Received June 11, 2018, accepted July 17, 2018, date of publication July 23, 2018, date of current version August 15, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2858282

The Security Network Coding System With Physical Layer Key Generation in Two-Way Relay Networks

YUANYUAN KONG[1,2], **BIN LYU**[1], **FENG CHEN**[3], **AND ZHEN YANG**[1]

[1] Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China
[2] Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[3] Internet of Things Branch, China Telecom Corporation Ltd., Nanjing 210036, China

Corresponding author: Zhen Yang (yangz@njupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grants 61671252 and 61772287, and in part by the project of Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks under Grant WSNLBKF 201802.

ABSTRACT Network coding is one of the key technologies to improve the throughput, efficiency, and reliability of two-way relay networks (TWRNs). However, it also brings some new security problems when the physical layer security is considered. In this paper, we present security network coding schemes with key generation from multipath channels to enhance the security performance for TWRN. First, a joint key generation (JKG) approach is proposed, which generates secret keys based on channel impulse responses of multipath channels. Different from the traditional approaches, key exchange is not necessary for the JKG approach such that the eavesdroppers cannot obtain any information about secret keys. Then, an adaptive quantization algorithm is proposed to adaptively choose different parameters for quantization in key generation, which can improve the secret key rate with an acceptable secret key disagreement probability and can still work even if the SNR is low. Finally, security network coding systems are constructed to combine the key generation approaches with the proposed algorithm. Simulation results show that the proposed schemes are valid and secure against wiretap attacks.

INDEX TERMS Physical layer security, security network coding, channel impulse response, secret key generation.

I. INTRODUCTION

Network coding is a key technology to maximize the information flow in a network [1], a typical application scenario of which is the two-way relay network (TWRN). As shown in Fig. 1, the TWRN includes two wireless nodes (Alice and Bob) which have no direct link but exchange information through a relay node (Relay). Due to the broadcast characteristics of radio propagation, the transmitted signals in TWRN can be received by all legitimate users and illegal users, which make a great security challenge for TWRN, especially when the network coding is applied. To guarantee that the illegal users cannot obtain any information from the legitimate users, security network coding techniques have been proposed [2]–[4]. Recently, most studies about security network coding focus on the classical encryption, which depends on computational security. However, the computational security nature may be cracked by the rapid development of hardware technology. Moreover, the complex key management infrastructure makes the computational security less attractive for the incoming 5G applications.

Recently, physical layer security has attracted a great deal of attention for secure communication. Usually, physical layer security can be classified into two types, i.e., keyless

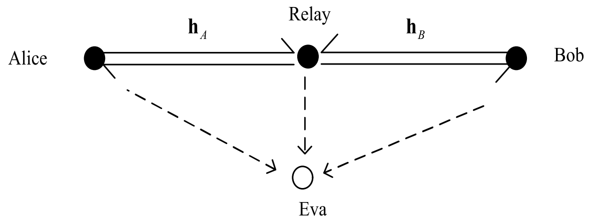

FIGURE 1. The structure of a two-way relay network (TWRN).

security and secret key-based secrecy [5]. The keyless security is achieved by designing transmit coding strategies, such as artificial noise injection [6], beamforming [7], lattice codes [8], and structured interference [9]. In [10], Wang *et al.* proposed a hybrid cooperative beamforming and jamming mechanism for physical layer security of an amplify forward (AF)-TWRN. In [11], Karpuk and Chorti investigated physical layer network coding schemes with embedded perfect secrecy by exploiting structured interference in TWRN. In [12], Forutan and Fischer studied the coset coding applied on the nested lattice codes to achieve information theoretic security in network coding. In [13], Deng *et al.* studied a physical layer security enhancement scheme based on artificial noise in analog network coding systems.

Key generation from wireless channels is a way to achieve the secret-key based secrecy in the physical layer, which exploits the wireless communication medium to develop secret keys over public channels [14]. This is because that wireless channels have the inherent properties of reciprocity, spatial variability and temporal variation [15]. The secret key can be generated from channels based on different features, such as the strength, envelop and phase of the received signal [16]–[18], the channel impulse response (CIR) and channel frequency response (CFR) of channels [19], [20].

For the application of key generation from wireless channels in TWRN systems, the researches mainly focus on the relay-assisted key generation [21], [22]. In TWRN systems shown in Fig. 1, there are no direct channels between two legitimate users (Alice and Bob), and channels between the legitimate users (Alice and Bob) and the relay (Relay) can act as random sources for key generation. Due to channel reciprocity, the channel response from Alice to Relay is the same as the channel response from Relay to Alice, which is denoted as $\boldsymbol{h}_A$. Similarly, the channel response between Bob and Relay is denoted as $\boldsymbol{h}_B$. So Alice and Relay can gain the secret key k_A from $\boldsymbol{h}_A$, Bob and Relay can gain the secret key k_B from $\boldsymbol{h}_B$. For spatial variability, the channel response between legitimate users and Eva is uncorrelated with $\boldsymbol{h}_A$ and $\boldsymbol{h}_B$, so Eva cannot generate the correct secret keys. Through key generation from wireless channels in TWRN systems, Alice can gain k_A but do not know k_B generated by Bob. Generally, the key exchange between Alice and Bob via Relay is required in TWRN. In [21], the exclusive-or (XOR) operation of two secret keys ($k_A \oplus k_B$) was transmitted by Relay such that the secret keys can be exchanged between Alice and Bob. But the XOR operation of two secret keys can also be listened by the illegal user (Eva), which may disclosure some information. Hence, a significant challenge is to reduce the risk of key disclosure during its exchange. In [23], the key generation approach without key exchange was proposed, in which the product of two channel gains (the channel gains between Alice and Relay and between Bob and Relay) can serve as the common randomness for the secret key generation. This approach is suitable for key generation based on the feature of received signals [21]–[23], but not suitable for key generation based on CIRs of multipath channels. Moreover, a secure network coding system with key generation consists of two core phases: key generation phase and information transmission phase. Previous researches mostly focus on the key generation approach in key generation phase, but few on the encryption and decryption process in information transmission phase. Different from the aforementioned works, we build a security network coding TWRN system and concentrate on both key generation approach in key generation phase and data encryption in information transmission phase.

In this paper, we apply the physical layer security technique with key generation based on CIRs of multipath channels in a TWRN system with network coding. A joint key generation (JKG) approach is proposed which performs in key generation phase and applies the convolution of two CIRs to generate secret key. Hence, the information leak for key exchange is avoided, and the legitimate users can get the same secret key naturally during the key generation. Then, we evaluate the secret key capacity of the TWRN system. Furthermore, we propose an adaptive quantization algorithm to adaptively convert different parameters of channels into a sequence of secret key bits. This algorithm can significantly improve the secret key rate, and the performance of which is still acceptable when the SNR is low. Finally, we construct a security network coding scheme with data encryption using secret keys generated from channels, which combines key generation from channels with network coding.

The rest of this paper is organized as follows. In Section II, we introduce two classical key generation approaches, and then propose a joint key generation approach. In Section III, we evaluate and compare the secret key capacity of three key generation approaches. In Section IV, we propose the adaptive quantization algorithm of key generation based on CIRs. In Section V, we construct two security schemes which combine network coding system with key generation. In section VI, we present simulation results to validate our models and algorithms. In section VII, we conclude this paper.

II. KEY GENERATION APPROACH

The classical procedure of key generation from channels includes four steps: channel probing, quantization, reconciliation, and privacy amplification [19], which perform in key generation phase. First, the channel state information (CSI) is estimated during the channel probing step. Then, the obtained CSI is converted to binary bit sequences during the quantization step. Reconciliation and privacy amplification are performed to reconcile bit discrepancies and improve the randomness of the generated keys [15]. In this paper, we concentrate on the first two steps. The key generation approaches performed during the channel probing step are studied in this section, and the quantization method performed during the quantization step will be studied in section IV.

The correct key generation is based on the accuracy of the estimated CSI. The channel impulse response (CIR) and channel frequency response (CFR) are two kinds of CSI, here we use the channel impulse response (CIR) to generate secret keys. There are two classical key generation approaches used in relay-assisted key generation, i.e., single key generation (SKG) approach [24] and concatenation single key generation (CSKG) approach [21], which are introduced as follows.

A. CLASSICAL KEY GENERATION APPROACH

A classical key generation approach is shown in Fig. 2, which adopts network coding to exchange the keys generated from channels over Relay. The total procedure is done during four time slots. In the 1st time slot, Alice first sends a known training sequence to Relay, then Relay gains $\boldsymbol{h}_{AR}$ via channel estimation and distills k_A from $\boldsymbol{h}_{AR}$, where $\boldsymbol{h}_{AR}$ is the estimated CIR from Alice to Relay. In the 2nd time slot, Bob sends a known training sequence to Relay and Relay gains $\boldsymbol{h}_{BR}$ to generate the key k_B , where $\boldsymbol{h}_{BR}$ is the estimated CIR from Bob to Relay. We assume the channel estimation is perfect such that $\boldsymbol{h}_{AR} = \boldsymbol{h}_{RA} = \boldsymbol{h}_A$ and $\boldsymbol{h}_{BR} = \boldsymbol{h}_{RB} = \boldsymbol{h}_B$, where $\boldsymbol{h}_{RA}$ is the estimated CIR from Relay to Alice, and $\boldsymbol{h}_{RB}$ is the estimated CIR from Relay to Bob. During the first two time slots, the key generation is finished at Relay. In the 3rd time slot, Relay sends a known training sequence to Alice and Bob, Alice (Bob) gains $\boldsymbol{h}_{RA}$ ($\boldsymbol{h}_{RB}$) via channel estimation and distills k_A (k_B). In the 4th time slot, network coding is adopted at Relay with a simple XOR operation $k_A \oplus k_B$. Alice can gain k_B from $k_A \oplus k_B$ received in the 4th time slot since k_A is obtained in the 3rd time slot. Bob gains k_A as the same way. Finally, the key generation and exchange between Alice and Bob can be achieved during the four time slots. However, during the 4th time slot, $k_A \oplus k_B$ can also be obtained by eavesdroppers. Hence, for the SKG approach, Alice and Bob use the generated keys k_A and k_B respectively. But the lengths of k_A and k_B may be not the same, which causes that some bits of the longer key will be discarded. To overcome this limitation, the CSKG approach is proposed in [21] where Alice and Bob use the same key concatenating k_A and k_B. Generally, the key rate of the CSKG approach is larger than that of the SKG approach.

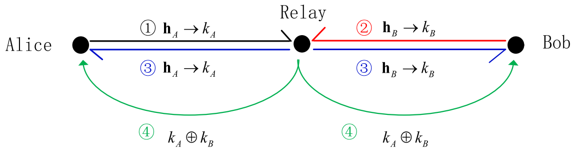

FIGURE 2. Classical key generation approach.

As stated that the exchange of secret keys of the SKG and CSKG approaches may disclosure some information. To address this problem, we propose a new key generation approach called joint key generation (JKG) approach to avoid key exchange.

B. PROPOSED KEY GENERATION APPROACH

As shown in Fig. 3, the proposed JKG approach uses the convolution of estimated CIRs to generate secret keys. Hence, the legitimate users can get the same secret key without key exchange. The total procedure includes four steps, each of which corresponds to a time slot.

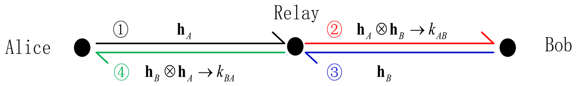
Alice
Relay
Bob
① $\mathbf{h}_A$
② $\mathbf{h}_A \otimes \mathbf{h}_B \to k_{AB}$
③ $\mathbf{h}_B$
④ $\mathbf{h}_B \otimes \mathbf{h}_A \to k_{BA}$

FIGURE 3. The proposed JKG approach.

In the 1st time slot, Alice sends a known training sequence to Relay. While in the 2nd time slot, Relay sends the received signal from Alice to Bob directly. Bob thus gains $\boldsymbol{h}_{AR} \otimes \boldsymbol{h}_{RB}$ via channel estimation and then obtains the secret key k_{AB}. Similarly, Alice can gain $\boldsymbol{h}_{BR} \otimes \boldsymbol{h}_{RA}$ and obtain the secret key k_{BA} during the 3rd and 4th time slots. Assume that the channel estimation is perfect, thus have $\boldsymbol{h}_{AR} \otimes \boldsymbol{h}_{RB} = \boldsymbol{h}_A \otimes \boldsymbol{h}_B$, and $\boldsymbol{h}_{BR} \otimes \boldsymbol{h}_{RA} = \boldsymbol{h}_B \otimes \boldsymbol{h}_A$. Since $\boldsymbol{h}_A \otimes \boldsymbol{h}_B = \boldsymbol{h}_B \otimes \boldsymbol{h}_A$, we obtain that $k_{AB} = k_{BA}$ where k_{BA} and k_{AB} are generated by Alice and Bob respectively. It is obvious that Alice and Bob can generate the same secret keys without key exchange, due to which the eavesdroppers cannot gain any information about the generated secret keys. Hence, the security performance of the proposed JKG approach is superior to that of the classical approaches.

III. SECRET KEY CAPACITY

In this section, we evaluate the secret key capacity of the proposed JKG approach. First, we give the preliminaries according to [25], [26]. Then, we give the expressions of secret key capacity based on the preliminaries.

The preliminaries are given as follows. Denote the L-path fading channel between node X and node Y as H , where the average power of each path is given as p_l . Then, the channel observations of node X and node Y are given by $H_X = H + Z_X$ and $H_Y = H + Z_Y$, respectively, where Z_X and Z_Y serve as noises corrupting the channel observations at X and Y, respectively, $Z_X \sim CN(0, \sigma_X^2)$ and $Z_y \sim CN(0, \sigma_Y^2)$. If $L = 1$, i.e. , one-path fading channel case, the mutual information between H_X and H_Y according to [25] is given by

$$I(H_X; H_Y) = \log_2(1 + \frac{p_1}{\sigma_X^2 + \sigma_Y^2 + \frac{\sigma_X^2 \sigma_Y^2}{p_1}}). \tag{1}$$

For simplicity, we consider the case that $\sigma_X^2 = \sigma_Y^2 = \sigma^2$. When the observed channel is a L-path fading channel ($L > 1$), from Eq. (1), the mutual information between CIR observations on the l-th path is

$$C_l = \log_2(1 + \frac{p_l}{2\sigma^2 + \frac{\sigma^4}{p_l}}). \tag{2}$$

Based on Eq. (2), we then compute the mutual information for the multipath channel case, for which it is difficult to obtain a closed-form expression. However, an upper bound can be derived according to [26], which is given by

$$I(H_X; H_Y) \leq \sum_{l=1}^{L} \log_2(1 + \frac{p_l}{2\sigma^2 + \frac{\sigma^4}{p_l}}). \tag{3}$$

Based on the above preliminaries, we then compute the secret key capacity. Note that in the sequel of this paper, we use the upper bound of mutual information to express the secret key capacity directly. Let L_A be the length of $\boldsymbol{h}_A$ and L_B be the length of $\boldsymbol{h}_B$. Denote the power of each path of $\boldsymbol{h}_A$ and $\boldsymbol{h}_B$ as $p_{A,l}$ and $p_{B,l}$ respectively. The relative path power of $\boldsymbol{h}_A$ and $\boldsymbol{h}_B$ is thus expressed as $(\bar{p}_{A,1}, \cdots, \bar{p}_{A,L})$ and $(\bar{p}_{B,1}, \cdots, \bar{p}_{B,L})$, where $\bar{p}_{A,l} = \frac{p_{A,l}}{p_{A,1}}$ and $\bar{p}_{B,l} = \frac{p_{B,l}}{p_{B,1}}$. The noise power is denoted as σ^2 .

Denote $L = \min(L_A, L_B)$. To evaluate the key capacity of the SKG approach, we take the case that $L = L_A$ as the example. From Eq. (3) , the key capacity of the SKG approach is given by

$$C_{\mathrm{SKG}} = \sum_{l=1}^{L} \log_2\Big(1 + \frac{\gamma_A \bar{p}_{A,l}}{2 + \frac{1}{\gamma_A \bar{p}_{A,l}}}\Big), \qquad (4)$$

where $\gamma_A = \frac{p_{A,1}}{\sigma^2}$ is the signal to noise ratio for the reference path. Then, the secret key capacity of CSKG is given by

$$\begin{aligned} C_{\mathrm{CSKG}} = &\sum_{l=1}^{L_A} \log_2\Big(1 + \frac{\gamma_A \bar{p}_{A,l}}{2 + \frac{1}{\gamma_A \bar{p}_{A,l}}}\Big) \\ &+ \sum_{l=1}^{L_B} \log_2\Big(1 + \frac{\gamma_B \bar{p}_{B,l}}{2 + \frac{1}{\gamma_B \bar{p}_{B,l}}}\Big), \qquad (5) \end{aligned}$$

where $\gamma_B = \frac{p_{B,1}}{\sigma^2}$ is the signal to noise ratio for the reference path. Finally, the key capacity of JKG is

$$C_{\mathrm{JKG}} = \sum_{l=1}^{L_A+L_B-1} \log_2\Big(1 + \frac{\gamma_{A\otimes B} \bar{p}_{A\otimes B,l}}{2 + \frac{1}{\gamma_{A\otimes B} \bar{p}_{A\otimes B,l}}}\Big), \qquad (6)$$

where $\otimes$ denotes convolution operation, $L_A + L_B - 1$ is the length of $\boldsymbol{h}_A \otimes \boldsymbol{h}_B$, $p_{A\otimes B,l}$ is the power of each path of $\boldsymbol{h}_A \otimes \boldsymbol{h}_B$, $(\bar{p}_{A\otimes B,1}, \cdots, \bar{p}_{A\otimes B,L_A+L_B-1})$ is the relative path power of $\boldsymbol{h}_A \otimes \boldsymbol{h}_B$ with $\bar{p}_{A\otimes B,l} = \frac{p_{A\otimes B,l}}{p_{A\otimes B,1}}$, and $\gamma_{A\otimes B} = \frac{p_{A\otimes B,1}}{\sigma^2}$ is the signal to noise ratio for the reference path.

We assume that $\boldsymbol{h}_A$ is a WG4 Case3 channel, which has four paths with relative average power $\{0\ -3.0\ -6.0\ -9.0\}$ (dB), and $\boldsymbol{h}_B$ is an ITU PA3 channel, which also has four paths with relative average power $\{0\ -9.7\ -19.2\ -22.8\}$ (dB). Under these parameters, the secret key capacity of three key generation approaches (SKG, CSKG and JKG) is shown in Fig. 4. From Fig. 4, we know that when the SNR is small ($\leq$ 15 dB), the performances of the JKG approach and the CSKG approach are mostly the same. As the SNR increases, the secret key gap between the CSKG approach and the JKG approach becomes larger. But the secret key of the JKG approach is always larger than that of the SKG approach. Compared with the CSKG approach, the proposed JKG may depress the secret key capacity but the key exchange is avoided to reduce the risk of key disclosure.

IV. PROPOSED ADAPTIVE QUANTIZATION ALGORITHM

The classical procedure for key generation from channels includes four steps: channel probing, quantization, reconciliation and privacy amplification. The CIRs are extracted during channel probing. Quantization is typically used to convert the extracted values into bits. Let $q = \log_2 Q$, where q is the number of quantization bits and Q is the number of quantization levels. The key rate in term of bits per channel observation increases as q increases. Many parameters about CIRs can be used for quantization. In the following subsections, we present three quantization methods with different parameters for key generation.

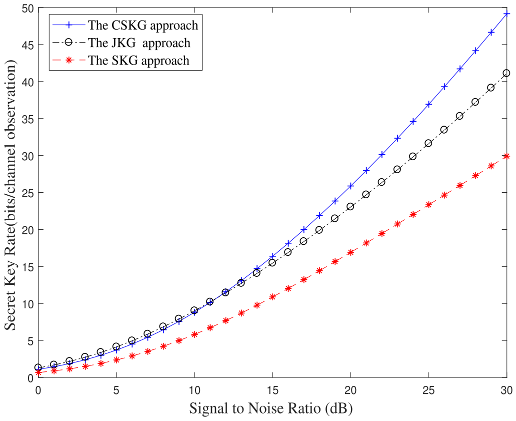

FIGURE 4. The secret key capacity of three key generation approaches.

A. QA1 METHOD

We first present the QA1 method, where the in-phase component $\mathrm{Re}(h_l)$ and the quadrature component $\mathrm{Im}(h_l)$ are separately quantized. With this method, the secret key rate of the SKG approach is given by

$$R_{1\mathrm{SKG}} = \begin{cases} 2L_A q, & \text{if } L_A \leq L_B, \\ 2L_B q, & \text{if } L_A > L_B, \end{cases} \qquad (7)$$

the secret key rate of the CSKG approach is given by

$$R_{1\mathrm{CSKG}} = 2(L_A + L_B)q, \qquad (8)$$

and the secret key rate of the JKG approach is given by

$$R_{1\mathrm{JKG}} = 2(L_A + L_B - 1)q. \qquad (9)$$

B. QA2 METHOD

We then introduce the QA2 method, which quantizes the average power of each path $\|h_l\|^2$. The secret key rates for the SKG approach, the CSKG approach, and the JKG approach with QA2 are denoted as $R_{2\mathrm{SKG}}$, $R_{2\mathrm{CSKG}}$, and $R_{2\mathrm{JKG}}$, which are respectively given by

$$R_{2\mathrm{SKG}} = \begin{cases} L_A q, & \text{if } L_A \leq L_B, \\ L_B q, & \text{if } L_A > L_B, \end{cases} \qquad (10)$$

$$R_{2\mathrm{CSKG}} = (L_A + L_B)q, \qquad (11)$$

$$R_{2\mathrm{JKG}} = (L_A + L_B - 1)q. \qquad (12)$$

C. QA3 METHOD

Finally, the QA3 method is presented, which quantizes the average power of channel $\bar{p} = \frac{1}{L}\sum_{l=1}^{L} p_l$. Denote the secret key rate for the SKG approach, the CSKG approach, and the JKG approach with QA3 as $R_{3\text{SKG}}$, $R_{3\text{CSKG}}$, and $R_{3\text{JKG}}$, which are respectively given by

$$R_{3\text{SKG}} = q, \tag{13}$$

$$R_{3\text{CSKG}} = 2q, \tag{14}$$

$$R_{3\text{JKG}} = q. \tag{15}$$

Note that the secret key capacity is an upper bound of the secret key rate. Hence, the choice of q should satisfy this constraint. Under this constraint, we then find the optimal number of quantization bis. The optimization problem is formulated as follows.

$$\begin{aligned} &\max_{q,\ q\in\mathcal{N}} \ R(q) \\ &\text{s.t. } R(q) < C, \end{aligned} \tag{16}$$

where q is an integer, R is the secret rate showed in Eqs. (7)-(15), C is the approximate key capacity showed in Eqs. (4)-(6). Denote the optimal solution for Eq. 16 as q^*.

Besides the secret key rate, the secret key disagreement probability is another important factor of secret keys. Due to asymmetrical channel probing and noise, there is a certain deviation between channel parameters obtained by both pairs. This deviation will lead to disagreement between secret keys generated separately by both pairs. The size of deviation is proportional to the number of quantization bits and the noise power. That is to say, as the number of quantization bits or the noise power increases, the secret key disagreement probability increases. The effect of number of quantization bits and the noise power (SNR) on the secret key disagreement is shown in Fig. 5.

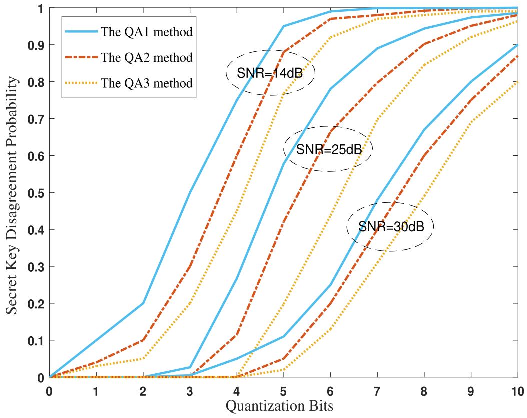

FIGURE 5. The secret key disagreement probability versus quantization bits.

From Fig. 5, we know that with a given SNR, the secret key disagreement probability of the QA3 method is lowest and of the QA1 method is highest. It is because that the average power of all channel paths quantized by the QA3 method and the average power of each channel path quantized by the QA2 method are statistical characteristics of channels and less sensitive to Gaussian noise (including channel estimation error) than the in-phase component and the quadrature component quantized in the QA1 method. Moreover, since the QA3 method uses the average power of all channel paths, which are more robust than the QA2 method. Furthermore, as the SNR increases, the secret key disagreement probability for each quantization scheme reduces. From Eqs. (7)-(15), we know that the secret key rate is an linear function with respect to the number of quantization bits. Given q, it is obvious that the secret key rate of the QA1 method is largest and of the QA3 method is smallest. Hence, the tradeoff between the secret key rate and the secret key disagreement should be considered for the quantization methods. To address this issue, an adaptive quantization algorithm is proposed, which is summarized in Algorithm 1. The basic idea of Algorithm 1 is to maximize the secret key rate with the minimal number of quantization bits. Hence, we first use the QA1 method, then the QA2 method, and finally the QA3 method.

Algorithm 1 Algorithm for the Adaptive Quantization

- **Step 1**: Derive secret key capacity by Eqs. (4)-(6).
- **Step 2**: Find q^* by Eq. (16), where the secret key rate R is derived by Eqs. (7)-(9). If $q^* > 0$, choose QA1 to generate secret keys. Otherwise, go to Step 3.
- **Step 3**: Find q^* by Eq. (16), where the secret key rate R is derived by Eq. (10)-(12). If $q^* > 0$, choose QA2 to generate secret keys. Otherwise, go to Step 4.
- **Step 4**: Find q^* by Eq. (16), where the secret key rate R is derived by Eq.(13)-(15). If $q^* > 0$, choose QA3 to generate secret keys. Otherwise, key generation is failed.

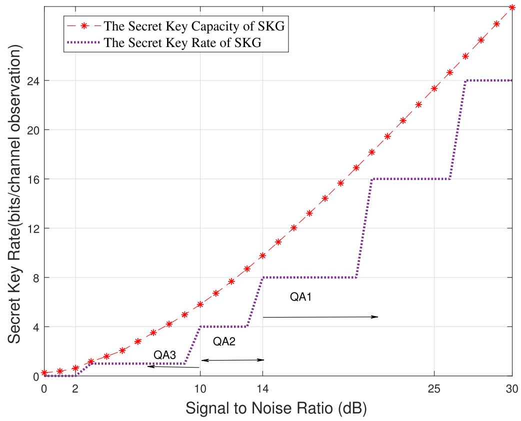

FIGURE 6. The secret key rate of the SKG approach.

Using the proposed adaptive quantization algorithm, the secret key rates of the SKG approach, the CSKG approach, and the JKG approach are shown in Fig. 6, Fig. 7, and Fig. 8, respectively. We take the results shown in Fig. 8 to discuss the proposed algorithm. In Fig. 8, when the SNR is not smaller than 14 dB, the QA1 method is chosen for quantization. When the SNR is larger than 10 dB and smaller than 14 dB, the QA2 method is used to quantize the average power of each path into bits. When SNR is not larger than

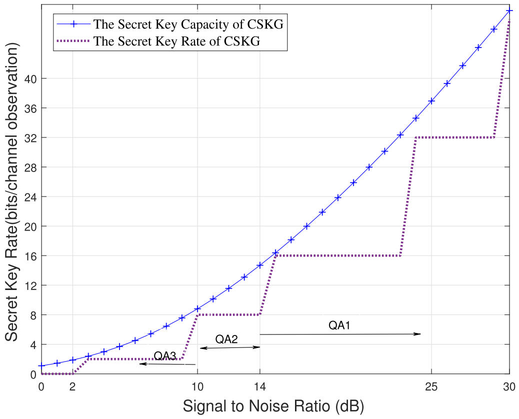

FIGURE 7. The secret key rate of the CSKG approach.

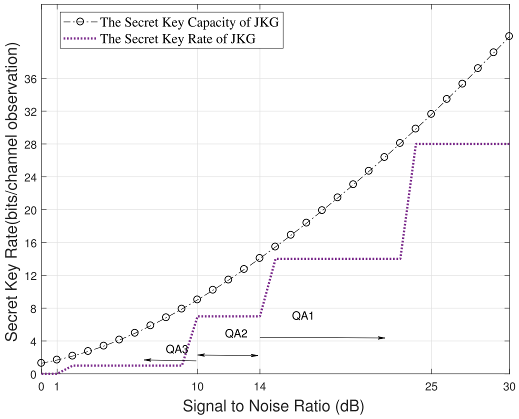

FIGURE 8. The secret key rate of the JKG approach.

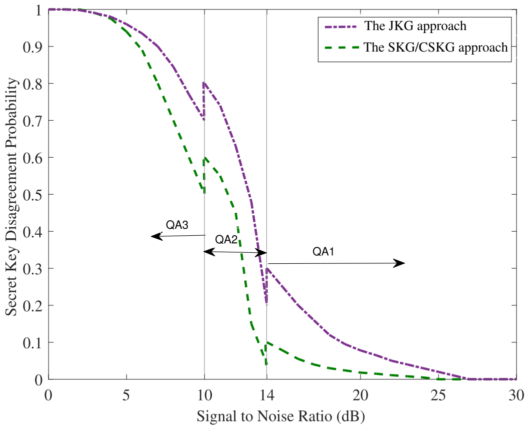

FIGURE 9. The comparison of secret key disagreement probabilities versus SNR.

10 dB, the QA3 method is chosen to quantize the average power of all channel paths into bits.

Using the proposed adaptive quantization algorithm, the secret key disagreement probabilities of the SKG/CSKG approach and the JKG approach are shown in Fig. 9. It can be observed that as the SNR increases, the QA3 method, the QA2 method, and the QA1 method are sequentially taken to quantize bits. Moreover, the secret key disagreement probability of the JKG approach is higher than that of the SKG/CSKG approach. It is because that the amplify-and-forward relay scheme is adopted for the JKG approach such that the noise power is also amplified.

We then compare the proposed algorithm with the existing quantization algorithms that only one of the three quantization methods mentioned above is used with all SNR. If only the QA1 method is used, the secret key rate of the JKG approach is equal to zero when the SNR is smaller than 14 dB as shown in Fig. 8 If only the QA2 method is used, the secret key rate of the JKG approach is equal to zero when the SNR is smaller than 10 dB as shown in Fig. 8, and the secret key disagreement probability for the QA2 method is 0.1 while for the proposed algorithm is equal to zero when the SNR is equal to 25 dB as shown in Fig. 5. If only the QA3 method is used, the secret key rate of the JKG approach is equal to zero when the SNR is smaller than 1 dB, but the secret key disagreement probability for the QA3 method is approximately equal to 1, while for the proposed algorithm is equal to zero when the SNR is equal to 25 dB as shown in Fig. 5.

In conclusion, Algorithm 1 is proposed to choose one of the three quantization methods adaptively with optimal performance, which can improve the secret key rate with an acceptable secret key disagreement probability and can still work even if the SNR is low.

Remark 1: In this paper, we assume that the perfect CSIs are available at the legitimate users and relay. However, it is difficult to obtain the perfect CSIs in practice. If the imperfect CSIs are used, the QA1 method fails to quantize bits, but the QA2 and QA3 method still work since they use the statistical characteristics of channels. Hence, the proposed algorithm still works for the imperfect CSIs scenario.

V. SECURE SCHEMES

After generating secret key during the key generation phase, we then turn to the information transmission phase, where useful information is first encrypted, then transmitted, and finally decrypted. In a TWRN system with network coding, we consider two network coding schemes at Relay, i.e., straight forward network coding (SFNC) scheme and the physical layer network coding (PLNC) scheme, based on which we build two security network coding systems with secret key generated from CIRs.

A. SECURITY SCHEME IN SFNC SYSTEM

We first introduce the security SFNC system, which is shown in Fig. 10. In this system, three time slots are required to achieve security SFNC. The details are given as follows.

In the 1st time slot (black line), the bits $\boldsymbol{s}_A$ from Alice are first encrypted by the secret keys generated from CIRs based the approaches introduced in Section II. $E_{K_A}(\bullet)$ denotes encryption algorithms. The encrypted bits $\boldsymbol{c}_A$ are then modulated to $\boldsymbol{x}_A$, which are transmitted to Relay through wireless channel $\boldsymbol{h}_A$. Finally, Relay obtain the encrypted bits $\boldsymbol{c}_A$ after channel equalization and demodulation sequentially. In the

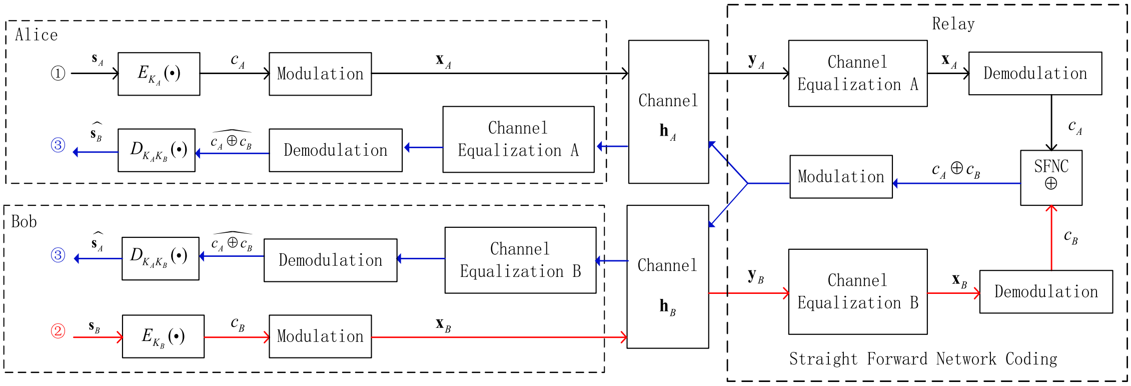

FIGURE 10. The straight-forward network coding (SFNC) system encrypted by secret key from channels.

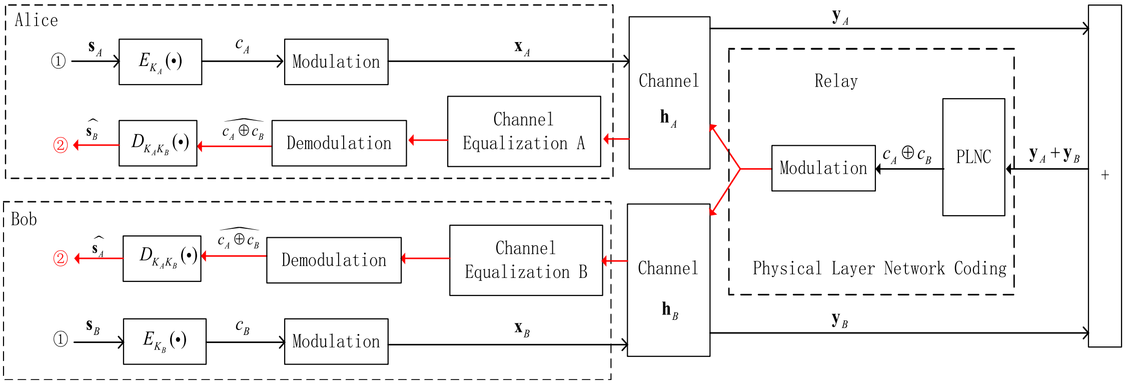

FIGURE 11. The physical layer network coding (PLNC) system encrypted by secret key from channels.

2nd time slot (red line), Relay receives the bits c_B, which are the encryption of transmitted bits from Bob. In the 3rd time slot (blue line), Relay first modulates $\boldsymbol{c}_A \oplus \boldsymbol{c}_B$ and transmits the modulated signals to both Alice and Bob. Alice and Bob gain $\widehat{\boldsymbol{c}_A \oplus \boldsymbol{c}_B}$ after channel equalization and demodulation, respectively. Then, Alice obtains $\widehat{c_B}$ with the XOR operation of $\widehat{\boldsymbol{c}_A \oplus \boldsymbol{c}_B}$ and $\boldsymbol{c}_A$, which is described as follows

$$\widehat{\boldsymbol{c}_A \oplus \boldsymbol{c}_B} \oplus \boldsymbol{c}_A = \widehat{c_B}, \tag{17}$$

and Bob obtains $\widehat{\boldsymbol{c}_A}$ with the XOR operation of $\widehat{\boldsymbol{c}_A \oplus \boldsymbol{c}_B}$ and $\boldsymbol{c}_B$, which is described as follows

$$\widehat{\boldsymbol{c}_A \oplus \boldsymbol{c}_B} \oplus \boldsymbol{c}_B = \widehat{\boldsymbol{c}_A}. \tag{18}$$

Finally, Alice decrypts $\widehat{c_B}$ with K_B to gain $\widehat{s_B}$ and Bob decrypts $\widehat{c_A}$ with K_A to gain $\widehat{s_A}$.

B. SECURITY SCHEME IN PLNC SYSTEM

We then introduce the security PLNC system, which is shown in Fig. 11. In this system, the security PLNC is achieved during only two time slots. In the 1st time slot (black line), Alice and Bob send their own signals to Relay simultaneously. Relay first receives a superimposition of signals $\boldsymbol{y}_A$ and $\boldsymbol{y}_B$, i.e., $\boldsymbol{y}_A + \boldsymbol{y}_B$, and then obtain $\boldsymbol{c}_A \oplus \boldsymbol{c}_B$ via PLNC algorithms. In the 2nd time slot (red line), Relay modulates $\boldsymbol{c}_A \oplus \boldsymbol{c}_B$ and transmits the modulated signals to both Alice and Bob, then Alice obtains $\boldsymbol{s}_B$ and Bob obtains $\boldsymbol{s}_A$ after some operations as described in the 3rd time slot of the security SFNC system.

Note that Relay in the PLNC system does not decode its received signals from Alice and Bob and directly maps the combined signals into network-coded symbols. For more details, please refer to [28], [29].

C. THE CHOICE OF ENCRYPTION ALGORITHMS

In the subsection, we briefly discuss the encryption algorithm used in the security SFNC system and the security PLNC system. Since the three parts share the same secret keys, we only discuss the symmetric key cryptography algorithms. It is know that the XOR operation is a simple encryption algorithm. However, the XOR operation cannot be applied in both the security SFNC system and the security PLNC system, since the unencrypted information may be gained by the eavesdroppers. Fortunately, some symmetric encryption algorithms with high-complexity, e.g., DES, AES, and RC2, can be used in the proposed security systems. In this paper, we use DES as the encryption algorithm in [30].

VI. SIMULATION RESULTS

In this section, we present simulation results and analysis. To simplify the descriptions, the SFNC system with the SKG approach, the PLNC system with the SKG approach,

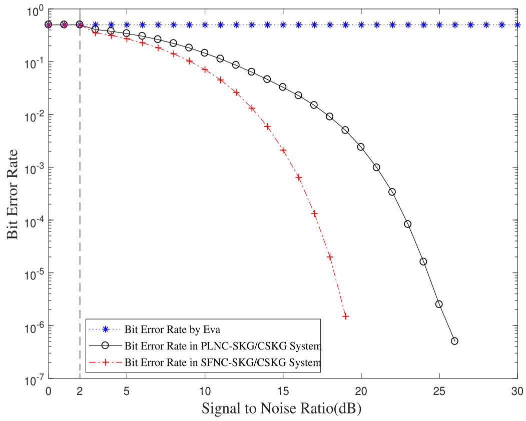

FIGURE 12. The BER performances in SFNC-SKG/CSKG and PLNC-SKG/CSKG system.

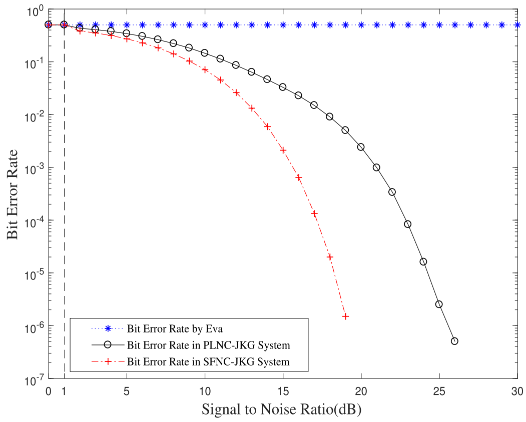

FIGURE 13. The BER performances in SFNC-JKG and PLNC-JKG system.

the SFNC system with the CSKG approach, the PLNC system with the CSKG approach, the SFNC system with the JKG approach, and the PLNC system with the JKG approach are termed as SFNC-SKG, PLNC-SKG, SFNC-CSKG, PLNC-CSKG, SFNC-JKG, and PLNC-JKG, respectively. The simulation parameters are given as follows. $\boldsymbol{h}_A$ is a WG4 Case3 channel, the relative average path power of which is given by $\{0\ -3.0\ -6.0\ -9.0\}$ (dB). $\boldsymbol{h}_B$ is an ITU PA3 channel, the relative average path power of which is given by $\{0\ -3.0\ -6.0\ -9.0\}$ (dB). We take Algorithm 1 for secret key generation, QPSK for modulation adopted, and DES for encryption.

We investigate the effect of SNR on bit error rate (BER) for different systems, which are shown in Fig. 12, and Fig. 13, From the two figures, we have the following observations. The first one is that the BER of the security SFNC system is lower than that of the security PLNC system. The second one is that Eva fails to eavesdrop since the BER achieved by Eva is approximately equal to 0.5. The third one is that Alice and Bob can only communication with each other in security when the SNR is larger than some thresholds, which are 2 dB for the SKG approach or CSKG approach, and 1 dB for the JKG approach.

VII. CONCLUSION

In this paper, we have investigated security network coding schemes with key generation from multipath channels in TWRNs. First, we have designed the JKG approach to generate secret key without key exchange. Then, we have proposed an adaptive quantization algorithm to adaptively choose the quantization method in key generation. Finally, we have constructed the security network coding systems, which integrate the key generation approaches with the proposed algorithm. In future work, we will use the CFR of channels to generate secret key.

REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[2] Y. Jiang, H. Zhu, M. Shi, X. Shen, and C. Lin, "An efficient dynamic-identity based signature scheme for secure network coding," *Comput. Netw.*, vol. 54, no. 1, pp. 28–40, 2010.

[3] N. Cai and T. Chan, "Theory of secure network coding," *Proc. IEEE*, vol. 99, no. 3, pp. 421–437, Mar. 2011.

[4] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.

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

[6] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xiaobo, "Artificial-noise-aided secure multicast precoding for directional modulation systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6658–6662, Jul. 2018.

[7] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[8] C. Ling, "Achieving capacity and security in wireless communications with lattice codes," in *Proc. 9th Int. Symp. Turbo Codes Iterative Inf. Process.*, Sep. 2016, pp. 171–175.

[9] X. He and A. Yener, "Strong secrecy and reliable byzantine detection in the presence of an untrusted relay," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 177–192, Jan. 2013.

[10] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[11] D. A. Karpuk and A. Chorti, "Perfect secrecy in physical-layer network coding systems from structured interference," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1875–1887, Aug. 2016.

[12] V. Forutan and R. F. H. Fischer, "On the security of lattice-based physical-layer network coding against wiretap attacks," in *Proc. 10th Int. ITG Conf. Syst., Commun. Coding*, Feb. 2015, pp. 1–6.

[13] D. Deng, Z.-L. Yang, and M. Zhao, "PHY security enhancement in analog network coding based on artificial noise," in *Proc. 6th Int. Conf. Wireless Commun. Signal Process.*, Oct. 2014, pp. 1–6.

[14] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[15] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Netw.*, vol. 21, no. 6, pp. 1835–1846, Mar. 2015.

[16] Z. Li, H. Wang, and H. Fang, "Group-based cooperation on symmetric key generation for wireless body area networks," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1955–1963, Dec. 2017.

[17] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

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

[19] M. Bulenok, I. Tunaru, L. Biard, B. Denis, and B. Uguen, "Experimental channel-based secret key generation with integrated ultra wideband devices," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun.*, Sep. 2016, pp. 888–893.

[20] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 3048–3056.

[21] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[22] H. Zhou, L. Huie, and L. F. Lai, "Key generation in two-way relay wireless channels," in *Proc. 47th Annu. Conf. Inf. Sci. Syst.*, Mar. 2013, pp. 1–6.

[23] R. Guillaume, S. Ludwig, A. Müller, and A. Czylwik, "Secret key generation from static channels with untrusted relays," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun.*, Oct. 2015, pp. 635–642.

[24] F. He, W. Wang, X. Xu, L. Zhou, and H. Man, "A network coding method for channel signatures based key distribution," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2012, pp. 5036–5041.

[25] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2593–2597.

[26] C. Ye, A. Reznik, G. Sternburg, and Y. Shah, "On the secrecy capabilities of ITU channels," in *Proc. IEEE 66th Veh. Technol. Conf.*, Sep./Oct. 2007, pp. 2030–2034.

[27] J. Cui, G. Dong, H. Li, and G. Feng, "Prospect of application of physical layer network coding in deep space communication," in *Proc. IEEE Int. Conf. Online Anal. Comput. Sci.*, May 2016, pp. 131–134.

[28] G. Bartoli, R. Fantacci, D. Marabissi, and R. Simoni, "Physical layer network coding in multipath channel: Effective precoding-based transmission scheme," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2011, pp. 1–5.

[29] H. Zhang, L. Zheng, and L. Cai, "Design and analysis of hierarchical physical layer network coding," *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 7966–7981, Dec. 2017.

[30] H. Tang, Q. T. Sun, X. Yang, and K. Long, "A network coding and DES based dynamic encryption scheme for moving target defense," *IEEE Access*, vol. 6, pp. 26059–26068, 2018.

YUANYUAN KONG received the B.E. degree in communication and information system from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2007, where she is currently pursuing the Ph.D. degree in signal and information processing. Her research interests span the areas of security communication, network coding, and cooperation communication.

BIN LYU received the B.E. degree in electronic and information engineering and the Ph.D. degree in signal and information processing from the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China, in 2013 and 2018, respectively. He is currently a Lecturer with NUPT. His research interests include wireless power transfer and backscatter communication.

FENG CHEN received the B.E. degree in communication and information system from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2007. He is currently an Engineer with the Internet of Things Branch, China Telecom Corporation Ltd. His research interests span the areas of security communication and Internet of Things.

ZHEN YANG received the B.E. and M.E. degrees from the Nanjing University of Posts and Telecommunications, China, in 1983 and 1988, respectively, and the Ph.D. degree from Shanghai Jiao Tong University, China, in 1999, all in electrical engineering. Initially, he was a Lecturer with the Nanjing University of Posts and Telecommunications in 1983, where he was promoted to an Associate Professor in 1995 and then a Full Professor in 2000. He was a Visiting Scholar with Bremen University, Germany, from 1992 to1993, and an Exchange Scholar with Maryland University, USA, in 2003. He has published over 200 papers in academic journals and conferences. His research interests include various aspects of signal processing and communication, such as communication systems and networks, cognitive radio, spectrum sensing, speech and audio processing, and compressive sensing and wireless communication. He is currently a fellow of the Chinese Institute of Communications, the Vice Chairman of the Chinese Institute of Communications, and the Vice Director of the Editorial Board of the *Journal of Communications*. He was the Chairman of the Jiangsu Institute of Communications from 2010 to 2015, and the Chair of Asia-Pacific Conference on Communications Steering Committee from 2013 to 2014.