B)} = \frac{b^2_i \sigma_A^2}{(b^2_i \sigma_A^2 + \sigma^2)}.$$

Substituting (13) and (15) into (9), we have

$$I(x_A; Y_B) = -\frac{1}{2T} \sum_{i=1}^{\lfloor \frac{T}{2\Delta} \rfloor} \log \left[ 1 - \frac{1}{1 + \frac{\sigma^2}{b^2_i \sigma_A^2}} \right].$$

Similarly, the third term of (7) can be expressed as

$$I(x_B; Y_A) = -\frac{1}{2T} \sum_{i=1}^{\lfloor \frac{T}{2\Delta} \rfloor} \log \left[ 1 - \frac{1}{1 + \frac{\sigma^2}{b^2_i \sigma_B^2}} \right].$$

Finally, we get the secret key rate as

$$R = \frac{1}{2T} \left\{ \log \left[ 1 - \frac{1}{1 + \frac{\sigma^2}{\sigma_A^2 \sigma_B^2}} \right] + \sum_{i=1}^{\lfloor \frac{T}{2\Delta} \rfloor} \log \left[ 1 - \frac{1}{1 + \frac{\sigma^2}{b^2_i \sigma_A^2}} \right] + \log \left[ 1 - \frac{1}{1 + \frac{\sigma^2}{b^2_i \sigma_B^2}} \right] \right\}.$$

In order to generate a secret key having the rate in (18), it is necessary for Alice to transmit helper data to Bob over the public channel using Slepian–Wolf code [15] to coordinate the influence of noise in its channel estimation. Somewhat notable is that although the helper data can be obtained by Eve, Eve learns nothing about the key. More specifically, in every coherent time $T$, Alice has $m = \lfloor \frac{T}{2\Delta} \rfloor$ observations. These observations can be expressed as a vector $g_A = [g_A(1), ..., g_A(m)^T]$, where $g_A(i) = x_A y_{A_i}$ and $g_A(i)$ represents a quantized version of $g_A(i)$ with quantization interval being $\Delta$. We note that all of these $g_A(i)$'s are independent of each other. Similar to this process, Bob also has a vector $g_B = [g_B(1), ..., g_B(m)]^T$. Alice randomly divides the typical $g_A$ sequences into non-overlapping bins, with each bin having $2^{\text{var}(x_A, y_B)}$ typical sequences. Each sequence contains two indexes: the bin number and the index within the bin. In the next step, Alice sets the key to the index of the sequence in its bin after observing the vector $g_A$, and then transmits the bin number as a secondary information to Bob over the public channel. In this step, Alice should transmit $H(g_A(1:B))$ bits of information over the public channel. Based on the information observed from the common channel and on $g_B$, Bob can recover the value of $g_A$ with any probability closing to one and then recover the key. Due to the independence of bin number and index within the bin, Eve learns nothing about the key though it can obtain the bin number over public channel. Now, in the limit where the quantization level $\Delta$ tends to zero, one achieves the secret key rate (18). In this place, we should note that the key generated according to this approach can be proved to be uniformly distributed [23], so they are suitable for encryption according to the one-time pad technique.

**4 | COOPERATIVE SECRET KEY GENERATION SCHEME WITH ASSISTANCE OF RELAY NODES**

In this section, we propose a cooperative scheme for secret key generation which increases the secret key rate by utilizing relay nodes in UWNs. The cooperative secret key generation model is shown in Figure 2. Alice and Bob want to agree on a secret key aided by $N$ relay nodes. We assume that all of $N$ relay nodes follow the designed protocols and do not leak information to Eve. The channel gains are $h_1, h_{1:A}, h_{1:B}, ..., h_{N:A}, h_{N:B}$ and the noise in each channel are all Gaussian distributed. For simplicity, we assume the channel gains $h_i \sim \mathcal{N}(0, \sigma^2_i)$, where $h_i$ represents $h_{i:A}$ and $h_{i:B}$ with $i = 1, 2, ..., N$. All other assumptions about the system model are the same with the description in Section 2.

The proposed method can be summarized as three steps: (1) randomness sending, in which Alice, Bob and $R_i$ send random signals $x_A, x_B, x_{R_i}$, respectively, in turn, where $i = 1, 2, ..., N$;
(2) relays sending help information, in which relay node $R_i$ sends help information $b_i = x_{R_i}Y_{R_i,A} \oplus x_{R_i}Y_{R_i,B}$ in turn, where $i = 1, 2, ..., N$, and $\oplus$ denotes the XOR operation; (3) key agreement, in which Alice and Bob agree on a common randomness secret key according to their obtained information using Slepian–Wolf code. Next, we will elaborate on the first two steps.

In the randomness sending step, firstly, Alice transmits a Gaussian random signal $x_A \sim \mathcal{N}(0, \sigma_A^2)$ with power $P_A$ over wireless channel, the received signal of Bob and $R_i$ can be expressed as

$$Y_{R_i,A} = h_{R_i} x_A + N_{R_i,A},$$

$$Y_{R_i,B} = h_{R_i} x_A + N_{R_i,B},$$

respectively, where $i = 1, 2, ..., N$. Similarly, Bob transmits a Gaussian random signal $x_B \sim \mathcal{N}(0, \sigma_B^2)$ with power $P_B$ over wireless channel, the received signal of Alice and $R_i$ can be expressed as

$$Y_{A,R_i} = h_{A} x_B + N_{A,R_i},$$

$$Y_{B,R_i} = h_{B} x_B + N_{B,R_i},$$

respectively. Then relay $R_i$ transmits a Gaussian random signal $x_{R_i} \sim \mathcal{N}(0, \sigma_{R_i}^2)$ with power $P_{R_i}$ in turn; the received signal of Alice and Bob can be expressed as

$$Y_{A,R_i} = h_{A} x_{R_i} + N_{A,R_i},$$

$$Y_{B,R_i} = h_{B} x_{R_i} + N_{B,R_i},$$

respectively. Due to the reciprocity of wireless channels, we have $x_{R_i}Y_{R_i,A} = x_A Y_{A,R_i}$ and $x_{R_i}Y_{R_i,B} = x_B Y_{B,R_i}$. Then Alice and Bob obtain estimations

$$Y_A = x_{R_i} Y_{R_i,B},$$

$$Y_B = x_{R_i} Y_{R_i,A},$$

respectively. After this step, Alice and Bob obtain three sets of correlated information, $(x_A Y_{A,R_i}, x_B Y_{R_i,R_i})$, $(x_A Y_{R_i,B}, x_B Y_{B,R_i})$, and $(x_A Y_{A,R_i}, x_B Y_{R_i,R_i})$. The step of key agreement is similar to that in Section 3 and we do not illustrate here. The resulting cooperative secret key rate is given by

$$R_c = \frac{1}{T} \left\{ \sum_{i=1}^{N} \min\{I(x_{R_i} Y_{R_i,B}; x_B Y_{R_i,R_i}), I(x_A Y_{A,R_i}; x_B Y_{R_i,R_i})\} \right.$$ 

$$+ I(x_A Y_{A,R_i}; x_B Y_{R_i,R_i}) \right\}. \quad (24)$$

5 MODIFIED DEVICE-TO-DEVICE SECRET KEY GENERATION SCHEME OVER CORRELATED CHANNELS

In this section, we investigate a more general and realistic scenario in which the reciprocity of wireless channels is varied while the forward channel gain and backward channel gain are correlated in every coherent time. All other assumptions about the model are the same as that in Section 2. Since the forward channel gain and backward channel gain are no longer equal, the protocol developed above is not applicable. We present a modified secret key generation scheme via layered coding, which is proved to be theoretically optimal. The process of information reconciliation is depicted in Figure 3. The basic principle of the modified scheme is the correlation of error rates of the same symbol at different bit layers [29]. For instance, considering the model where $b^k$ is uniformly distributed on $\{0, 1, ..., g - 1\}$, where $g = 2^k$ for integer $k$, and $P(b_k|b_A)$ is a uniform-error channel (i.e. if $b_R \neq b_A$, $b_R$ takes value in the remaining $2^k - 1$ symbols with equal probabilities). If any symbol errors in one bit layer, then the probability that it errors in the next bit layer is 0.5, and the next bit can be considered as erased [30].
We suppose Alice transmits a signal $x_A$ over the wireless fading channel, then the received signal of Bob can be expressed as
\[ Y_B = h_0 x_A + N_B, \]
where $h_0$ denotes the channel gain from Alice to Bob.

If Bob transmits a signal $x_B$ over the wireless fading channel, the received signal of Alice can be expressed as
\[ Y_A = h_0^* x_B + N_A, \]
where $h_0^*$ denotes the channel gain from Bob to Alice.

In order to obtain common information from received signals, Alice and Bob estimate the channel gain. The channel gain estimation can be expressed as
\[
\begin{align*}
    h_A &= \frac{x_B^T}{||x_B||^2} Y_A, \\
    h_B &= \frac{x_A^T}{||x_A||^2} Y_B,
\end{align*}
\]
respectively, in which $||.||$ denotes the norm of its argument. Then, quantifying $h_A$ and $h_B$ into $h^A \in \{0, 1, \ldots, q-1\}$ and map every symbol $j^A$ to $k$ bits $(b_1, b_2, \ldots, b_k)$. For instance, we may use the unique function $f_{bi}(j) : \{0, 1, \ldots, 2^k-1\} \rightarrow \{0, 1\}^k$ and $f_{bi}(j) = (b_1, b_2, \ldots, b_k)$, where $b = \sum_{j=1}^{k} b_j 2^{j-1}$. Then Alice generates a message $(E_1, E_2, \ldots, E_k)$ by utilizing a binary Slepian–Wolf coding to each bit layer and sends it to Bob. Note that $h_0$ and $h_0^*$ is not equal but $h_A$ and $h_B$ are correlated. Fixing $P_{b_A}$, we can consider $b_A$ as the output signal after transmitting an input signal $b_A$ over wireless channel, which is characterized by the transition law $P(b_B|b_A)$.

Based on the messages transmitted and on $h_A$ and $h_B$, respectively, Alice generates a message $M \in \{0, 1\}^n$ and Bob generates a message $M' \in \{0, 1\}^n$, a Alice and Bob try to make $M = M'$ through information reconciliation and then privacy amplification is applied to extract the secret key, which is the same as conventional ones [31]. The key rate of information reconciliation can be expressed as
\[
R = P(M = M') \frac{H(M|M = M')}{n} - t,
\]
where $t$ represents the number of bits communicated between Alice and Bob.

In the following, we analyze the theoretical limit of achievable key rate of the proposed scheme. Let $t_j$ be the length of the message $E_j$, we assume that for each bit layer, an asymptotically optimal Slepian–Wolf code can be found, then in the limit where the probability that $M = M'$ tends to one and where block length $n$ tends to infinity, the secret key rate is
\[
R = P(h = h) \frac{H(h|h = h)}{n} - \sum_{j=1}^k t_j.
\]
We first have
\[
H(h) \leq H(h|\{h = h_1\}) + 1
\]
\[
\leq P(h_1 = h_1) H(h|h_1 = h_1) + \epsilon kn + 1
\]
\[
\leq H(h_1) + \epsilon kn + 1,
\]
so
\[
H(h|h_1) = h_1 \geq H(h) - \epsilon kn - 1.
\]
If the first $j - 1$ bit layers are decoded successfully, then we have
\[
\lim_{n \rightarrow \infty} \frac{t_j}{H(h_j|h_B, h_1^{j-1})} = 1,
\]
Using the chain rule for entropies, for any positive $\epsilon$, $P(h_j \neq h_j) < \epsilon$, we have
\[
\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^{k} t_j = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^{k} H(h_j|h_B, h_1^{j-1}) = \frac{H(h_A|h_B)}{n}.
\]
Since the sequence $h_A$ and $h_B$ are memoryless, in the limit where block length $n$ tends to infinity, we have
\[
\lim_{n \rightarrow \infty} \frac{H(h_A|h_B)}{n} = H(b_A|b_B).
\]
Letting $n \rightarrow \infty$, we have
\[
R \geq (1 - \epsilon k) \frac{H(h) - \epsilon kn - 1 - \sum_{j=1}^{k} t_j}{n}
\]
\[
= (1 - \epsilon k) H(h_A) - \epsilon k - H(b_A|h_B)
\]
\[
= I(b_A; h_B) - \epsilon k (H(b_A) + 1).
\]
Setting $\epsilon$ arbitrarily small, thus the maximum secret key rate of the modified secret key generation scheme is
\[
R^* = I(b_A; h_B).
\]
That is, the proposed modified secret key generation scheme is theoretically optimal.

## 6 Simulation Results

In this section, we analyze the effects of the key parameters through numerical results and put insights to obtain a higher
key rate via wireless channel reciprocity. Furthermore, the performance of the modified secret key generation scheme based on LDPC codes is also tested.

Figure 4 illustrates the secret key generation rates against $\sigma_i$ with $h_0 = 0.4, 0.6, 0.8$, respectively. In this test, we set $T = 10$, $T_0 = 1$, $\sigma^2 = \sigma_0^2 = 3$, $P_A = P_B = 3$. It is not difficult to find that the secret key generation rate of the MR scheme can be improved with the increase of $\sigma_i$ when other parameters are fixed.

Figure 5 illustrates the secret key generation rates against $h_0$ using the proposed scheme, Xiao’s scheme [26], Lai’s scheme [15], and the conventional scheme without relay nodes. Without loss of generality, we assume $T = 10$, $T_0 = 1$, $\sigma^2 = \sigma_0^2 = \sigma_i^2 = 3$, $P_A = P_B = 3$. We can find that the generated secret key rate of the proposed MR scheme can be improved with the increase of $h_0$, while the secret key rates of the other three schemes do not change with the increase of $h_0$. This is because in the proposed scheme, the effective information in $Y_A$ and $Y_B$ increases with the increase of $h_0$ when other parameters are fixed, and in the other three schemes, the key rates are independent of $h_0$. We can also observe that the proposed scheme outperforms the other two relay schemes when $h_0$ is greater than 0.6. However, the proposed scheme does not require additional relay nodes and reduces hardware overhead.

Figure 6 illustrates the secret key generation rates against $T$ with $T_0 = 1, \sigma^2 = \sigma_0^2 = \sigma_i^2 = 3, P_A = P_B = 3, h_0 = 0.75$. It is obvious that the secret key generation rate of the MR scheme hardly changes with the increase of $T$ while the key rate of the conventional no relay algorithm decreases with the increase of $T$. This is because in the proposed scheme, as $T$ increases, Alice and Bob could send more random signals and thus the correlated information obtained by them increases.

Figure 7 illustrates the cooperative secret key generation rates against the number of relays $N$ using the proposed scheme,
Xiao’s scheme [26] and Lai’s scheme [15]. In this test, we assume $T = 12$, $T_0 = 1$, $\sigma^2 = \sigma_J^2 = \sigma_R^2 = 3$, $P_A = P_B = 3$, $h_0 = 0.78$. It is obvious that the proposed cooperative scheme has a better performance. We can also observe that each line in the diagram has a horizontal segment; this is because when $T = 12$, at most four relay nodes can help the two legitimate nodes in the proposed cooperative scheme and Xiao’s scheme, and at most two relay nodes can help the two legitimate nodes in Lai’s scheme.

Figure 8 shows the performance of the modified secret key generation scheme based on LDPC codes with $q = 32$ and $n = 4500$. We can find a small gap between the key rates of the modified secret key generation scheme and the maximal key rate, since the regular LDPC codes are imperfect. From the point of view of engineering requirements, the modified secret key generation scheme can satisfy the practical application in UWNs.

7 | CONCLUSION

To improve the secret key generation rate and the security of ubiquitous wireless communications networks, we propose a novel multi-randomness (MR) device-to-device secret key generation strategy and develop a novel cooperative communication mechanism aided by relay nodes over quasi-static block fading channels. In the proposed secret key generation scheme, the common randomness between two communication nodes is enhanced by exploiting the two-way random signals, and the generated secret key rate outperforms traditional relay-aided schemes. In addition, we consider the scenario with the reciprocity of wireless channels varied but the forward channel gain and backward channel gain are correlated in the coherent time. In this case, we present a modified secret key generation scheme via layered coding, which is proved to be theoretically optimal. The theoretical analysis and simulation results demonstrate that the proposed scheme outperforms traditional approaches with favourable application prospects in ubiquitous wireless communications networks. In the future work, we will consider the case of the eavesdropping channel and the legitimate channel possessing a certain correlation.

ACKNOWLEDGEMENTS

This work was supported in part by the Natural Science Foundation of Shandong Province under Grant ZR2019MF038, in part by the Open Fund of the National Key Laboratory of Electromagnetic Environment under the Grant 202003006, in part by the Qingdao Science and Technology Project under the Grant 2022XHL, and in part by the Open Fund of State Key Laboratory of Integrated Services Networks under the Grant ISN22-06.

ORCID

Hailiang Xiong https://orcid.org/0000-0002-6489-9495

REFERENCES

1. Xie, H., et al.: Data collection for security measurement in wireless sensor networks: a survey. IEEE Int. Things J. 6(2), 2205–2224 (2019)
2. Afiani, F., Wirawan Suryani, T.: Lightweight and DoS resistant multiuser authentication in wireless sensor networks for smart grid environments. IEEE Access 7, 67107–67122 (2019)
3. Chang, C., Le, H.: A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. IEEE Trans. Wireless Commun. 15(1), 357–366 (2016)
4. Shim, K.: A survey of public-key cryptographic primitives in wireless sensor networks. IEEE Commun. Surv. Tut. 18(1), 577–601 (2016)
5. Kim, D., An, S.: PKC-based DoS attacks-resistant scheme in wireless sensor networks. IEEE Sensors J. 16(8), 2217–2228 (2016)
6. Adekojule, A.A.: A symmetric cryptographic construct for securing wireless sensor network communications. In: Proceedings of the International Wireless Communications and Mobile Computing Conference, Dubrovnik, Croatia, Aug. 2015, pp. 935–940
7. Carliti, M., Steenhaut, K., Braeken, A.: Symmetric-key based security for multicast communication in wireless sensor networks. In: Proceedings of the International Conference on Cloud Computing Technologies and Applications, Brussels, Belgium, Nov. 2018, pp. 1–6
8. Mansour, I., Chalboud, G., Bakhache, B.: Evaluation of a fast symmetric cryptographic algorithm based on the chaos theory for wireless sensor networks. In: Proceedings of IEEE International Conference on Trust, Privacy and Security in Computing and Communications, Liverpool, UK, Jun. 2012, pp. 913–919
9. Chopra, R., Murthy, C.R., Annavajjala, R.: Physical layer security in wireless sensor networks using distributed co-phasing. IEEE Trans. Inf. Forens. Security 14(10), 2662–2675 (2019)
10. Albashier, M.A.M., Abdrazz, A., Ghani, H.A.: Performance analysis of physical layer security over different error correcting codes in wireless sensor networks. In: Proceedings of the International Symposium on Wireless Personal Multimedia Communications, Bali, Indonesia, Dec. 2017, pp. 191–195
11. Moara-Nkwe, K., et al.: A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. IEEE Access 6, 11374–11387 (2018)
12. Zhu, J., Zou, Y., Zheng, B.: Physical-layer security and reliability challenges for industrial wireless sensor networks. IEEE Access 5, 5313–5320 (2017)
13. Zeng, K.: Physical layer key generation in wireless networks: challenges and opportunities. IEEE Commun. Mag. 53(6), 33–39 (2015)
14. Thai, C.D.T., Lee, J., Quoc, T.Q.: Physical-layer secret key generation with colluding untrusted relays. IEEE Trans. Wireless Commun. 15(2), 1517–1530 (2016)
15. Lai, L., Liang, Y., Du, W.: Cooperative key generation in wireless networks. IEEE J. Sel. Areas Commun. 30(8), 1578–1583 (2012)
16. Shimizu, T., Iwai, H., Sasaoka, H.: Physical-layer secret key agreement in two-way wireless relaying systems. IEEE Trans. Inf. Forens. Security 6(3), 650–660 (2011)
17. Chou, T., Draper, S.C., Sayeed, A.M.: Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness. In: Proceeding of the IEEE International Symposium on Information Theory, Austin, USA, Jun. 2010, pp. 2518–2522
18. Ye, C., et al.: Information-theoretically secret key generation for fading wireless channels. IEEE Trans. Inf. Forens. Security 5(2), 240–254 (2010)
19. Wang, Q., Xu, K., Ren, K.: Cooperative secret key generation from phase estimation in narrowband fading channels. IEEE J. Sel. Areas Commun. 30(9), 1666–1674 (2012)
20. Khisti, A.: Interactive secret key generation over reciprocal fading channels. In: Proceedings of Allerton Conference on Communication, Control, and Computing, Monticello, VA, Oct. 2012, pp. 1374–1381
21. Thai, C.D.T., et al.: Secret group-key generation at physical layer for multi-antenna mesh topology. IEEE Trans. Inf. Forens. Security 14(1), 18–33 (2019)
22. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory 39(3), 733–742 (1993)
23. Ahlswede, R., Csiszar, I.: Common randomness in information theory and cryptography. I. Secret sharing. IEEE Trans. Inf. Theory 39(4), 1121–1132 (1993)
24. Zhou, H., Huie, L.M., Lai, L.: Secret key generation in the two-way relay channel with active attackers. IEEE Trans. Inf. Forens. Security 9(3), 476–488 (2014)
25. Wang, C., Wang, H., Xia, X.: Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks. IEEE Trans. Wireless Commun. 14(2), 589–605 (2015)
26. Xiao, S., et al.: High-rate secret key generation aided by multiple relays for internet of things. IET Electr. Lett. 53(17), 1198–1200 (2017)
27. Thai, C.D.T., et al.: Physical-layer secret key generation with untrusted relays. In: Proceedings of IEEE Globecom Workshops, Austin, USA, Dec. 2014, pp. 1385–1390
28. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley, New York (2003)
29. Zhou, H., Wang, L., Wornell, G.: Layered schemes for large-alphabet secret key distribution. In: Proceedings of the Information Theory and Applications Workshop, San Diego, CA, Feb. 2013, pp. 1–10
30. Weidmann, C.: Coding for the q-ary symmetric channel with moderate q. In: Proceedings of the IEEE International Symposium on Information and Theory, Toronto, Canada, Jul. 2008, pp. 2156–2159
31. Bennett, C.H., et al.: Generalized privacy amplification. IEEE Trans. Inf. Theory 41(6), 1915–1923 (1995)