IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 24, 2019, accepted March 9, 2019, date of publication March 21, 2019, date of current version April 5, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2906639*

# Joint Relay and Eavesdropper Selection Strategy Against Multiple Eavesdroppers over Nakagami-*m* Fading Channels in Cooperative Decode-and-Forward Relay Networks

**QIAN GUO[1] AND WEI FENG[2]**
[1]College of Mechanical and Electrical Engineering, China Jiliang University, Hangzhou 310018, China
[2]School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

Corresponding author: Qian Guo (guoqmail@cjlu.edu.cn)

This work was supported in part by the Program of Zhejiang Provincial Natural Science Foundation of China under Grant LY19F010011.

**ABSTRACT** Physical layer security (PLS) in the presence of multiple eavesdroppers over Nakagami-*m* fading channels for cooperative decode-and-forward (DF) relay network that consists of one source, one destination, and multiple relays is investigated. Different from the recent PLS system model that only considers one eavesdropper during eavesdropping attack, this paper extends the one-eavesdropper case to a multiple-eavesdropper scenario and investigates joint relay and eavesdropper selection (JRES) strategy against eavesdropping attack over Nakagami-*m* fading channels. In the proposed strategy, the best relay is selected via the maximum relay forward channel capacity. In addition, since eavesdroppers are non-cooperative, the worst case is considered. Namely, the wiretap channel between the best relay and the chosen eavesdropper has the maximum capacity. Traditional direct transmission and opportunistic relay selection (ORS) scheme in the presence of one eavesdropper over Rayleigh channel are regarded as benchmarks. Moreover, a security–reliability tradeoff (SRT) performance is analyzed, where the reliability performance is expressed by outage probability (OP), while the security performance is measured by intercept probability (IP). Closed-form expressions of OP and IP are derived. The numerical results show that the proposed JRES scheme outperforms the traditional direct transmission and the ORS scheme in the presence of one eavesdropper over Rayleigh channel. The SRT performance is enhanced obviously with the increasing of relay numbers and Nakagami channel fading factor *m* for a given number of eavesdroppers, which extends the PLS and SRT performance analysis to a more general case in a cooperative DF relay network.

**INDEX TERMS** Decode-and-forward (DF) relay network, joint relay and eavesdropper selection (JRES), Nakagami-*m* fading channels, physical layer security (PLS), security-reliability tradeoff (SRT).

## I. INTRODUCTION

In wireless communication, signals can easily be overheard by eavesdroppers because of the broadcast nature of the wireless medium. In order to achieve safe transmission, many techniques have been studied. Traditional secret communication is mainly based on cryptography-related encryption technology [1], that is, even if the eavesdroppers and the legitimate users obtain the same message, eavesdroppers can not decrypt the original message since they do not know the secret key. With the development of computer technology, the encryption technology becomes less secure because the secret key can be easily decrypted.

Recently, physical layer security (PLS) technology has attracted much attention [2]. It acts as an effective means to defeat eavesdroppers with the utilization of physical characteristics of the wireless channel rather than the complex encryption algorithm [3]. Shannon [4] proved that there is an optimal secure communication system. After that, Wyner [5] pointed out that if the quality of eavesdroppers' channel is

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

worse than the legitimate receivers, the channel code can always be found so that eavesdroppers can not get any information from the received signal. Secrecy capacity is developed and shows the difference between the capacity of the main link (from source (S) to destination (D)) and that of the wiretap link (from S to eavesdropper (E)) [5]. It was proved that if the capacity of the main link is less than that of the wiretap link, the eavesdropper can succeed in intercepting the signal transmission [6]. In order to improve transmission security against eavesdropping attacks, it is important to reduce intercept events via the improvement of secrecy capacity. However, wireless secrecy capacity is degraded in the multipath fading channels.

To overcome the channel fading characteristics, some techniques are proposed for secure transmission, such as PLS in multiple-input multiple-output (MIMO) power line communication networks [7], beamforming techniques to enhance PLS [8] and optimal relay selection for PLS in cooperative wireless networks [9]. In [7], it mainly focuses on the secrecy capacity of MIMO power line communication (PLC). It shows that multi-conductor PLC network enables more secure communication compared to the single conductor case. In [8], it shows the security-oriented beamforming technique allows the source to send its information to legitimate receivers in a particular direction, whereas the eavesdroppers receive the signal with destructive interference. Hence, signal strength at the legitimate receiver is much higher than that at the eavesdropper receiver. With the help of beamforming technology, it can also be enhanced in confidentiality. In addition, relays can be used for defeating against eavesdropping attack. Several relay selection schemes are proposed and compared in [9] for enhancing wireless secrecy capacity under amplify-and-forward (AF) and decode-and-forward (DF) relay protocols respectively.

Recently, PLS techniques for 5G wireless networks and 5G based large scale social networks are investigated [10], [11]. In [10], it provides a latest survey of PLS research on various promising 5G technologies, such as PLS coding, massive MIMO, millimeter wave communications, heterogeneous networks, non-orthogonal multiple access (NOMA), full duplex technology, etc. PLS features in large scale social networks are discussed in [11]. It is pointed out that some opportunities and challenges such as the detection of wire-tap users, the utilization of high dynamic range and the information exchanging in cross layer design should be considered in PLS for 5G based large scale social networks [11]. In addition, dynamic spectrum access with PLS for spectrum overlay cognitive radio networks is investigated with a cooperative jamming approach based on Stackelberg game [12]. Under the proposed scheme, the optimal strategies of primary and secondary users that are jointly referred to as Stackelberg equilibrium are analyzed via numerical simulations [12]. Experimental study on key generation for PLS in wireless communications is studied in [13]. It offers insights to the design of a secure and efficient key generation system.

The above references are mainly focused on the improvement of wireless security without paying much attention to communication reliability. For this reason, Y. Zou investigated the *security-reliability trade-off* (SRT) strategies in wireless communication [14]–[16]. Security is quantified by eavesdroppers successfully intercepting the source signal whereas reliability represents that the outage event is occurred at the legitimate destination. These probabilities are denoted as intercept probability (IP) and outage probability (OP) respectively [14]–[16]. The OP can be reduced by increasing the transmit power of S, however, the enhancement of power also improves the S-E channel capacity and increases the IP at the same time. According to [14] and [15], the increasing of IP will lead to the reduction of the OP and vice versa, which indicates a trade-off between security and reliability. In addition, the authors propose single best-relay selection scheme to achieve SRT enhancement. It is shown that relay collaboration outperforms direct transmission. As the number of relay increases, the SRT performance is enhanced significantly [16]. Moreover, the comparison of multi-relay selection with single-relay selection is investigated and it is shown that SRT performance of multi-relay selection outperforms single-relay selection scenario [14].

Zhu *et al.* [14] and Zou *et al.* [15] investigated relay selection scheme of cooperative wireless network in the presence of one eavesdropper under DF protocol over Rayleigh channels. In this paper, we extend the one-eavesdropper case to a multiple-eavesdroppers scenario. There are generally two kinds of eavesdropping scenarios: 1) non-cooperative case, where the eavesdroppers are independent of each other during the interception of legitimate transmission phase; 2) cooperative case, where the eavesdroppers collaborate to intercept the legitimate transmission [17]. In this paper, we mainly focus on the first scenario and select the optimal relay, where the worst case (the maximum wiretap channel capacity) is considered. Then, we extend Rayleigh channel model to Nakagami-*m* channel model [18], and propose joint relay and eavesdropper selection (JRES) strategy against eavesdropping attack over Nakagami-*m* fading channels.

Although some literatures have studied joint relay and jammer selection scheme to improve PLS in cooperative networks [19]–[22], the system models of these schemes are mainly composed of multiple relays and jammers in the presence of one eavesdropper in different scenarios. Joint relay and jammer selection scheme for secure two-way relay networks is investigated in [19]. It selects two or three intermediate nodes to enhance security against one eavesdropper. The first selected node operates in the conventional relay mode and assists the source to deliver data to the destination using AF protocol, the second and third nodes are used in different communication phases as jammers in order to create interference upon the eavesdropper [19]. Literature [20] enhances PLS of amplify-and-forward relaying networks with the aid of joint relay and jammer selection scheme in the presence of channel state information (CSI) feedback delays. In this literature, reliability-security ratio (RSR) is introduced for

characterizing the relationship between reliability and security. RSR results demonstrate that, the reliability improves more substantially than security degrades [20]. Literatures [21], [22] studies PLS for DF relay networks with joint relay and jammer selection scheme against one eavesdropper. In [21], one intermediate node is selected as relay while the remaining intermediate nodes are acted as friendly jammers that broadcast artificial noise to disturb the eavesdropper. It investigates power allocation with the target of secrecy rate maximization. The highest secrecy rate can be achieved via optimal relay and jammer selection scheme. Then, the authors propose joint cooperative beamforming and jamming scheme to improve PLS in the presence of one eavesdropper [22]. System model is the same as that in [21]. It selects one intermediate node as relay to forward source transmission simultaneously by employing a beamforming weight vector, while the remaining intermediate nodes are acted as jammers to disturb the eavesdropper by sending artificial noise. It also studies power allocation with the assumptions of the wiretap link's CSI [22].

Different from the above literatures that only consider one eavesdropper during eavesdropping attack, the paper extends the one-eavesdropper case to a multiple-eavesdroppers scenario and investigates *joint relay and eavesdropper selection* (JRES) strategy against eavesdropping attack over Nakagami-*m* fading channels with SRT performance analysis. The main contributions of this paper are summarized as follows. JRES strategy for cooperative DF relay network with multiple relays in the presence of multiple eavesdroppers is investigated. We use the direct transmission without relay and *opportunistic relay selection* (ORS) scheme in the presence of one eavesdropper over Rayleigh channel as our benchmark scheme. We derive the closed-form expressions of OP and IP for direct transmission and JRES strategy over Nakagami-*m* fading channels and present SRT performance analysis of the proposed strategy.

The remainder of this paper is organized as follows. In Section II, system model of direct transmission and JRES strategy are introduced. In Section III, we derive the closed expression of OP and IP with SRT analysis for direct transmission and JRES strategy, respectively. Numerical results and performance analysis are presented in Section IV. Finally, conclusions are drawn in Section V.

## II. SYSTEM MODEL

### A. DIRECT TRANSMISSION

We first study the direct transmission model with S and D in the presence of multiple eavesdroppers. As shown in Fig. 1, we denote the set of $K$ eavesdroppers as $E = \{e_j | j = 1, 2, ..., K\}$, where the solid and dashed lines represent the S-D main link and the S-$e_j$ wiretap link, respectively. The S-$e_j$ and S-D channel parameters are denoted as $h_{se_j}$ and $h_{sd}$, respectively. The channel parameters follow independent identically distributed (i.i.d.) Nakagami-*m* fading with channel fading factor $m_{se_j}$ and $m_{sd}$. S transmits signal $x$ to D,

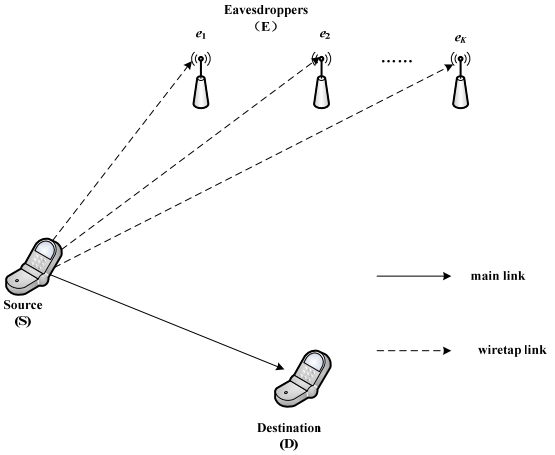



**FIGURE 1.** Wireless network consists of S and D in the presence of multiple eavesdroppers.

while eavesdroppers try to wiretap the signal. According to [14]–[16], $e_j$ is assumed to know the secret key of the direct S-D transmission and try to decrypt out the source signal $x$. Suppose source S transmits $x$ with power $P$ and transmission rate $R_d$, the received signal at D can be expressed as

$$y_d = h_{sd}\sqrt{P}x + n_d \tag{1}$$

where $n_d$ denotes the zero-mean additive white Gaussian noise (AWGN) with variance $N_0$. According to the assumption, the signal received at $e_j$ can be written as

$$y_{e_j} = h_{se_j}\sqrt{P}x + n_e \tag{2}$$

where $n_e$ also denotes the zero-mean AWGN with variance $N_0$ (Suppose that AWGN noise power at all eavesdroppers are the same). From (1), we can obtain the direct channel capacity between S and D as

$$C_{sd} = \log_2\left(1 + |h_{sd}|^2 \frac{P}{N_0}\right) \tag{3}$$

Similarly, the wiretap channel capacity between S and $e_j$ can be expressed as

$$C_{se_j} = \log_2\left(1 + \left|h_{se_j}\right|^2 \frac{P}{N_0}\right) \tag{4}$$

For multiple-eavesdroppers case, we consider the worst case, namely, the maximum wiretap channel capacity. Hence, one eavesdropper that has the maximum wiretap channel capacity is chosen, denoted as

$$C_{se} = \max_{e_j \in E} C_{se_j} = \max_{e_j \in E} \log_2\left(1 + \left|h_{se_j}\right|^2 \frac{P}{N_0}\right) \tag{5}$$

### B. JOINT RELAY AND EAVESDROPPER SELECTION

In this section, we investigate cooperative wireless network shown in Fig. 2. We assume that the direct transmission S-D is not feasible, which is assisted via $N$ relays. Channels from S to $R_i$, $R_i$ to D and $R_i$ to $e_j$ are denoted as $h_{si}$, $h_{id}$ and $h_{ie_j}$, and follow i.i.d. Nakagami-*m* fading with channel fading

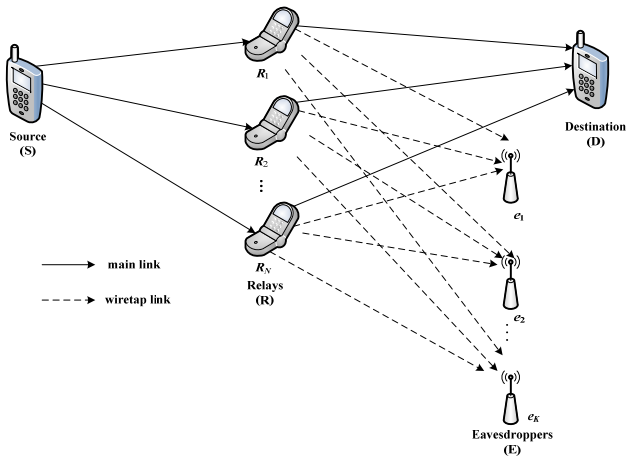



**FIGURE 2.** Cooperative wireless network consists of S, D and *N* relays in the presence of *K* eavesdroppers.

factor $m_{si}$, $m_{id}$ and $m_{ie_j}$, respectively. We denote the set of $N$ relays as $R = \{R_i | i = 1, 2, ..., N\}$, where these relays employ DF cooperative protocol to forward the signals.

S first broadcasts the signal $x$ to $N$ relays. These relays try to decode the original signal $x$. For convenience, we use a set $\Phi$ to represent relays that can successfully decode the signal. Given $N$ relays, there are $2^N$ possible subsets. Hence, the decoding sample set is given as

$$\Phi = \left\{\phi, D_1, D_2, ..., D_{2^N-1}\right\} \tag{6}$$

where $\phi$ denotes the empty set, and $D_n$ represents the $n$th nonempty subset of $N$ relays. If $\Phi$ is empty, it indicates that all relays remain silent, and R and E can not decode the original signal $x$. If $\Phi$ is nonempty, we choose a best relay to decode and forward the signal $x$ to D. Considering S transmits $x$ to $N$ relays with power $P$ and rate $R_d$, we can express the received signal at $R_i$ as

$$y_i = h_{si}\sqrt{P}x + n_i \tag{7}$$

where $n_i$ is a zero-mean AWGN with variance $N_0$. We obtain the channel capacity between S and $R_i$ as

$$C_{si} = \frac{1}{2}\log_2\left(1 + |h_{si}|^2 \frac{P}{N_0}\right) \tag{8}$$

where 1/2 exists because of the requirement for two time slots to complete the transmission from S to D via $R_i$. According to Shannon coding theorem, when the channel capacity is lower than the transmission rate $C_{si} < R_d$, the $R_i$ is unable to decode the original transmit signal $x$. Hence, the case of $\Phi = \phi$ can be expressed as

$$\frac{1}{2}\log_2\left(1 + |h_{si}|^2 \frac{P}{N_0}\right) < R_d, \quad R_i \in R \tag{9}$$

Similarly, the decoding sample set $\Phi = D_n$ can be described as the following two equations

$$\begin{aligned} &\frac{1}{2}\log_2\left(1 + |h_{si}|^2 \frac{P}{N_0}\right) > R_d, \quad R_i \in D_n \\ &\frac{1}{2}\log_2\left(1 + |h_{sr}|^2 \frac{P}{N_0}\right) < R_d, \quad R_r \in \overline{D_n} \end{aligned} \tag{10}$$

where $\overline{D_n} = R - D_n$ is the complement of $D_n$. When $\Phi = D_n$, we choose a relay from $D_n$ as the best relay to forward its decoded signal with power $P$ and rate $R_d$, hence, the received signal at D can be written as

$$y_d = h_{id}\sqrt{P}x + n_d \tag{11}$$

where $n_d$ is a zero-mean AWGN with variance $N_0$. From (11), the capacity between $R_i$ and D can be expressed as

$$C_{id} = \frac{1}{2}\log_2\left(1 + |h_{id}|^2 \frac{P}{N_0}\right) \tag{12}$$

We choose the best relay that has the highest channel capacity $C_{id}$. From (12), the best relay selection criterion is described as

$$\text{Best relay} = \arg\max_{R_i \in D_n} C_{id} = \arg\max_{R_i \in D_n} |h_{id}|^2 \tag{13}$$

From the best relay selection criterion, we only need to know the channel information $|h_{id}|^2$ rather than the information of eavesdroppers. From (12) and (13), the capacity between the best relay and D can be written as

$$C_{bd} = \frac{1}{2}\max_{R_i \in D_n} \log\left(1 + |h_{id}|^2 \frac{P}{N_0}\right) \tag{14}$$

From (14), the subscript 'b' represents the best relay. However, the eavesdroppers can overhear the transmission between the best relay and D at the same time. We denote the signal received at the eavesdroppers as

$$y_{e_j} = h_{be_j}\sqrt{P}x + n_e \tag{15}$$

Wiretap channel capacity spanning from the best relay to $e_j$ can be written as

$$C_{be_j} = \frac{1}{2}\log_2\left(1 + \left|h_{be_j}\right|^2 \frac{P}{N_0}\right) \tag{16}$$

Assume that the eavesdroppers are independent of each other during the interception of legitimate transmission phase. Without loss of generality, the worst case that the maximum wiretap channel capacity between the best relay and the selected eavesdropper is considered. That is,

$$C_{be} = \max_{e_j \in E} \frac{1}{2}\log_2\left(1 + \left|h_{be_j}\right|^2 \frac{P}{N_0}\right) \tag{17}$$

## III. SECURITY-RELIABILITY TRADEOFF ANALYSIS OVER NAKAGAMI-m FADING CHANNELS

In this section, we perform SRT analysis on direct transmission and JRES strategy over Nakagami-*m* fading channels. The channel fading coefficients $|h_{sd}|^2$, $|h_{si}|^2$, $|h_{id}|^2$, $\left|h_{ie_j}\right|^2$, $\left|h_{be_j}\right|^2$ follow gamma distribution, with average power $\Omega_{sd}, \Omega_{si}, \Omega_{id}, \Omega_{ie_j}, \Omega_{be_j}$. We refer to [23] and [24], the probability density function (PDF) of $Z \in \left\{|h_{sd}|^2, |h_{si}|^2, |h_{id}|^2, \left|h_{ie_j}\right|^2, \left|h_{be_j}\right|^2\right\}$ can be expressed as

$$f_Z(z) = \frac{z^{m_z - 1}}{\Gamma(m_z)}\left(\frac{m_z}{\Omega_z}\right)^{m_z} e^{-z\frac{m_z}{\Omega_z}} \tag{18}$$

where $m = 1$ is Rayleigh distribution, and $\Gamma(x)$ is gamma function defined by $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$ [24]. In (18), $\Omega_Z = E[Z^2]$ and the parameter $m_Z$ is defined as the ratio of moments shown as $m_Z = \frac{\Omega_Z^2}{E[(Z^2-\Omega_Z)^2]}$, $m_Z \geq \frac{1}{2}$ [24]. We use OP and IP to quantify reliability and security respectively. If channel capacity of the main link is lower than the transmission rate, an outage event occurs, whereas the channel capacity of the wiretap link is higher than the transmission rate, an intercept event occurs [14]–[16], [25], [26]. Here, we discuss the direct transmission of OP, IP and SRT analysis.

### A. DIRECT TRANSMISSION

According to the concept described above and the direct transmission channel capacity shown in (3), the OP of direct transmission can be written as

$$\begin{aligned}\Pr_{\text{out}}^{\text{direct}} &= \Pr\left(C_{sd} < R_d\right) \\ &= \Pr\left(|h_{sd}|^2 < \alpha\right)\end{aligned} \tag{19}$$

where $\alpha = \left(2^{R_d} - 1\right)/\gamma$, $\gamma = \frac{P}{N_0}$. Since $|h_{sd}|^2$ follows the gamma distribution with PDF shown in (18), (19) becomes

$$\Pr_{\text{out}}^{\text{direct}} = 1 - \frac{\Gamma\left(m_{sd}, \frac{m_{sd}}{\Omega_{sd}}\alpha\right)}{\Gamma\left(m_{sd}\right)} \tag{20}$$

where $\Gamma(x, y)$ is an incomplete gamma function and $\Gamma(x)$ is gamma function [24]. Additionally, combining with the concept of IP and the wiretap channel capacity shown in (5) [26], we can obtain the IP of direct transmission as below.

$$\begin{aligned}\Pr_{\text{int}}^{\text{direct}} &= \Pr\left(C_{se} > R_d\right) \\ &= \Pr\left(\max_{e_j \in E} |h_{se_j}|^2 > \alpha\right) \\ &= 1 - \prod_{e_j \in E}\left[1 - \frac{\Gamma\left(m_{se_j}, \frac{m_{se_j}}{\Omega_{se_j}}\alpha\right)}{\Gamma\left(m_{se_j}\right)}\right]\end{aligned} \tag{21}$$

Without loss of generality, we assume that $m_{sd} = m_m$, $m_{se_j} = m_e$, $\Omega_{sd} = \Omega_m$, $\Omega_{se_j} = \Omega_e$. Eqs. (20) and (21) can be expressed as

$$\Pr_{\text{out}}^{\text{direct}} = 1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\alpha\right)}{\Gamma\left(m_m\right)} \tag{22}$$

$$\Pr_{\text{int}}^{\text{direct}} = 1 - \left[1 - \frac{\Gamma\left(m_e, \frac{m_e}{\Omega_e}\alpha\right)}{\Gamma\left(m_e\right)}\right]^K \tag{23}$$

### B. JOINT RELAY AND EAVESDROPPER SELECTION

When $\Phi = \phi$, no relay can decode signal $x$, and D can not receive any information. Hence, the outage event occurs. When $\Phi = D_n$, some relays can successfully decode the original signal, and we choose the best relay to forward its decoded signal to D. However, if $C_{bd}$ is less than the transmission rate, the outage event also occurs. Thus, we use the law of total probability, the OP of best relay selection scheme is obtained as

$$\Pr_{\text{out}}^{\text{JRES}} = \Pr\left(\Phi = \phi\right) + \sum_{n=1}^{2^N-1} \Pr\left(\Phi = D_n\right) \Pr\left(C_{bd} < R_d\right) \tag{24}$$

From (9), the probability of $\Phi = \phi$ is obtained as

$$\begin{aligned}\Pr\left(\Phi = \phi\right) &= \prod_{i=1}^{N} \Pr\left(\frac{1}{2}\log_2\left(1 + |h_{si}|^2 \frac{P}{N_0}\right) < R_d\right) \\ &= \prod_{i=1}^{N} \Pr\left(|h_{si}|^2 < \beta\right) \\ &= \prod_{i=1}^{N}\left[1 - \frac{\Gamma\left(m_{si}, \frac{m_{si}}{\Omega_{si}}\beta\right)}{\Gamma\left(m_{si}\right)}\right]\end{aligned} \tag{25}$$

where $\beta = \left(2^{2R_d} - 1\right)/\gamma$. Similarly, from (10), the probability of $\Phi = D_n$ is given by

$$\begin{aligned}&\Pr\left(\Phi = D_n\right) \\ &= \prod_{R_i \in D_n} \Pr\left(\frac{1}{2}\log_2\left(1 + |h_{si}|^2 \frac{P}{N_0}\right) > R_d\right) \\ &\quad \times \prod_{R_r \in \overline{D_n}} \Pr\left(\frac{1}{2}\log_2\left(1 + |h_{sr}|^2 \frac{P}{N_0}\right) < R_d\right) \\ &= \prod_{R_i \in D_n} \Pr\left(|h_{si}|^2 > \beta\right) \times \prod_{R_r \in \overline{D_n}} \left(\Pr|h_{sr}|^2 < \beta\right) \\ &= \prod_{R_i \in D_n} \frac{\Gamma\left(m_{si}, \frac{m_{si}}{\Omega_{si}}\beta\right)}{\Gamma\left(m_{si}\right)} \times \prod_{R_i \in \overline{D_n}}\left[1 - \frac{\Gamma\left(m_{sr}, \frac{m_{sr}}{\Omega_{sr}}\beta\right)}{\Gamma\left(m_{sr}\right)}\right]\end{aligned} \tag{26}$$

In (24), $\Pr\left(C_{bd} < R_d\right)$ can be obtained from (14) as

$$\begin{aligned}\Pr\left(C_{bd} < R_d\right) &= \Pr\left(\frac{1}{2}\max_{R_i \in D_n} \log\left(1 + |h_{id}|^2 \frac{P}{N_0}\right) < R_d\right) \\ &= \Pr\left(\max_{R_i \in D_n} |h_{id}|^2 < \beta\right) \\ &= \prod_{R_i \in D_n}\left[1 - \frac{\Gamma\left(m_{id}, \frac{m_{id}}{\Omega_{id}}\beta\right)}{\Gamma\left(m_{id}\right)}\right]\end{aligned} \tag{27}$$

Here, we assume that $m_{si} = m_{id} = m_{rd} = m_m$, $\Omega_{si} = \Omega_{id} = \Omega_{rd} = \Omega_m$, and we can simplify Eqs. (24) to (26) as the following equations.

$$\Pr\left(\Phi = \phi\right) = \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right]^N \tag{28}$$

$$\begin{aligned}\Pr\left(\Phi = D_n\right) = &\left[\frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right]^{|D_n|} \\ &\times \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right]^{|\overline{D_n}|}\end{aligned} \tag{29}$$

$$\Pr\left(C_{bd} < R_d\right) = \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right]^{|D_n|} \tag{30}$$

where $|D_n|$ and $\left|\overline{D_n}\right|$ represent the cardinalities of the set $D_n$ and $\overline{D_n}$. Substituting (28) and (30) into (24), we can get the closed-form expression of outage probability for the best relay selection scheme shown as below.

$$\begin{aligned}\Pr_{\text{out}}^{\text{JRES}} &= \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right]^N \\ &\quad \times \left[1 + \sum_{n=1}^{2^N-1}\left[\frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right]^{|D_n|}\right] \\ &= \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right]^N \times \left[1 + \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right]^N \\ &= \left[1 - \left(\frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right)^2\right]^N \end{aligned} \tag{31}$$

Additionally, when $\Phi = \phi$, no relay is able to decode the signal. Hence, no relay will assist to transmit signal to D and $C_{be} = 0$. When $\Phi = D_n$, eavesdropper E will overhear the transmission between the best relay and D. If $C_{be} > R_d$, an intercept event occurs [14]–[16], [26]. The probability of IP can be expressed as

$$\Pr_{\text{int}}^{\text{JRES}} = \sum_{n=1}^{2^N-1} \Pr\left(\Phi = D_n\right) \Pr\left(C_{be} > R_d\right) \tag{32}$$

From (17), we get the expression of $\Pr\left(C_{be} > R_d\right)$ shown as below.

$$\begin{aligned}\Pr\left(C_{be} > R_d\right) &= \Pr\left(\max_{e_j \in E} \left|h_{be_j}\right|^2 > \beta\right) \\ &= 1 - \prod_{e_j \in E} \Pr\left(\left|h_{be_j}\right|^2 < \beta\right) \end{aligned} \tag{33}$$

In addition, according to the derivation in the Appendix, we obtain $\Pr\left(\left|h_{be_j}\right|^2 < \beta\right)$ as shown in (34),

$$\begin{aligned}\Pr\left(\left|h_{be_j}\right|^2 < \beta\right) &= \sum_{R_i \in D_n}\left[1 + \sum_{q=1}^{2^{|D_n|-1}-1}\sum_{p=0}^{(m_m-1)|A_q|}(-1)^{|A_q|}\right. \\ &\quad \left.\times \frac{\Gamma\left(p + m_m\right)}{\Gamma\left(m_m\right)} \frac{a_p^{|A_q|,m_m}}{\left(\left|A_q + 1\right|\right)^{p+m_m}}\right] \\ &\quad \times \left[1 - \frac{\Gamma\left(m_{ie_j}, \frac{m_{ie_j}}{\Omega_{ie_j}}\beta\right)}{\Gamma\left(m_{ie_j}\right)}\right] \end{aligned} \tag{34}$$

where $A_q$ is the $q$-th non-empty subset of $\{D_n - i\}$, and $\left|A_q\right|$ is the cardinalities of the set $A_q$. According to [23], $a_w^{c,d}$ $(0 \le w \le c\,(d-1))$ can be calculated by

$$\begin{aligned} a_0^{c,d} &= 1, \quad a_1^{c,d} = c, \\ a_w^{c,d} &= \frac{1}{w}\sum_{i=1}^{\min(w,d-1)} \frac{i\,(c+1) - w}{i!} a_{w-i}^{c,d}, \quad 2 \le w < c\,(d-1) \\ a_w^{c,d} &= \frac{1}{[(d-1)!]^c}, \quad w = c\,(d-1) \end{aligned}$$

Thus, we can substitute (34) into (33) to get $\Pr\left(C_{be} > R_d\right)$. Then, it is combined with (29) to get the closed-form of IP expression. To simplify the formula [14]–[16], [26], we consider $m_{ie_j} = m_e$, $\Omega_{ie_j} = \Omega_e$, and rewrite (34) as

$$\Pr\left(\left|h_{be_j}\right|^2 < \beta\right) = 1 - \frac{\Gamma\left(m_e, \frac{m_e}{\Omega_e}\beta\right)}{\Gamma\left(m_e\right)} \tag{35}$$

From (33), we can obtain $\Pr\left(C_{be} > R_d\right)$ as follows

$$\Pr\left(C_{be} > R_d\right) = 1 - \left[1 - \frac{\Gamma\left(m_e, \frac{m_e}{\Omega_e}\beta\right)}{\Gamma\left(m_e\right)}\right]^K \tag{36}$$

Substituting (29) and (36) into (32), and we consider $m_{se} = m_{ie} = m_e$, $\Omega_{se} = \Omega_{ie} = \Omega_e$ for simplicity [14]–[16], [26]. We can get the probability of IP shown as below

$$\begin{aligned}\Pr_{\text{int}}^{\text{JRES}} &= \left[1 - \left(1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}\beta\right)}{\Gamma\left(m_m\right)}\right)^N\right] \\ &\quad \times \left[1 - \left[1 - \frac{\Gamma\left(m_e, \frac{m_e}{\Omega_e}\beta\right)}{\Gamma\left(m_e\right)}\right]^K\right] \end{aligned} \tag{37}$$

When $N \to \infty$, the former part of (37) approaches 1. Hence, the closed expression of IP can be written as

$$\Pr_{int}^{\text{JRES}} = 1 - \left[1 - \frac{\Gamma\left(m_e, \frac{m_e}{\Omega_e}\beta\right)}{\Gamma\left(m_e\right)}\right]^K \tag{38}$$

## IV. NUMERICAL RESULTS AND PERFORMANCE ANALYSIS

In this section, we provide numerical SRT performance of direct transmission and the proposed JRES scheme. The IP and OP of the direct transmission and JRES schemes are presented via Eqs. (22), (23), (31) and (38). Here, the mean powers are specified as $\Omega_m = 1$ and $\Omega_e = 0.1$. Furthermore, we assume the normalized transmission rate as $R_d = 1$ bit/s/Hz [14]–[16], [25].

Fig. 3 indicates SRT performance of direct transmission and JRES scheme with different channel fading factors. We assume that the number of eavesdropper $K = 2$ and the number of relay $N = 4$. It shows that OP is increasing whereas IP is decreasing, which reveals that it has a tradeoff between OP and IP. The proposed JRES scheme outperforms direct transmission for the same channel fading factor $m$. For Rayleigh channel fading factor $m = 1$, it performs the same

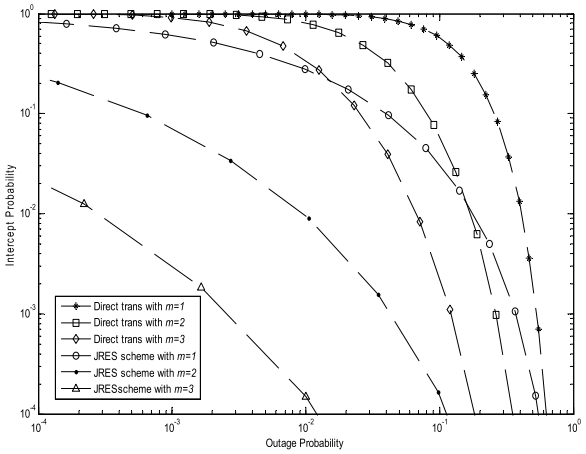



**FIGURE 3.** SRT performance of direct transmission and JRES scheme with different channel fading factors.

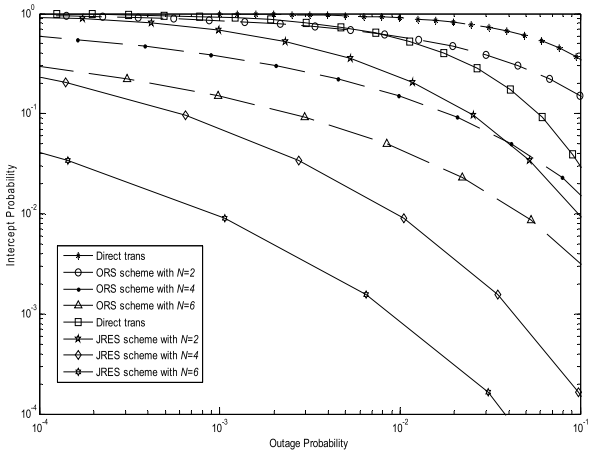



**FIGURE 5.** SRT performance of direct transmission and JRES scheme with multiple relays.

as SRT performance shown in [14], which indicates that the proposed JRES scheme extends the SRT performance to general cases with different channel fading factors. It is revealed that the increasing of channel fading factor $m$ improves SRT performance for both direct transmission and JRES strategy.

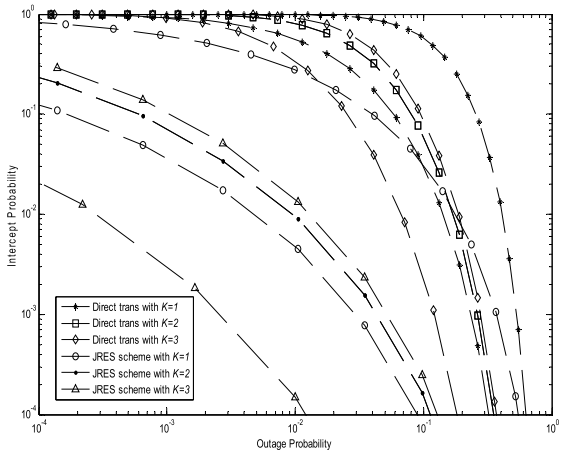



**FIGURE 4.** SRT performance of direct transmission and JRES scheme with multiple eavesdroppers.

Fig. 4 shows SRT performance of direct transmission and JRES scheme with different number of eavesdroppers. We assume that Nakagami channel fading factor $m = 2$ and the number of relay $N = 4$. It shows that OP is increased whereas IP is decreased. The proposed JRES scheme outperforms direct transmission in the same number of eavesdropper scenario. For multiple eavesdroppers, the proposed JRES scheme selects the eavesdropper via the worst case that the maximum wiretap channel capacity is considered for each independent eavesdropper non-cooperative case. It is apparent that the proposed JRES scheme enhances SRT performance and significantly improves system security. In addition, either for direct transmission or for JRES scheme, SRT performance is decreased with the increasing of eavesdropper numbers, which indicates eavesdropping attack affect relay transmission obviously.

Fig. 5 shows the SRT performance of direct transmission and JRES scheme with different number of relays. The dotted lines are SRT performance of ORS shown in [15], whereas the solid lines are SRT performance of the proposed JRES scheme. We set Nakagami channel fading factor $m = 2$ and the number of eavesdropper $K = 2$. From this figure, we observe that IP is inversely proportional to OP. For ORS scheme, it considers Rayleigh fading channel factor $m = 1$ and there is only one eavesdropper $K = 1$ [15]. For a special value of OP, the IP of JRES scheme corresponding to $N = 2, N = 4$ and $N = 6$ are lower than that of direct transmission, which implies that JRES scheme outperforms direct transmission. Compared with the dotted line of ORS scheme [15], it shows that JRES scheme performs better in the same relay and eavesdropper number scenario. Hence, it extends the performance of ORS scheme to a general case.

## V. CONCLUSIONS

In this paper, JRES scheme for cooperative DF relay network with multiple relays in the presence of multiple eavesdroppers over Nakagami-*m* fading channels is investigated. Different from the present literatures about joint relay and jammer selection for PLS in cooperative communication networks, the proposed JRES strategy investigates multiple eavesdroppers attacking scenario, and extends PLS and SRT performance analysis to a more general case. We use the direct transmission and ORS scheme over Rayleigh fading channel as the benchmark. SRT performance analysis shows that the proposed JRES scheme outperforms the direct transmission and ORS scheme over Rayleigh channel. Moreover, with the increasing of relay numbers and Nakagami channel fading factors, SRT performance of the proposed JRES scheme outperforms ORS scheme, which enhances the security significantly for cooperative DF relay networks.

## APPENDIX
## DERIVATION OF (34)

According to (13), we choose the best relay from $D_n$ to transmit signal to D. We have $|h_{id}|^2 > \max\limits_{R_r\in\{D_n-i\}} |h_{rd}|^2$, where "-" represents the difference set. Then, we use the law of total probability, (34) can be expressed as

$$\Pr\left(\left|h_{be_j}\right|^2 < \beta\right) = \sum_{R_i\in D_n} \Pr\left(\left|h_{ie_j}\right|^2 < \beta\right) \Pr\left(\max_{R_r\in\{D_n-i\}} |h_{rd}|^2 < |h_{id}|^2\right) \quad \text{(A1)}$$

where

$$\Pr\left(\left|h_{ie_j}\right|^2 < \beta\right) = 1 - \frac{\Gamma\left(m_{ie_j}, \frac{m_{ie_j}}{\Omega_{ie_j}}\beta\right)}{\Gamma\left(m_{ie_j}\right)} \quad \text{(A2)}$$

Let $|h_{id}|^2 = y$, we have the following equation (A3).

Assume that $m_{id} = m_{rd} = m_m$, $\Omega_{id} = \Omega_{rd} = \Omega_m$, we can rewrite (A3) as (A4).

With the reference of [15, eqs. (3.326.2), (8.339.1), and (8.352.7)], we can get (A5).

Substituting (A2) and (A5) into (A1), and we have (34).

$$\begin{aligned}
&\Pr\left(\max_{R_r\in\{D_n-i\}} |h_{rd}|^2 < |h_{id}|^2\right) \\
&= \int_0^\infty \prod_{R_r\in\{D_n-i\}} \left[1 - \frac{\Gamma\left(m_{rd}, \frac{m_{rd}}{\Omega_{rd}}y\right)}{\Gamma\left(m_{rd}\right)}\right] \frac{y^{m_{id}-1}}{\Gamma\left(m_{id}\right)} \left(\frac{m_{id}}{\Omega_{id}}\right)^{m_{id}} \\
&\quad \times \exp\left(-y\frac{m_{id}}{\Omega_{id}}\right) dy \\
&= \int_0^\infty \left[1 + \sum_{q=1}^{2^{|D_n|-1}-1} (-1)^{|A|_q} \prod_{R_r\in A_q} \frac{\Gamma\left(m_{rd}, \frac{m_{rd}}{\Omega_{rd}}y\right)}{\Gamma\left(m_{rd}\right)}\right] \\
&\quad \times \frac{y^{m_{id}-1}}{\Gamma\left(m_{id}\right)} \left(\frac{m_{id}}{\Omega_{id}}\right)^{m_{id}} \exp\left(-y\frac{m_{id}}{\Omega_{id}}\right) dy \\
&= 1 + \sum_{q=1}^{2^{|D_n-1|}-1} (-1)^{|A_q|} \frac{1}{\Gamma\left(m_{id}\right)} \left(\frac{m_{id}}{\Omega_{id}}\right)^{m_{id}} \\
&\quad \times \int_0^\infty \prod_{R_r\in A_q} \frac{\Gamma\left(m_{rd}, \frac{m_{rd}}{\Omega_{rd}}y\right)}{\Gamma\left(m_{rd}\right)} y^{m_{id}-1} \exp\left(-y\frac{m_{id}}{\Omega_{id}}\right) dy
\end{aligned} \quad \text{(A3)}$$

$$\begin{aligned}
&\Pr\left(\max_{R_r\in\{D_n-i\}} |h_{rd}|^2 < |h_{id}|^2\right) \\
&= 1 + \sum_{q=1}^{2^{|D_n-1|}-1} (-1)^{|A_q|} \frac{1}{\Gamma\left(m_m\right)} \left(\frac{m_m}{\Omega_m}\right)^{m_m} \\
&\quad \times \int_0^\infty \left[\frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m}y\right)}{\Gamma\left(m_m\right)}\right]^{|A_q|} y^{m_m-1} \exp\left(-y\frac{m_m}{\Omega_m}\right) dy
\end{aligned} \quad \text{(A4)}$$

$$\begin{aligned}
&\Pr\left(\max_{R_r\in\{D_n-i\}} |h_{rd}|^2 < |h_{id}|^2\right) \\
&= 1 + \sum_{q=1}^{2^{|D_n-1|}-1} \sum_{p=0}^{(m_m-1)|A_q|} (-1)^{|A_q|} \frac{\Gamma\left(p+m_m\right)}{\Gamma\left(m_m\right)} \\
&\quad \times \frac{a_p^{|A_k, m_m|}}{\left(|A_q+1|\right)^{p+m_m}}
\end{aligned} \quad \text{(A5)}$$

## REFERENCES


[1] S. V. Kartalopoulos, "A primer on cryptography in communications," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 146–151, Apr. 2006.

[2] 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, Aug. 2014.

[3] Manu and A. Goel, "Encryption algorithm using dual modulus," in *Proc. 3rd Int. Conf. Comput. Intell. Commun. Technol. (CICT)*, Ghaziabad, India, Feb. 2017, pp. 1–4.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[5] A. D. Wyner, "The wiretap channel" *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] S. K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[7] Y. Zhuang and L. Lampe, "Physical layer security in MIMO power line communication networks," in *Proc. 18th IEEE Int. Symp. Power Line Commun. Apps.*, Glasgow, U.K., Mar./Apr. 2014, pp. 272–277.

[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[9] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[10] 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.

[11] Y. Gao *et al.*, "Physical layer security in 5G based large scale social networks: Opportunities and challenges," *IEEE Access*, vol. 6, pp. 26350–26357, 2018.

[12] Y. Yao, W. Zhou, B. Kou, and Y. Wang, "Dynamic spectrum access with physical layer security: A game-based jamming approach," *IEEE Access*, vol. 6, pp. 12052–12059, 2018.

[13] J. Zhang *et al.*, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[14] J. Zhu, Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Security–reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5825–5831, Jul. 2016.

[15] 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.

[16] Y. Zou, J. Zhu, X. Li, and L. Hanzo, "Relay selection for wireless communications against eavesdropping: A security-reliability trade-off perspective," *IEEE Netw.*, vol. 30, no. 9, pp. 74–79, Sep. 2016.

[17] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

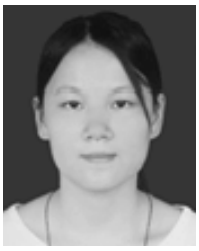
[18] Y. Yuan, R. Zhao, H. Lin, and A. Liu, "Secrecy outage probability of cognitive decode-and-forward relay networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 260–265.

[19] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[20] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259–6274, Aug. 2016.

[21] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2180–2193, May 2017.
[22] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Joint cooperative beamforming and jamming for physical-layer security of decode-and-forward relay networks," *IEEE Access*, vol. 5, pp. 19620–19630, 2017.
[23] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, and D. Zwillinger, Eds., *Table of Integrals, Series, and Products*, 7th ed. San Francisco, CA, USA: Academic, 2007, pp. 659–667.
[24] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2008, pp. 365–367.
[25] H. Huang, W. Sun, J. Yang, and G. Gui, "Relay selections for security and reliability in mobile communication networks over Nakagami-*m* fading channels," *Secur. Commun. Netw.*, vol. 2017, no. 9, Sep. 2017, Art. no. 2569239. doi: 10.1155/2017/2569239.
[26] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 780–787, Apr. 2016.

**QIAN GUO** received the B.Eng. and Ph.D. degrees in electrical engineering from Zhejiang University (ZJU), Hangzhou, China, in 2010 and 2016, respectively. She is currently a Lecturer with the College of Mechanical and Electrical Engineering, China Jiliang University (CJLU), Hangzhou. Her research interests include energy efficiency and physical layer security in cooperative communication and microgrids, control of inverters in microgrids, and distributed generation systems. She is also a member of the Working Committee of the Women Scientists in China Power Supply Society.



**WEI FENG** received the B.Eng. degree in electronics and information engineering from Hubei Engineering University, Xiaogan, China, in 2005, and the M.Eng. and Ph.D. degrees in information and communication engineering from the South China University of Technology, Guangzhou, China, in 2009 and 2014, respectively. From 2005 to 2006, she was an FAE with LITE-ON Technology Cooperation, Guangzhou. From 2009 to 2011, she was a Network Engineer with Huaxin Consulting Co. Ltd., Hangzhou, China. She is currently a Lecturer with the School of Communication Engineering, Hangzhou Dianzi University (HDU), Hangzhou. Her research interests include energy efficiency and physical layer security in future wireless communication.