IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 3, 2019, accepted November 19, 2019, date of publication November 22, 2019, date of current version December 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2955108

Secrecy Transmission for Self-Energy Recycling Untrusted Relay Networks With Imperfect Channel State Information

SIYANG XU[1,2], XIN SONG[1,2], ZHIGANG XIE[1,2], JING CAO[1,2,3], AND JINGPU WANG[1,2]

[1] School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China
[2] Engineering Optimization and Smart Antenna Institute, Northeastern University, Qinhuangdao 066004, China
[3] School of Mathematics and Information Science and Technology, Hebei Normal University of Science and Technology, Qinhuangdao 066004, China

Corresponding author: Xin Song (sxin78916@neuq.edu.cn)

This work was supported in part by the National Nature Science Foundation of China under Grant 61473066 and Grant 61601109, in part by the Fundamental Research Funds for the Central Universities under Grant N152305001, and in part by the Natural Science Foundation of Hebei Province under Grant F2017501039.

ABSTRACT For the self-energy recycling (SER) untrusted relay network, a two-phase destination-based jamming (DBJ) protocol is proposed, in which the destination transmits the jamming signal to reduce the received SNR of the untrusted relay node in the first phase and the relay node operated in full-duplex (FD) mode for simultaneous energy transfer and information relaying in the second phase. In addition, the loopback interference (LI) generated by FD relay node can be reused as part of energy. To satisfy some practical application scenarios, we consider the imperfect channel estimation error at the destination. Considering the total power constraint and the quality of service (QoS) requirement at the destination, the secrecy rate maximization problem is formulated by optimizing the transmission power of source and destination. However, the formulated problem is non-convex and difficult to solve directly. To cope with this difficulty, an iterative power allocation algorithm is proposed. The key idea of the proposed algorithm first integrates the non-convex constraint into the objective function by the exact penalty method. Then the difference of convex functions (DC) programming can be utilized to convert the non-convex objective function into the approximate convex function and the sub-optimal transmission power of source and destination can be obtained by the traditional convex programming. Simulation results show the superiority security performance of the proposed scheme with the traditional schemes.

INDEX TERMS Physical layer security, self-energy recycling, power allocation, imperfect channel estimation error, secrecy rate.

I. INTRODUCTION

To achieve long-distance communication transmission, distributed cooperative systems have been applied to many different communication scenarios. However, the auxiliary transmission of relay nodes changes the communication process from one-time slot to two-time slots or even multiple-time slots, which lead to serious information leakage. The existing encryption and decryption techniques at the expense of the computational complexity, cannot be adapted to the nodes with a simple upper layer protocol stack. As an alternative to complex cryptographic techniques, physical layer security (PLS) is emerging as a promising paradigm to protect wireless cooperative networks from eavesdropping attacks. The basis of PLS was first proposed by Wyner, who introduced the eavesdropping channel and the legitimate channel [1], [2]. Then the Wyner's theory was applied to broadcast channel [3] and Gaussian channel [4], respectively.

Another pivotal issue in distributed cooperative systems is the continuous powering of relay nodes. Since the relay nodes are solely powered by batteries and placed into the dangerous environment, changing batteries are expensive and unrealistic. Therefore, energy harvesting (EH) technology was proposed to solve the power constraint of the relay nodes [5]. There were two major EH relay protocols, which were named as time-switching relay (TSR) protocol and power splitting relay (PSR) protocol [6]–[8]. However, these two relay protocols utilize additional time or the energy of the useful signals to help the relay node harvest energy. To achieve uninterrupted information transmission and self-interference (SI)

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

reuse, a novel two-phase relay protocol named as SER relay protocol was proposed, in which the relay node was operated in FD mode to achieve simultaneous information relaying and energy transfer [9]. As the extension of [9], the wireless-powered relay nodes were equipped with multi-antenna in [10], [11]. Subsequently, the closed forms of outage probability and optimal power allocation were formulated with decode-and-forward SER relay protocol [12].

For the distributed cooperative systems, external eavesdroppers and unauthorized relay nodes are the two main threats [13]. When there was an external eavesdropper, the PLS of SER relay protocol was studied to maximize the worst-case secrecy rate, and the security performance of the SER system was analyzed [14]. Except for external eavesdroppers, the relay nodes may not have the same security clearance as the source and the destination in sensor and cognitive cooperative networks, which means that the relay nodes were trusted at the service level but were untrusted at information level [15]. Since the unauthorized relay nodes can process confidential information directly, the problem of untrusted relays is more serious in the cooperative system than in the case of external eavesdroppers. Currently, a major method to increase security performance in the untrusted relay network is to weaken the ability of eavesdropper to decode confidential information by utilizing controlled jamming or artificial noise [16]–[18]. Using the friendly jammer, a joint cooperative beamforming, jamming and power allocation policy was proposed to safeguard the confidential information [19]. Without EH in [19], it is difficult for an unauthorized relay node or jammer to consume its own energy to assist interference. Then the EH jammers and relay nodes are integrated into the two-way relay system [20], [21]. To simplify the system model and reduce additional overhead, destination-based jamming (DBJ) was proposed to guarantee security transmission in wireless-powered relay networks [23]–[27]. In [23], [24], the resource division factors were optimized to improve the secrecy rate. And the outage performance was analyzed in [25]. Subsequently, traditional single-destination node was expanded into multi-destination nodes [26], [27].

Without EH technologies, power allocation is an effective method to further improve security performance in cooperative systems [28]–[35]. To optimize the transmission power of source and relay nodes, the power allocation algorithms nesting mixed-integer programming, fractional programming, dual decomposition, alternative search, exact penalty and DC programming were proposed [28]–[32]. And the PLS issues in cooperative systems and the above power allocation algorithms were summarized in [33]. In the wireless-powered untrusted cooperative networks, the transmission power of source and destination are joint optimized based on the exact penalty method or alternative search method to maximize the secrecy rate [34], [35]. In summary, the above algorithms can be effectively utilized to solve the non-convex power allocation problem in untrusted SER relay systems.

In general, the key contributions of this work can be summarized as follows:

Different from [14], the situation of the untrusted relay is first considered in SER relay networks. To achieve the secure transmission of confidential information, we first integrate the DBJ protocol to enhance the security performance of the SER untrusted relay system. In the proposed two-phase DBJ protocol, the destination transmits jamming to reduce the received SNR of untrusted relay node in the first phase. And during the second phase, the relay node is operated in FD mode to achieve simultaneous energy and information transmission. In addition, the untrusted relay node can harvest more energy from the LI generated by the FD operation. To guarantee the total power constraint and the QoS requirement at the destination, the secrecy rate maximization problem is formulated with consideration of the imperfect self-interference cancellation (SIC) at the destination. Then a power allocation algorithm based on the exact penalty method and DC programming is proposed to obtain the sub-optimal transmission power of source and destination, in which the original non-convex optimization problem can be transformed into an approximate convex problem. Simulation results show the significant secrecy rate gain achieved by our proposed design.

The rest of this paper is organized as follows: Section 2 describes the proposed two-phase DBJ wireless-powered relay network with SER, and the secrecy rate maximization problem is formulated with the total power constraint and the minimum information rate requirement at the destination. To solve the non-convex optimization of secrecy rate maximization, the iterative algorithm based on the exact penalty method and DC programming is proposed in Section 3. In Section 4, simulation results are presented to verify the effectiveness of the proposed scheme and algorithm. Finally, Section 5 concludes the key idea of the paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. THE PROPOSED TWO-PHASE DBJ WIRELESS-POWERED RELAY NETWORK

As shown in Figure. 1 and Figure. 2, we propose a two-phase DBJ protocol for the SER untrusted relay network, in which a source S transmits confidential signals to a legal receiver D with the help of a untrusted wireless-powered relay R. Although the relay assists the information transmission, the source and the destination still keep the information secret from the relay [15]. The relay node is operated in amplify-and-forward (AF) protocol for information relaying, i.e., the relay node does not need to decode the source signal and just amplifies and forwards the received signal using the harvested energy. We assume that there is no direct link between the source and the destination node due to severe path loss and shadow fading. All channels are quasi-static flat Rayleigh fading and statistically independent from each other. The whole transmission process T is divided into two equal phases. In the first phase duration $T/2$, the single

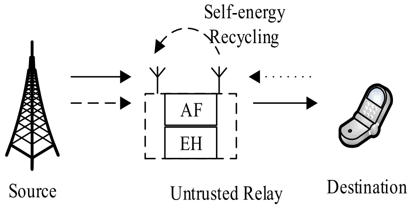


FIGURE 1. The system model of full-duplex wireless-powered relay networks.

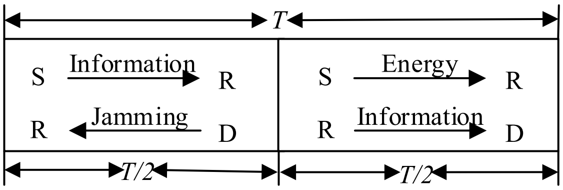


FIGURE 2. The transmission process of the proposed full-duplex wireless-powered relay networks.

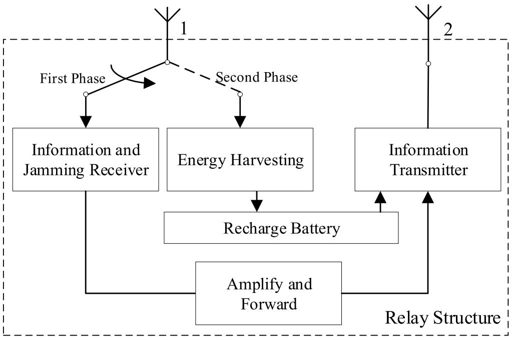


FIGURE 3. The architecture of wireless-powered relay node.

antenna source and the single antenna destination simultaneously transmit the confidential signal and the jamming signal to the relay node. In the remaining duration $T/2$, the relay is operated in FD mode to achieve simultaneous energy transmission from source to relay and the amplified information transmission from the relay to destination, in which the LI generated by the FD relay node can also be harvested as energy for information transmission. Therefore, the relay does not require additional energy supply. As shown in Figure. 3, the antenna 1 of the relay node is used for information and jamming reception in the first phase and EH in the second phase, while antenna 2 is used for the relaying of the amplified signal in the second phase.

In the first phase, R receives the confidential signal transmitted from S and the jamming signal transmitted from D simultaneously. The received signal at R during the first phase can be presented as

$$y_R^1 = \sqrt{P_S} h_{SR} x + \sqrt{P_D} h_{DR} j + n_R, \tag{1}$$

where P_S and P_D denote the transmission power of S and D, respectively. x and j are the information-bearing symbol and jamming-bearing symbol with unit power. The channel gains from S to R and from D to R are h_{SR} and h_{DR}, whose distributions follow $CN\left(0, \sigma^2\right)$. The additive white Gaussian noise (AWGN) at the relay R is represented as n_R with zero mean and variance N_0. In the high SNR, the signal-to-interference-plus-noise ratio (SINR) at R can be approximated as

$$\gamma_R = \frac{P_S \left|h_{SR}\right|^2}{P_D \left|h_{DR}\right|^2 + N_0} \approx \frac{P_S \left|h_{SR}\right|^2}{P_D \left|h_{DR}\right|^2}. \tag{2}$$

In the second phase, the relay node is operated in FD mode to harvest energy from S and transfer the amplified information to D. Particularly, the relay node not only harvests the dedicated energy sent from S, but also recycles a part of its own transmitted energy via a loopback channel expressed as f. The received signals at R can be expressed as

$$y_R^2 = \sqrt{P_S} h_{SR} x_E + \sqrt{P_R} f G y_R + n_R, \tag{3}$$

where x_E denotes the energy-bearing signal sent by S during the second phase; P_R is the transmission power of R. Since R adopts AF protocol, G is the normalization coefficient, which can be expressed as

$$G = \sqrt{\frac{1}{P_S \left|h_{SR}\right|^2 + P_D \left|h_{DR}\right|^2 + N_0}}. \tag{4}$$

Based on linear EH model, the total harvested energy at the relay node can be given by

$$\begin{aligned} E_R &= \frac{T}{2}\eta \left(P_S \left|h_{SR}\right|^2 + P_R \left|f\right|^2 G^2 E\left[\left|y_R^1\right|^2\right]\right) \\ &\approx \frac{T}{2}\eta \left(P_S \left|h_{SR}\right|^2 + P_R \left|f\right|^2\right), \end{aligned} \tag{5}$$

where $\eta \in (0, 1)$ denotes the energy conversion efficiency. Here, the power of noise can be ignored, since it is much smaller than the energy signal. In addition, we assume that the total harvested energy is used to forward the scaled version of the overlapped signal. Therefore, the expression of P_R can be expressed as

$$P_R = \frac{\eta P_S \left|h_{SR}\right|^2}{1 - \eta \left|f\right|^2}. \tag{6}$$

Following the equations (1), the received signal at the destination can be written as

$$\begin{aligned} y_D &= \sqrt{P_R} G h_{RD} y_R^1 + n_D \\ &= \sqrt{P_R} G h_{RD} \sqrt{P_S} h_{SR} x + \sqrt{P_R} G h_{RD} n_R \\ &\quad + \sqrt{P_R} G h_{RD} \sqrt{P_D} h_{DR} j + n_D, \end{aligned} \tag{7}$$

where h_{RD} denote the channel gain from R to D and n_D is the AWGN at destination with power N_0. Note that, due to the assumption of channel reciprocity, we can obtain that $h_{RD} = h_{DR}$ [18]. In equation (7), j is the jamming signal transmitted by D itself in the first phase, in which the self-interference term $\sqrt{P_R} G h_{RD} \sqrt{P_D} h_{DR} j$ can be exactly eliminated when D has perfect channel state information.

For more practical scenarios where the channel state information cannot perfectly be known at D. Only some statistical information about channel estimation error is available to D, which means that SIC only eliminates the statistical part of $\sqrt{P_R} G h_{RD} \sqrt{P_D} h_{DR} j$ at the destination node [32]. Since we only perform SIC operations at the destination node, the channel estimation error of h_{SR} can be ignored. Therefore, the imperfect channel state information can be modelled as two parts, i.e., a known part $\hat{h}$ and an additive probabilistic term h_e, which can be expressed as

$$h_{DR} = \hat{h} + h_e, \tag{8}$$

where $\hat{h}$ denotes the estimated channel gain between D and R, and h_e denotes the channel error of h_{DR}. In addition, the expectation of h_{DR} and h_e are $E\left[h_{DR}\right] = \hat{h}$ and $E\left[h_e\right] = 0$, respectively. Substituting the imperfect channel model (8) into the equation (7), we have

$$\begin{aligned} y_D = {} & \sqrt{P_R} G h_{RD} \sqrt{P_S} h_{SR} x + \sqrt{P_R} G h_{RD} n_R \\ & + \sqrt{P_R} G \sqrt{P_D} \left(\hat{h} + h_e\right)^2 j + n_D. \end{aligned} \tag{9}$$

After the non-perfect self-interference cancellation, the remaining received signal at D can be given by

$$\begin{aligned} \tilde{y}_D = {} & \sqrt{P_R} G h_{RD} \sqrt{P_S} h_{SR} x + \sqrt{P_R} G h_{RD} n_R \\ & + \sqrt{P_R} G \sqrt{P_D} \left(2 \hat{h} h_e + h_e^2\right) j + n_D. \end{aligned} \tag{10}$$

The equation (10) can be re-represented as

$$\begin{aligned} \tilde{y}_D = {} & \sqrt{P_R} G h_{RD} \sqrt{P_S} h_{SR} x + \sqrt{P_R} G h_{RD} n_R \\ & + \sqrt{P_R} G \sqrt{P_D} \left(2 h_e h_{DR} - h_e^2\right) j + n_D. \end{aligned} \tag{11}$$

Substituting the equations (4) and (6) into (11), the SINR at D can be formulated as

$$\begin{aligned} \gamma_D = {} & \frac{P_S \left|h_{SR}\right|^2 P_R \left|h_{RD}\right|^2}{\left(P_R P_D \left|2 h_e h_{DR} - h_e^2\right|^2 + P_R \left|h_{RD}\right|^2 N_0 + N_0/G^2\right)} \\ \approx {} & \frac{\eta P_S^2 \left|h_{SR}\right|^4 \left|h_{RD}\right|^2 / N_0}{\left(P_S P_D \mathrm{I}/N_0 + \left(\Phi + \eta \left|h_{RD}\right|^2\right) P_S \left|h_{SR}\right|^2 + \Phi P_D \left|h_{DR}\right|^2\right)}. \end{aligned} \tag{12}$$

where $\mathrm{I} = \eta \left|h_{SR}\right|^2 \left|2 h_e h_{DR} - h_e^2\right|^2$ and $\Phi = 1 - \eta \left|f\right|^2$. Furthermore, the instantaneous information rates at R and D can be expressed as

$$R_R = \frac{1}{2} \log_2 \left(1 + \gamma_R\right) = \frac{1}{2} \log_2 \left(1 + \frac{P_S \left|h_{SR}\right|^2}{P_D \left|h_{DR}\right|^2}\right), \tag{13}$$

$$\begin{aligned} R_D = {} & \frac{1}{2} \log_2 \left(1 + \gamma_D\right) \\ = {} & \frac{1}{2} \log_2 \left(1 + \frac{A P_S^2 / N_0^2}{\left(P_S P_D \mathrm{I}/N_0^2 + B P_S / N_0 + C P_D / N_0\right)}\right). \end{aligned} \tag{14}$$

where $A = \eta \left|h_{SR}\right|^4 \left|h_{RD}\right|^2$, $B = \left(\Phi + \eta \left|h_{RD}\right|^2\right) \left|h_{SR}\right|^2$ and $C = \Phi \left|h_{DR}\right|^2$.

B. SECRECY RATE MAXIMIZATION PROBLEM

For the untrusted relay networks, the achieved secrecy rate is defined as the difference between the information rate achieved by D and R. Thus, the instantaneous secrecy rate of the considered network can be given by

$$\begin{aligned} R_{sec} &= \left[R_D - R_R\right]^+ \\ &= \frac{1}{2} \left[\log_2 \left(1 + \gamma_D\right) - \log_2 \left(1 + \gamma_R\right)\right]^+, \end{aligned} \tag{15}$$

where $[x]^+ = \max(0, x)$. Therefore, it must satisfy the condition of $\gamma_D > \gamma_R$ to guarantee the positive secrecy rate. The factor $1/2$ in (15) is because the whole information transmission from S to D is divided into two phases. With the consideration of the total power constraint and the QoS requirement at the destination, the secrecy rate maximization problem with respect to P_S and P_D can be formulated as

$$\begin{aligned} & \max_{P_S, P_D} R_{sec}\left(P_S, P_D\right) \\ & \text{s.t. } R_D\left(P_S, P_D\right) \geq R_{th} \\ & \qquad P_S + P_D \leq P_T \\ & \qquad P_S > 0, \quad P_D > 0, \end{aligned} \tag{16}$$

where R_{th} is the minimum information rate requirement at D and P_T is the total power constraint.

III. POWER ALLOCATION ALGORITHM FOR SECRECY RATE MAXIMIZATION PROBLEM

As shown in (16), the optimization problem with respect to P_S and P_D is non-convex because of the non-convex objective function $R_{sec}\left(P_S, P_D\right)$ and non-convex constraint $R_D\left(P_S, P_D\right) \geq R_{th}$. To solve the non-convexity, we proposed an iterative algorithm based on the exact penalty method and DC programming. The exact penalty can be used to integrate non-convex constraints into the objective function. By using DC programming, the non-convex objective function can be converted to the approximate convex problem. Finally, the convex programming can be used to obtain the sub-optimal transmission power of source and destination.

A. EXACT PENALTY METHOD FOR NON-CONVEX CONSTRAINT

The tricky problem of the optimization is that both the objective function and constraint are non-convex. To further address the problem, we merge the minimum information rate requirement into the objective function by the exact penalty method. The initial feasible domain in (16) can be expressed as

$$\Omega = \left\{ \begin{array}{l} \left(P_S, P_D\right) : R_D\left(P_S, P_D\right) \geq R_{th}, \\ P_S + P_D \leq P_T, P_S > 0, P_D > 0 \end{array} \right\}. \tag{17}$$

From [31], we utilize the exact penalty method to convert the non-convex constraint $R_D\left(P_S, P_D\right) \geq R_{th}$ into the objective function by the penalty factor, which can be expressed as

$$\min_{P_S, P_D \in \overset{\sim}{\Omega}} \left\{ H\left(P_S, P_D\right) \triangleq -R_{sec}\left(P_S, P_D\right) + \sigma_m R^+\left(P_S, P_D\right) \right\}, \tag{18}$$

where $\tilde{\Omega} = \{(P_S, P_D) : P_S + P_D \le P_T, P_S > 0, P_D > 0\}$ is the changed feasible domain; σ_m is the suitable penalty factor. The key idea of the exact penalty method is as follows. When the solutions P_S and P_D go out of the feasible domain, a penalty term is imposed forcing the iteration point to approach the feasible domain step by step. The difficulty is to choose a suitable σ_m, while a too large σ_m may lead to more difficult to solve the penalty function. Thus, we first choose a small initial value σ_0, and then the penalty can be scaled by a factor $c > 1$. Furthermore, the penalty function can be constructed as

$$R^+ (P_S, P_D) = \max \{-R_D (P_S, P_D) + R_{th}, 0\}. \tag{19}$$

By decomposing the equation (15), we rewrite the penalty function as

$$R^+ (P_S, P_D) = \max \{-f (P_S, P_D) + R_{th}, -g (P_S, P_D)\} + g (P_S, P_D), \tag{20}$$

where

$$f (P_S, P_D) = \frac{1}{2} \log_2 \begin{pmatrix} AP_S^2/N_0^2 + P_S P_D \mathrm{I}/N_0^2 \\ +BP_S/N_0 + CP_D/N_0 \end{pmatrix} \tag{21}$$

and

$$g (P_S, P_D) = \frac{1}{2} \log_2 \begin{pmatrix} P_S P_D \mathrm{I}/N_0^2 + BP_S/N_0 \\ +CP_D/N_0 \end{pmatrix}. \tag{22}$$

Then the auxiliary variable $t \in R$ is introduced to further process the optimization problem. The optimization problem can be reformulated as

$$\begin{aligned} \min_{P_S, P_D, t} \; & \{-R_{sec} (P_S, P_D) + \sigma_m (t + g (P_S, P_D))\} \\ \text{s.t.} \; & - f (P_S, P_D) + R_{th} \le t \\ & - g (P_S, P_D) \le t \\ & P_S, \quad P_D \in \tilde{\Omega}. \end{aligned} \tag{23}$$

It is easy to prove that the first-order and second-order sequential principal minors of $\mathrm{H}[-f (P_S, P_D)]$ and $\mathrm{H}[-g (P_S, P_D)]$ are positive, where $\mathrm{H}[\bullet]$ denotes the Hessian Matrix. In addition, it can be proved that the changed feasible domain is a convex set, which can be written as

$$\tilde{\Omega}^t = \left\{ \begin{array}{l} (P_S, P_D, t) : -f (P_S, P_D) + R_{th} \le t, \\ -g (P_S, P_D) \le t, \\ P_S + P_D \le P_T, P_S > 0, P_D > 0. \end{array} \right\} \tag{24}$$

Proposition 1: The sequence of $R^+ (P_S, P_D)$ with the updated penalty factor σ_m is decreasing.

Proof: For simplicity, let $(P_S, P_D)^{\sigma_m}$ denotes the optimal solutions with the obtained σ_m. According to the expression (18) with the given σ_{m+1} and σ_m, we conclude

$$\begin{aligned} & -R_{sec} (P_S, P_D)^{\sigma_m} + \sigma_m R^+ (P_S, P_D)^{\sigma_m} \\ & \quad \le -R_{sec} (P_S, P_D)^{\sigma_{m+1}} + \sigma_m R^+ (P_S, P_D)^{\sigma_{m+1}}. \end{aligned} \tag{25}$$

Furthermore, we also have that

$$\begin{aligned} & -R_{sec} (P_S, P_D)^{\sigma_{m+1}} + \sigma_{m+1} R^+ (P_S, P_D)^{\sigma_{m+1}} \\ & \quad \le -R_{sec} (P_S, P_D)^{\sigma_m} + \sigma_{m+1} R^+ (P_S, P_D)^{\sigma_m} \end{aligned} \tag{26}$$

Algorithm 1 Exact Penalty Algorithm

```
Input and Initialization: Given an initial value $\sigma_0$, convergence tolerance $\xi$ and set $m = 0$;
Output: $P_S^*$, $P_D^*$;
1: Repeat
2: For the given $\sigma_m$, obtain the solutions $(P_S, P_D)^{\sigma_m}$ of (23)
     by DC programming;
3: Calculate $\sigma_m R^+ (P_S, P_D)^{\sigma_m}$ and update $\sigma_{m+1} = c\sigma_m$;
4: $m = m + 1$;
5: Until $\sigma_{m-1} R^+ (P_S, P_D)^{\sigma_{m-1}} \le \xi$;
6: Return $P_S^* = P_S^{\sigma_m}$ and $P_D^* = P_D^{\sigma_m}$.
```

Adding (24) to (25), we can obtain

$$R^+ (P_S, P_D)^{\sigma_{m+1}} \le R^+ (P_S, P_D)^{\sigma_m}. \tag{27}$$

Therefore, Proposition 1 can be proved. □

By the above exact penalty method, the original optimization problem (16) is converted into (23) with the updated σ_m. The exact penalty algorithm is shown in Algorithm 1, where m and ξ denote the index number and convergence tolerance, respectively. Although the feasible domain (24) is a convex set, the objection function in (23) is still non-convex. Therefore, we utilize DC programming to obtain the sub-optimal transmission power of source and destination, which is present in the next sub-section.

B. DC PROGRAMMING FOR SUB-OPTIMAL TRANSMISSION POWER WITH THE FIXED σ_m

With the given σ_m, the optimization (23) is still a non-convex function. Therefore, we use DC programming to convert the non-convex problem into an approximate convex function. Then the traditional convex programming can be used to obtain the transmission power of source and destination.

The standard DC optimization problem can be modeled as

$$\min_X \{F (x) = F_1 (x) - F_2 (x)\}, \tag{28}$$

where X is the convex feasible domain; $F_1 (x)$ and $F_2 (x)$ are two convex components. From [36], the optimization can be solved iteratively by solving a sequential convex problem

$$\min_X \{F_1 (x) - F_2 (x (n)) - \langle \nabla F_2 (x (n)), x - x (n)\rangle\}, \tag{29}$$

where $x (n)$ is the optimal solution at $n - 1$th iteration; $\nabla F_2 (x (n))$ is the gradient of $F_2 (x)$ at $x (n)$.

By decomposing the expression (13), the instantaneous information rate at R can be re-expressed as

$$\begin{aligned} R_R &= \frac{1}{2} \log_2 \left(1 + \frac{P_S |h_{SR}|^2}{P_D |h_{DR}|^2}\right) \\ &= \mu (P_S, P_D) - \nu (P_S, P_D), \end{aligned} \tag{30}$$

where

$$\mu (P_S, P_D) = \frac{1}{2} \log_2 \left(P_S |h_{SR}|^2 + P_D |h_{DR}|^2\right) \tag{31}$$

and

$$\nu\left(P_S,P_D\right)=\frac{1}{2}\log_2\left(P_D\left|h_{DR}\right|^2\right). \tag{32}$$

To utilize the DC programming and solve the non-convex objective function in (23), the objective function in (23) can be rewritten as

$$\min_{P_S,P_D,t\in\tilde{\Omega}^t}\left\{G\left(P_S,P_D,t\right)=G_1\left(P_S,P_D,t\right)-G_2\left(P_S,P_D\right)\right\}, \tag{33}$$

where

$$G_1\left(P_S,P_D,t\right)=-f\left(P_S,P_D\right)-\nu\left(P_S,P_D\right)+\sigma_m t \tag{34}$$

and

$$G_2\left(P_S,P_D\right)=-\left(\sigma_m+1\right)g\left(P_S,P_D\right)-u\left(P_S,P_D\right). \tag{35}$$

It is obvious that both $-\mu\left(P_S,P_D\right)$ and $-\nu\left(P_S,P_D\right)$ are convex functions. Moreover, $-f\left(P_S,P_D\right)$ and $-\left(\sigma_m+1\right)g(P_S,P_D)$ are convex functions. $\sigma_m t$ is an affine function. Based on [37], the sum of the two convex functions is still a convex function. Therefore, the expressions of (34) and (35) are two convex functions.

Since the equations (34) and (35) are two convex functions, the objective function of (23) has been transferred to the subtraction form of two convex functions, which corresponds to the standard form of DC programming. Based on DC programming, the objective function in (23) can be solved iteratively by solving convex function

$$\begin{aligned}\hat{Q}^k&\left(P_S,P_D\right)\\&=G_1\left(P_S(k),P_D(k),t\right)-G_2\left(P_S(k-1),P_D(k-1)\right)\\&\quad-\left.\frac{\partial G_2\left(P_S,P_D(k-1)\right)}{\partial P_S}\right|_{P_S(k-1)}\left(P_S(k)-P_S(k-1)\right)\\&\quad-\left.\frac{\partial G_2\left(P_S(k-1),P_D\right)}{\partial P_D}\right|_{P_D(k-1)}\left(P_D(k)-P_D(k-1)\right),\end{aligned} \tag{36}$$

where k is the iteration number. With the given σ_m, the partial derivative about $P_S(k)$ can be calculated as

$$\begin{aligned}&\frac{\partial G_2\left(P_S,P_D\right)}{\partial P_S}\\&\quad=-\frac{\left(\sigma_m+1\right)\left(P_D\mathrm{I}/N_0^2+B/N_0\right)}{2\ln(2)\left(P_SP_D\mathrm{I}/N_0^2+BP_S/N_0+CP_D/N_0\right)}\\&\qquad-\frac{\left|h_{SR}\right|^2}{2\ln(2)\left(P_S\left|h_{SR}\right|^2+P_D\left|h_{DR}\right|^2\right)}.\end{aligned} \tag{37}$$

Likewise, the partial derivative about $P_D(k)$ can be calculated as

$$\begin{aligned}&\frac{\partial G_2\left(P_S,P_D\right)}{\partial P_D}\\&\quad=-\frac{\left(\sigma_m+1\right)\left(P_S\mathrm{I}/N_0^2+C/N_0\right)}{2\ln(2)\left(P_SP_D\mathrm{I}/N_0^2+BP_S/N_0+CP_D/N_0\right)}\\&\qquad-\frac{\left|h_{DR}\right|^2}{2\ln(2)\left(P_S\left|h_{SR}\right|^2+P_D\left|h_{DR}\right|^2\right)}.\end{aligned} \tag{38}$$

Moreover, the optimal solutions at $k+1$th iteration can be updated by

$$\left(P_S(k+1),P_D(k+1)\right)=\min_{P_S,P_D,t\in\tilde{\Omega}^t}\hat{Q}^k\left(P_S(k),P_D(k)\right). \tag{39}$$

Proposition 2: For a given penalty factor σ_m, the sequence of $F\left(P_S,P_D\right)$ with the updated optimal solutions $P_S(k)$ and $P_D(k)$ are decreasing.

Proof: Since $F_2\left(P_S(k),P_D(k)\right)$ is a convex function, we can obtain that

$$\begin{aligned}&G_2\left(P_S(k+1),P_D(k+1)\right)\\&\quad\geq G_2\left(P_S(k),P_D(k)\right)\\&\qquad+\left.\frac{\partial G_2\left(P_S,P_D(k)\right)}{\partial P_S}\right|_{P_S=P_S(k)}\left(P_S(k+1)-P_S(k)\right)\\&\qquad+\left.\frac{\partial G_2\left(P_S(k),P_D\right)}{\partial P_D}\right|_{P_D=P_D(k)}\left(P_D(k+1)-P_D(k)\right).\end{aligned} \tag{40}$$

At the $k+1$th iterations, $P_S(k+1)$ and $P_D(k+1)$ denote the optimal solutions of (36) while $P_S(k)$ and $P_D(k)$ are only the feasible solutions. Thus, we have

$$\begin{aligned}&G_1\left(P_S(k+1),P_D(k+1),t\right)-G_2\left(P_S(k),P_D(k)\right)\\&\quad-\left.\frac{\partial G_2\left(P_S,P_D(k)\right)}{\partial P_S}\right|_{P_S(k)}\left(P_S(k+1)-P_S(k)\right)\\&\quad-\left.\frac{\partial G_2\left(P_S(k),P_D\right)}{\partial P_D}\right|_{P_D(k)}\left(P_D(k+1)-P_D(k)\right)\\&\quad\leq G\left(P_S(k),P_D(k)\right)\end{aligned} \tag{41}$$

Adding the inequalities (40) to (41), we can obtain that

$$G\left(P_S(k+1),P_D(k+1)\right)\leq G\left(P_S(k),P_D(k)\right). \tag{42}$$

The above formulation implies that the sequence of $G\left(P_S(k),P_D(k)\right)$ is monotonic decreasing. □

The transmission power of source and destination can be obtained by Algorithm 2, where k and ϖ denote the index number and convergence tolerance, respectively.

IV. SIMULATION RESULTS

In this section, the simulation results are presented to evaluate the secrecy rate performance of the proposed wireless-powered network with imperfect channel state information and the proposed algorithm. For simplicity, we assume the source, the destination and the untrusted relay are placed on a horizontal line, where d_{SR} and d_{RD} denote the distances of source-relay and relay-destination. The distance between the source and the destination is fixed at 80m. Furthermore, the mean channel power gains λ_{SR} and λ_{RD} of the exponential random variables $\left|h_{SR}\right|^2$ and $\left|h_{DR}\right|^2$ are $d_{SR}^{-\rho}$ and $d_{RD}^{-\rho}$, respectively, where ρ denotes the path-loss exponent [25]. The specific simulation parameters are shown in Table 1.

The convergence of the secrecy rate with different minimum information rate requirements R_{th} at the destination

Algorithm 2 DC Programming With the Given σ_m

```
Input and Initialization: Given the initial value $P_S(0)$ and $P_D(0)$, convergence tolerance $\varpi$ and set $k = 0$;
Output: $P_S^*$ and $P_D^*$;
1: Calculate $F(P_S(k), P_D(k))$;
2: Repeat
3: Solve (36) to update $P_S(k+1)$ and $P_D(k+1)$ by convex programming;
4: Calculate $F(P_S(k), P_D(k))$;
5: $k = k + 1$;
6: Until $|F(P_S(k-1), P_D(k-1)) - F(P_S(k), P_D(k))| \leq \varpi$;
7: Return $P_S^* = P_S(k)$ and $P_D^* = P_D(k)$.
```

TABLE 1. Simulation parameters.

Parameter	Value
Path loss exponent ρ	3
The distance between source and destination d_{SD}	80m
Noise power density N_0	-100dBm
Energy conversion efficiency η	0. 5
Channel estimation error σ_e^2	0.01
Strength of LI $\|f\|^2$	0.8
Total transmission power	30dBm

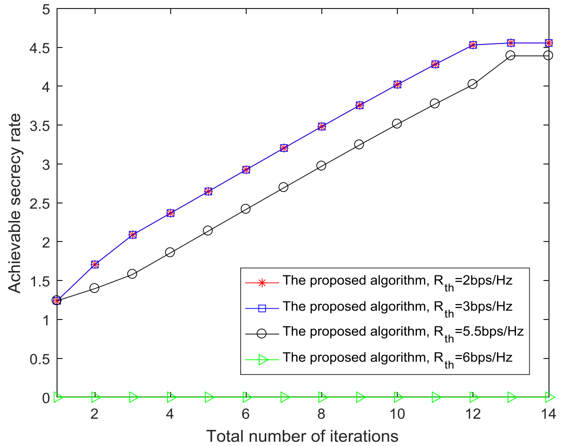


FIGURE 4. The achievable secrecy rate evolution of the proposed algorithm versus the total iterations with different minimum information rate requirements.

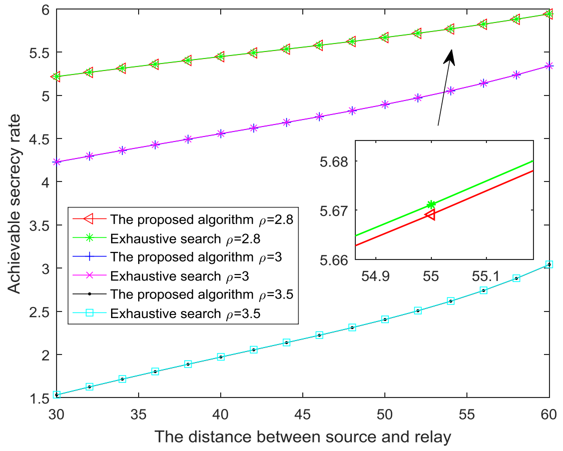


FIGURE 5. Achievable secrecy rate of two algorithms versus the distance between source and relay with different path-loss exponent ρ.

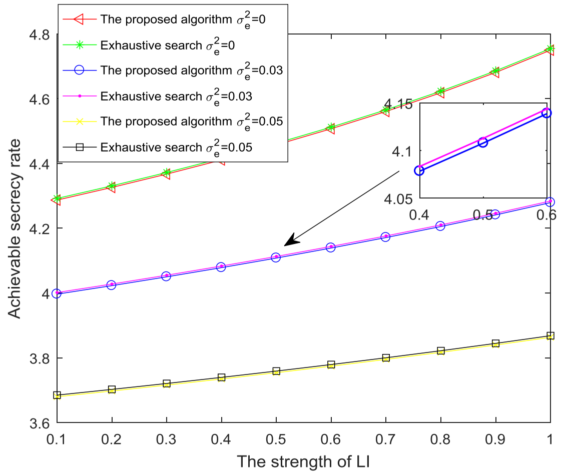


FIGURE 6. Achievable secrecy rate versus the strength of LI between source and relay with different imperfect channel errors σ_e^2.

of the proposed power allocation algorithm can be observed in Figure 4. The distance between the source and the relay is fixed at 40m. As illustrated in Figure 4, the minimum information rate threshold has an impact on the achievable secrecy rate and the proposed algorithm converges within 14 iterations, which shows the proposed iterative algorithm has lower computational complexity. The achievable secrecy rate of the proposed algorithm has the same values when R_{th} = 2bps/Hz and R_{th} = 3bps/Hz, while the achievable secrecy rate with R_{th} = 5.5bps/Hz reducing to 4.39bps/Hz. However, the achievable secrecy rate is always equal to 0 when R_{th} = 6bps/Hz. The reason is that the information rate at the destination is always less than the threshold.

For investigating the effect on the security performance caused by different system parameters and the convergence behavior, the achievable secrecy rate of the proposed algorithm can be observed in Figure 5, Figure 6 and Figure 7 by contrast with exhaustive search. From Figure 5, Figure 6 and Figure 7, the exhaustive search method can always achieve a higher secrecy rate value compared with the proposed algorithm. However, there is a very small performance loss of the proposed algorithm. Besides, the proposed iterative algorithm only requires 14 iterations in Figure 4, which proves the effectiveness of the proposed algorithm with lower computational complexity.

Figure 5 shows the achievable secrecy rate of the proposed algorithm and the exhaustive search when the distance between the source and relay varies from 30m to 60m, in which the different path-loss exponents are ρ = 2.8, ρ = 3 and ρ = 3.5. The information rate threshold is

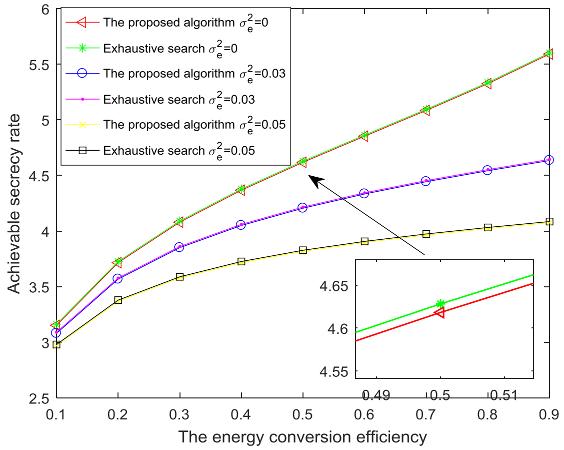


FIGURE 7. Achievable secrecy rate versus the strength of LI between source and relay with different imperfect channel errors σ_e^2.

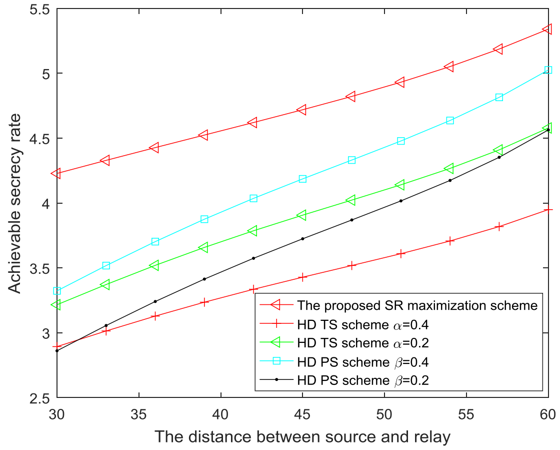


FIGURE 8. The proposed secrecy rate maximization scheme versus half-duplex DBJ schemes with different time switching factor α power splitting factor β.

set $R_{th} = 3$bps/Hz, and the other parameters are the same as Table 1. The six curves in Figure 5 have the same trend. Meanwhile, it can be observed that the secrecy rate increases when the distance between the source and the relay increases. The reason is that the jamming signal has more of an effect on decreasing γ_R when the relay is close to the destination. However, we can see that, the achievable secrecy rate decreases as pass-loss exponent increases.

In Figure 6, the achievable secrecy rate of the proposed algorithm and the exhaustive search with different imperfect channel estimation errors $\sigma_e^2 = 0$, $\sigma_e^2 = 0.03$ and $\sigma_e^2 = 0.05$. Particularly, it means that perfect self-interference cancellation at the destination when $\sigma_e^2 = 0$. The achievable secrecy rate increases with the strength of LI varying from 0.1 to 1. When the strength of LI approaches 1, it means that almost all the energy transmitted by the relay can be recycled, and large performance improvement can be achieved. As shown in Figure 6, the proposed algorithm and the exhaustive search method have the best output performance when $\sigma_e^2 = 0$. That is because the influence of the jamming signal on the destination node is completely eliminated. With the increasing of imperfect channel estimation error, the secrecy rate is decreasing. For example, the achievable secrecy rate of the proposed algorithm can achieve about 3.789bps/Hz when $\sigma_e^2 = 0.05$ and $|f|^2 = 0.5$.

When the energy conversion efficiency varying from 0.1 to 0.9, Figure 7 displays the achievable secrecy rate of the proposed algorithm and the exhaustive search with different imperfect channel estimation error. It can be seen as we found earlier, the security performance of the proposed algorithm remains very close to that of exhaustive search in all cases. In addition, the imperfect channel estimation error has a negative impact on security performance. One may note that the output performance monotonously increases with the energy conversion efficiency increases. The reason is that more energy can be harvested by the relay node for information transmission. For example, the security performance can achieve 4.333bps/Hz when $\sigma_e^2 = 0.03$ and $|f|^2 = 0.6$.

For examining the advantage of the proposed system and the proposed algorithm, we compare with the half-duplex (HD) DBJ schemes in [25] over different locations of the relay node. In [25], the relay node can harvest energy from the source by two methods named as time switching (TS) and power splitting (PS). Since the PS factor and the TS factor are not optimized, we choose the TS factor and PS factor to be 0.4 and 0.2 with the total power constraint. From Figure 8, it is obvious that the proposed scheme has the best output security performance, which shows that the proposed scheme can achieve simultaneous wireless information and energy transfer in the same phase. In addition, the four curves have some intersections, which indicate that the HD TS scheme and HD PS scheme have their own advantages region.

With the different total power constraints, we compare the achievable secrecy rate of the proposed algorithm with equal power allocation scheme, secrecy rate maximization scheme in [34] and the no cooperative jamming (CJ) scheme in [8], which is shown in Figure 9. The equal power allocation scheme divides the total power P_T into two equal parts $P_S = P_T/2$ and $P_D = P_T/2$. The secrecy rate maximization scheme in [34] divides the power of the source and the destination into energy stream and information stream with different factors θ and ϑ. Besides, the relay harvests energy by TS protocol and the TS factor is fixed as $\alpha = 1/3$. The sub-optimal power splitting factor can be obtained by the alternative search method. The no CJ SER scheme in [8] is the original system model of SER. The relay can harvest more energy from LI and the source, but the relay node is considered as untrusted and the full power is allocated to the source. From Figure 9, the comparison of the proposed scheme and the equal power allocation scheme prove the improvement of the secrecy rate of the proposed power allocation scheme. Moreover, the proposed scheme is better than the schemes in [34] with different TS factor $\alpha = 1/2$, $\alpha = 1/3$ and $\alpha = 1/5$. However, the achievable secrecy rate of the no CJ SER scheme is equal to 0bps/Hz. The reason is that the

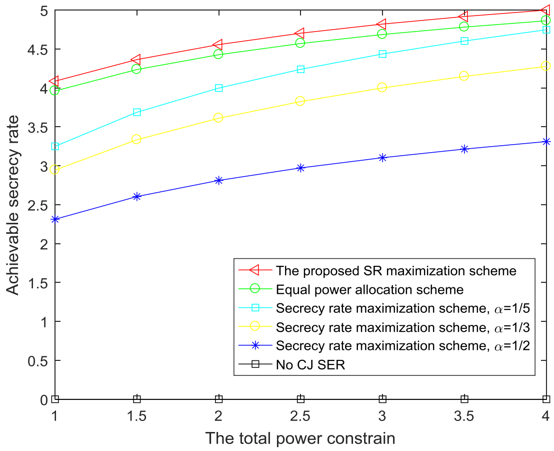


FIGURE 9. **The proposed secrecy rate maximization scheme versus other algorithms.**

SNR of the relay node is always bigger than the SNR of the destination.

V. CONCLUSION

In this paper, a two-phase DBJ relay protocol for a SER untrusted relay network is proposed to guarantee secure information and energy transmission. With the consideration of the total power constraint and the QoS requirement, the maximization secrecy rate optimization is formulated with the imperfect channel estimation error at the destination. To solve the non-convex constraint and objective function, we proposed an iterative power allocation algorithm based on the exact penalty method and DC programming. The exact penalty can handle the non-convex constraint and the DC programming can convert the non-convex objective function into approximate convex optimization. Finally, the sub-optimal transmission power can be obtained by convex programming. Simulation results show that the proposed scheme and algorithm significantly improve the secrecy rate in comparison to the traditional schemes. In the future network, we will extend the relay node to the multi-antenna structure and study the scenarios where both external eavesdroppers and untrusted relay exist.

REFERENCES

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

[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] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[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, Jul. 1978.

[5] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.

[6] L. Liu, R. Zhang, and K.-C. Chua, "Wireless information and power transfer: A dynamic power splitting approach," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3990–4001, Sep. 2013.

[7] K.-H. Liu and P. Lin, "Toward self-sustainable cooperative relays: State of the art and the future," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 56–62, Jun. 2015.

[8] X. Song and S. Xu, "Joint optimal power allocation and relay selection in full-duplex energy harvesting relay networks," in *Proc. 10th Int. Conf. Commun. Softw. Netw. (ICCSN)*, Jul. 2018, pp. 80–84.

[9] Y. Zeng and R. Zhang, "Full-duplex wireless-powered relay with self-energy recycling," *IEEE Wireless Commun. Lett.*, vol. 4, no. 2, pp. 201–204, Apr. 2015.

[10] S. Hu, Z. Ding, and Q. Ni, "Beamforming optimisation in energy harvesting cooperative full-duplex networks with self-energy recycling protocol," *IET Commun.*, vol. 10, no. 7, pp. 848–853, May 2016.

[11] D. Hwang, S. S. Nam, and J. Yang, "Multi-antenna beamforming techniques in full-duplex and self-energy recycling systems: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 160–167, Oct. 2017.

[12] Y. Su, L. Jiang, and C. He, "Decode-and-forward relaying with full-duplex wireless information and power transfer," *IET Commun.*, vol. 11, no. 13, pp. 2110–2115, Sep. 2017.

[13] M. Forouzesh, P. Azmi, and A. Kuhestani, "Secure transmission with covert requirement in untrusted relaying networks," in *Proc. 9th Int. Symp. Telecommun. (IST)*, Dec. 2018, pp. 670–675.

[14] J. Qiao, H. Zhang, F. Zhao, and D. Yuan, "Secure transmission and self-energy recycling with partial eavesdropper CSI," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1531–1543, Jul. 2018.

[15] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.

[16] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[17] L. Sun, T. Zhang, Y. Li, and N. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 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, Feb. 2017.

[19] M. Moradikia, H. Bastami, A. Kuhestani, H. Behroozi, and L. Hanzo, "Cooperative secure transmission relying on optimal power allocation in the presence of untrusted relays, a passive eavesdropper and hardware impairments," *IEEE Access*, vol. 7, pp. 116942–116964, 2019.

[20] M. T. Mamaghani, A. Kuhestani, and K.-K. Wong, "Secure two-way transmission via wireless-powered untrusted relay and external jammer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8451–8465, Sep. 2018.

[21] M. T. Mamaghani, A. Mohammadi, P. L. Yeoh, and A. Kuhestani, "Secure two-way communication via a wireless powered untrusted relay and friendly jammer," in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.

[22] A. El Shafie, A. Mabrouk, K. Tourki, N. Al-Dhahir, and R. Hamila, "Securing untrusted RF-EH relay networks using cooperative jamming signals," *IEEE Access*, vol. 5, pp. 24353–24367, 2017.

[23] K. Lee, J.-T. Lim, and H.-H. Choi, "Impact of outdated CSI on the secrecy performance of wireless-powered untrusted relay networks," *IEEE Trans. Inf. Forensics Security*, to be published.

[24] K. Lee, J.-P. Hong, H.-H. Choi, and M. Levorato, "Adaptive wireless-powered relaying schemes with cooperative jamming for two-hop secure communication," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2793–2803, Aug. 2018.

[25] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.

[26] B. He, J. Chen, Y. Kuo, and L. Yang, "Cooperative jamming for energy harvesting multicast networks with an untrusted relay," *IET Commun.*, vol. 11, no. 13, pp. 2058–2065, Sep. 2017.

[27] H. Shi, Y. Cai, D. Chen, J. Hu, W. Yang, and W. Yang, "Physical layer security in an untrusted energy harvesting relay network," *IEEE Access*, vol. 7, pp. 24819–24828, 2019.

[28] J.-H. Lee, "Optimal power allocation for physical layer security in multi-hop DF relay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 28–38, Jan. 2016.

[29] D. Wang, B. Bai, W. Chen, and Z. Han, "Energy efficient secure communication over decode-and-forward relay channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 892–905, Mar. 2015.

[30] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication for amplify-and-forward relaying with eavesdroppers," in *Proc. IEEE ICC*, Jun. 2015, pp. 4468–4473.

[31] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 740–752, Jan. 2016.

[32] T. Mekkawy, R. Yao, F. Xu, and L. Wang, "Optimal power allocation in an amplify-and-forward untrusted relay network with imperfect channel state information," *Wireless Pers. Commun.*, vol. 101, no. 3, pp. 1281–1293, Aug. 2018.

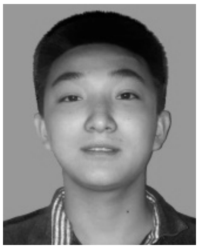
[33] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart., 2019.

[34] R. Yao, Y. Lu, T. A. Tsiftsis, N. Qi, T. Mekkawy, and F. Xu, "Secrecy rate-optimum energy splitting for an untrusted and energy harvesting relay network," *IEEE Access*, vol. 6, pp. 19238–19246, 2018.

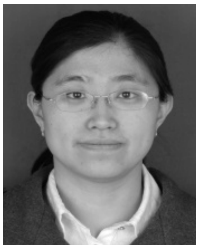
[35] R. Yao, F. Xu, T. Mekkawy, and J. Xu, "Optimised power allocation to maximise secure rate in energy harvesting relay network," *Electron. Lett.*, vol. 52, no. 22, pp. 1879–1881, Oct. 2016.

[36] H. A. Le Thi, T. P. Dinh, H. M. Le, and X. T. Vo, "DC approximation approaches for sparse optimization," *Eur. J. Oper. Res.*, vol. 244, no. 1, pp. 26–46, Jul. 2015.

[37] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.



SIYANG XU received the B.E. degree in electronics and information engineering from the University of Science and Technology, Liaoning, China, in 2016, and the M.S. degree from the Computer Science and Engineering Department, Northeastern University (NEU), Shenyang, China, in 2018, where he is currently pursuing the Ph.D. degree in communication and information system. His research interests include energy harvesting, physical-layer security, and cooperative communication.



XIN SONG was born in Jilin, China, in 1978. She received the Ph.D. degree in communication and information system from Northeastern University, China, in 2008. She is currently a Teacher with Northeastern University, Qinhuangdao, China. Her research interests are in the areas of robust adaptive beam-forming and wireless communication.

ZHIGANG XIE received the B.E. degree in communications engineering from Northeastern University at Qinhuangdao (NEUQ), Qinhuangdao, China, in 2012, and the M.E. degree in software engineering from Northeastern University (NEU), Shenyang, China, in 2016, where he is currently pursuing the Ph.D. degree in communication and information system. His research interests include 5G networks, the Internet of Things, mobile edge computing, and green wireless communications.

JING CAO received the B.E. degree in economics and business from Hebei University and the M.S. degree from Yanshan University. She is currently pursuing the Ph.D. degree in communication and information system with Northeastern University, Shenyang, China. Her research interests include D2D resource allocation and green wireless communications.

JINGPU WANG received the B.E. and M.S. degrees in communications engineering from Dalian Maritime University (DMU), Dalian, China, in 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree in communication and information system with Northeastern University (NEU), Shenyang, China. His research interests include device-to-device communications, non-orthogonal multiple access, and wireless resource allocation.