IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 12, 2018, accepted August 20, 2018, date of publication September 4, 2018, date of current version October 8, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2868500

Cooperative Interference and Power Allocation in a Bidirectional Untrusted Relay Network With Channel Estimation Errors

LIHUA GONG[1], XIAOXIU DING[1], QIBIAO ZHU[1], AND NANRUN ZHOU[1,2], (Member, IEEE)

[1]Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
[2]Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding author: Nanrun Zhou (znr21@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61561033, in part by the Major Academic Discipline and Technical Leader of Jiangxi Province under Grant 20162BCB22011, in part by the Natural Science Foundation of Jiangxi Province under Grant 20171BAB202002, and in part by the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security under Grant AGK2018002 and AGK201602.

ABSTRACT The secure communication of a two-way untrusted amplify-and-forward relay network under the imperfect channel state information is investigated. To improve the secrecy of the relay wiretap system, artificial noise is introduced into each source signal. The total and the individual power constraint conditions are considered. To maximize the attainable secrecy rate, an iterative power allocation algorithm is designed under the total power constraint. As a more practical system design, a suboptimal power allocation scheme is proposed. For the sake of comparison, the security performances of the noncooperative interference strategy and the one-way cooperative interference strategy are also investigated. Simulation results demonstrate that the proposed bidirectional cooperative interference schemes perform better in the secrecy rate of communication system.

INDEX TERMS Untrusted relay network, imperfect channel state information, physical layer security, cooperative interference, power allocation.

I. INTRODUCTION

The inherent broadcast nature and the explosive increase of wireless media bring challenges to wireless communication security. The traditional security scheme is to adopt encryption algorithms and encryption keys on upper layers [1]. Considering the cost of traditional encryption algorithms and the improvement of computer processors, physical layer security (PLS) emerges as a complement or substitute for the upper layer encryption algorithm [2]. The pioneer work of PLS can be traced to Wyner, who built a wiretap channel model and indicated that secure communication can be achieved without using pre-shared secret key if the source-eavesdropper channel is inferior to the main one [3]. Later, Wyner's result was extended to broadcast channel and Gaussian wiretap channel [4], [5]. Subsequently, researchers studied the security issues of single-user multi-antenna systems such as multiple-input-multiple-output (MIMO) systems and multiple-input-single-output (MISO) systems [6], [7].

Based on multi-antenna technology, wireless cooperative communication technology was proposed, where cooperative relays were employed in single antenna systems to gain spatial diversity [8]. Several basic relay protocols, i.e., decode-and-forward (DF), amplify-and-forward (AF), were considered in single-relay and multi-relay systems [9], [10]. Multiple relay nodes could employ beamforming technology to adjust the phase and the amplitude of the emission signal to maximize the signal-noise ratio at the receiver [10]. Several relay selection schemes, such as, maximizing system capacity, maximizing energy-efficiency and minimizing system outage probability were proposed to enhance the transmission effectiveness [11]–[14].

To ensure that the quality of the channel of the legitimate users is superior to that of the eavesdropping channels, Dong *et al.* further proposed a cooperative interference technique based on cooperative communication technology, where the relay node transmits artificial noise signals to weaken the hacking channel quality [15]. Huang *et al.* introduced the destination assisted collaborative jamming technology [16]. Jeong *et al.* introduced jammers from external networks to ensure secure communication of MIMO systems [17]. A new cooperative interference method namely self-interference was devised, in which the source sends

a mixture of useful and interfering signals to confuse eavesdroppers [18].

All schemes mentioned above involve trusted relays. The relay node may also assist the eavesdropper or the relay node itself may also be an eavesdropper, where the latter case is called untrusted relay. It was proved that the untrusted AF relay network can still achieve secure transmission [19]. The trade-off between secrecy rate and energy efficiency was researched in the simultaneous wireless information and power transfer untrusted bidirectional relaying network [20].

The combination of two-way relay network and physical-layer network coding (PLNC) can fully exploit the spectrum potential and has become a promising research topic. Several two-way relay strategies such as denoise-and-forward (DNF) scheme and DNF-AF selection scheme have been presented to alleviate noise and improve bandwidth efficiency [21], [22]. The performances of the cooperative interference technique in two-way relay scenarios were also investigated. Long investigated the performance of the self-interference approach in a two-way multi-antenna relay scenario [23]. The self-interference technique was employed to enhance the security performance of the bidirectional untrusted relay network in [24].

Considering that perfect channel state information (CSI) is hard to obtain in realistic scenario, Mekkawy discussed the optimal power allocation of cooperative interference in a one-way AF untrusted relay network with bounded channel estimation error [25]. The impact of channel estimation errors on the achievable secrecy rate in the PLNC based full-duplex two-way relay system was investigated [26], [27].

The work in this paper differs from most previous works: (1) No jammers are introduced, thus there is no need to consider the synchronization of source and jammers, extra overhead of the system is avoided, and system network node resources are fully utilized; (2) To our best knowledge, the security performance of the bidirectional untrusted relay system based on cooperative interference under imperfect CSI has never been discussed so far. In fact, it isn't always possible to know the perfect CSI. It is more practical to discuss the security performance of the model under imperfect CSI.

An in-vehicle communication system adopting a mobile vehicle as a relay will be considered, where two sources could communicate via an untrusted in-vehicle communication relay. The transmit power of each source includes two parts: a message portion and an artificial noise one. The model is investigated under the imperfect CSI with detailed physical-layer security analysis. The optimal power allocation for the two-way two-slot untrusted relay system under the imperfect CSI is investigated to reach the maximal secrecy rate. For the sake of comparison, the power allocation schemes and security performances of the baseline strategies (the noncooperative interference strategy and the one-way cooperative interference strategy) under the imperfect CSI are also studied. Our contributions include: (1) we discuss the security performance of artificial noise-aided two-way untrusted relay networks under imperfect CSI; (2) we provide an iterative power allocation algorithm under the total power constraint; (3) we derive a power allocation closed-form optimal solution under per-node power constraint.

The style of this paper is as follows. The considered system model is introduced in Section II. Power allocation schemes and their corresponding secrecy rates are described in Section III. Simulation results with discussions are demonstrated in Section IV and a brief conclusion is drawn in Section V.

II. SYSTEM MODEL

As shown in Fig. 1, the considered communication system is composed of two sources S_1 and S_2 and an untrusted in-vehicle relay R, where two sources can only communicate with the help of the untrusted relay. The source nodes and the untrusted relay node are all equipped with single antenna working in the time-division half-duplex mode. During the information transmission, both S_1 and S_2 broadcast hybrid data involving message signal and jamming signal to the untrusted relay node, while the relay intercepts and amplifies the received information from S_1 and S_2 before forwarding it to the two sources [24]. Assume the channel of the considered wireless cooperative communication system is a slow, flat and Rayleigh fading channel.

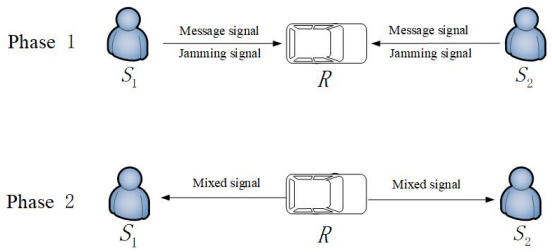

FIGURE 1. System model for two-way untrusted relay network.

In the first phase, $S_i(i = 1, 2)$ sends signal $X_{S_i,R}$ to the untrusted relay.

$$X_{S_1,R} = \sqrt{k_1 P} I_1 + \sqrt{k_3 P} J_1 \tag{1}$$

$$X_{S_2,R} = \sqrt{k_2 P} I_2 + \sqrt{k_4 P} J_2 \tag{2}$$

The signal received by the relay, i.e., the eavesdropper, can be written as

$$Y_R = \sqrt{k_1 P} h I_1 + \sqrt{k_2 P} f I_2 + \sqrt{k_3 P} h J_1 + \sqrt{k_4 P} f J_2 + n_R. \tag{3}$$

In practice, CSI can be obtained through pilot-symbol-assisted channel estimation techniques. Given the estimation errors, the channel coefficients can be expressed as [28]

$$h = \hat{h} + e_h, \tag{4}$$

$$f = \hat{f} + e_f. \tag{5}$$

For simplicity, the orthogonality between the estimated channel gain and the estimation error is assumed. According to [29], $\tau = \frac{\sigma_{e_h}^2}{\sigma_h^2} = \frac{\sigma_{e_f}^2}{\sigma_f^2}$ is defined as the channel estimation error factor. The nodes only know the estimated channel.

TABLE 1. Symbols and definitions.

Symbol	Description
S_i	Source node
R (E)	Untrusted relay node
P	Transmit power of R. Total transmit power of two sources.
h	Channel gain between S_1 and R. $h \sim \mathrm{CN}(0, \sigma_h^2)$, where $\sigma_h^2 = d_{S_1R}^{-u}$.
f	Channel gain between S_2 and R. $f \sim \mathrm{CN}\left(0, \sigma_f^2\right)$, where $\sigma_f^2 = d_{S_2R}^{-u}$.
d_{S_iR}	Channel gain between S_i and R.
u	Path-loss exponent
$\hat{h}$	Channel gain estimation between S_1 and R. $\hat{h} \sim \mathrm{CN}(0, (1-\tau)\sigma_h^2)$
$\hat{f}$	Channel gain estimation between S_2 and R. $\hat{f} \sim \mathrm{CN}\left(0, (1-\tau)\sigma_f^2\right)$
e_h	Channel estimation error between S_1 and R. $e_h \sim \mathrm{CN}(0, \sigma_{e_h}^2)$
e_f	Channel estimation error between S_2 and R. $e_f \sim \mathrm{CN}(0, \sigma_{e_f}^2)$
τ	Channel gain estimation error factor
I_i	Information signal sent by S_i with expectation $E\left\{\lvert I_i\rvert^2\right\} = 1$
J_i	Jamming signal sent by S_i with expectation $E\left\{\lvert J_i\rvert^2\right\} = 1$
k_1	Information signal power allocation factor of S_1
k_2	Information signal power allocation factor of S_2
k_3	Jamming signal power allocation factor of S_1
k_4	Jamming signal power allocation factor of S_2
n_R	Additive white Gaussian noise (AWGN) of R. $n_R \sim \mathrm{CN}(0, N_0)$
n_{S_i}	Additive white Gaussian noise of S_i. $n_{S_i} \sim \mathrm{CN}(0, N_0)$
$\Gamma_{S_i \to S_j}$	The signal interference noise ratio (SINR) of link from S_i to S_j
$\Gamma_{S_i \to E}$	The signal interference noise ratio (SINR) of link from S_i to E
R_{S_i}	Achievable secrecy rate for source S_i
R_S	System sum secrecy rate
$R_{S_i}^{\mathrm{I}}$	Achievable secrecy rate for source S_i of the suboptimal scheme
γ_1	$P\lvert h\rvert^2 / N_0$
γ_2	$P\lvert f\rvert^2 / N_0$
γ_3	$P\left\lvert \hat{h}\right\rvert^2 / N_0$
γ_4	$P\left\lvert \hat{f}\right\rvert^2 / N_0$
γ_5	$P{\sigma_{e_h}}^2 / N_0$
γ_6	$P{\sigma_{e_f}}^2 / N_0$

In the second phase, the relay amplifies and forwards the received signals to the two sources with the amplification coefficient ρ.

$$\rho = \sqrt{\frac{P}{N_0 + (k_1 + k_3) P\hat{h}^2 + (k_2 + k_4) P\hat{f}^2}} \tag{6}$$

By considering the channel estimation error, the received signals at two sources after self-interference cancellation are

$$\begin{aligned} Y_{S_1} = {} & \underbrace{\rho\sqrt{k_2 P}\hat{h}\hat{f} I_2}_{\text{signal}} + \underbrace{\rho\sqrt{k_1 P}{e_h}^2 I_1 + \rho\sqrt{k_3 P}{e_h}^2 J_1}_{\text{self - interference}} \\ & + \underbrace{(\hat{h}e_f + \hat{f}e_h + e_h e_f)(\rho\sqrt{k_2 P} I_2 + \rho\sqrt{k_4 P} J_2)}_{\text{additional noise}} \\ & + \underbrace{\rho(\hat{h} + e_h) n_R + n_{S_1}}_{\text{noise}}, \end{aligned} \tag{7}$$

$$\begin{aligned} Y_{S_2} = {} & \underbrace{\rho\sqrt{k_1 P}\hat{h}\hat{f} I_1}_{\text{signal}} + \underbrace{\rho\sqrt{k_2 P}{e_f}^2 I_2 + \rho\sqrt{k_4 P}{e_f}^2 J_2}_{\text{self - interference}} \\ & + \underbrace{(\hat{h}e_f + \hat{f}e_h + e_h e_f)(\rho\sqrt{k_1 P} I_1 + \rho\sqrt{k_3 P} J_1)}_{\text{additional noise}} \\ & + \underbrace{\rho(\hat{f} + e_f) n_R + n_{S_2}}_{\text{noise}}. \end{aligned} \tag{8}$$

The secrecy rate is the difference between the rates of main channel and eavesdropper channel [3]. Thus, the achievable secrecy rate for source S_i is

$$R_{S_i} = \left[\frac{1}{2}\log_2(1 + \Gamma_{S_i \to S_j}) - \frac{1}{2}\log_2(1 + \Gamma_{S_i \to E})\right]^+, \tag{9}$$

where $[x]^+ = \max\{0, x\}$, and $1/2$ means that the whole signal transmission is divided into two time slots. $\Gamma_{S_i \to S_j}$ $(i, j = 1, 2$ and $i \neq j)$ represents the SINR of link from S_i to S_j, while $\Gamma_{S_i \to E}$ represents the SINR of link from S_i to E. The sum secrecy rate of the whole system can be expressed as

$$\begin{aligned} R_S &= R_{S_1} + R_{S_2} \\ &= \left[\frac{1}{2}\log_2 \frac{1 + \Gamma_{S_1 \to S_2}}{1 + \Gamma_{S_1 \to E}}\right]^+ + \left[\frac{1}{2}\log_2 \frac{1 + \Gamma_{S_2 \to S_1}}{1 + \Gamma_{S_2 \to E}}\right]^+. \end{aligned} \tag{10}$$

III. POWER ALLOCATION AND SECURITY ANALYSIS

Two strategies can be applied to maximize the secrecy rate of the wireless cooperative communication system: (1) Increasing the rate of the main channel by increasing the transmit power of secrecy messages; (2) Reducing the rate of eavesdropping links by adding jamming to confuse eavesdroppers. In the following, we make a trade-off between the two approaches by rationally distributing the desired signal power and the interference signal power.

A. TOTAL POWER CONSTRAINT (THE OPTIMAL SCHEME)

We consider that the total power constraint of two source nodes is P. Under the imperfect CSI, channel coefficient estimates inevitably have deviations. The SINRs of link from S_i to S_j are respectively described in (11) and (12), as shown at the top of the next page.

The SINR of link from S_i to E is

$$\Gamma_{S_1 \to E}^{\mathrm{T}} = \frac{k_1 \gamma_1}{(k_2 + k_4)\gamma_2 + k_3 \gamma_1 + 1}, \tag{13}$$

$$\Gamma_{S_2 \to E}^{\mathrm{T}} = \frac{k_2 \gamma_2}{(k_1 + k_3)\gamma_1 + k_4 \gamma_2 + 1}. \tag{14}$$

Substituting (11) $\sim$ (14) into (10), one can deduce the secrecy rate of communication system for the total power constraint case under imperfect CSI. To obtain the maximal secrecy rate, source nodes S_1 and S_2 allocate the desired

$$\Gamma^{\mathrm{T}}_{S_1\to S_2} = \frac{k_1\gamma_3\gamma_4}{(k_2+k_4)\,\gamma_6{}^2 + (k_1+k_3)\,(\gamma_4\gamma_5+\gamma_3\gamma_6+\gamma_5\gamma_6+\gamma_3) + (1+k_2+k_4)\,\gamma_4+\gamma_6+1} \tag{11}$$

$$\Gamma^{\mathrm{T}}_{S_2\to S_1} = \frac{k_2\gamma_3\gamma_4}{(k_1+k_3)\,\gamma_5{}^2 + (k_2+k_4)\,(\gamma_4\gamma_5+\gamma_3\gamma_6+\gamma_5\gamma_6+\gamma_4) + (1+k_1+k_3)\,\gamma_3+\gamma_5+1} \tag{12}$$

signal power and the interference signal power properly by adjusting k_1, k_2, k_3 and k_4. The multi-variable optimization problem can be described as

$$\text{OP1:}\quad \max R_s\,(k_1,k_2,k_3,k_4)$$
$$\text{s.t.}\quad \begin{cases} k_1,k_2,k_3,k_4 \geq 0 \\ k_1+k_2+k_3+k_4 \leq 1 \\ \Gamma_{S_1\to S_2}\,(k_1,k_2,k_3,k_4) > \Gamma_{S_1\to E}\,(k_1,k_2,k_3,k_4) \\ \Gamma_{S_2\to S_1}\,(k_1,k_2,k_3,k_4) > \Gamma_{S_2\to E}\,(k_1,k_2,k_3,k_4). \end{cases}$$

OP1 is a nonlinear programming problem (NLP) under nonlinear inequality constraints. The interior-point method is very effective for solving large-scale nonlinear constraints. The basic idea of the interior-point method is to utilize the barrier function constructed by the objective function and the constraint functions to transform the original constraint optimization problem into an unconstrained optimization problem, and then solve the unconstrained optimization problem [30]. The inverse barrier function is used in this paper, and we will convert OP1 to an unconstrained optimization problem.

$$\arg\min F(x,\tau) = -R_s(x) + \tau\sum_{i=1}^{4}\frac{1}{g_i\,(x)}, \tag{15}$$

where $x=[k_1,k_2,k_3,k_4]$ and τ is the penalty factor and is a strict descending sequence in the optimization process. $g_i\,(x)$ is the bound constraint.

The quasi-Newton method [31] is adopted to solve the unconstrained optimization problem (15). For iterative point x_z^{c-1}, $p_z=-B_z^{-1}\nabla F(x_z^{c-1},\tau)$ is defined as the search direction. $\nabla F(x_z^{c-1},\tau)$ is the gradient of augmented objective function. According to the BFGS algorithm [32], the approximate Hessian matrix B_z instead of the real Hessian matrix is employed.

$$B_{z+1} = B_z - \frac{B_z s_z s_z^T B_z}{s_z^T B_z s_z} + \frac{y_z y_z^T}{y_z^T s_z}, \tag{16}$$

where $s_z = x_{z+1}^{c-1} - x_z^{c-1}$, s_z^T is the transposition of s_z, $y_k = \nabla F(x_{z+1}^{c-1},\tau) - \nabla F(x_z^{c-1},\tau)$, and B_0 is an identity matrix. Given the tolerance, the optimal solution to the unconstrained optimization problem (15) can be obtained after limited iterations. x^c and τ can be updated according to the solution of the (15). And the iterations will be terminated until the value of $\tau\sum_{i=1}^{4}\frac{1}{g_i(x^c)}$ is less than the tolerance of the interior point method.

B. INDIVIDUAL POWER CONSTRAINTS (THE SUBOPTIMAL SCHEME)

By taking into account the computational complexity of the interior-point method, an equal power allocation scheme is proposed as a suboptimal power allocation scheme, i.e., the transmit powers of S_1 and S_2 are assumed to be $P/2$. This can also be seen as a per-node power constraint case. The SINRs of link from S_i to S_j are respectively described as (17) and (18), as shown at the top of the next page.

The SINRs of link from S_i to E are

$$\Gamma^{\mathrm{I}}_{S_1\to E} = \frac{k_1\gamma_1}{0.5\gamma_2+(0.5-k_1)\,\gamma_1+1}, \tag{19}$$

$$\Gamma^{\mathrm{I}}_{S_2\to E} = \frac{k_2\gamma_2}{0.5\gamma_1+(0.5-k_2)\,\gamma_2+1}. \tag{20}$$

Considering (17) and (19), one obtains (21), where $A = 0.5\left(\gamma_4\gamma_5+\gamma_3\gamma_6+\gamma_5\gamma_6+\gamma_3+\gamma_6{}^2\right)+1.5\gamma_4+\gamma_6+1$ and $B = 0.5\gamma_2+1$. Quadratic function in (21), as shown at the top of the next page, is a convex univariate function, and the number of solutions depends on $\Delta = (0.5\gamma_1\gamma_3\gamma_4+B\gamma_3\gamma_4-A\gamma_1)^2+4\gamma_1\gamma_3\gamma_4\,(AB+0.5A\gamma_1)$.

Obviously, Δ is strictly positive, therefore one obtains

$$k_1^{\mathrm{I}} = \min\left(\max\left(0,\frac{0.5\gamma_1\gamma_3\gamma_4+B\gamma_3\gamma_4-A\gamma_1}{2\gamma_1\gamma_3\gamma_4}\right),0.5\right), \tag{22}$$

$$k_3^{\mathrm{I}} = 0.5-k_1^{\mathrm{I}}. \tag{23}$$

Similarly, considering (18) and (20), one obtains (24), as shown at the top of the next page.

$$k_2^{\mathrm{I}} = \min\left(\max\left(0,\frac{0.5\gamma_2\gamma_3\gamma_4+D\gamma_3\gamma_4-C\gamma_2}{2\gamma_2\gamma_3\gamma_4}\right),0.5\right), \tag{25}$$

$$k_4^{\mathrm{I}} = 0.5-k_2^{\mathrm{I}}, \tag{26}$$

where $C = 0.5\left(\gamma_4\gamma_5+\gamma_3\gamma_6+\gamma_5\gamma_6+\gamma_4+\gamma_5{}^2\right)+1.5\gamma_3+\gamma_5+1$ and $D = 0.5\gamma_1+1$. Substituting (22), (23), (25) and (26) into (10), one can deduce the maximal secrecy rate of communication system under the suboptimal power allocation scheme in the total power constraint case. (22), (23), (25) and (26) are also the power allocation closed-form optimal solutions under the individual power constraint.

C. NONCOOPERATIVE INTERFERENCE STRATEGY

Noncooperative interference strategy is a specific case of cooperative interference, i.e., $k_3 = k_4 = 0$. So the

$$\Gamma^{\mathrm{I}}_{S_1\to S_2} = \frac{k_1\gamma_3\gamma_4}{0.5\left(\gamma_4\gamma_5+\gamma_3\gamma_6+\gamma_5\gamma_6+\gamma_3+\gamma_6{}^2\right)+1.5\gamma_4+\gamma_6+1} \tag{17}$$

$$\Gamma^{\mathrm{I}}_{S_2\to S_1} = \frac{k_2\gamma_3\gamma_4}{0.5\left(\gamma_4\gamma_5+\gamma_3\gamma_6+\gamma_5\gamma_6+\gamma_4+\gamma_5{}^2\right)+1.5\gamma_3+\gamma_5+1} \tag{18}$$

$$R^{\mathrm{I}}_{S_1} = \left[\frac{1}{2}\log_2\left(\frac{1+\Gamma^{\mathrm{I}}_{S_1\to S_2}}{1+\Gamma^{\mathrm{I}}_{S_1\to E}}\right)\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{-\gamma_1\gamma_3\gamma_4k_1^2+\left(0.5\gamma_1\gamma_3\gamma_4+B\gamma_3\gamma_4-A\gamma_1\right)k_1+\left(AB+0.5A\gamma_1\right)}{AB+0.5A\gamma_1}\right)\right]^+ \tag{21}$$

$$R^{\mathrm{I}}_{S_2} = \left[\frac{1}{2}\log_2\left(\frac{1+\Gamma^{\mathrm{I}}_{S_2\to S_1}}{1+\Gamma^{\mathrm{I}}_{S_2\to E}}\right)\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{-\gamma_2\gamma_3\gamma_4k_2^2+\left(0.5\gamma_2\gamma_3\gamma_4+D\gamma_3\gamma_4-C\gamma_2\right)k_2+\left(CD+0.5C\gamma_2\right)}{CD+0.5C\gamma_2}\right)\right]^+ \tag{24}$$

$$\Gamma^{\mathrm{O}}_{S_1\to S_2} = \frac{k_1\gamma_3\gamma_4}{k_1\left(\gamma_4\gamma_5+\gamma_3\gamma_6+\gamma_5\gamma_6-\gamma_6{}^2+\gamma_3-\gamma_4\right)+\gamma_6{}^2+2\gamma_4+\gamma_6+1} \tag{31}$$

optimization problem can be rewritten as

$$\mathrm{OP2}: \max R_s\left(k_1,k_2\right) \quad \text{s.t.} \begin{cases} k_1,k_2\geq 0 \\ k_1+k_2\leq 1 \\ \Gamma_{S_1\to S_2}\left(k_1,k_2\right) > \Gamma_{S_1\to E}\left(k_1,k_2\right) \\ \Gamma_{S_2\to S_1}\left(k_1,k_2\right) > \Gamma_{S_2\to E}\left(k_1,k_2\right). \end{cases}$$

The SINRs of link from S_i to S_j of noncooperative interference strategy are

$$\Gamma^{\mathrm{N}}_{S_1\to S_2} = \frac{k_1\gamma_3\gamma_4}{1+\gamma_2+k_2\gamma_4+k_1\left(\gamma_3+\gamma_1\gamma_2-\gamma_3\gamma_4\right)}, \tag{27}$$

$$\Gamma^{\mathrm{N}}_{S_2\to S_1} = \frac{k_2\gamma_3\gamma_4}{1+\gamma_1+k_1\gamma_3+k_2\left(\gamma_4+\gamma_1\gamma_2-\gamma_3\gamma_4\right)}. \tag{28}$$

The SINRs of link from S_i to E are

$$\Gamma^{\mathrm{N}}_{S_1\to E} = \frac{k_1\gamma_1}{k_2\gamma_2+1}, \tag{29}$$

$$\Gamma^{\mathrm{N}}_{S_2\to E} = \frac{k_2\gamma_2}{k_1\gamma_1+1}. \tag{30}$$

Substituting (27) $\sim$ (30) into OP2, one can acquire the power allocation factors of noncooperative interference strategy and the secrecy rate of communication system with imperfect CSI through an iterative algorithm.

D. ONE-WAY COOPERATIVE INTERFERENCE STRATEGY

We consider a special case, i.e., $k_2 = k_3 = 0$, under the total power constraint. The system becomes a traditional one-way relay system, where the destination node S_2 transmits jamming signals to confuse the eavesdroppers when the source node S_1 sends the message.

The SINR of link from S_1 to S_2 is described as (31), as shown at the top of this page.

The SINR of link from S_1 to E is

$$\Gamma^{\mathrm{O}}_{S_1\to E} = \frac{k_1\gamma_1}{\left(1-k_1\right)\gamma_2+1}. \tag{32}$$

The secrecy rate R^{O}_S of the communication system is

$$R^{\mathrm{O}}_S = \frac{1}{2}\log_2\frac{\theta_1k_1^2+\theta_2k_1+\theta_3}{\theta_4k_1^2+\theta_5k_1+\theta_3}, \tag{33}$$

where $\theta_0 = \gamma_4\gamma_5+\gamma_3\gamma_6+\gamma_5\gamma_6-\gamma_6^2+\gamma_3-\gamma_4$, $\theta_1 = -\gamma_2\left(\theta_0+\gamma_3\gamma_4\right)$, $\theta_2 = \left(\theta_0+\gamma_3\gamma_4\right)\left(1+\gamma_2\right)-\gamma_2\gamma_6^2-2\gamma_2\gamma_4-\gamma_2\gamma_6-\gamma_2$, $\theta_3 = \gamma_2\gamma_6^2+\gamma_6^2+2\gamma_4+\gamma_6+2\gamma_2\gamma_4+\gamma_2\gamma_6+\gamma_2+1$, $\theta_4 = \theta_0\left(\gamma_1-\gamma_2\right)$ and $\theta_5 = \theta_0\left(\gamma_2+1\right)+\gamma_1\gamma_6^2-\gamma_2\gamma_6^2+2\gamma_1\gamma_4+\gamma_1\gamma_6-2\gamma_2\gamma_4-\gamma_2\gamma_6+\gamma_1-\gamma_2$.

One should resolve $\frac{\mathrm{d}R^{\mathrm{O}}_S}{\mathrm{d}k_1}=0$ to obtain the maximal secrecy rate and the optimal power allocation factor for one-way cooperative interference strategy. Considering the monotony of logarithmic function, one has

$$\begin{cases} \dfrac{\mathrm{d}\omega\left(k_1\right)}{\mathrm{d}k_1}=0; \\ \dfrac{\mathrm{d}^2\omega\left(k_1\right)}{\mathrm{d}^2k_1}<0, \end{cases} \tag{34}$$

where $\omega\left(k_1\right) = \frac{\theta_1k_1^2+\theta_2k_1+\theta_3}{\theta_4k_1^2+\theta_5k_1+\theta_3}$. And the optimal power allocation factor can be obtained.

$$k_1^{\mathrm{O}} = \begin{cases} \min\left(\max\left(0, \dfrac{\theta_3\theta_4-\theta_1\theta_3-\sqrt{\Delta_1}}{\theta_1\theta_5-\theta_2\theta_4}\right), 1\right), & \Delta_1\geq 0; \\ 1, & \Delta_1<0, \end{cases} \tag{35}$$

where $\Delta_1 = \left(\theta_3\theta_4-\theta_1\theta_3\right)^2-\left(\theta_1\theta_5-\theta_2\theta_4\right)\left(\theta_2\theta_3-\theta_3\theta_5\right)$. Substituting (35) into (33), one can deduce the secrecy rate of system.

IV. SIMULATION RESULTS AND DISCUSSION

In this section, Monte Carlo simulations of four schemes (OPT, IND, NCP and ONEWAY) are performed with 30000 independent trials. As shown in Fig. 2, all nodes are located in a two-dimensional coordinate plane, where S_1 and S_2 are located at $(-50, 0)$ and $(50, 0)$, respectively. R moves from $(-100, 20)$ to $(100, 20)$. Some simulation

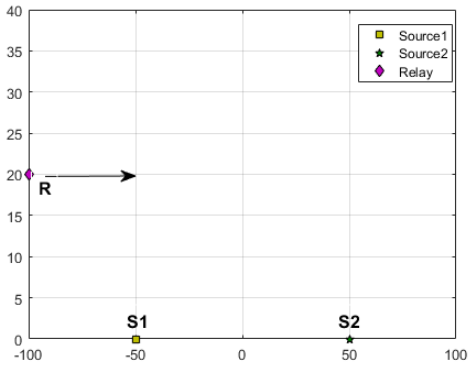

FIGURE 2. The model used for numerical experiments.

TABLE 2. Default simulation parameters.

Total transmit power of two sources	$P = 40$ dBm
Path loss index	$u = 2$
Default channel estimation error factor	$\tau = 0.01$
AGWN	$N_0 = -30$ dBm

TABLE 3. Description of the legends.

Description	Illustration
OPT	Optimal power allocation scheme under total power constraint
IND	Suboptimal power allocation scheme under total power constraint
	Power allocation scheme under individual power constraints
NCP	Noncooperative interference strategy under total power constraint
ONEWAY	One-way cooperative interference strategy under total power constraint

TABLE 4. Comparison of execution time with different methods.

Scheme	OPT	IND	NCP	ONEWAY
Average execution time(s)	0.0779	0.0000	0.0403	0.0000
Average secrecy rate(b/s/Hz)	1.5335	1.5161	1.4631	0.8667

parameters are shown in Table 2 unless otherwise stated. The legends are described in Table 3.

A. EXECUTION TIME

The cooperative interference power allocation problem is modeled as an NLP problem. The interior point method is very effective in solving such problems. There is a shortcoming in interior point method since the computational complexity is relative high. Considering this defect, a low-complexity equal power allocation scheme (IND) is proposed. To compare the execution time, the computer with an octa-core CPU at 3.40 GHz, 8.00 GB RAM, Win 10, MATLAB R2016b is utilized as the computing platform. Assume that the relay is located in 0. The results are shown in Table 4. It can be seen from Table 4 that the OPT and the NCP schemes based on the interior point method run longer than other schemes, but the secrecy rate is also much improved. The above two methods use the power allocation complexity in exchange for a higher secrecy rate. The OPT scheme achieves a higher secrecy rate than the NCP scheme by reasonably allocating a portion of the source power to transmit the interference signal.

B. SECURITY PERFORMANCE

Fig. 3 demonstrates the relationship between secrecy rates of four power allocation schemes (OPT, IND, NCP and ONEWAY) and different locations of untrusted relay when total source power is 40 dBm. As is shown, the curve of the OPT scheme is always topmost. Under the same conditions (the same source power and the same relay location), the OPT scheme performs better than other schemes. The curves for the OPT, IND and NCP schemes are symmetric about $x_R = 0$. It is because the topology roles of sources S_1 and S_2 are completely equivalent and interchangeable in the considered schemes. From Fig. 3, the secrecy rates of the OPT, IND and NCP schemes gradually become higher if the relay approaches the midpoint. When $x_R = 0$, the secrecy rates of the OPT, IND and NCP schemes reach the peak values of 1.53 b/s/Hz, 1.52 b/s/Hz and 1.46 b/s/Hz, respectively. The ONEWAY policy reaches a peak value (1.04 b/s/Hz) when $x_R = 36$. At this case, the relay is near S_2 which is regarded as the destination node in the ONEWAY scheme.

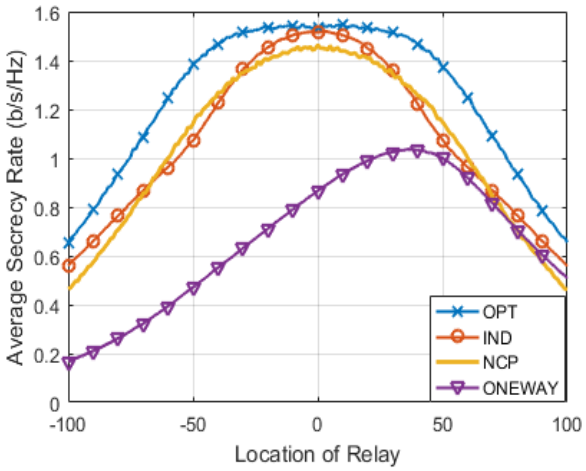

FIGURE 3. Secrecy rate for different x_R.

Figs. 4 and 5 demonstrate the change trend of secrecy rates of four schemes (OPT, IND, NCP and ONEWAY) as the source power varies. Two special cases are considered, i.e., $x_R = 0$ and $x_R = 25$. It can be observed that the secrecy rates of four schemes are all increasing functions of the source power. When the source power exceeds 50 dBm, the secrecy rate flattens out, because the enhanced transmit power also increases the received signal strength of the sniffing node. The OPT scheme performs better than the suboptimal scheme (IND) and the baseline schemes (NCP and ONEWAY). The suboptimal power allocation scheme can achieve the same secrecy rate as the OPT scheme when the relay is in certain positions. Figs. 3 $\sim$ 5 indicate the superiority of the proposed bidirectional cooperative interference

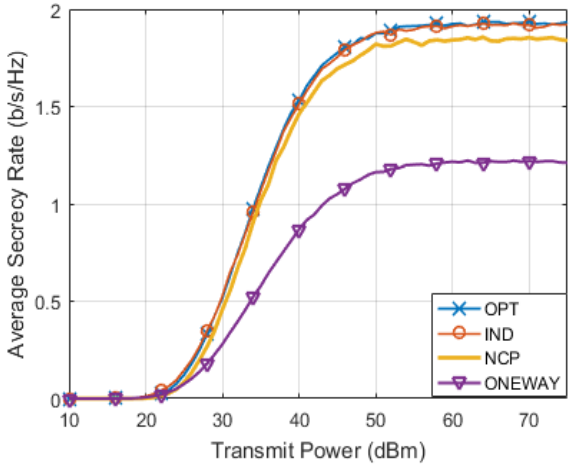

FIGURE 4. Secrecy rate for different transmit powers when $x_R = 0$.

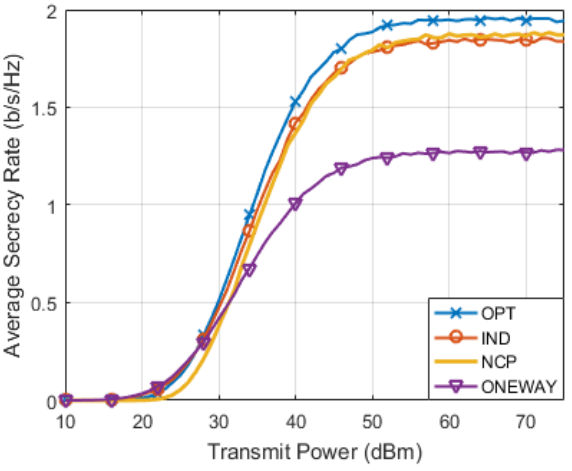

FIGURE 5. Secrecy rate for different transmit powers when $x_R = 25$.

schemes (OPT, IND and NCP). It is shown in Figs. 3 $\sim$ 5 that the security performance of the system can be effectively improved by allocating the interference signal power and the useful signal power of two sources reasonably.

C. POWER ALLOCATION FACTOR

The relationship among power allocation factors and the position of the untrusted relay is shown in Figs. 6 $\sim$ 9. In the OPT scheme, when R is close to S_1, a small fraction of the total source power will be allocated to S_1 ($k_1 + k_3 < 0.5$) to overcome the asymmetry of the channel link. S_1 allocates a portion of the power for artificial noise to confuse the untrusted relay while the remaining fraction for message signal processing. This can interfere with the eavesdropper as much as possible and reveal as little useful information as possible. S_2 will obtain most of the total power, and S_2 will transmit the useful signal with most power (k_4 is close to 0). As the relay moves closer to S_2, k_1 will gradually increase to the peak value, then decrease. k_2 will gradually decrease and k_4 will increase. In the IND scheme, the variation trends of

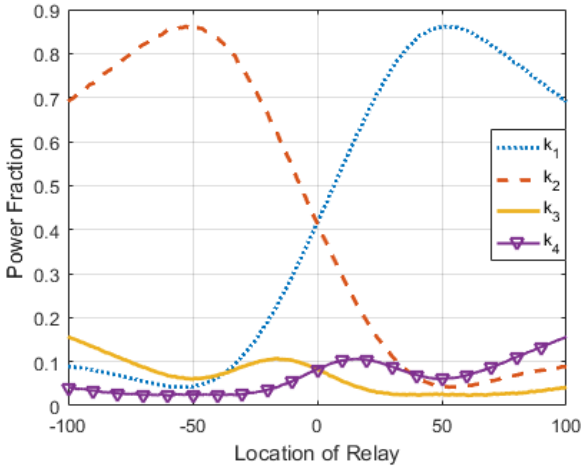

FIGURE 6. Power allocation factors for different x_R in OPT scheme.

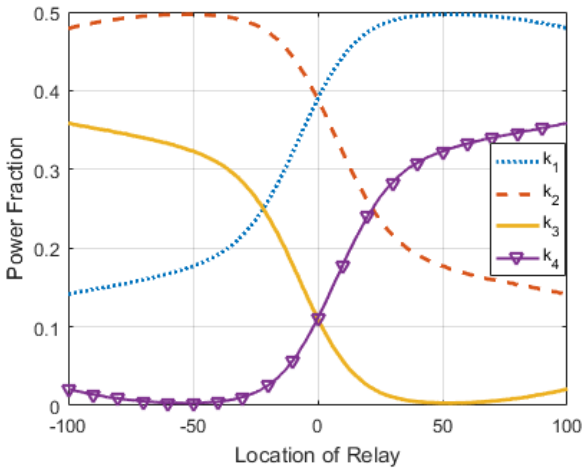

FIGURE 7. Power allocation factors for different x_R in IND scheme.

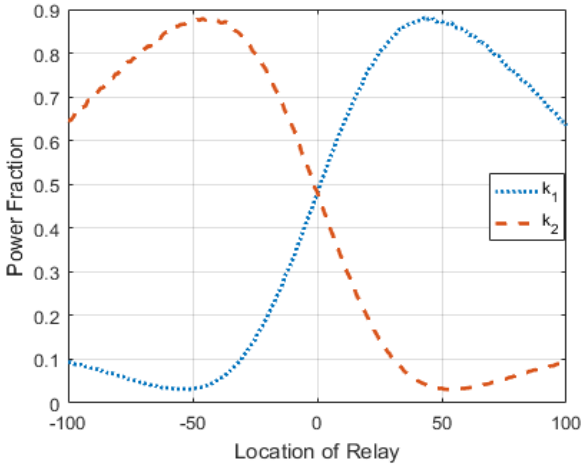

FIGURE 8. Power allocation factors for different x_R in NCP scheme.

power allocation factors are similar. The powers allocated to S_1 and S_2 are equal. In the NCP scheme, S_1 and S_2 use all the powers to send useful message. The transmission power

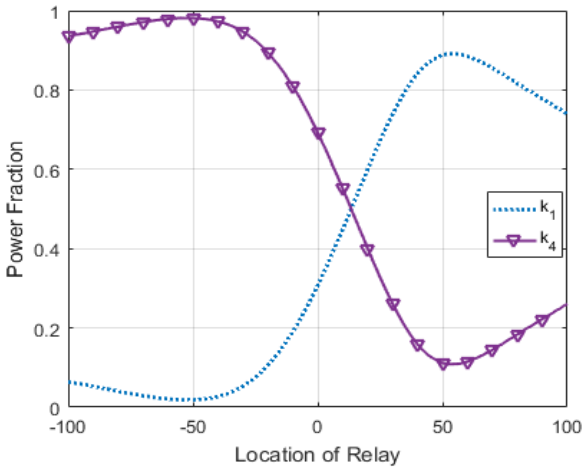

FIGURE 9. Power allocation factors for different x_R in ONEWAY scheme.

of the source near the untrusted relay will be smaller than that of the remote source, so as to ensure that the information of the two sources can be accurately received by each other. In the ONEWAY scheme, when the untrusted relay is close to the source, the transmit power of the source will decrease. Thus the most part of the total power is allocated to S_2 to send the interference signal. Compared with the IND scheme and the baseline schemes (NCP and ONEWAY), the OPT scheme can allocate power more flexibly to overcome the inequality of the channel link and then can achieve a higher secrecy rate.

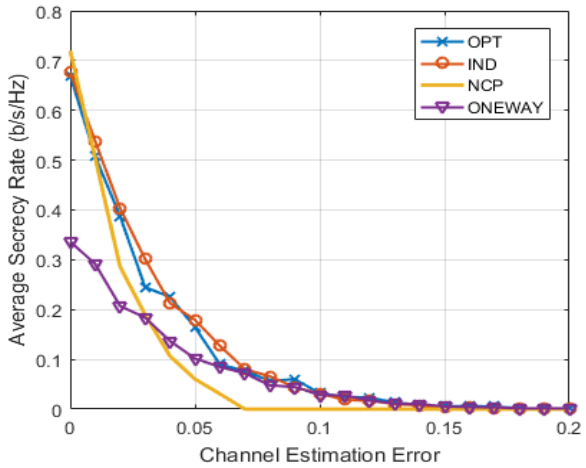

FIGURE 10. Secrecy rate versus channel estimation error.

D. CHANNEL ESTIMATION ERROR FACTOR

Fig. 10 further investigates the effect of the channel estimation error factor τ on the security performance. As illustrated in Fig.10, when CSI is inaccurate, the secrecy rates of the four schemes will drop significantly. The NCP scheme is more sensitive to the channel estimation error. The secrecy rate of the NCP scheme quickly drops to 0 as the channel estimation error increases. The security performances of the OPT scheme and the suboptimal scheme (IND) are still better than those of the baseline schemes (NCP and ONEWAY).

V. CONCLUSION

An optimal power allocation scheme based on interior point method under the imperfect CSI is proposed. By considering the complexity of the interior point method, a suboptimal power allocation scheme is designed. In practice, if the maximal secrecy rate is required, the OPT scheme can be considered. If the low complexity of power allocation scheme is required but a better secrecy rate is desired, the IND scheme can be considered. Our current work is limited to single relay, and the security performance of multi-relay or multi-antenna single relay under imperfect CSI should be studied further.

REFERENCES

[1] T. Woo and Y. Yacobi, "Topics in wireless security," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 6–7, Feb. 2004.
[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, 3rd Quart., 2014.
[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, May 1978.
[5] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, Aug. 1978.
[6] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2471–2475.
[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[8] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, Oct. 2004.
[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[10] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Nov. 2012.
[11] N. R. Zhou, X. R. Liang, Z. H. Zhou, and A. Farouk, "Relay selection scheme for amplify-and-forward cooperative communication system with artificial noise," *Secur. Commun. Netw.*, vol. 9, no. 11, pp. 1398–1404, Jul. 2016.
[12] M. Al-Jamali, A. Al-Nahari, and M. Alkhawlani, "Relay selection schemes for secure transmission in cognitive radio networks," *Wireless Netw.*, vol. 24, no. 3, pp. 911–923, Apr. 2018.
[13] Z. Tang, H. Wang, and Q. Hu, "An energy-efficient relay selection strategy based on optimal relay location for AF cooperative transmission," *Int. J. Wireless Inf. Netw.*, vol. 20, no. 4, pp. 355–364, Dec. 2013.
[14] K. Ho-Van, "Exact outage probability analysis of proactive relay selection in cognitive radio networks with MRC receivers," *J. Commun. Netw.*, vol. 18, no. 3, pp. 288–298, Jun. 2016.
[15] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE/SP 15th Workshop Statist. Signal Process.*, Aug. 2009, pp. 417–420.
[16] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.
[17] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.
[18] L. Lv, J. Chen, L. Yang, and Y. Kuo, "Improving physical layer security in untrusted relay networks: Cooperative jamming and power allocation," *IET Commun.*, vol. 11, no. 3, pp. 393–399, Jul. 2017.

[19] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.
[20] J. Zhang, X. Tao, H. Wu, and X. Zhang, "Secure transmission in SWIPT-powered two-way untrusted relay networks," *IEEE Access*, vol. 6, pp. 10508–10519, Feb. 2018.
[21] P. Popovski and H. Yomo, "Physical network coding in two-way wireless relay channels," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 707–712.
[22] T. Zhang, W. Chen, and Z. Cao, "DNF–AF selection two-way relaying," *Wireless Pers. Commun.*, vol. 80, no. 2, pp. 805–818, Jan. 2015.
[23] H. Long, W. Xiang, and Y. Li, "Precoding and cooperative jamming in multi-antenna two-way relaying wiretap systems without eavesdropper's channel state information," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1309–1318, Jun. 2017.
[24] H. Long, W. Xiang, J. Wang, Y. Zhang, and W. Wang, "Cooperative jamming and power allocation with untrusty two-way relay nodes," *IET Commun.*, vol. 8, no. 13, pp. 2290–2297, Sep. 2014.
[25] T. Mekkawy, R. Yao, F. Xu, and L. Wang, "Optimal power allocation for achievable secrecy rate in an untrusted relay network with bounded channel estimation error," in *Proc. 26th Wireless Opt. Commun. Conf. (WOCC)*, Apr. 2017, pp. 1–5.
[26] J. Li, J. Ge, C. Zhang, J. Shi, Y. Rui, and M. Guizani, "Impact of channel estimation error on bidirectional MABC-AF relaying with asymmetric traffic requirements," *IEEE Trans. Veh. Technol.*, vol. 62, no. 4, pp. 1755–1769, May 2013.
[27] L. Si, Q. Li, and S. Shao, "Robust secrecy beamforming for full-duplex two-way relay networks under imperfect channel state information," *Sci. China Inf. Sci.*, vol. 61, no. 2, pp. 022307-1–022307-10, Feb. 2018.
[28] S. Wang, M. Wang, B. Jia, and Y. Li, "Outage analysis of two-way amplify-and-forward relaying system with imperfect channel state information," in *Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC)*, May 2017, pp. 1642–1646.
[29] Y. Zhang, J. Ge, J. Men, F. Ouyang, and C. Zhang, "Joint relay selection and power allocation in energy harvesting AF relay systems with ICSI," *IET Microw. Antennas Propag.*, vol. 10, no. 15, pp. 1656–1661, Dec. 2016.
[30] S. P. Boyd and L. Vandenberghe, *Convex Optimization*, 7th ed. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[31] J. Nocedal and S. J. Wright, *Numerical Optimization*, 2nd ed. Berlin, Germany: Springer-Verlag, 1999.
[32] R. Fletcher, *Practical Methods of Optimization*, 2nd ed. Hoboken, NJ, USA: Wiley, 1987.

LIHUA GONG received the B.S. degree in physics from Jiangxi Normal University, in 2001, and the master's degree in electronic and information engineering from Nanchang University, in 2011. She is currently an Associate Professor with the Department of Electronic Information Engineering, Nanchang University. She has published over 70 papers in refereed international conferences and journals. Her areas of interests include information security and image encryption.

XIAOXIU DING received the B.S. degree from the Department of Physics, Nanchang University, Nanchang, China, where she is currently pursuing the master's degree within the Department of Electronic Information Engineering, School of Information Engineering. Her current research interests include physical layer security and wireless communications.

QIBIAO ZHU received the B.S. and the M.S. degrees from the China University of Mining and Technology, Xuzhou, China, in 2003 and 2006, respectively. He is currently pursuing the Ph.D. degree in communications and information systems with the Huazhong University of Science and Technology, Wuhan, China. Since 2006, he has been with the School of Information Engineering, Nanchang University, Nanchang, China. His current research interests include orbital angular momentum and its applications in future wireless communications.

NANRUN ZHOU received the Ph.D. degree in communication and information systems from Shanghai Jiao Tong University, in 2005. Since 2006, he has been serving as one of the faculty members of the Department of Electronic Information Engineering, Nanchang University, where he has been a Professor since 2010 and a Gang Jiang Distinguished Professor since 2014. He has published over 170 papers in refereed international conferences and journals. He has been selected in the first or second rank of the Jiangxi Province Baiqianwan Talent for the New Century Programme, the Young Scientist of Jiangxi Province (Jinggang Star), Ganpo Programme 555 for Outstanding Talent and the Major Academic Discipline and Technical Leader of Jiangxi Province, leading a team of researchers carrying out cutting-edge research in the field of information security. He is currently an Associate Editor of *IET Optoelectronics* and an Editorial Board Member of *China Communications*.