IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 17, 2019, accepted February 28, 2019, date of publication March 5, 2019, date of current version April 1, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2903253

Secure Communications in Cooperative D2D Networks by Jointing Wyner's Code and Network Coding

HONGLIANG HE AND PINYI REN, (Member, IEEE)
School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China
Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an Jiaotong University, Xi'an 710049, China

Corresponding author: Pinyi Ren (pyren@mail.xjtu.edu.cn)

This work was supported in part by the Key Research and Development Program of Shannxi Province under Grant 2017ZDXM-GY-012, and in part by the National Natural Science Foundation of China under Grant 61431011.

ABSTRACT Due to the broadcast nature of wireless device-to-device networks, the transmission of private information is threatened by the exterior eavesdropping. Targeting at this problem, we jointly exploit the Wyner's code and the linear network coding, in this paper, to improve the security. The function of the Wyner's code requires the legitimate channel better than the eavesdropper's channel, so we propose a novel relay selection scheme to achieve this objective. Specifically, two groups of relays have been selected. Relays in one of the groups are selected to forward the private information, and relays in the other group are selected to transmit artificial noise. In this way, we make sure that the signal-to-noise ratio (SNR) at the legitimate receiver is larger than a target value but the SNR at the eavesdropper has a certain probability less than the target value so that the security can be enhanced. Moreover, focusing on the problem that the Wyner's code cannot achieve security if the SNR at the eavesdropper is larger than the target value, we propose a network coding method. In this method, the message to be transmitted is divided into multiple parts, and then these parts are correlated with each other by using network coding. Thus, the eavesdropper also cannot decode the private information even its SNR larger than the target value. We analyze the secrecy outage probability in theory, and the simulation results are provided to confirm our analysis.

INDEX TERMS D2D, physical-layer security, cooperative communications.

I. INTRODUCTION

Wireless Device-to-device (D2D) communications enable the devices with a short range in the cellular network to communicate directly, which improves the efficiency of spectral utilization and resource scheduling [1]–[3]. However, due to the inherently broadcast nature of wireless communications, the private information transmitted by D2D devices is vulnerable to eavesdropping. To address this problem, an emerging method called physical-layer security has been extensively studied recently [4]–[6]. Different from the traditional encryption-based methods, physical-layer security is able to achieve keyless secrecy by using the Wyner's code [7] if the legitimate channel is better than the eavesdropper's channel. Motivated by this enlightening result, a large number of works aim to improve security by enhancing the legitimate channel or/and degrading the eavesdropper's channel. Among these works, one of the important branches is the study of cooperative communications. The cooperative communication was originally employed to extend the transmission range and to improve the reliability. Recently, it is used to enhance security. In the cooperative communication, there are generally two roles for a relay or a helper node to assist the secure transmission: forward the information or send artificial noise. Specifically, when forwarding the private information, amplified-and-forward (AF) and decode-and-forward (DF) are the most common protocols.

When there are multiple relays in the network, relay selection is an efficient way to improve security. In [8], Feng *et al.* consider a multiuser and multi-relay network and select the best user and the best relay to maximize the received signal-to-interference-to-noise ratio (SINR). In [9], a buffer-aided relay selection scheme is proposed, and the authors analyze the trade-off between the security and the delay. In [10],

The associate editor coordinating the review of this manuscript and approving it for publication was Mauro Fadda.

relay selection is used in the large-scale MIMO systems, and power allocation is employed to further enhance the security. In [18], relay selection is used to improve both the security and the reliability of cognitive radio systems. In these works, a common character is that the direct link between the transmitter and the legitimate receiver does not exist. However, for the D2D communications, the direct link is very likely in existence, so it should be taken into account. Considering this problem, an opportunistic relay selection scheme is proposed in [12] and [13]. In their works, the relay which can decode the private information from the transmitter and has the best channel to the legitimate receiver is selected to forward the private information. However, in practice, if the objective is to select the best relay, each relay should share the knowledge about the channel side information (CSI) to other relays. Obviously, this will be complex and inefficient if there are numerous relays in the network. Moreover, all the works discussed above do not consider the situation after secrecy outage happens when using the Wyner's code. This indicates that the eavesdropper can decode the private information directly if it has a better channel quality.

Network coding is usually used in the multicast networks to improve the throughput. Recently, it has been employed to enhance the security in wireless communications. In [14], Niu *et al.* propose a fountain code to improve the security, where the private file is secure if the legitimate receiver is able to decode all the packets before the eavesdropper. In [15] and [16], a joint network coding and automatic-repeat-request (ARQ) technique is proposed, and the security of private data is enhanced even the eavesdropper has superiority in the channel quality. However, all these works consider the direct transmission without a relay, or the cooperative communicates with a single relay.

Different from all the works discussed above, we propose a novel relay selection and coding method to improve security. We first describe the relay selection scheme and then discuss the coding method. Compared to the existed works that usually select only one relay (e.g., the optimal relay) to help the transmission, our method selects two groups of relays. Users in one of the groups forward private information and users in the other group send artificial noise. By using this method, the signal-to-noise ratio (SNR) at the legitimate receiver is larger than a target value, but the SNR at the eavesdropper is possibly lower than the target value. In this case, the security can be achieved by using the Wyner's code. However, because the randomness of the wireless channel, the SNR at Eve is also possible larger than the target value, so only using the Wyner's code cannot achieve security. Targeting at this problem, we further combine the Wyner's code with a linear network coding method. In this method, the message to be transmitted will be divided into several parts, and then each part is related to other parts by using the linear network coding. Once the eavesdropper loses two or more parts of the message, it cannot decode any other parts and also the message. To the best of our knowledge, this is the first work to combine the Wyner's code and network coding. The secrecy outage probability is used in our work to measure the security performance, and we analyze it in theory. We also consider the transmission reliability and analyze the outage probability theoretically.

The reminder of this paper is organized as follows. Section II presents the system model. Section III discusses the proposed cooperative transmission scheme. Section IV analyzes the secrecy outage probability and the transmission outage probability. Simulation results are provided in Section V and conclusions are given in Section VI.

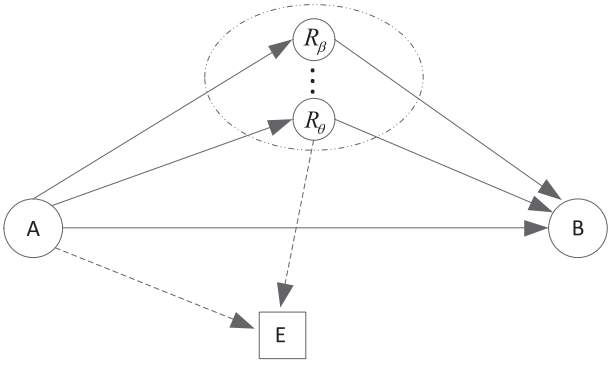


FIGURE 1. System Model.

II. SYSTEM MODEL

We consider a cooperative D2D network, as shown in Fig. 1. A D2D user Alice (A) intends to transmit private information to another D2D user Bob (B), but the transmission is wiretapped by an eavesdropper (E). Since the transmission in the direct link is possible to experience an outage, there are N D2D users as relays to help the information transmission. All the relays exploit the decode-and-forward (DF) protocol and only when the channel quality between Alice and Bob is worse than a threshold, the relays work; otherwise, they will keep silence. Also, the eavesdropper is able to wiretap all the information transmitted by the relays.

The channel coefficient from Alice to i-th relay $R_i \in \mathcal{R}$ $(i = 1, 2, \cdots, N)$ is denoted as h_{ai}, the channel coefficients from R_i to Bob and Eve are denoted as h_{ib} and h_{ie}, and the channel coefficients from Alice to Bob and Eve are denoted as h_{ab} and h_{ae}. All channels are assumed to be independent and experience Rayleigh fading, and all the channel coefficients are modeled as zero-mean complex Gaussian variables. Especially, we assume all the relays are homogenous, so the channels from the relays to Bob (or the eavesdropper) are independent and identically distributed (i.i.d.). The distance between arbitrary two users is denoted as d_{mn} with $m, n \in \{a, b, e, i\}$, and the variance of the channel coefficient from node m to node n is denoted as $\sigma_{mn}^2 = d_{mn}^{-\alpha}$, where α is the pass loss exponent. Since Eve is passive, all legitimate users including Alice, Bob and the relays do not know the channel side information (CSI) of wiretap channels, i.e., h_{ie} and h_{ae}. The additive noise at all users are assumed to be complex Gaussian random variables with zero-mean and unit variance.

For a relay R_i, it only knows the channel from Alice to itself and the channel from itself to Bob. Alice only knows the channel from itself to Bob. However, the eavesdropper knows the CSI of all the channels in the network. The transmit power at Alice is P; the transmit power at a relay is P_r if the relay forwards the private information, and is P_j if the relay sends artificial noise. We define $\gamma_{mn} = P'|h_{mn}|^2$ with $P' \in \{P, P_j, P_r\}$, which is exponential distribution with parameter $\lambda_{mn} = 1/(P'\sigma_{mn}^2)$.

The Wyner's code [7], [17] is used in this system, in which two rates will be designed. The first one is the codeword transmission rate R_0, and the second one is the confidential information rate R_s. If the rate difference of R_0 and R_s, i.e., $R_0 - R_s$, is larger than the capacity of the eavesdropper's channel, the security can be achieved. Otherwise, security cannot be achieved. The secrecy outage probability is used in this paper to measure the security performance, which is defined as the probability that the capacity of the eavesdropper's channel is not less than the rate difference $R_0 - R_s$. Note that the secrecy outage probability is different to another metric called intercept probability [18]. The intercept probability is defined as the probability that the capacity of eavesdropper's channel is not less than the codeword transmission rate R_0, which is unrelated to the confidential information rate R_s. Moreover, the rate R_0 is the codeword transmission rate instead of the capacity of the legitimate channel, which can be larger than, less than or equal to the capacity of the legitimate channel. However, only when the capacity of the legitimate channel is not less than R_0, Bob can decode the private information.

III. SECURE TRANSMISSION VIA WYNER'S CODE AND NETWORK CODING

In this section, we consider the secure and reliable transmission in cooperative D2D networks. First, we consider the direct transmission, and then we consider the cooperative transmission if the direct link is not good enough. In the cooperative transmission, we select a group of users who can decode x and whose channel quality is larger than a target value to forward the private information. Simultaneously, to degrade the eavesdropper's channel, we select another group of users to transmit artificial noise.

A. DIRECT TRANSMISSION

Now, we consider the direct transmission. Alice transmits a codeword (or message) x with $E[x^2] = 1$, and the codeword transmission rate is R_0. The received signal at Bob is given by

$$y_b = \sqrt{P}h_{ab}x + n_b, \tag{1}$$

the received signal at the i-th relay is given by

$$y_i = \sqrt{P}h_{ai}x + n_i, \tag{2}$$

and the received signal at the eavesdropper is given by

$$y_e = \sqrt{P}h_{ae}x + n_e, \tag{3}$$

where n_b, n_i and n_e are the additive white Gaussian noise at Bob, the i-th relay, and the eavesdropper. In this respect, the capacity of the direct channel from Alice to Bob is obtained as

$$C_{ab} = \log_2(1 + P|h_{ab}|^2). \tag{4}$$

The capacity of the wiretap channel from Alice to Eve is given by

$$C_{ae} = \log_2(1 + P|h_{ae}|^2). \tag{5}$$

Since Alice does not know the CSI of the wiretap channel, she cannot obtain the capacity of the wiretap channel.

In this process, Bob can decode the codeword transmitted by Alice only when the codeword transmission rate R_0 is not larger than the capacity of the Alice-Bob link, i.e., $R_0 \leq C_{ab}$ should be satisfied. Otherwise, if $C_{ab} < R_0$, Bob cannot decode the codeword by just using the direct link. In this case, Bob will feed back a negative acknowledgement (NACK) to Alice and the relays. We assume the feedback is detected reliably by Alice and all the relays. Then the selected relays will forward the message x to Bob.

B. COOPERATIVE TRANSMISSION

As discussed above, the relays will be active when $C_{ab} < R_0$. In this subsection, we provide the principle to select the expected relays. First, we should notice that the prerequisite of a relay to forward the message x is that the relay can decode x successfully. From (2), we can obtain the capacity of the channel from Alice to R_i as

$$C_{ai} = \log_2(1 + P|h_{ai}|^2). \tag{6}$$

Thus, relay R_i can decode the codeword x only when the capacity C_{ai} is larger than the codeword transmission rate R_0, i.e., $C_{ai} > R_0$. We allocate the relays satisfying $C_{ai} > R_0$ to set $\mathcal{A}$. This indicates that all the relays in set $\mathcal{A}$ can decode the message x. Then we design two parameters H_1 and H_2 to select two kinds of relays. Specifically, the relays in $\mathcal{A}$ have $|h_{ib}|^2 \geq H_2$ are allocated to set $\mathcal{C}$, and the relays in $\mathcal{R}$ have $|h_{ib}|^2 < H_1$ are allocated to set $\mathcal{D}$. When Bob cannot decode the message x by only using the direct link, the relays in set $\mathcal{C}$ forward x and the relays in set $\mathcal{D}$ transmit artificial noise. The cardinality of set $\mathcal{A}$ is expressed as $|\mathcal{A}|$, the cardinality of set $\mathcal{C}$ is expressed as $|\mathcal{C}|$, and the cardinality of set $\mathcal{D}$ is expressed as $|\mathcal{D}|$. Therefore, the received signal at Bob is given by

$$y'_b = \sqrt{P_r}\sum_{\theta=1}^{|\mathcal{C}|} h_{\theta b}x + \sqrt{P_J}\sum_{\beta=1}^{|\mathcal{D}|} h_{\beta b}J_\beta + n'_b, \tag{7}$$

where $\theta = 1, 2, \cdots, |\mathcal{C}|$, $\beta = 1, 2, \cdots, |\mathcal{D}|$ and n'_b is the AWGN at Bob. Similarly, the received signal at Eve is given by

$$y'_e = \sqrt{P_r}\sum_{\theta=1}^{|\mathcal{C}|} h_{\theta e}x + \sqrt{P_J}\sum_{\beta=1}^{|\mathcal{D}|} h_{\beta e}J_\beta + n'_e, \tag{8}$$

where n'_e is the AWGN at Eve.

Based on (7) and (8), we can obtain the SNR at Bob as

$$\gamma_b' = \frac{P_r \sum_{\theta=1}^{|\mathcal{C}|} |h_{\theta b}|^2}{P_J \sum_{\beta=1}^{|\mathcal{D}|} |h_{\beta b}|^2 + 1}, \tag{9}$$

and obtain the SNR at Eve as

$$\gamma_e' = \frac{P_r \sum_{\theta=1}^{|\mathcal{C}|} |h_{\theta e}|^2}{P_J \sum_{\beta=1}^{|\mathcal{D}|} |h_{\beta e}|^2 + 1}. \tag{10}$$

After receiving the signals from Alice and the relays, we assume the maximum ration combination (MRC) is used by Bob and Eve, so the capacity of the hybrid direct and relay channels at Bob is given by

$$C_{arb} = \frac{1}{2} \log_2 \left(1 + P|h_{ab}|^2 + \frac{P_r \sum_{\theta=1}^{|\mathcal{C}|} |h_{\theta b}|^2}{P_J \sum_{\beta=1}^{|\mathcal{D}|} |h_{\beta b}|^2 + 1} \right), \tag{11}$$

and the capacity of the hybrid channels at Eve is given by

$$C_{are} = \frac{1}{2} \log_2 \left(1 + P|h_{ae}|^2 + \frac{P_r \sum_{\theta=1}^{|\mathcal{C}|} |h_{\theta e}|^2}{P_J \sum_{\beta=1}^{|\mathcal{D}|} |h_{\beta e}|^2 + 1} \right). \tag{12}$$

Here, the coefficient $1/2$ is due to the two phases to transmit x when using the relay. Note that $C_{arb} \geq R_0/2$ must be satisfied, or Bob cannot decode the message x even with the help of the relay. Also, it is worth noticing that $C_{arb} \geq R_0/2$, rather than $C_{arb} \geq R_0$, is enough to ensure the decoding of x at Bob.

Since we have $|h_{\theta b}|^2 \geq H_2$ and $|h_{\beta b}|^2 < H_1$, we can obtain the following inequality

$$\begin{aligned} \gamma_b' &= \frac{P_r \sum_{\theta=1}^{|\mathcal{C}|} |h_{\theta b}|^2}{P_J \sum_{\beta=1}^{|\mathcal{D}|} |h_{\beta b}|^2 + 1} \\ &> \frac{P_r |\mathcal{C}| H_2}{P_J |\mathcal{D}| H_1 + 1} = \gamma_{b0}. \end{aligned} \tag{13}$$

Here, we define $\frac{P_r |\mathcal{C}| H_2}{P_J |\mathcal{D}| H_1 + 1} = \gamma_{b0}$. In this respect, once we ensure the capacity of the channels from the relays to Bob satisfies the following inequality, Bob can decode the message x:

$$\begin{aligned} \log_2(1 + \gamma_b') &> \log_2(1 + \gamma_{b0}) \\ &\geq R_0. \end{aligned} \tag{14}$$

If we define $R_0 = \log_2(1 + PH_0)$, inequality (14) is equivalent to

$$\gamma_{b0} = \frac{P_r |\mathcal{C}| H_2}{P_J |\mathcal{D}| H_1 + 1} > PH_0, \tag{15}$$

Observing (15), we find that by controlling the parameters in γ_{b0}, i.e., P_r, P_J, $|\mathcal{C}|$, $|\mathcal{D}|$, H_1, and H_2, we can always find a solution to make sure $\gamma_{b0} > PH_0$ since PH_0 is a constant and is public. This indicates that as long as there are relays in set $\mathcal{A}$, the message x can be decoded successfully by Bob.

C. NETWORK CODING

Because we do not know the capacity of the wiretap channel, it is possible that the capacity of the wiretap channel is larger than the rate difference $R_0 - R_s$ in both direct transmission and cooperative transmission. As discussed in Section II, the security cannot be achieved by only using the Wyner's code if this situation happens. Thus, in order to further improve the security in this case, we joint the Wyner's code and the network coding in this subsection.

First, instead of considering only one message x, we assume that Alice intends to transmit a short file consisting of M messages to Bob. For example, using OFDM, there are M available subcarrier, and Alice transmits x_j ($j = 1, 2, \cdots, M$) in the j-th subcarrier. Then we relate the M messages by using the linear network coding method [15], which is provided as follows. If M is odd, the encoding method is given by

$$\begin{aligned} v_1 &= x_1 \oplus x_2 \\ v_2 &= x_1 \oplus x_3 \\ &\vdots \\ v_{M-1} &= x_1 \oplus x_M \\ v_M &= x_1 \oplus x_2 \oplus \cdots \oplus x_M. \end{aligned} \tag{16}$$

If N is even, the encoding method is given by

$$\begin{aligned} v_1 &= x_1 \oplus x_2 \\ v_2 &= x_1 \oplus x_3 \\ &\vdots \\ v_{M-1} &= x_1 \oplus x_M \\ v_M &= x_2 \oplus x_3 \oplus \cdots \oplus x_M. \end{aligned} \tag{17}$$

Note that no matter M is odd or even, the decoding method is the same, given by

$$\begin{aligned} x_1 &= v_1 \oplus v_2 \oplus \cdots \oplus v_M, \\ x_j &= v_1 \oplus v_2 \oplus \cdots \oplus v_M \oplus v_{j-1} \ (j = 2, 3, \cdots, M). \end{aligned} \tag{18}$$

From (18), we can find that the decoding of x_1 requires all the M coded messages (i.e., $v_1, v_2, \cdots, v_M$), and the decoding of v_j with $j = 2, 3, \cdots, M$ requires $M - 1$ coded messages (i.e., $v_1, v_2, \cdots, v_M$ except v_{j-1}). This means that if the eavesdropper intends to decode an arbitrary message x_j, it requires at least $M - 1$ coded messages. Now, instead of transmitting x, Alice transmits v_j to Bob, and v_j is further processed by the Wyner's code. Thus, the property of the code message v_j, i.e., the reliability or security, is exactly the same with the message x without using network coding, but the security of the message x_j using network coding is enhanced.

IV. PERFORMANCE ANALYSIS

In this section, we consider the performance of the proposed scheme. The outage probability and the secrecy outage probability are analyzed in theory.

A. OUTAGE PROBABILITY

First, we consider the outage probability. The outage probability measures the probability that Bob cannot decode x. We define $C_{ab} < R_0$ in the direct transmission as event $\mathcal{O}_1$, and define the situation $|\mathcal{A}| = 0$ as event $\mathcal{O}_2$. Therefore, the outage probability is given by

$$P_{out} = \Pr(\mathcal{O}_1 \cap \mathcal{O}_2). \tag{19}$$

Note that we do not consider the situation $C_{arb} < R_0/2$ here is because inequality (14) or (15) can be satisfied by properly designing the parameters in γ_{b0}. Specifically, we have

$$\begin{aligned}\Pr(\mathcal{O}_1) &= \Pr(C_{ab} < R_0)\\ &= 1 - e^{-\lambda_{ab}\gamma},\end{aligned} \tag{20}$$

where $\gamma = 2^{R_0} - 1$, and $\lambda_{ab} = 1/(P\sigma_{ab}^2)$. Note that event $\mathcal{O}_2$ indicates that all the relays in the network cannot decode the message x, so the probability of event $\mathcal{O}_2$ is obtained as

$$\begin{aligned}\Pr(\mathcal{O}_2) &= [\Pr(C_{ai} < R_0)]^N\\ &= (1 - e^{-\lambda_{ai}\gamma})^N,\end{aligned} \tag{21}$$

where $\lambda_{ai} = 1/(P\sigma_{ai}^2)$. In this respect, the outage probability is obtained as

$$\begin{aligned}P_{out} &= \Pr(\mathcal{O}_1 \cap \mathcal{O}_2)\\ &= \Pr(\mathcal{O}_1) \cap \Pr(\mathcal{O}_2)\\ &= (1 - e^{-\lambda_{ab}\gamma})(1 - e^{-\lambda_{ai}\gamma})^N.\end{aligned} \tag{22}$$

Here, the result is based on the fact that $\mathcal{O}_1$ and $\mathcal{O}_2$ are independent each other.

B. SECRECY OUTAGE PROBABILITY ONLY USING WYNER'S CODE

According to the principle of the Wyner's code, in the direct transmission, security can be achieved if $R_0 - R_s > C_{ae}$, and security cannot be achieved if $R_0 - R_s \le C_{ae}$. Similar to the situation in the direct transmission, when with the help of the relays, the security can be achieved if $(R_0 - R_s)/2 > C_{are}$, and the security cannot be achieved if $(R_0 - R_s)/2 \le C_{are}$. Combining the situation in the direct transmission and the cooperative transmission, we can obtain the probability when the security cannot be achieved, i.e., the secrecy outage probability, which is given by

$$\begin{aligned}P_{s,out} &= \Pr(R_0 - R_s \le C_{ae}|\overline{\mathcal{O}}_1)\Pr(\overline{\mathcal{O}}_1)\\ &\quad + \Pr(R_0 - R_s \le 2C_{are}|\mathcal{O}_1\overline{\mathcal{O}}_2)\Pr(\mathcal{O}_1\overline{\mathcal{O}}_2)\\ &\quad + \Pr(R_0 - R_s \le C_{ae}|\mathcal{O}_1\mathcal{O}_2)\Pr(\mathcal{O}_1\mathcal{O}_2)\\ &= \Pr(R_0 - R_s \le C_{ae})\Pr(\overline{\mathcal{O}}_1)\\ &\quad + \Pr(R_0 - R_s \le 2C_{are})\Pr(\mathcal{O}_1)\Pr(\overline{\mathcal{O}}_2)\\ &\quad + \Pr(R_0 - R_s \le C_{ae})\Pr(\mathcal{O}_1)\Pr(\mathcal{O}_2).\end{aligned} \tag{24}$$

The first term in (24) indicates the security outage in the direct transmission; the second term in (24) indicates the security outage in the cooperative transmission; and the third term in (24) means that Bob and all the relays cannot decode x, but the information will leak to the eavesdropper. Specifically, the probability of $R_0 - R_s \le C_{ae}$ in (24) is given by

$$\begin{aligned}P_1 &= \Pr(R_0 - R_s \le C_{ae})\\ &= \Pr(\gamma_{ae} \ge 2^{\Delta} - 1)\\ &= e^{-\lambda_{ae}\gamma_s},\end{aligned} \tag{25}$$

where $\Delta = R_0 - R_s$, $\gamma_s = 2^{\Delta} - 1$ and $\lambda_{ae} = 1/(P\sigma_{ae}^2)$. The probability of $R_0 - R_s \le 2C_{are}$ in (24) is given by

$$\begin{aligned}P_2 &= \Pr(R_0 - R_s \le 2C_{are})\\ &= \Pr(\gamma_{ae} + \gamma_e' > 2^{\Delta} - 1).\end{aligned} \tag{26}$$

Obviously, we require the distribution of $\gamma_{ae} + \gamma_e'$ to obtain P_2.

First, we denote $X = P_r \sum_{\theta=1}^{|\mathcal{C}|} |h_{\theta e}|^2 = \sum_{\theta=1}^{|\mathcal{C}|} \gamma_{\theta e}$. Because $\gamma_{\theta e}$ is exponentially distributed with parameter $\lambda_{\theta e} = 1/(P_r\sigma_{\theta e}^2)$, the random variable X is Erlang distributed, and its probability density function (p.d.f.) is expressed as

$$f_X(x) = \frac{\lambda_{\theta e}^{|\mathcal{C}|}}{(|\mathcal{C}| - 1)!} x^{|\mathcal{C}|-1} e^{-\lambda_{\theta e}x}. \tag{27}$$

Moreover, its cumulative distribution function (c.d.f.) is expressed as

$$F_X(x) = 1 - \sum_{n=0}^{|\mathcal{C}|-1} \frac{1}{n!} e^{-\lambda_{\theta e}x}(\lambda_{\theta e}x)^n. \tag{28}$$

Similarly, we denote $Y = P_J \sum_{\beta=1}^{|\mathcal{D}|} |h_{\beta e}|^2 = \sum_{\beta=1}^{|\mathcal{D}|} \gamma_{\beta e}$, whose p.d.f. is expressed as

$$f_Y(y) = \frac{\lambda_{\beta e}^{|\mathcal{D}|}}{(|\mathcal{D}| - 1)!} y^{|\mathcal{D}|-1} e^{-\lambda_{\beta e}y}, \tag{29}$$

where $\lambda_{\beta e} = 1/(P_J\sigma_{\beta e}^2)$. Thus, the c.d.f. of the random variable $Z = X/(Y + 1)$ is given by

$$\begin{aligned}F_Z(z) &= \Pr(Z < z)\\ &= \Pr\left(\frac{X}{Y+1} < z\right)\\ &= \int_0^{\infty}\int_0^{z(y+1)} f_X(x)f_Y(y)\mathrm{d}x\mathrm{d}y\\ &= \int_0^{\infty} f_Y(y)\int_0^{z(y+1)} f_X(x)\mathrm{d}x\mathrm{d}y\\ &= \int_0^{\infty} f_Y(y)F_X(z(y+1))\mathrm{d}y\\ &= 1 - \int_0^{\infty} f_Y(y)\sum_{n=0}^{|\mathcal{C}|-1}\frac{1}{n!}e^{-\lambda_{\theta e}z(y+1)}(\lambda_{\theta e}z(y+1))^n\mathrm{d}y\end{aligned} \tag{31}$$

Since we assume all the channels from the relays to the eavesdropper are i.i.d., we can define $\lambda_{\beta e} = \lambda_{\theta e} = \lambda_e$. Then substituting (29) into (31), we can further obtain the result of $F_Z(z)$ as (23), shown at the top of the next page. Note that

$$
\begin{aligned}
F_Z(z) &= 1-\int_0^{\infty}\frac{\lambda_e^{|\mathcal{D}|}}{(|\mathcal{D}|-1)!}y^{|\mathcal{D}|-1}e^{-\lambda_e y}\sum_{n=0}^{|\mathcal{C}|-1}\frac{1}{n!}e^{-\lambda_e z(y+1)}(\lambda_e z(y+1))^n\mathrm{d}y\\
&= 1-\frac{\lambda_e^{|\mathcal{D}|}}{(|\mathcal{D}|-1)!}\int_0^{\infty}y^{|\mathcal{D}|-1}e^{-\lambda_e y}\sum_{n=0}^{|\mathcal{C}|-1}\frac{1}{n!}e^{-\lambda_e z(y+1)}(\lambda_e z(y+1))^n\mathrm{d}y\\
&= 1-\frac{\lambda_e^{|\mathcal{D}|}}{(|\mathcal{D}|-1)!}\sum_{n=0}^{|\mathcal{C}|-1}\frac{1}{n!}(\lambda_e z)^n e^{-\lambda_e z}\int_0^{\infty}y^{|\mathcal{D}|-1}e^{-\lambda_e(z+1)y}(y+1)^n\mathrm{d}y\\
&= 1-\frac{\lambda_e^{|\mathcal{D}|}}{(|\mathcal{D}|-1)!}\sum_{n=0}^{|\mathcal{C}|-1}\frac{1}{n!}(\lambda_e z)^n e^{-\lambda_e z}\int_0^{\infty}y^{|\mathcal{D}|-1}e^{-\lambda_e(z+1)y}\sum_{q=0}^{n}\binom{n}{q}y^q\mathrm{d}y\\
&= 1-\frac{\lambda_e^{|\mathcal{D}|}}{(|\mathcal{D}|-1)!}\sum_{n=0}^{|\mathcal{C}|-1}\frac{1}{n!}(\lambda_e z)^n e^{-\lambda_e z}\sum_{q=0}^{n}\binom{n}{q}\int_0^{\infty}y^{|\mathcal{D}|+q-1}e^{-\lambda_e(z+1)y}\mathrm{d}y\\
&= 1-\frac{\lambda_e^{|\mathcal{D}|}}{(|\mathcal{D}|-1)!}\sum_{n=0}^{|\mathcal{C}|-1}\sum_{q=0}^{n}\frac{1}{n!}(\lambda_e z)^n e^{-\lambda_e z}\binom{n}{q}(|\mathcal{D}|+q-1)!(\lambda_e(z+1))^{-(|\mathcal{D}|+q)}.
\end{aligned}
\tag{23}
$$

$$
\begin{aligned}
F_T(t) &= \int_0^t \lambda_{ae}e^{-\lambda_{ae}x}\left(1-\frac{\lambda_e^{|\mathcal{D}|}}{(|\mathcal{D}|-1)!}\sum_{n=0}^{|\mathcal{C}|-1}\sum_{q=0}^{n}\frac{1}{n!}(\lambda_e(t-x))^n e^{-\lambda_e z}\binom{n}{q}(|\mathcal{D}|+q-1)!(\lambda_e(t-x+1))^{-(|\mathcal{D}|+q)}\right)\mathrm{d}x\\
&= 1-e^{-\lambda_{ae}t}-\frac{\lambda_e^{|\mathcal{D}|}}{(|\mathcal{D}|-1)!}\int_0^t\sum_{n=0}^{|\mathcal{C}|-1}\sum_{q=0}^{n}\frac{1}{n!}(\lambda_e(t-x))^n e^{-\lambda_e z}\binom{n}{q}(|\mathcal{D}|+q-1)!(\lambda_e(t-x+1))^{-(|\mathcal{D}|+q)}\mathrm{d}x.
\end{aligned}
\tag{30}
$$

$F_Z(z)$ is also the distribution of γ_e', so we can further obtain the c.d.f. of $T=\gamma_{ae}+\gamma_e'$ as

$$
\begin{aligned}
F_T(t) &= \Pr(T\le t)\\
&= \Pr(\gamma_{ae}+\gamma_e'\le t)\\
&= \int_0^t f_{\gamma_{ae}}(x)F_Z(t-x)\mathrm{d}x.
\end{aligned}
\tag{32}
$$

Substituting (23) into (32), we can obtain the distribution of $T=\gamma_{ae}+\gamma_e'$ as (30), shown at the top of this page. In this respect, the secrecy outage probability is obtained as

$$
\begin{aligned}
P_{s,out} &= e^{-\lambda_{ae}\gamma_s}e^{-\lambda_{ab}\gamma}\\
&\quad+(1-F_T(\gamma_s))(1-e^{-\lambda_{ab}\gamma})[1-(1-e^{-\lambda_{ai}\gamma})^N]\\
&\quad+e^{-\lambda_{ae}\gamma_s}(1-e^{-\lambda_{ab}\gamma})(1-e^{-\lambda_{ai}\gamma})^N.
\end{aligned}
\tag{33}
$$

C. SECURITY PERFORMANCE AFTER USING WYNER'S CODE AND NETWORK CODING

In last subsection, we have obtained the secrecy outage probability of the message x when Wyner's code is used. In this subsection, we will analyze the secrecy outage probability of x_j when both Wyner's code and network coding are exploited. Note that after using network coding, the transmitted information is v_j instead of x_j, so the secrecy outage probability for an arbitrary coded message v_j is equal to that of the original message x without using network coding, given by (33), but the secrecy outage probability of x_j is related to that of $v_1, v_2, \cdots, v_M$. Since the transmission of all the M coded messages is independent, the secrecy outage probability of x_j after using the network coding is obtained as

$$
P_{s,out}^{\mathrm{NC}} = (P_{s,out})^{M-1}. \tag{34}
$$

Equation (34) indicates that the eavesdropper has to obtain at least $M-1$ coded messages to decode x_j, or it cannot decode any part of x_j.

V. SIMULATION RESULTS

In this section, we provide simulation results to show the performance of the proposed scheme. In the simulations, the distance between Alice and Bob is $d_{ab}=10$m, between Alice and the relays is $d_{ai}=5$m, between Alice and the eavesdropper is $d_{ae}=6$m, and between the relays and the eavesdropper is $d_{ie}=5$m. The pass loss exponent α is 2, and the transmit power is 20dB. The number of relays in the network are $N=5$.

Fig. 2 compares the outage probability in the direct transmission and the cooperative transmission. It can be seen that the direct link almost cannot ensure reliable transmission when the target rate R_0 larger than 1. This means that the direct link only helps the transmission when R_0 is small. In addition, although the relays can help the transmission, the outage probability increases and becomes intolerable when R_0 is large, e.g., $R_0=3$. In this respect, Alice should select a proper transmission rate in practice to ensure the basic reliability. Moreover, in Fig. 3, we further show the relationship between the outage probability and the number

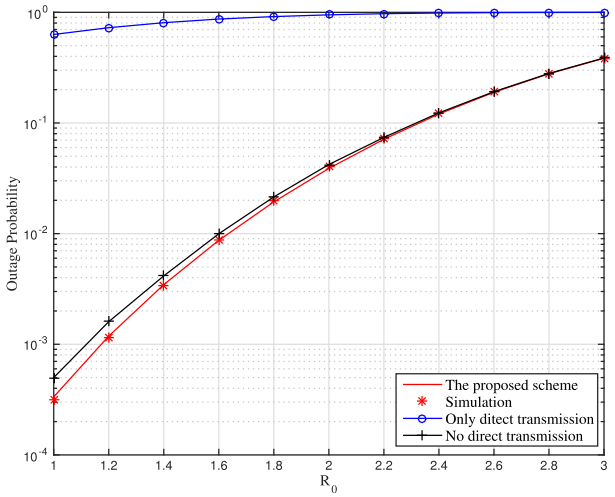


FIGURE 2. Outage probability vs. the transmission rate R_0.

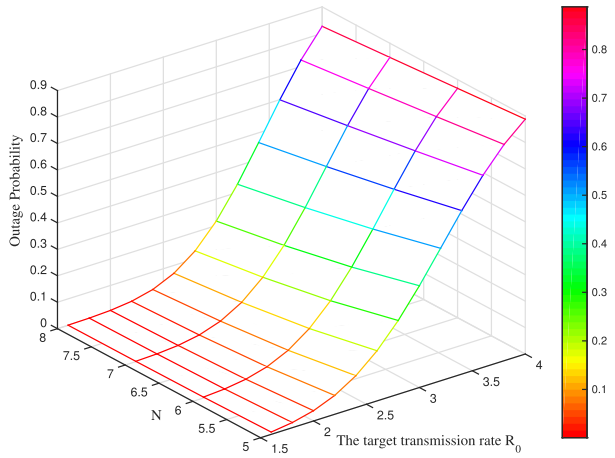


FIGURE 3. Outage probability vs. the transmission rate R_0 and the number of relays.

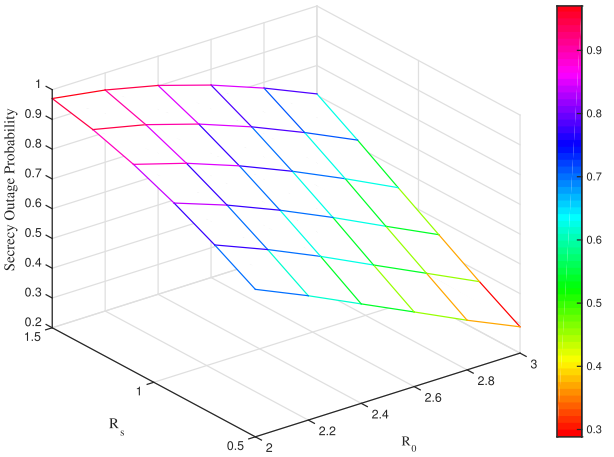


FIGURE 4. Secrecy outage probability vs. the transmission rate R_0 and the secrecy rate R_S.

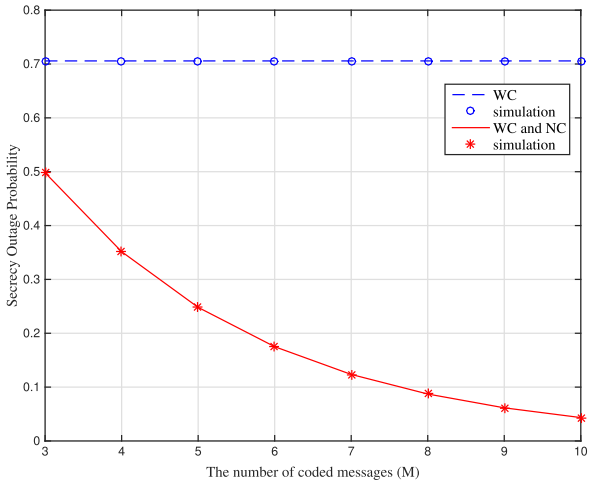


FIGURE 5. Secrecy outage probability vs. the number of coded messages, M.

of relays. It can be seen that increasing the number of relays can help to ensure the reliability. Thus, if there are enough number of D2D users in the network, the transmitter can increase the transmission rate appropriately.

Fig. 4 exhibits the secrecy outage probability versus the secrecy rate and the transmission rate. It can be that if we fix R_s, the secrecy outage probability will decrease with the increase of R_0. However, if we fix the transmission rate R_0, the growth of the secrecy rate will increase the secrecy outage probability. Combining with the relationship between R_0 and the outage probability shown in Fig. 3, we should consider the trade-off between the reliability and the security in practice, and choose appropriate R_0 and R_s.

Fig. 5 compares the security performance when using and not using network coding, in which 'WC' means Wyner's code and 'NC' means network coding. We can see that if only Wyner's code is used, the secrecy outage keeps constant and is unrelated to the number of messages to be transmitted. However, if we combine the Wyner's code and the network coding, secrecy outage probability falls off significantly.

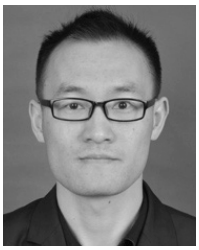
VI. CONCLUSION

In this paper, we study the secure transmission in cooperative D2D networks. A novel relay selection scheme is proposed, in which two groups of relays are select to transmit private information and artificial noise. The relays selected to transmit private information improve the reliability of the transmission, and the relays selected to transmit artificial noise improve the security. In the relay selection scheme, global CSI is not necessary, and each relay only knows its own CSI, so the scheme is easy to be achieved. Moreover, different from the traditional physical-layer security methods that only using the Wyner's code, we combine the Wyner's code and the network coding to further improve the security. Demonstrated by the theoretical and simulation results, the proposed method can enhance security significantly especially when the number of messages to be transmitted is relatively large.

REFERENCES

[1] H. Tang and Z. Ding, "Mixed mode transmission and resource allocation for D2D communication," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 162–175, Jan. 2016.

[2] W. Wang, K. C. Teh, and K. H. Li, "Enhanced physical layer security in D2D spectrum sharing networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 106–109, Feb. 2017.
[3] B. Fan, H. Tian, L. Jiang, and A. V. Vasilakos, "A social-aware virtual MAC protocol for energy-efficient D2D communications underlying heterogeneous cellular networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8372–8385, Sep. 2018.
[4] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.
[5] X. Lu, D. Niyato, N. Privault, H. Jiang, and P. Wang, "Managing physical layer security in wireless cellular networks: A cyber insurance approach," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1648–1661, Jul. 2018.
[6] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, "Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 671–684, Mar. 2018.
[7] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[8] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "User and relay selection with artificial noise to enhance physical layer security," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10906–10920, Nov. 2018.
[9] X. Liao, Y. Zhang, Z. Wu, Y. Shen, X. Jiang, and H. Inamura, "On security-delay trade-off in two-hop wireless networks with buffer-aided relay selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1893–1906, Mar. 2018.
[10] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 341–355, Feb. 2018.
[11] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.
[12] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756–1770, May 2015.
[13] S. Poursajadi and M. H. Madani, "Analysis and enhancement of joint security and reliability in cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12003–12012, Dec. 2018.
[14] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting fountain codes for secure wireless delivery," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 777–780, May 2014.
[15] H. He and P. Ren, "Secure ARQ protocol for wireless communications: Performance analysis and packet coding design," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7158–7169, Aug. 2018.
[16] N. Abuzainab and A. Ephremides, "Secure distributed information exchange," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1126–1135, Feb. 2014.
[17] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.
[18] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.



HONGLIANG HE received the B.E. degree in information and communication engineering from Harbin Engineering University, in 2013. He is currently pursuing the Ph.D. degree with the School of Electronic and Information Engineering, Xi'an Jiaotong University, China. His research interests include wireless physical-layer security, the Internet of Things, and cooperative communications.

PINYI REN (M'10) received the B.S. degree in Information and Control Engineering, the M.S. degree in information and communications engineering, and the Ph.D. degree in electronic and communications system from Xi'an Jiaotong University, China, in 1994, 1997, and 2001, respectively. He is currently a Professor with the Information and Communications Engineering Department, Xi'an Jiaotong University, China. He has published over 100 technical papers on international journals and conferences. He has over 15 Patents (First Inventor) authorized by Chinese Government. He frequently serves as the Technical Program Committee member for IEEE GLOBECOM, IEEE ICC, and IEEE CCNC. He is a member of the IEEE Communications Society. He was a recipient of the Best Letter Award of the IEICE Communications Society 2010. He has served as the General Chair of ICST WICON 2011. He serves as an Editor for the Journal of Xi'an Jiaotong University, and has served as the Leading Guest Editor of the Special Issue of *Mobile Networks and Applications* on Distributed Wireless Networks and Services and the Leading Guest Editor of the Special Issues of *Journal of Electronics* on Cognitive Radio.