Hindawi
Mobile Information Systems
Volume 2017, Article ID 2192606, 10 pages
https://doi.org/10.1155/2017/2192606

Research Article

Secrecy in Wireless Information and Power Transfer for One-Way and Two-Way Untrusted Relaying with Friendly Jamming

Lin Xiao,[1] Tao Zhang,[1] Xue Shen,[1] Dingcheng Yang,[1] and Laurie Cuthbert[2]

[1]*Information Engineering School, Nanchang University, Nanchang, China*
[2]*Information Systems Research Centre, Macao Polytechnic Institute, Rua de Luis Gonzaga Gomes, Macau*

Correspondence should be addressed to Dingcheng Yang; ydcxuanyuan@msn.com

Received 18 January 2017; Revised 12 May 2017; Accepted 2 July 2017; Published 10 August 2017

Academic Editor: Stefania Sardellitti

An untrusted relay system combined with a simultaneous wireless information and power transfer (SWIPT) scheme is considered in one-way and two-way relaying transmission strategies. In the system, two source nodes can only communicate with each other via an untrusted energy harvesting relay node, which sends the message by using its harvested energy from the source nodes. Specifically, we classify the intermediate relay as an eavesdropper into two modes: active eavesdropper and nonactive eavesdropper, depending on whether it has sufficient energy of its own to transmit the message or not. Under a simplified three-node fading wiretap channel setup, the transmit power allocation and power splitting ratio are jointly optimized to minimize the outage probability in the delay-sensitive case and to maximize the average rate in the delay-insensitive case, subject to the average and peak total power constraints. Applying the dual-decomposition method, the optimization problem can be efficiently solved in the delay-sensitive scenario. Moreover, an iterative algorithm is proposed to derive the solution to maximize the average rate in the delay-insensitive scenario. Numerical results demonstrate the performance of system outage probability in the two modes versus different rates and how efficiently the secrecy rate is improved compared with traditional schemes.

1. Introduction

Cooperative relaying is an effective approach for energy saving in wireless network, and two-way relay cooperation with network coding can enhance the capacity, coverage, and diversity. However, it does sacrifice the relay node's energy to cooperate with the source node to achieve optimal system throughput. The relay node may lack the proper incentives to cooperate, since the energy consumption would severely degrade the donor's experience, especially when the relay node is a battery constrained user. Recently, energy harvesting communication networks have emerged as alternative solutions with two different lines of research: the SWIPT scheme [1] and the wireless powered communication networks (WPCN) [2]. SWIPT has attracted many researchers' interest since it is a promising technology to overcome the bottleneck of energy constrained wireless networks. Combining SWIPT with two-way relay communications, the relay node consumes the harvested energy instead of its own energy to cooperate with two source nodes to communicate with each other. From the perspective of the physical-layer security, the relay node can be friendly and protect the message from being eavesdropped by others. In heterogeneous networks, the relay node and source node are served by different network operators, so the message transmitted by the source node has different security levels. Moreover, the relay node should generally not be trusted in real life since the source nodes are likely to choose an untrusted relay to forward information. The untrusted relay can act as an essential relay that would strictly execute the forward behavior with specified power, as well as a malicious eavesdropper that has the incentive to eavesdrop on the information. When considering SWIPT with an untrusted relay, it is important to investigate the performance on the outage probability and the system secrecy rate.

For the security communication, if the fading wiretap channel has a better channel gain than the main channel,

the secrecy capacity of the system will be zero. Untrusted relay channels with confidential messages were first studied in [3], where the intermediate relay acted as both an eavesdropper and a helper. The papers [4–7] studied the security of the untrusted relay in different scenarios. The paper [4] considered the relay channel with a relay that was an eavesdropper and whether the untrusted relay may help the source and the destination. The work [5] investigated the problem of secure communication for amplify-and-forward (AF) systems with untrustworthy relay nodes and revealed the system performance worsened as the number of relays increased. In [6], a successive relaying scheme was proposed to secure the AF relaying network with multiple untrusted nodes and it was shown that the scheme could improve the security performance. In addition, secure beamforming with untrusted relay was considered in [7, 8].

The idea of the SWIPT scheme was first proposed in [9], and since then, it has been extended to wireless relay networks [10–18]. For the one-way single-antenna relay channel, time switching (TS) was proposed for AF relay networks in [10] and power splitting (PS) was proposed for DF relaying networks in [11]. More complex but efficient two-way relay systems were analyzed in [12–15]. The authors in [16–18] studied SWIPT in relay channels with the goal of minimizing the outage probability by jointly optimizing time assignment ratio and power splitting ratio. The papers [19, 20] considered the multirelay cooperative networks where the system throughput and SWIPT with rateless code were studied, respectively.

These previous works presented the minimized outage probability in SWIPT-aware two-way relay systems. However, the authors did not consider that the relay could act as an eavesdropper with the SWIPT scheme. Besides, Liu et al. first analyzed the secrecy issue in multiple-input and single-output (MISO) systems combined with SWIPT in [21] where the joint information and energy beamforming design at the transmitter were investigated. In [22–24], the authors considered the application of the multiple-input multiple-output (MIMO) technique with SWIPT, which improved the energy efficiency and also the spectral efficiency in the relay systems. Furthermore, for a fading wiretap channel, Xing et al. considered the optimal AN-aided secrecy design for SWIPT systems [25]. From the literature review above, it is noted that there have been limited studies of the untrusted relay combined with the SWIPT scheme.

In this paper, we focus on the SWIPT scheme with the untrusted relay and the goal is to minimize the outage probability and maximize the secrecy rate in an untrusted relay network with SWIPT. There are two important issues to address in this paper:

(i) The first one is how to reduce the outage probability in the delay-sensitive scenario, subject to the average and peak total power constraints. We formulate the optimization problem, which is a nonconvex problem. However, due to the strong duality of this problem, the Lagrange duality method can be used to address this issue. We propose a dual-decomposition method to optimize the power allocation and the splitting ratio can be obtained by the simple 1D search.

(ii) The second issue is how to optimize the secrecy capacity for the source node in the delay nonsensitive scenario. Using the Lagrange duality method, the optimization problem can be decoupled into parallel subproblems. Then an iterative algorithm is proposed to find the local optimal power allocation. Furthermore, different scenarios are studied to show the performance for the source node that is acting as the information transmitter or friendly jammer.

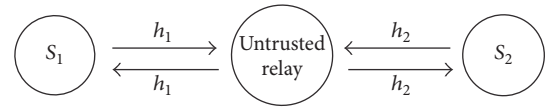

Figure 1: System model.

The remainder of this paper is organized as follows. In Section 2, the untrusted relay system with SWIPT is described and the corresponding secrecy rate is formulated. Section 3 introduces the formulation of the problem including the outage probability minimization problem and ergodic secrecy capacity maximization problem with power constraints. Section 4 gives the numerical simulations to prove the efficiency of the proposed method. Finally, conclusions are drawn in Section 5.

2. System Model

This paper considers a typical untrusted relay network with SWIPT scheme in a fading channel; the model consists of one untrusted relay node with energy harvesting capability and two source nodes S_1 and S_2 as shown in Figure 1. It is assumed that all users are wireless powered and all nodes are assumed to be equipped with a single antenna and operate in the time division mode with the same frequency band. The two source nodes exchange their information via the untrusted relay node, where there is no direct link between them. The source nodes would act as friendly jammer to enhance the security rate with each other. The complex channel coefficients from source nodes to the relay node for one particular transmission fading state are denoted as $h_1(\nu), h_2(\nu)$, where ν denotes the joint fading state in each block. Furthermore, it is assumed that the channel fading state ν remains constant during one round-back block transmission of two time slots but can vary from block to block as ν changes. The channel reciprocity is also assumed for the uplink and downlink transmission between source nodes and the relay node. The complete round trip transmission of the untrusted relay with SWIPT can be divided into two phases as discussed below.

During the first phase, two source nodes transmit their information to the intermediate relay simultaneously. $s_1, s_2 \sim \mathcal{CN}(0, 1)$ are the transmit signals which are circularly symmetric complex Gaussian (CSCG) random variables with zero mean and unit variance. The received signal at the

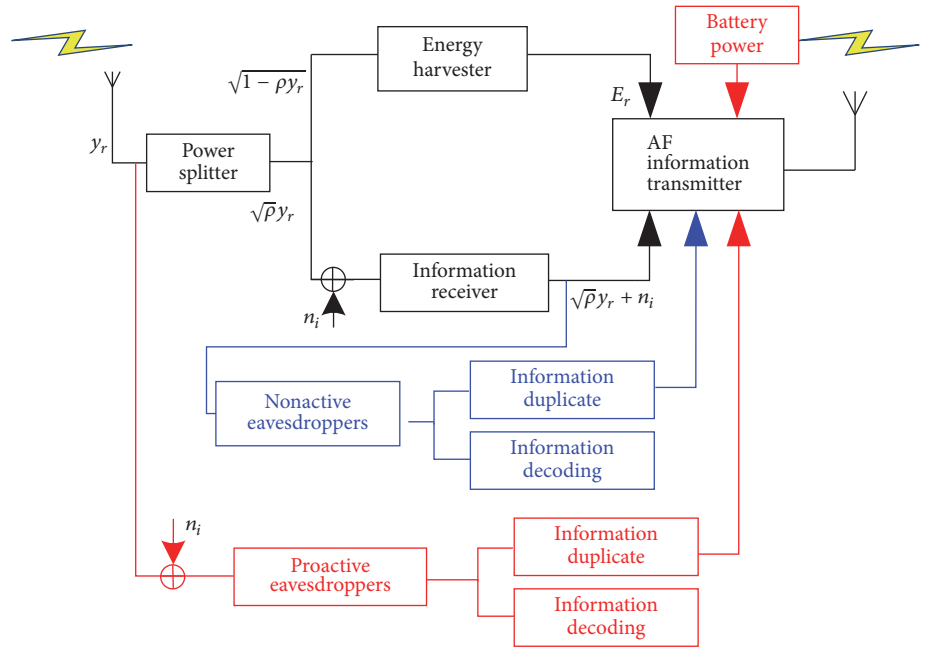

Figure 2: The SWIPT scheme for untrusted relay flow diagram.

untrusted relay can be presented as

$$y_r = \sqrt{P_1(\nu)}h_1(\nu)s_1 + \sqrt{P_2(\nu)}h_2(\nu)s_2 + n_r, \quad (1)$$

where P_1, P_2 are the transmit power of source nodes. $n_r \sim \mathcal{CN}(0, \sigma_r^2)$ denotes the thermal noise at the antenna of the relay node. As shown in Figure 2, the relay node is equipped with a power splitter to divide the received signal into two power streams with the power splitting ratio ρ. One is used for energy harvesting, and the other one is used for the information transceiver. For the energy harvesting part, the harvested energy can be expressed as

$$E_r = \zeta(1-\rho(\nu))\left(P_1(\nu)\left|h_1(\nu)\right|^2 + P_2(\nu)\left|h_2(\nu)\right|^2 + \sigma_r^2\right), \quad (2)$$

where ζ is the energy conversion efficiency factor in converting the RF signal into electrical power. For the information receiver part, the received signal is sent to an information transceiver, which can be represented as

$$y_i = \sqrt{\rho(\nu)}\left(\sqrt{P_1(\nu)}h_1(\nu)s_1 + \sqrt{P_2(\nu)}h_2(\nu)s_2 + n_r\right) + n_i, \quad (3)$$

where $n_i \sim \mathcal{CN}(0, \sigma_i^2)$ is the circuit noise.

It is proposed to classify the intermediate untrusted relay into two modes: nonactive eavesdrop mode and proactive eavesdrop mode.

For the nonactive eavesdrop mode, the relay node would only attempt to decode the message at the information receiver after the power splitting process. The untrusted relay amplifies and forwards the message by using the harvested energy. As shown in Figure 2, the blue diagram describes the nonactive eavesdrop flow chart. Then, the untrusted relay has the capacity with respect to S_1 and S_2 at the fading state ν as

$$\mathscr{C}_1^N = \frac{W}{2}\log_2\left(1 + \frac{\rho(\nu)P_1 g_1(\nu)}{\rho(\nu)P_2(\nu)g_2(\nu) + \rho(\nu)\sigma_r^2 + \sigma_i^2}\right),$$
$$\mathscr{C}_2^N = \frac{W}{2}\log_2\left(1 + \frac{\rho(\nu)P_2(\nu)g_2(\nu)}{\rho(\nu)P_1(\nu)g_1(\nu) + \rho(\nu)\sigma_r^2 + \sigma_i^2}\right), \quad (4)$$

where $g_1(\nu) = |h_1(\nu)|^2$, $g_2(\nu) = |h_2(\nu)|^2$, and W denotes the channel bandwidth.

For the proactive eavesdrop mode that is described in red diagram in Figure 2, the relay node would attempt to decode the message directly via the antenna receiver without the power splitting process. The untrusted relay would duplicate the information and forward it using its own energy from the battery. Moreover, the untrusted relay would obey the optimal forwarding strategy with the assumption that it does not eavesdrop on the message as a regular relay. Then, the untrusted relay has the capacity with respect to S_1 and S_2 at the fading state ν as

$$\mathscr{C}_1^P = \frac{W}{2}\log_2\left(1 + \frac{P_1(\nu)g_1(\nu)}{P_2(\nu)g_2(\nu) + \sigma_r^2 + \sigma_i^2}\right),$$
$$\mathscr{C}_2^P = \frac{W}{2}\log_2\left(1 + \frac{P_2(\nu)g_2(\nu)}{P_1(\nu)g_1(\nu) + \sigma_r^2 + \sigma_i^2}\right). \quad (5)$$

During the second phase, the information transceiver forwards the information receiver signal y_i by an amplification factor β and then broadcasts the signal to both source nodes with the energy harvested power E_r. The transmit signal at the intermediate relay can be expressed as

$$\begin{aligned} x_r &= \sqrt{\beta}\left(\left(\sqrt{\rho P_1}h_1(\nu)s_1 + \sqrt{\rho P_2}h_2(\nu)s_2 + \sqrt{\rho}n_r\right) + n_i\right), \\ \beta &= \frac{\zeta(1-\rho(\nu))\left(P_1(\nu)\left|h_1(\nu)\right|^2 + P_2(\nu)\left|h_2(\nu)\right|^2 + {\sigma_r}^2\right)}{\rho(\nu)\left(P_1(\nu)\left|h_1(\nu)\right|^2 + P(\nu)_2\left|h_2(\nu)\right|^2 + {\sigma_r}^2\right) + {\sigma_i}^2}. \end{aligned} \tag{6}$$

Then, the corresponding signal received at the source nodes can be written as

$$\begin{aligned} x_1 &= h_1(\nu)\sqrt{\beta}\left(\sqrt{\rho(\nu)}\left(\sqrt{P(\nu)_1}h_1(\nu)s_1 + \sqrt{P_2(\nu)}h_2(\nu)s_2 + n_r\right) + n_i\right) + n_1, \\ x_2 &= h_2(\nu)\sqrt{\beta}\left(\sqrt{\rho(\nu)}\left(\sqrt{P_1(\nu)}h_1(\nu)s_1 + \sqrt{P_2(\nu)}h_2(\nu)s_2 + n_r\right) + n_i\right) + n_2. \end{aligned} \tag{7}$$

Since each source node knows its own transmit information in the first phase, the perfect self-interference (self-friendly jamming) can be cancelled. Then, the received signal can be rewritten as

$$\begin{aligned} x_1 &= h_1(\nu)\cdot\left(\sqrt{\beta\rho(\nu)P_2(\nu)}h_2(\nu)s_2 + \sqrt{\beta\rho(\nu)}n_r + \sqrt{\beta}n_i\right) + n_1, \\ x_2 &= h_2(\nu)\left(\sqrt{\beta\rho P_1}h_1(\nu)s_2 + \sqrt{\beta\rho}n_r + \sqrt{\beta}n_i\right) + n_2, \end{aligned} \tag{8}$$

where $n_1, n_2 \sim \mathcal{CN}(0, \sigma_s^2)$ are the AWGN at the source nodes. By applying the Shannon formula, the system rate of the relay system between two source nodes at the fading state ν can be expressed as

$$\begin{aligned} \mathscr{C}_1 &= \frac{W}{2}\log_2\left(1 + \frac{\beta\rho(\nu)P_1g_1(\nu)g_2(\nu)}{\beta\rho(\nu)g_1(\nu)\sigma_r^2 + \beta g_1(\nu)\sigma_i^2 + \sigma_s^2}\right), \\ \mathscr{C}_2 &= \frac{W}{2}\log_2\left(1 + \frac{\beta\rho(\nu)P_2g_1(\nu)g_2(\nu)}{\beta\rho(\nu)g_2(\nu)\sigma_r^2 + \beta g_2(\nu)\sigma_i^2 + \sigma_s^2}\right). \end{aligned} \tag{9}$$

Then, the secrecy rate for source nodes S_1 and S_2 in the two-way untrusted relay at fading state ν can be written as follows.

Nonactive Eavesdrop Mode

$$\mathscr{C}_1^{s,N} = \left(\mathscr{C}_1 - \mathscr{C}_1^N\right)^+, \tag{10a}$$

$$\mathscr{C}_2^{s,N} = \left(\mathscr{C}_2 - \mathscr{C}_2^N\right)^+. \tag{10b}$$

Proactive Eavesdrop Mode

$$\mathscr{C}_1^{s,P} = \left(\mathscr{C}_1 - \mathscr{C}_1^P\right)^+, \tag{11a}$$

$$\mathscr{C}_2^{s,P} = \left(\mathscr{C}_2 - \mathscr{C}_2^P\right)^+, \tag{11b}$$

where $(x)^+$ indicates that $\max(x, 0)$. Until now, we have obtained the secrecy rate expressions of the two-hop secrecy communication in the untrusted relay with SWIPT in nonactive and proactive eavesdrop mode.

For the two-way relay system, the system rate of the two eavesdrop modes can be concluded as (10a) and (10b) and (11a) and (11b). For the one-way relay system, the destination node acts as a friendly jammer to help the source node to transmit the secrecy information. The link from the destination node to the source node is not used to decode the information just for friendly jamming.

Note the antenna noise power σ_r^2 can be neglected compared to the circuit power σ_i^2 at the untrusted relay in practice. Without loss of generality, we assume $\sigma_r^2 = 0$ and $\sigma_i^2 = \sigma_s^2 = 1$.

3. Problem Formulation and Optimal Solution in Different Scenarios

In this section, we consider the system outage probability performance in the delay-sensitive scenario and the average system secrecy rate performance in the delay nonsensitive scenario. The optimization problems are formulated as follows.

3.1. Secrecy Information Transmission in Delay-Sensitive Scenario. Firstly, it is assumed that two source nodes have the instantaneous rate constraints with the two-way relaying scheme, and we consider the optimization problem of minimizing the system outage probability performance. Given the target rates r_1, r_2 at the specific fading state ν, the secrecy outage probability can be presented as

$$\begin{aligned} \gamma_N &= \Pr\left(\mathscr{C}_1^{s,N}(\nu) \le r_1 \parallel \mathscr{C}_2^{s,N}(\nu) \le r_2\right), \\ \gamma_P &= \Pr\left(\mathscr{C}_1^{s,P}(\nu) \le r_1 \parallel \mathscr{C}_2^{s,P}(\nu) \le r_2\right). \end{aligned} \tag{12}$$

It is supposed that the channel coefficients are all known at the source node sides, and the minimized secrecy outage probability problem can be converted into the power allocation strategy to maximize the instantaneous rate. For convenience, it is proposed to adopt the indicator function for the event of successful link to present the outage probability function as

follows:

$$X(\nu) = \begin{cases} 0 & \text{if } \mathscr{C}_1^s(\nu) \geq r_1,\ \mathscr{C}_2^s(\nu) \geq r_2 \\ 1 & \text{otherwise,} \end{cases} \tag{13}$$

where $\mathscr{C}_1^s(\nu)$ and $\mathscr{C}_2^s(\nu)$ denote the secrecy rates in both eavesdrop modes. Then the outage probability function can be rewritten as

$$\gamma_s = \Pr\left(\mathscr{C}_1^s(\nu) \leq r_1 \parallel \mathscr{C}_2^s(\nu) \leq r_2\right) = E_\nu\left[X(\nu)\right]. \tag{14}$$

Considering the total instantaneous peak transmit power constraints $P_{T,\text{peak}}$ and average transmit power constraints P_{avg}, we aim to minimize the system secrecy outage probability by jointly optimizing power allocation at each source node and power splitting ratio at the relay node. The optimization problem can be formulated as follows.

(P1) is

$$\begin{aligned} \underset{P_1(\nu),P_2(\nu),\rho(\nu)}{\text{Minimize}} \quad & E_\nu\left[X(\nu)\right] \\ \text{subject to} \quad & E_\nu\left[P_1(\nu) + P_2(\nu)\right] \leq P_{\text{avg}} \\ & P_1(\nu) + P_2(\nu) \leq P_{T,\text{peak}} \\ & 0 \leq \rho(\nu) \leq 1. \end{aligned} \tag{15}$$

Generally, the optimization problem is nonconvex since the objective function is nonconvex. Adopting a similar analysis drawn in [26], the optimization problem can be verified to obey the "time sharing" condition proposed in [27] under the assumption that the channel fading is a continuous distribution. Moreover, if the investigated time is enough long, strong duality would hold for this optimization problem [28]. Therefore, we can apply the Lagrange duality method to obtain the optimal solution of (P1), and it can be shown as follows.

The Lagrangian of (P1) can be written as

$$\begin{aligned} &\mathscr{L}\left(\left\{P_1(\nu), P_2(\nu), \rho(\nu)\right\}\right) \\ &\quad = E_\nu\left[X(\nu)\right] + \lambda\left(E_\nu\left[P_1(\nu) + P_2(\nu)\right] - P_{\text{avg}}\right) \\ &\quad = E_\nu\left[X(\nu) + \lambda P_1(\nu) + \lambda P_2(\nu)\right] - \lambda P_{\text{avg}}, \end{aligned} \tag{16}$$

where λ is the dual variable with the average power constraint.

The partial Lagrange dual function of (P1) is expressed as

$$\begin{aligned} &\mathscr{G}(\lambda) \\ &\quad = \min_{P_1(\nu)+P_2(\nu)\leq P_{T,\text{peak}}, \rho(\nu)\in\{0,1\}} \mathscr{L}\left(\left\{P_1(\nu), P_2(\nu), \rho(\nu)\right\}\right). \end{aligned} \tag{17}$$

Apparently, the minimization problem can be decoupled into parallel subproblems for each fading state. Then, for one particular fading state ν, the subproblem with the determined λ can be presented as follows.

(P1)-sub is

$$\begin{aligned} \text{Minimize} \quad & \mathscr{L}_1\left(P_1, P_2, \rho\right) \\ \text{subject to} \quad & P_1 + P_2 \leq P_{T,\text{peak}} \\ & 0 \leq \rho \leq 1, \end{aligned} \tag{18}$$

where $\mathscr{L}_1(P_1, P_2, \rho) = X + \lambda(P_1 + P_2)$. Apparently, the secrecy rate of each link is a monotonically increasing function for (P_1, P_2). Given any fixed ρ, in order to maintain the target secrecy rates r_1, r_2, the minimum required power can be obtained by solving the following equations:

$$\begin{aligned} \frac{1 + A_1 P_1}{1 + B_1 P_1 / \left(B_2 P_2 + 1\right)} &= C_1, \\ \frac{1 + A_2 P_2}{1 + B_2 P_2 / \left(B_1 P_1 + 1\right)} &= C_2, \end{aligned} \tag{19}$$

where $A_1 = \zeta\rho(1-\rho)g_1g_2/(\zeta g_1(1-\rho) + \rho)$, $A_2 = \zeta\rho(1-\rho)g_1g_2/(\zeta g_2(1-\rho) + \rho)$, $B_1 = \rho g_1$, $B_2 = \rho g_2$, $C_1 = 2^{2r_1/W}$, and $C_2 = 2^{2r_2/W}$. It is a binary quadratic equation. The solution can be easily obtained as

$$\begin{aligned} P_2^* &= \begin{cases} \dfrac{-B + \sqrt{B^2 - 4AC}}{2A} & \text{if } 0 < \rho < 1 \\ 0 & \text{otherwise,} \end{cases} \\ P_1^* &= \frac{C_1 - 1}{A_1 - B_1 C_1 / \left(B_2 P_2^* + 1\right)}, \end{aligned} \tag{20}$$

where $A = A_1A_2B_2 - A_2B_1B_2 - A_1{B_2}^2C_2 + A_2B_1B_2C_1$, $B = (A_1 - B_1)(A_2 + B_2) - 2A_1B_2C_2 + B_1B_2(C_1 + C_2)$, and $C = (B_1 - A_1)(C_2 - 1)$.

Then, the following problem is formulated to find the optimal solution for ρ.

(P1)-search is

$$\begin{aligned} \text{Minimize} \quad & P_1^* + P_2^* \\ \text{subject to} \quad & 0 \leq \rho \leq 1. \end{aligned} \tag{21}$$

The optimal power splitting ratio $\overline{\rho}^*$ can be obtained by a simple 1D search. Therefore, the optimal power allocation and power splitting ratio can be expressed as

$$\begin{cases} P_1^*\left(\overline{\rho}^*\right), P_2^*\left(\overline{\rho}^*\right) & \text{if } P_1^*\left(\overline{\rho}^*\right) + P_2^*\left(\overline{\rho}^*\right) \leq P_{T,\text{peak}} \\ 0, 0 & \text{otherwise.} \end{cases} \tag{22}$$

It is noted that if the optimal power allocation exceeds the maximum transmit peak power, and the outage event is inevitable. There is no need to allocate the power in this transmission block.

With the given λ, the (P1)-sub problem can be efficiently solved by using (18). For the original optimization problem 1, it can be solved by iteratively updating λ via the gradient method mentioned in [29].

Considering the proactive eavesdropper mode, the optimal solution can be obtained by instituting $B_1' = g_1$ and $B_2' = g_2$ into (20).

Secondly, for the one-way relaying scheme, the outage probability of the link $S_1 \to S_2$ can be represented as

$$\gamma_N^1 = \Pr\left(\mathscr{C}_1^{s,N}(\nu) \leq r_1\right), \tag{23a}$$

$$\gamma_P^1 = \Pr\left(\mathscr{C}_1^{s,P}(\nu) \leq r_1\right). \tag{23b}$$

For the case of link from $S_2 \rightarrow S_1$, it is omitted due to the space limitation. Using the same method as in the two-way relaying scenario, the optimal power allocation in each transmission block is given by the following equations:

$$\frac{1 + A_1 P_1}{1 + B_1 P_1 / \left(B_2 \left(P_T - P_1\right) + 1\right)} = C_1, \tag{24}$$

where P_T is the total transmit power of two source nodes in this block. Then the optimal power allocation for the one-way relaying scenario can be expressed as

$$P_1'^{*} = \left[\frac{-B' \pm \sqrt{B'^2 - 4A'C'}}{2A'}\right]^{+}, \tag{25}$$

where $A' = A_1 B_2$, $B' = B_2 - A_1 - A_1 B_2 P_T - B_2 C_1 + B_1 C_1$ and $C' = C_1 - B_2 P_T + B_2 C_1 P_T - 1$. It is noted that if (25) has no positive real solution, it means that the total transmit power is lower than the required energy power. It is proposed to adopt the gradient method to update the Lagrange variable λ until the optimal solution is obtained.

3.2. Secrecy Information Transmission in Delay Nonsensitive Scenario. Considering the delay nonsensitive scenario, we aim to maximize the ergodic secrecy capacity for the source node, which is subject to the same constraints as mentioned in optimization problem 1 of the delay-sensitive scenario. The optimization problem of maximizing the ergodic secrecy capacity can be represented as follows.

(P2) is

$$\begin{aligned} \underset{P_1(\nu), P_2(\nu), \rho(\nu)}{\text{Maximize}} \quad & E_\nu \left[\mathscr{C}\left(\nu\right)\right] \\ \text{subject to} \quad & E_\nu \left[P_1\left(\nu\right) + P_2\left(\nu\right)\right] \le P_{\text{avg}} \\ & P_1\left(\nu\right) + P_2\left(\nu\right) \le P_{T,\text{peak}} \\ & 0 \le \rho\left(\nu\right) \le 1, \end{aligned} \tag{26}$$

where $[\mathscr{C}(\nu)]$ can be expressed as $\mathscr{C}_1^{s,N}$ or $\mathscr{C}_2^{s,N}$ for the one-way relaying scheme and as $\mathscr{C}_1^{s,N} + \mathscr{C}_2^{s,N}$ for the two-way relaying scheme. Similar to the case in delay-sensitive scenario, adopting the Lagrange duality method, the optimization problem 2 can be decoupled into parallel subproblems with the same structure for each fading state. Therefore, the subproblem can be expressed as follows.

(P2)-sub is

$$\begin{aligned} \text{Maximize} \quad & \mathscr{L}_2\left(P_1, P_2, \rho\right) = \mathscr{C} - \mu\left(P_1 + P_2\right) \\ \text{subject to} \quad & P_1 + P_2 \le P_{T,\text{peak}} \\ & 0 \le \rho \le 1. \end{aligned} \tag{27}$$

Fading state index ν is omitted for brevity. Firstly, considering the one-way relaying scenario, the $\mathscr{C}_1^{s,N}$ or $\mathscr{C}_2^{s,N}$ in the (P2)-sub is nonconvex. It is difficult to be solved by applying convex optimization techniques. Thus, we adopt the temp total transmit power P_T' to find the optimal relationship between P_1 and P_2. Then, (P2)-sub for one-way relaying scheme can be represented as follows.

(P2)-sub-ONE is

$$\begin{aligned} \text{Maximize} \quad & \mathscr{L}_{2,\text{one}}\left(P_1, P_2, \rho\right) = \mathscr{C}_1^{s,N} - \mu\left(P_1 + P_2\right) \\ \text{subject to} \quad & P_1 + P_2 = P_T' \\ & P_T' \le P_{T,\text{peak}} \\ & 0 \le \rho \le 1. \end{aligned} \tag{28}$$

Fixing the power splitting ratio ρ, then, using the KKT conditions for the (P2)-sub-ONE, the optimal power of source node P_1'' can be represented by the temp variable P_T' as follows:

$$\begin{aligned} P_1^{*\prime\prime} &= \left[\frac{A_1 B_2 + A_1 B_2^2 P_T' \pm \sqrt{\Delta}}{A_1 B_2^2 - A_1 B_1 B_2}\right]^{+}, \\ P_2^{*\prime\prime} &= P_T' - P_1^{*\prime\prime}, \end{aligned} \tag{29}$$

where $\Delta = A_1 B_1 B_2 (1 + B_2 P_T')(A_1 - B_1 + B_2 + A_1 B_2 P_T')$. It is noted that the optimal power allocation between two nodes in each transmission block can be substituted by the temp variable P_T'. Then the optimal transmission rate can be obtained by 1D-search for the optimal power splitting ratio ρ. Since the water-filling level cannot be figured out. It is proposed to adopt the iterative method to obtain the local optimal solution. Firstly, we set $P_{T,0}$ as the initial value $P_{T,0} = P_T^l$ of iteration for the number of N channel fading blocks. Secondly, we suppose the initial power step ΔP and then the secrecy rate for this iteration can be updated as

$$\begin{aligned} C_u^l &= 0.5 * \log_2\left(1 + \frac{A_1 * P_1}{1 + \left(B_1 * P_1\right) / \left(\left(\left(P_T + \Delta P\right) - P_1\right) * B_2 + 1\right)}\right), \\ & \qquad l \in \{1, 2, \ldots, N\} \\ C_d^l &= 0.5 * \log_2\left(1 + \frac{A_1 * P_1}{1 + \left(B_1 * P_1\right) / \left(\left(\left(P_T - \Delta P\right) - P_1\right) * B_2 + 1\right)}\right), \\ & \qquad l \in \{1, 2, \ldots, N\}, \end{aligned} \tag{30}$$

where C_u^l and C_d^l are secrecy rates calculated with transmit power of $(P_T + \Delta P)$ and $(P_T - \Delta P)$, respectively. Then, the maximum value of $C_d^{l_B}$ and the minimum value of $C_d^{l_S}$ are selected to calculate the secrecy rate increment ΔC.

$$\Delta C = \left[\left(C_d^{l_B} - C^l\right) - \left(C^l - C_d^{l_S}\right)\right]^{+}. \tag{31}$$

If $l^B = l^S$, the maximum increment and the minimum increment are in the same channel states. This means that power allocation for this channel block is completed. Then the iteration will continue in other remaining channel blocks. It is noted that the selected channel would expend the same energy to obtain a larger secrecy rate compared with other channel blocks. The concept behind this algorithm is that the power step ΔP would be allocated to the specific channel block that can obtain the largest rate increment. And P_T^l is updated as follows:

$$P_T^l = \begin{cases} P_T^l, & \text{others} \\ P_T^{l_B} + \Delta P, & \text{channel selected to obtain energy} \\ P_T^{l_S} - \Delta P, & \text{channel selected to share energy.} \end{cases} \tag{32}$$

Until now, a whole complete iteration process has been introduced. The iteration process will converge when the condition $\Delta C < \varepsilon$ is satisfied, where ε is a small value. This means that the average secrecy rate would not increase anymore. Moreover, the rate fluctuation is small enough. Therefore it has converged to a local optimal point. The iteration process can be summarized in Algorithm 1.

For the two-way relaying scenario, the optimization problem can be expressed as follows.

(P2)-sub-TWO is

$$\begin{aligned} \text{Max:} \quad & \mathscr{L}_{2,\text{two}}(P_1, P_2, \rho) \\ & = \mathscr{C}_1^{s,N} + \mathscr{C}_2^{s,N} - \mu(P_1 + P_2) \\ \text{subject to} \quad & P_1 + P_2 = P_T' \\ & P_T' \le P_{T,\text{peak}} \\ & 0 \le \rho \le 1. \end{aligned} \tag{33}$$

Firstly, we find the optimal relationship between P_1, P_2, and P_T' by solving the following equation:

$$\frac{\partial\left(\mathscr{C}_1^{s,N} + \mathscr{C}_2^{s,N}\right)}{\partial P_1} = \frac{\partial}{\partial P_1}\left(\left(1 + A_1 P_1\right)\left(1 + A_2\left(P_T' - P_1\right)\right)\left(1 + B_1 P_1\right)\frac{\left(1 + B_2\left(P_T' - P_1\right)\right)}{\left(1 + B_1 P_1 + B_2\left(P_T' - P_1\right)\right)^2}\right). \tag{34}$$

We denote the optimal expression as $\widehat{P}_1^{*\prime\prime} = F(P_T')$ and omit the complex expression for the sake of simplicity. Secondly, we adopt the iteratively updating method by firstly fixing the power splitting ratio to find the optimal P_T' for each transmission block, then fixing P_T' to get the optimal splitting ratio until the local optimal point is obtained. Similar to the one-way relay scenario, the proposed iteration scheme is used to solve the optimal power allocation for the two-way relay case.

4. Simulation Results

In this section, we provide the numerical results to evaluate the performance of the SWIPT scheme with one-way and two-way relaying transmission strategies for the proactive mode and the nonactive mode. It is supposed that the untrusted relay is in the middle of two source nodes. The simulation parameters are set up as follows: the transmission bandwidth $W = 100$ KHz and the number of channel blocks $N = 100$; antenna noise power $\sigma_r^2 = 0$ and circuit power $\sigma_i = 1$; the energy conversion efficiency factor ζ is set to 0.6; $P_{T,\text{peak}}$ is 70 dBm; the convergence coefficient is 10^{-5} and the initial step value ΔP is 10 dBm.

For the two-way relay case, we firstly study the minimum outage probability for the proactive eavesdrop mode and the nonactive eavesdrop mode. Figure 3 depicts the outage probability versus the average transmit power with different secrecy rates. It is noted that, for any given secrecy rate, the outage probability for the two-way scheme decreases sharply as the average transmit power increases. For different secrecy rates, the curve tends to decline slowly when the secrecy rate is higher. This is due to the fact that when the target secrecy rate increases, it needs more transmit power and a better channel state to satisfy the condition, which leads to a lower outage probability. Moreover, it can be seen that even if the transmit power is large enough, the outage probability can be less than 0.01%. Figure 3 also shows that the outage probability in the nonactive mode is lower than that in the proactive mode for a fixed secrecy rate. This indicates that the power splitting process after the information decoding has a more positive effect on the signal-to-interference-plus-noise ratio (SINR) than decoding information directly via the antenna receiver. Actually, the relay mode selection depends on the practical scenario.

Figure 4 plots the outage probability performance of one-way relay versus the transmit power. It can be observed that when the secrecy rate is larger, the outage probability is higher, which is similar to the outage probability of the two-way relaying. However, the difference is that the outage probability of one-way relay decreases faster than the two-way scheme. This is because of the effect of friendly jamming which would bring benefits and the impacts of two-way channel conditions are more complex than one-way relay scheme. It is also noticed that the curves of the nonactive scheme and the proactive scheme are very close to each other. This indicates that the power splitting at the information receiver and the antenna receiver have a very similar effect on the system outage performance. Moreover, the gap between curves with different secrecy rates is quite clear. The reason is that the higher secrecy rate demands more power to transmit

INPUT: initial value P_T^0, step value ΔP, convergence rate ε, numbers of channel blocks N
OUTPUT: optimal power allocation ${}^*P_T^l$, $l = 1, 2, \ldots, N$
STEPS:
(1) Based on P_T^0, ΔP and N, calculates P_1^l, P_2^l and C^l
(2) **Repeat:**
(3) calculate C_u^l, C_d^l and C^l
(4) find $C_u^{l_B}$ and $C_u^{l_S}$
(5) **If** $l_B \neq l_S$,
(6) calculate $P_T^{l_B}$ and $P_T^{l_S}$ for updating power allocation
(7) **Else**
(8) the lth channel state completes the power allocation,
(9) **until:** the condition $\Delta C < \varepsilon$ where the rate is convergent.

Algorithm 1: Power allocation algorithm in two-way relay case.

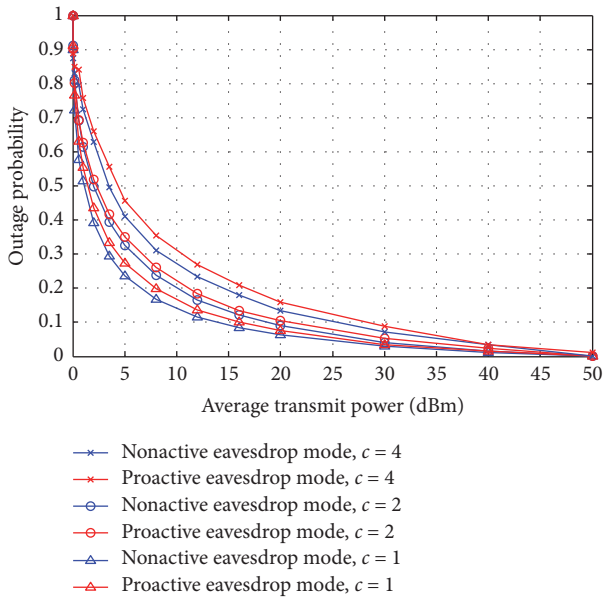

Figure 3: The outage probability for different P_{avg} in the two-way relay case.

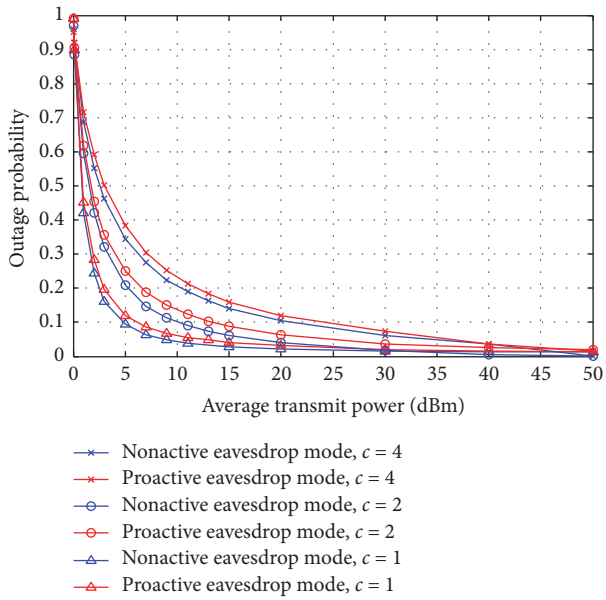

Figure 4: The outage probability for different P_{avg} in the one-way relay case.

the information, which is less likely to satisfy the constraints and leads to a higher outage probability.

For the secrecy information transmission in the delay nonsensitive scenario, we show the performance of maximum secrecy rate versus different values of P_{avg} in Figure 5. For a better comparison, we use the average transmit power allocation scheme as a benchmark. It is shown that the proposed iteration scheme increases faster than the average transmit power allocation scheme, which indicates that the proposed scheme outperforms the average transmit power allocation scheme. Besides, we can note that the secrecy rate cannot always increase with the increase of the average transmit power because of the limitation of channels. We also notice that there is a gap between the curves of the nonactive scheme and the proactive scheme. For instance, when the average transmit power $P_{\text{avg}} = 40$ dBm, the secrecy rate achieved by the nonactive mode is more than 0.25 bits/s/Hz compared with the proactive mode. As mentioned above, this is due to the fact that the SINR is higher in the nonactive mode, which contributes to a larger secrecy rate in the nonactive mode. It also indicates that decoding messages at the information receiver can enhance the system performance.

Figure 6 shows the maximum secrecy rate of the two-way relay versus different average transmit power. It can be seen that the secrecy rate of four scenarios increases with the increment of the average transmit power. It can also be observed that the secrecy rate of the proposed scheme is nearly twice the secrecy rate of the average power allocation scheme. For example, in nonactive mode, when the average transmit power is 40 dBm, the secrecy rate for the

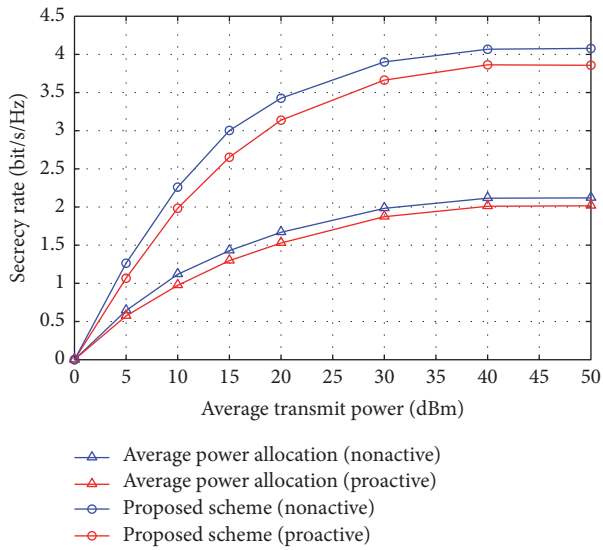

FIGURE 5: The secrecy rate for different P_{avg} in the two-way relay case.

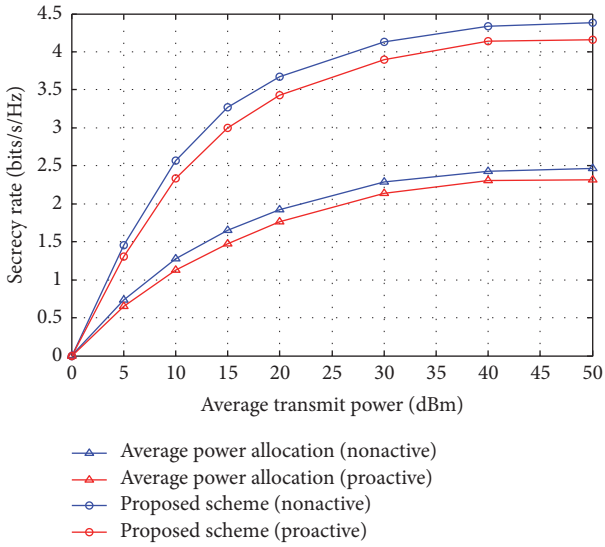

FIGURE 6: The secrecy rate for different P_{avg} in the one-way relay case.

proposed scheme is about 4.3 bits/s/Hz nearly twice the value of 2.4 bits/s/Hz for the average power allocation scheme. Moreover, the rate for the two-way relay scenario is lower than the rate in the one-way relay scenario. This is not only because of the friendly jamming in the one-way relay case but also because of more complex channel conditions in the two-way relay case.

5. Conclusion

This paper investigates a relay system with SWIPT in a fading channel, which includes one untrusted relay node with energy harvesting capability in the one-way and the two-way relaying scenarios. The source nodes exchange their information via the untrusted relay since there is no other link between them. The intermediate relay is divided into two modes: active eavesdropper and nonactive eavesdropper depending on whether the harvested energy can support the transmission cost. We jointly optimize the transmit power allocation and power splitting ratio with the objective of minimizing the outage probability in the delay nonsensitive scenario and maximizing the average rate in the delay-sensitive scenario, subject to the average and peak total power constraints. The outage probability optimization can be solved by dual decomposition efficiently and an iteration algorithm is proposed to optimize the secrecy rate. Numerical results demonstrate the performance of the nonactive mode is better than the proactive mode and the proposed scheme also has significant improvement in terms of system outage probability and the secrecy rate.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (61561032, 61461029), China/Jiangxi Postdoctoral Science Foundation Funded Project (2014MT561879, 2014KY046), Young Scientists Project Funding of Jiangxi Province (20153BCB23020, 20162BCB23010), the Natural Science Foundation of Jiangxi Province (20161BAB202043, 20114ACE00200), and Graduate Student Innovation Special Funds of Nanchang University (Grant no. cx2016265).

References

[1] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 1989–2001, 2013.

[2] Q. Wu, M. Tao, D. W. Kwan Ng, W. Chen, and R. Schober, "Energy-Efficient Resource Allocation for Wireless Powered Communication Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2312–2327, 2016.

[3] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '07)*, pp. 926–930, Nice, France, June 2007.

[4] X. He and A. Yener, "Cooperation with an untrusted relay: a secrecy perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827.

[5] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3801–3807, 2012.

[6] W. Wang, K. C. Teh, and K. H. Li, "Relay Selection for Secure Successive AF Relaying Networks With Untrusted Nodes," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2466–2476, 2016.

[7] M. Zhao, S. Feng, X. Wang, M. Zhang, Y. Liu, and H. Fu, "Joint power splitting and secure beamforming design in the wireless-powered untrusted relay networks," in *Proceedings of the 58th IEEE Global Communications Conference, GLOBECOM*, San Diego, Calif, USA, December 2015.

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

[9] L. R. Varshney, "Transporting information and energy simultaneously," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '08)*, pp. 1612–1616, IEEE, Toronto, Canada, July 2008.

[10] I. Krikidis, S. Timotheou, and S. Sasaki, "RF energy transfer for cooperative networks: data relaying or energy harvesting?" *IEEE Communications Letters*, vol. 16, no. 11, pp. 1772–1775, 2012.

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

[12] Z. Chen, B. Wang, B. Xia, and H. Liu, "Wireless information and power transfer in two-way amplify-and-forward relaying channels," in *Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP '14)*, pp. 168–172, Atlanta, Ga, USA, December 2014.

[13] Y. Liu, L. Wang, M. Elkashlan, T. Q. Duong, and A. Nallanathan, "Two-way relaying networks with wireless power transfer: Policies design and throughput analysis," in *Proceedings of the 2014 IEEE Global Communications Conference, GLOBECOM*, pp. 4030–4035, Austin, Tex, USA, December 2014.

[14] Z. Fang, X. Yuan, and X. Wang, "Distributed energy beamforming for simultaneous wireless information and power transfer in the two-way relay channel," *IEEE Signal Processing Letters*, vol. 22, no. 6, pp. 656–660, 2015.

[15] K. Xiong, Y. Zhang, Y. Chen, and X. Di, "Power splitting based SWIPT in network-coded two-way networks with data rate fairness: an information-theoretic perspective," *China Communications*, vol. 13, no. 12, pp. 107–119, 2016.

[16] H. Lee, C. Song, S. Choi, and I. Lee, "Outage probability analysis and power splitter designs for swipt relaying systems with direct link," *IEEE Communications Letters*, vol. 21, no. 3, pp. 648–651, 2017.

[17] R. Jiang, K. Xiong, Y. Zhang, and Z. Zhong, "Outage analysis and optimization of swipt in network-coded two-way relay networks," *Mobile Information Systems*, vol. 2017, Article ID 2516035, 16 pages, 2017.

[18] R. Hu and T.-M. Lok, "Power splitting and relay optimization for two-way relay SWIPT systems," in *Proceedings of the 2016 IEEE International Conference on Communications, ICC 2016*, Kuala Lumpur, Malaysia, May 2016.

[19] D. Yang, C. Zhu, L. Xiao, X. Shen, and T. Zhang, "An energy-efficient scheme for multirelay cooperative networks with energy harvesting," *Mobile Information Systems*, vol. 2016, Article ID 5618935, 10 pages, 2016.

[20] X. Di, K. Xiong, P. Fan, and H.-C. Yang, "Simultaneous wireless information and power transfer in cooperative relay networks with rateless codes," *IEEE Transactions on Vehicular Technology*, 2016.

[21] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Transactions on Signal Processing*, vol. 62, no. 7, pp. 1850–1863, 2014.

[22] Z. Ding, C. Zhong, D. W. K. Ng et al., "Application of smart antenna technologies in simultaneous wireless information and power transfer," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 86–93, 2015.

[23] K. Xiong, P. Fan, C. Zhang, and K. B. Letaief, "Wireless information and energy transfer for two-hop non-regenerative MIMO-OFDM relay networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 8, pp. 1595–1611, 2015.

[24] F. Benkhelifa, A. S. Salem, and M. Alouini, "SWIPT in Multiuser MIMO decode-and-forward relay broadcasting channel with energy harvesting relays," in *Proceedings of the 2016 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–7, Washington, DC, USA, December 2016.

[25] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 180–190, 2016.

[26] L. Liu, R. Zhang, and K.-C. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 288–300, 2013.

[27] R. T. Rockafellar, *Convex Analysis*, Princeton University Press, Princeton, NJ, USA, 1997.

[28] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Transactions on Communications*, vol. 54, no. 7, pp. 1310–1322, 2006.

[29] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.