Hindawi Publishing Corporation
International Journal of Antennas and Propagation
Volume 2015, Article ID 530632, 15 pages
http://dx.doi.org/10.1155/2015/530632

Research Article

Joint Power Allocation at the Base Station and the Relay for Untrusted Relay Cooperation OFDMA Network

Weiheng Jiang and Wenjiang Feng

College of Communication Engineering, Chongqing University, Chongqing 400044, China

Correspondence should be addressed to Weiheng Jiang; whjiang@cqu.edu.cn

Received 13 October 2014; Revised 17 March 2015; Accepted 17 March 2015

Academic Editor: Francisco Falcone

The secure communication that multiple OFDMA-based cell-edge mobile stations (MS) can only transmit confidential messages to base station (BS) through an untrusted intermediate relay (UR) is discussed. Specifically, with the destination-based jamming (DBJ) scheme and fixed MS transmission power assumption, our focus is on the joint BS and US power allocation to maximize system sum secrecy rate. We first analyze the challenges in solving this problem. The result indicates that our nonconvex joint power allocation is equivalent to a joint MS access control and power allocation. Then, by problem relaxation and the alternating optimization approach, two suboptimal joint MS access control and power allocation algorithms are proposed. These algorithms alternatively solve the subproblem of joint BS and UR power allocation and the subproblem of MS selection until system sum secrecy rate is nonincreasing. In addition, the convergence and computational complexity of the proposed algorithms are analyzed. Finally, simulations results are presented to demonstrate the performance of our proposed algorithms.

1. Introduction

Broadcast is a fundamental property of the wireless medium. This property makes wireless communication susceptible to eavesdropping. Traditionally, this problem is typically addressed via upper layer approaches, such as the cryptographic protocols in the application layer which relies on computational complexity. Nowadays, information-theoretic security which exploits the properties of wireless channel to secure communications has received considerable attention.

In fact, the secret communication in the presence of an eavesdropper was first introduced and studied by Wyner who considered a wiretap channel model [1]. Wyner showed that when eavesdropper's channel is a degraded version of the main channel, the source and destination can achieve a positive perfect information rate (defined as secrecy rate). The maximal secrecy rate from the source to the destination is defined as the secrecy capacity and for the degraded wiretap channel is given as the difference between the rate at the legitimate receiver and the rate at the eavesdropper. Inspired by the pioneering work of Wyner, Csiszar and Korner then considered the general broadcast wiretap channel [2]. Their research showed that even when the eavesdropper is not degraded with respect to the legitimate user, secure communication between the legitimate users is possible by exploiting the inherent randomness of the communication channel. Recently, the secret communication in wireless networks has been intensively studied for various scenarios [3–5].

Although the property of broadcasting makes wireless communication susceptible to eavesdropping, it also provides us with the opportunity to improve the security of wireless transmission by cooperation and relay [6, 7]. In recent years, the relay channel without security constraints has been studied under various scenarios. In most of these works, cooperation strategies such as decode-and-forward (DF), compress-and-forward (CF), and amplify-and-forward (AF) have been constructed to increase the transmission rate or reliability function [7, 8]. By using cooperative relay to enhance communication security, the research can be grouped into two types. The first type corresponds to the classical sense of cooperation, where the cooperating nodes strengthen the main transmission (from legitimate transmitter to the legitimate receiver) by using common relaying techniques such as AF and DF [6, 9–12]. For the strategies of

the second type, the cooperating parties improve the secrecy performance of the system by weakening the eavesdropping link (from legitimate transmitter to the eavesdropper), such as the noise-forwarding [13], cooperative jamming [10–12, 14], and artificial noise [15]. For these works of cooperation enhanced secure communication, an important assumption is that the cooperation node is trustworthy. In other words, the cooperation (or relay) node is not an eavesdropper and does not make malicious attack. As pointed out in [16–18], the assumption that the relay node is trustworthy is not always true in some sense, since the relay node may not belong to the same party as the source or the destination. Under this situation, we may wonder whether secure communication between the source and the destination is still possible with the cooperation of untrusted node, especially in the scenario that no direct link can be established between the source and the destination. In fact, this involves untrusted relay (UR) cooperation secure communication which has already been discussed in [16–28].

The untrusted relay model was first studied in [16] for the general relay channel. The secrecy capacity of this system will be zero if the relay channel is degraded and will equal the wiretap channel capacity if the channel is reversely degraded. Although it is a pessimistic result, one might wonder whether there exists any situation where the cooperation of UR can enable a higher secrecy rate than simply treating it as an eavesdropper. The positive response came from He and Yener [17]. Their research showed that using an CF-based UR to relay information can surely achieve a higher secrecy rate than just treating the relay as an eavesdropper. Later in [18], with the assumption that there is no direct link between the source and the destination, the destination-based jamming (DBJ) scheme was proposed to obtain positive secrecy rate even though the relay is untrusted. Following these information-theoretical developments, the joint source and relay beamforming design problem for an untrusted MIMO relay channel was studied in [19] and the secrecy outage probability for untrusted AF relay channels was investigated in [20]. The work in [21] considered secrecy rate maximization problem in untrusted two-way relaying channels with friendly jammers. Then game theory-based distributed joint jammer selection and power allocation algorithm was presented therein. In [22], the authors studied joint transmit design and relay node selection for a relay network with a group of untrusted relay nodes. Reference [23] presented a comprehensive analysis of the secrecy capacity for two-hop AF cooperative systems with untrustworthy relay nodes. The work in [24] considered the optimal source and relay transmission design for the hybrid network with both internal and external wiretappers. The optimal signal transmission power is calculated therein. The untrusted relay cooperation scenario also had been discussed in the cognitive radio networks [25]. The authors considered that the secondary users (SUs) helped the primary users (PUs) to relay their confidential messages in reward for being allowed to share their spectrum bands. However, the PUs might be reluctant to accept the SUs' help, since the SUs are untrustworthy and may try unauthorized decoding of the PUs' messages. Further research about this topic could be found in [26–28].

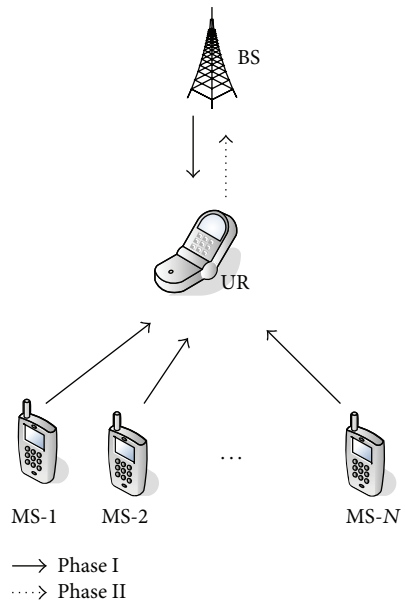

Figure 1: System model.

All the above-mentioned literatures [16–28] only considered the secure communication between one pair of nodes by the cooperation of untrusted relay. Our work in this paper extends these works to the multiuser case. In particular, multiple OFDMA-based cell-edge mobile stations (MS) transmit confidential messages to base station (BS) only through an untrusted intermediate relay (UR). To be specific, with the destination-based jamming (DBJ) scheme and fixed MS transmission power assumption, our focus is on the joint BS and US power allocation to maximize system sum secrecy rate. Firstly, we discuss the challenges in solving this problem. The result indicates that our nonconvex joint power allocation is equivalent to a joint MS access control and power allocation. Secondly, by problem relaxation and the alternating optimization approach, two suboptimal joint MS access control and power allocation algorithms are proposed. These algorithms alternatively solve the subproblem of joint BS and UR power allocation and the subproblem of MS selection until system sum secrecy rate is nonincreasing. Also, the convergence and computational complexity of the proposed algorithms are analyzed. Finally, simulations are conducted to evaluate the performance of our proposed algorithms. The following of the paper is organized as follows: system model and cooperation protocol are introduced in Section 2; the joint power allocation problem is discussed in Section 3 and suboptimal algorithms are also present therein; selected numerical results are shown in Section 4; and finally the conclusion is given.

2. System Model and Cooperation Protocol

2.1. System Model. As depicted in Figure 1, the system investigated herein is about a single cell network with one BS and multiple cell-edge MS which have secure communication requirements with BS in the uplink. Define the MS set by $\mathcal{N}$

and $N = |\mathcal{N}|$, and MS are indexed by $i = 1, \ldots, N$. Each of the MS in $\mathcal{N}$ has already been allocated one orthogonal channel (in frequency-domain with unit bandwidth, such as OFDMA-based broadband wireless network). Since these MS are all far away from BS, no direct link between MS and BS can be established. Suppose that another MS (not in $\mathcal{N}$) or heterogeneous network node is happening to be in the right place and has the will of cooperating with these MS as a volunteer of relay. (We do not discuss the motivations of UR cooperation and only focus on the joint power optimization. As in [21], the incentives of UR cooperation can be analyzed by game theory.) Unfortunately, this (relay) node (denoted by UR) may not belong to the same operator as BS and MS and thus has lower security clearance. Therefore, the UR has a dual role and acts as both an essential helper and a potential eavesdropper but not making any malicious attack. Under this setup, effective scheme should be introduced to complete the confidential message transmission and also to protect them not to be wiretapped by the UR. In this paper, there are no extra jammers existing and the DBJ scheme [18] is adopted to achieve the goal; that is, the BS plays the role of jammer. In addition, the following assumptions are used in our paper: (i) the cooperation strategy of UR is AF-based and full channel state information (CSI) is available at all nodes; (ii) BS, MS, and UR are all equipped with single antenna and operated in half-duplex mode; (iii) all MS transmit with fixed power; that is, $p_i^S (> 0)$, $\forall i \in \mathcal{N}$. The system aims at maximizing system sum secrecy rate by joint UR and BS power allocation. (Although the joint optimization of BS, UR, and MS power allocation can further improve the system sum secrecy rate, for simplicity, we only consider the problem of joint BS and UR power allocation herein.)

2.2. Cooperation Protocol. In our considered scenario, the MS-BS secure communication process is performed by two phases. During the first phase (Phase I, shown with solid lines in Figure 1), MS send their confidential messages to UR over their allocated channels. Simultaneously, the BS injects interference signals in the form of Gaussian noise over multiple MS working channels. Thus, the received signal at UR over channel i (for MS-i) is

$$y_i^R = \sqrt{p_i^S} h_i^{SR} x_i^S + \sqrt{p_i^B} g_i^{BR} x_i^B + n_i^R, \tag{1}$$

where p_i^B is the BS jamming signal power over channel-i. x_i^S and x_i^B (both with unit energy) denote the transmit modulated symbol by MS-i and the jamming signal by BS over channel i, respectively. Suppose that all channels are reciprocal; we use h_i^{SR} and g_i^{RB} (or g_i^{BR}) to denote the channel coefficients from MS-i to UR and from UR to BS over channel i, respectively. n_i^R stands for a complex valued additive white Gaussian noise (AWGN) at UR in channel i such that $n_i^R \sim \mathcal{CN}(0, \sigma_i^2)$.

During the secondary phase (Phase II, shown with dashed line in Figure 1), UR normalizes its received signals over different channels and forwards the scaled versions to BS. In channel i, the signal regenerated by UR is $x_i^R = \zeta_i \sqrt{p_i^R} y_i^R$, where $\zeta_i = (p_i^S |h_i^{SR}|^2 + p_i^B |g_i^{BR}|^2 + \sigma_i^2)^{-1/2}$ is the normalized factor at UR for MS-i and p_i^R is the power allocated by UR for MS-i. Thus, the signal received at BS for MS-i is $y_i^B = \zeta_i \sqrt{p_i^R} g_i^{RB} y_i^R + n_i^B$, $\forall i \in \mathcal{N}$, where n_i^B is the AWGN at BS over the channel for MS-i and $n_i^B \sim \mathcal{CN}(0, \sigma_i^2)$. Then, after canceling the self-interference, that is, $\zeta_i \sqrt{p_i^R p_i^B} g_i^{BR} g_i^{RB} x_i^B$, the instantaneous received signal at the BS over channel i can be written as

$$\begin{aligned} y_i^B = {} & \frac{\sqrt{p_i^S p_i^R} h_i^{SR} g_i^{RB}}{\sqrt{p_i^S |h_i^{SR}|^2 + p_i^B |g_i^{BR}|^2 + \sigma_i^2}} x_i^S \\ & + \frac{\sqrt{p_i^R} g_i^{RB}}{\sqrt{p_i^S |h_i^{SR}|^2 + p_i^B |g_i^{BR}|^2 + \sigma_i^2}} n_i^R + n_i^B. \end{aligned} \tag{2}$$

Let $|h_i^{SR}|^2/\sigma_i^2 = \gamma_i^{SR}$, $|g_i^{BR}|^2/\sigma_i^2 = \gamma_i^{BR}$, and $|g_i^{RB}|^2/\sigma_i^2 = \gamma_i^{RB}$ (since $g_i^{RB} = g_i^{BR}$, we have $\gamma_i^{BR} = \gamma_i^{RB}$). Then, the instantaneous received signal SNR (signal to noise ratio) at the UR (which is denoted by χ_i^R) and at the BS (which is denoted by χ_i^B) for MS-i can be expressed as, respectively,

$$\chi_i^R = \frac{p_i^S \gamma_i^{SR}}{1 + p_i^B \gamma_i^{BR}}, \qquad \chi_i^B = \frac{p_i^S p_i^R \gamma_i^{SR} \gamma_i^{RB}}{1 + p_i^S \gamma_i^{SR} + p_i^R \gamma_i^{RB} + p_i^B \gamma_i^{BR}}. \tag{3}$$

3. Jammer and Relay Power Allocation under Individual Power Constraint

In this section, the problem of system sum secrecy rate maximization is first introduced and we analyze the challenges in solving this problem. Second, the alternating optimization (AO) approach is provided to handle our problem and then an AO algorithm is given. The convergence and computational complexity of the AO algorithm are also analyzed. Finally, another suboptimal algorithm with lower complexity is presented.

3.1. Secrecy Rate Maximization Problem. As mentioned earlier, in our considered system, BS plays the role of jammer and relay is untrusted. The system aims to maximize sum secrecy rate by joint BS and UR power allocation. From [18, 21], we know that the achievable secrecy rate for MS-i at the BS is

$$R_i\left(p_i^B, p_i^R\right) = \frac{1}{2}\left[R_i^B\left(p_i^B, p_i^R\right) - R_i^R\left(p_i^B\right)\right]^+, \tag{4}$$

where the factor $1/2$ is due to the fact that the communication is divided into two phases and we will omit it below. $[\cdot]^+ \triangleq \max\{0, \cdot\}$, $R_i^B(p_i^B, p_i^R) = \log(1 + \chi_i^B)$, and $R_i^R(p_i^B) = \log(1 + \chi_i^R)$ represent the capacity between MS-i and BS and between MS-i and UR, without the secrecy constraint, respectively. Based on the formulation of χ_i^R and χ_i^B in (3), it is obvious that the obtained secrecy rate for MS-i depends on both relay power p_i^R and jammer power p_i^B. Therefore, the joint optimization of BS and UR power allocation to maximize sum secrecy

rate is required. Since the UR and BS have independently power constraint, consequently, the optimization problem (OP1) that we seek to solve is

$$\text{OP1:} \max_{(\mathbf{p}^R,\mathbf{p}^B)} R\left(\mathbf{p}^R,\mathbf{p}^B\right) = \sum_{i\in\mathcal{N}} R_i\left(p_i^B, p_i^R\right) \tag{5a}$$

$$\text{s.t. } 0 \leqslant \sum_{i\in\mathcal{N}} p_i^R \leqslant P^R, \qquad 0 \leqslant \sum_{i\in\mathcal{N}} p_i^B \leqslant P^B \tag{5b}$$

$$\mathbb{I}\left\{p_i^R > 0\right\} = \mathbb{I}\left\{p_i^B > 0\right\}, \quad \forall i \in \mathcal{N}, \tag{5c}$$

where $\mathbf{p}^R = (p_1^R, \ldots, p_N^R)$ and $\mathbf{p}^B = (p_1^B, \ldots, p_N^B)$ denote the power allocation vectors at UR and BS for the MS in $\mathcal{N}$, respectively. P^R and P^B are the corresponding power constraints at UR and BS, respectively. $\mathbb{I}\{X\}$ is an indicator function such that $\mathbb{I}\{X\} = 1$ if the event X is true and $\mathbb{I}\{X\} = 0$ otherwise. Constraint (5c) comes from the fact that the direct link between BS and MS does not exist. Therefore, zero jamming or relay power always leads to zero secrecy rate.

With the problem definition in (5a), (5b), and (5c), it is noted that three factors make OP1 hard to deal with: (i) the nonsmooth property of $R_i(p_i^B, p_i^R)$ which is caused by the nonnegative constraint of the secrecy rate definition; (ii) the nonconvex property of $R_i(p_i^B, p_i^R)$ (with respect to p_i^B and p_i^R), even without considering the nonnegative constraint of the secrecy rate definition; (iii) the potential combinatorial property of OP1 which is caused by the coupled relationship between p_i^B and p_i^R defined in (5c). In order to handle OP1, an important lemma is introduced first as below.

Lemma 1. *For MS-i, $\forall i \in \mathcal{N}$, with transmit power p_i^S and secrecy rate definition (4), the sufficient and necessary condition for MS-i to obtain positive secrecy rate is that the allocated jamming power p_i^B and relay power p_i^R satisfy*

$$p_i^R > p_{i,th}^R = \frac{\left(1 + \left(1 + p_i^S\gamma_i^{SR}\right)/\left(p_i^B\gamma_i^{RB}\right)\right)}{\gamma_i^{RB}}, \quad p_i^B > 0. \tag{6}$$

Also, the necessary condition for all MS in $\mathcal{N}$ to obtain positive secrecy rate is that the UR power P^R should satisfy (7). (One can note that the lower bound of condition (7) is loose, because we have assumed that the allocated jamming power is $p_i^B = \infty$ for $\forall i \in \mathcal{N}$. In fact, we can attain more tightly conditions by assuming that, for $\forall i \in \mathcal{N}$, $p_i^B = P^B$. Actually, this is unnecessary. Our purpose is to declare that OP1 is equivalent to a problem of joint MS access control and power allocation.) Consider

$$P^R > \sum_{i\in\mathcal{N}} \frac{1}{\gamma_i^{RB}}. \tag{7}$$

Proof. Please see Appendix A. □

By Lemma 1, the exact nonlinear coupled relationship between p_i^B and p_i^R which is caused by nonnegative secrecy rate definition is characterized by (6). For (7), it is worth strengthening that it is just the necessary condition for the system to promise all MS in $\mathcal{N}$ to achieve positive secrecy rate but not sufficient condition. Thus, if (7) is false, then surely some MS in $\mathcal{N}$ will be rejected by the system due to overload; while if it is true, then it is still possible for some MS in $\mathcal{N}$ being rejected. Therefore, in essence, OP1 is equivalent to the following joint MS access control and power allocation problem (which is denoted by OP2):

$$\text{OP2:} \max_{\mathcal{N}^\circ\subseteq\mathcal{N},(\mathbf{p}^R,\mathbf{p}^B)} R^\circ\left(\mathbf{p}^R,\mathbf{p}^B\right) = \sum_{i\in\mathcal{N}^\circ} R_i^\circ\left(p_i^B, p_i^R\right) \tag{8a}$$

$$\text{s.t.} \sum_{i\in\mathcal{N}^\circ} p_i^R \leqslant P^R, \qquad \sum_{i\in\mathcal{N}^\circ} p_i^B \leqslant P^B \tag{8b}$$

$$\mathbb{I}\left\{p_i^R > p_{i,\text{th}}^R\right\} = \mathbb{I}\left\{p_i^B > 0\right\}, \quad \forall i \in \mathcal{N}^\circ, \tag{8c}$$

where $\mathcal{N}^\circ$ is a MS subset. This subset is determined by the MS access control so that all MS in this subset can achieve positive secrecy rate. Define $N^\circ = |\mathcal{N}^\circ|$, and let $\mathbf{p}^R = (p_1^R, \ldots, p_{N^\circ}^R)$ and $\mathbf{p}^B = (p_1^B, \ldots, p_{N^\circ}^B)$ denote the power allocation vectors by UR and BS for MS in $\mathcal{N}^\circ$, respectively. (Although in OP1 we have used $\mathbf{p}^R = (p_1^R, \ldots, p_N^R)$ and $\mathbf{p}^B = (p_1^B, \ldots, p_N^B)$ to denote the power allocation vectors at UR and BS for the MS in $\mathcal{N}$, resp., for notational convenience, we use $\mathbf{p}^R = (p_1^R, \ldots, p_{N^\circ}^R)$ and $\mathbf{p}^B = (p_1^B, \ldots, p_{N^\circ}^B)$ below to denote the power allocation vectors at UR and BS for the MS in $\mathcal{N}^\circ$, resp.) In (8a), we define $R_i^\circ(p_i^B, p_i^R) = R_i^B(p_i^B, p_i^R) - R_i^R(p_i^B)$. Thus, $R_i^\circ(p_i^B, p_i^R)$ is equivalent to $R_i(p_i^B, p_i^R)$ under the condition that (6) (or (8c)) is satisfied. Constraint (8c) comes from (6) and (5c), in which $p_{i,\text{th}}^R$ is a function of p_i^B.

For OP2, constraint (8c) and MS access control requirements make OP2 still a mixed integer nonlinear programming (MINLP) and thus intractable. However, from OP2, a relaxed joint MS access control and power allocation problem can be attained as below (which is denoted by OP3):

$$\text{OP3:} \max_{\mathcal{N}^\circ\subseteq\mathcal{N}} \left\{ \begin{array}{c} \max\limits_{(\mathbf{p}^R,\mathbf{p}^B)} R^\circ\left(\mathbf{p}^R,\mathbf{p}^B\right) = \sum\limits_{i\in\mathcal{N}^\circ} R_i^\circ\left(p_i^B, p_i^R\right) \\ \text{s.t.} \sum\limits_{i\in\mathcal{N}^\circ} p_i^R \leqslant P^R, \sum\limits_{i\in\mathcal{N}^\circ} p_i^B \leqslant P^B \end{array} \right\}, \tag{9}$$

where the constraint (8c) is removed from OP2.

By observing OP3, one can find that it has three important properties: (i) OP3 can be decomposed into two subproblems: the inner joint power allocation and the outer MS access selection; (ii) the inner subproblem has convex constraint set; (iii) the optimal solution of OP3 and OP2 has the following relationship.

Proposition 2. *Let $\mathcal{S}_{OP3} = \{\mathcal{N}_{OP3}^\star, p_{i,OP3}^{\star R}, p_{i,OP3}^{\star B}\}$ be the optimal solution for OP3; then it is also the optimal solution for OP2. (Since both OP3 and OP2 are combinatorial-based problems, their optimal solution may be not unique. However, Proposition 2 is still valid for the case of more than one optimal solution.)*

Proof. Please see Appendix B. □

Due to the properties of OP3, solving OP3 instead of OP2 would be more sensible. However, there are four challenges should be overcome: (i) OP3 is still a MINLP which is known

to be nondeterministic polynomial-time hard (NP-hard); (ii) although OP3 could be handled by alternatively solving the outer and inner subproblem, the attained solution may be outside the feasible region of OP2 (because we have removed constraint (8c) to get OP3); (iii) the objective function of the inner subproblem is not jointly concave with decision variables; (iv) the outer subproblem of OP3 is combinatorial-based and we cannot construct rules about the optimal $\mathcal{N}^\circ$. In this paper, we provide a suboptimal scheme to explore the solution for OP3. In addition, it is proved that the obtained solution is at least suboptimality for OP2. To be specific, our suboptimal scheme is as follows: (i) we alternatively solve the inner and outer subproblem of OP3; (ii) in handling the inner subproblem, alternative optimization could be used as well. Although the objective function of OP3 is nonconcave, BS power optimization problem has unique solution with previously given UR power allocation; also, the optimal UR power allocation problem is convex for fixed BS power allocation; (iii) the outer subproblem of OP3 can be handled by a heuristic scheme. Based on the above analysis, in the following, our focus is on handling OP3 by AO approach.

3.2. AO Approach and the Algorithm. In this subsection, we first assume that the MS access set has been predetermined and alternatively discuss the relay and jammer power allocation. Then, a suboptimal MS access control scheme is proposed.

3.2.1. Optimal Relay Power Allocation under Fixed Jamming. We first discuss relay power allocation under fixed jamming power $\mathbf{p}^{\star B}$ and predetermined MS set $\mathcal{N}^\circ$. Then, we have the following optimization problem OP4:

$$\text{OP4:} \max_{\mathbf{p}^R} \sum_{i\in\mathcal{N}^\circ} R_i^\circ\left(p_i^{\star B}, p_i^R\right) \tag{10a}$$

$$\text{s.t.} \sum_{i\in\mathcal{N}^\circ} p_i^R \leqslant P^R, \quad \text{fixed } \mathbf{p}^{\star B}, \mathcal{N}^\circ. \tag{10b}$$

Since both $\mathcal{N}^\circ$ and $\mathbf{p}^{\star B}$ are fixed and also constraint (10b) is convex, it follows from [29] that OP4 is a degraded AF-based relay network power allocation problem with parallel orthogonal Gaussian relay channels. Therefore, the optimal solution of OP4 can be characterized by the following theorem.

Theorem 3. *For OP4, its optimal solution is as follows:*

$$p_i^{\star R} = \left[\frac{\sqrt{B_i^2 - 4A_iC_i} - B_i}{2A_i}\right]^+, \quad \forall i \in \mathcal{N}^\circ, \tag{11}$$

where $A_i = (\gamma_i^{BR})^2(1 + p_i^S\gamma_i^{SR})$, $B_i = \gamma_i^{RB}(2 + p_i^S\gamma_i^{SR})(1 + p_i^S\gamma_i^{SR} + p_i^{\star B}\gamma_i^{BR})$, $C_i = (1 + p_i^S\gamma_i^{SR} + p_i^{\star B}\gamma_i^{BR})^2 - p_i^S\gamma_i^{SR}\gamma_i^{RB}(1 + p_i^S\gamma_i^{SR} + p_i^{\star B}\gamma_i^{BR})/\lambda^\star$, *and* $\lambda^\star$ *takes the value such that* $\sum_{i\in\mathcal{N}^\circ} p_i^{\star R}(\lambda^\star, p_i^{\star B}) = P^R$.

Proof. Please see Appendix C. □

At the moment, one may note that, in the above relay power allocation, we have not used the conditions presented in Lemma 1 to restrict the relay power allocation or to exclude MS which cannot promise positive secrecy rate. The explanation is as follows: the purpose of introducing Lemma 1 is to uncover the fact that the joint relay and jammer power allocation is essentially equivalent to the joint MS access control and power allocation. In that case, the access control rather than power allocation is used to exclude MS which obtains negative secrecy rate.

3.2.2. Optimal Jamming under Fixed Relay Power Allocation. Now, our attention turns to the jamming power allocation at BS for given $\mathbf{p}^{\star R}$ and $\mathcal{N}^\circ$. Thus, we have the following optimization problem OP5:

$$\text{OP5:} \max_{\mathbf{p}^B} \sum_{i\in\mathcal{N}^\circ} R_i^\circ\left(p_i^B, p_i^{\star R}\right) \tag{12a}$$

$$\text{s.t.} \sum_{i\in\mathcal{N}^\circ} p_i^B \leqslant P^B, \quad \text{fixed } \mathbf{p}^{\star R}, \mathcal{N}^\circ. \tag{12b}$$

It is obvious that the jamming power constraint (12b) is convex. Therefore, the focus is on the objective function (12a). In order to verify the convexity of the objective function, we take the derivative of $\sum_{i\in\mathcal{N}^\circ} R_i^\circ(p_i^B, p_i^{\star R})$ with respect to p_i^B, $\forall i \in \mathcal{N}^\circ$, and then have

$$\frac{\partial \sum_{i\in\mathcal{N}^\circ} R_i^\circ\left(p_i^B, p_i^{\star R}\right)}{\partial p_i^B} = p_i^S\gamma_i^{SR}\gamma_i^{BR}\frac{D_i\left(p_i^B\right)^2 + E_ip_i^B + F_i}{O_i}, \tag{13}$$

where $D_i = (1 - p_i^{\star R}\gamma_i^{RB})(\gamma_i^{BR})^2$, $E_i = 2\gamma_i^{BR}(1 + p_i^{\star R}\gamma_i^{BR}) > 0$, $F_i = (1 + p_i^S\gamma_i^{SR})[(1 + p_i^{\star R}\gamma_i^{BR})(p_i^S\gamma_i^{SR} + p_i^{\star R}\gamma_i^{RB}) + 1] > 0$, and $O_i = [(1+p_i^S\gamma_i^{SR}+p_i^{\star R}\gamma_i^{RB}+p_i^B\gamma_i^{BR})^2+p_i^Sp_i^{\star R}\gamma_i^{SR}\gamma_i^{RB}(1+p_i^S\gamma_i^{SR}+p_i^{\star R}\gamma_i^{RB} + p_i^B\gamma_i^{BR})] \times [(1 + p_i^B\gamma_i^{BR})^2 + p_i^S\gamma_i^{SR}(1 + p_i^B\gamma_i^{BR})] > 0$. It can be noted that if $p_i^{\star R}\gamma_i^{RB} > 1$ (from Lemma 1, one may notice that it is the necessary condition for MS-i to obtain positive secrecy rate), then $R_i^\circ(p_i^B, p_i^{\star R})$ is a quasi-concave function of p_i^B and takes the maximum at

$$p_{i,1}^{\star B} = \frac{-E_i - \sqrt{E_i^2 - 4D_iF_i}}{2D_i}. \tag{14}$$

Namely, $R_i^\circ(p_i^B, p_i^{\star R})$ is an increasing function of p_i^B for $p_i^B \in [0, p_{i,1}^{\star B})$ and a decreasing function of p_i^B for $p_i^B \in (p_{i,1}^{\star B}, \infty)$, while if $p_i^{\star R}\gamma_i^{RB} \leqslant 1$ (from Theorem 3, one can find that this is possible after the relay power allocation), then we have $\partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B > 0$, $\partial^2 R_i^\circ(p_i^B, p_i^{\star R})/\partial(p_i^B)^2 < 0$, and $\partial^2 R_i^\circ(p_i^B, p_i^{\star R})/\partial(p_i^B)\partial(p_j^B) = 0, i \neq j$. Therefore, the objective function is a monotonically increasing and concave function with respect to p_i^B. With the BS power constraint P^B, it is known that $R_i^\circ(p_i^B, p_i^{\star R})$ will be maximized at $p_i^B = P^B$. Following these analyses, three cases may appear for OP5: (i) for $\forall i \in \mathcal{N}^\circ$ we have $p_i^{\star R}\gamma_i^{RB} > 1$ and then the objective function is quasi-concave and OP5 becomes nonconvex

(but quasi-concave); (ii) for $\forall i \in \mathcal{N}^\circ$ we have $p_i^{\star R}\gamma_i^{RB} \leqslant 1$ and then the objective function is concave and OP5 is a convex programming; (iii) $\exists i \in \mathcal{N}^\circ$ let $p_i^{\star R}\gamma_i^{RB} > 1$, and also $\exists j \in \mathcal{N}^\circ$ but $j \neq i$ let $p_j^{\star R}\gamma_i^{RB} \leqslant 1$; then OP5 is a hybrid quasi-concave and concave problem. Nevertheless, it is still possible to analyze and derive the optimal solution of OP5 by the KKT conditions [30]. In other words, the KKT conditions are the necessary conditions (not sufficient conditions due to may be nonconcavity of $R_i^\circ(p_i^B, p_i^{\star R})$ with respect to p_i^B, $\forall i \in \mathcal{N}^\circ$). Among the KKT conditions, we have

$$\frac{\partial R_i^\circ\left(p_i^B, p_i^{\star R}\right)}{\partial p_i^B} - \xi = 0, \quad \forall i \in \mathcal{N}^\circ, \tag{15}$$

where ξ is the Lagrange multiplier associated with the power constraint (12b) and $\xi \geqslant 0$. Based on (15), we use the following theorem to characterize the properties of the solution for OP5.

Theorem 4. *For OP5 with given $\mathbf{p}^{\star R}$ and $\mathcal{N}^\circ$ and $\forall i \in \mathcal{N}^\circ$, if $p_i^{\star R}\gamma_i^{RB} > 1$, let $p_{i,1}^{\star B}$ be defined as (14); if $p_i^{\star R}\gamma_i^{RB} \leqslant 1$, let $p_{i,1}^{\star B} = P^B$. Also let $p_{i,2}^{\star B}(\xi)$ be the real positive root of (15) for given ξ and define $\mathcal{X}_i(\xi) = \{p_{i,2}^{\star B}(\xi) \mid p_{i,2}^{\star B}(\xi) > 0,\ \partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B|_{p_{i,2}^{\star B}(\xi)} - \xi = 0\}$. The unique solution of OP5 is denoted by $\xi^\star, \{p_i^{\star B} : \forall i \in \mathcal{N}^\circ\}$, then we have the following:*

(1) *If $\sum_{i\in\mathcal{N}^\circ} p_{i,1}^{\star B} \leqslant P^B$, then $p_i^{\star B} = p_{i,1}^{\star B}$ and $\xi^\star = 0$; otherwise, $p_i^{\star B} = \widetilde{p}_i^{\star B}\mathbb{I}\{\mathcal{X}_i(\xi^\star) \neq \Phi\} + 0 \times \mathbb{I}\{\mathcal{X}_i(\xi^\star) = \Phi\}$, where $\widetilde{p}_i^{\star B} = \arg\max_{p_{i,2}^{\star B}(\xi^\star)\in\mathcal{X}_i(\xi^\star)} p_{i,2}^{\star B}(\xi^\star)$ and Φ is null set; $\xi^\star$ takes the value such that $\sum_{i\in\mathcal{N}^\circ} p_i^{\star B}(p_i^{\star R}, \xi^\star) = P^B$.*

(2) *If $\sum_{i\in\mathcal{N}^\circ} p_{i,1}^{\star B} > P^B$, then the term $\sum_{i\in\mathcal{N}^\circ} p_i^{\star B}(p_i^{\star R}, \xi)$ is a decreasing function of ξ.*

Proof. Please see Appendix D. □

By the results in Theorem 4, for jamming power allocation, we first calculate the jamming power $p_{i,1}^{\star B}$, $\forall i \in \mathcal{N}^\circ$, for each accessed MS. If $\sum_{i\in\mathcal{N}^\circ} p_{i,1}^{\star B}(p_i^{\star R}) \leqslant P^B$, that is, the sum of jamming power demand is less than or equal to the available power at BS, then all MS in $\mathcal{N}^\circ$ will be allocated the jamming power $p_i^{\star B} = p_{i,1}^{\star B}$, $\forall i \in \mathcal{N}^\circ$, while if $\sum_{i\in\mathcal{N}^\circ} p_{i,1}^{\star B}(p_i^{\star R}) > P^B$, we should perform a bisection search to obtain the optimal Lagrange multiplier $\xi^\star$ and calculate the corresponding jamming power $p_i^{\star B}$, $\forall i \in \mathcal{N}^\circ$, by (15).

3.2.3. Access Control Scheme and Alternating Optimization Algorithm. Based on the alternative optimization result, a suboptimal access control scheme which can find a feasible suboptimal solution for OP3 (or OP2) is provided herein. The main idea of this scheme is as follows: when the alternative relay and jamming power optimization is convergent, we remove the MS in $\mathcal{N}^\circ$ which has obtained the minimal (general) secrecy rate and then repeat the procedure until the system sum (general) secrecy rate does not increase. Therefore, the proposed suboptimal MS access control scheme and the AO-based power allocation together solve OP3. Hence, we have the following Algorithm 5.

Algorithm 5 (alternative relay power optimization and jamming power optimization (OptROptJam)).

Step 1. Initialize $t = 0$ and let $\mathcal{N}^\circ(t) = \mathcal{N}$, $\mathbf{p}^B(t) = \mathbf{p}_0^B$.

Step 2. Based on Theorems 3 and 4, alternatively optimize the relay and jamming power until convergence and obtain $p_i^B(t)$ and $p_i^R(t)$, respectively; then go to Step 3.

Step 3. Calculate the system sum (general) secrecy rate $\sum_{i\in\mathcal{N}^\circ(t)} R_i^\circ(p_i^B(t), p_i^R(t))$; if $\sum_{i\in\mathcal{N}^\circ(t)} R_i^\circ(p_i^B(t), p_i^R(t)) > \sum_{i\in\mathcal{N}^\circ(t-1)} R_i^\circ(p_i^B(t-1), p_i^R(t-1))$, then let $\mathcal{N}^\circ(t) = \mathcal{N}^\circ(t) \setminus i^\star$ and $t = t + 1$; go to Step 2, where $i^\star = \arg\min_{i\in\mathcal{N}^\circ(t)} R_i^\circ(t)$; otherwise, the algorithm is finished.

In Algorithm 5, t represents the iteration time of the algorithm, and $\mathcal{N}^\circ(t)$ denotes the accessed MS subset at t. In this paper, we set $\mathcal{N}^\circ(0) = \mathcal{N}$; that is, all MS are accessed by the system at the beginning. $\mathbf{p}^B(t) = \mathbf{p}_0^B$ is the start point of the algorithm; that is, we set a jamming power vector and then perform relay power iteration. The rule of start point setting is that it should satisfy the corresponding power constraint. The convergence condition in Step 2 is that the difference of two rounds of alternative relay and jamming power optimization is less than a threshold ε. In Step 3, if there are more than one MS feedback from $\arg\min_{i\in\mathcal{N}^\circ(t)} R_i^\circ(t)$, then one of them is randomly removed.

Suboptimality and Convergence. For Algorithm 5, its optimality is affected by two factors: (i) the optimality of the access control scheme and (ii) the performance of alternative power optimization. For the former, the rules of constructing the optimal MS access set are unclear. Thus, it is difficult to judge the optimality of the proposed suboptimal access control scheme. In this paper, we use simulation result to demonstrate its performance. For the alternating-based power optimization approach, in general, it may fail to locate the stationary points, not to mention the global convergence to the optimal solution. However, we have the following conclusion for Algorithm 5.

Proposition 6. *Algorithm 5 always has the limit point and any limit point generated by Algorithm 5 is at least a suboptimal solution for OP2.*

Proof. Please see Appendix E. □

Complexity. The complexity of Algorithm 5 is mainly affected by the alternative optimization and the access control. The former involves searching two optimal Lagrange multipliers which have the approximate complexity of $\mathcal{O}(N\log_2(\lambda^\star/\varepsilon))$ and $\mathcal{O}(N\log_2(\xi^\star/\varepsilon))$, respectively, where $\lambda^\star$ and $\xi^\star$ are provided in Theorems 3 and 4, respectively, and ε is the tolerable

error presented in Algorithm 5. The approximate complexity of the proposed access control scheme is $\mathcal{O}(N)$, where N is the number of MS in the system.

3.3. Another Suboptimal Algorithm. For two reasons, we propose another suboptimal algorithm for our problem: (i) pursuing lower complexity algorithm and (ii) as the benchmark scheme of Algorithm 5. This suboptimal algorithm is based on two suboptimal power allocation strategies at UR and BS, respectively, that is, equal relay power allocation and optimal proportional jamming power allocation. More precisely, at iteration t, the relay and jamming power allocation rules are as follows, respectively:

$$p_i^R(t) = \frac{P^R}{|\mathcal{N}^\circ(t)|} \tag{16}$$

$$p_i^B(t) = P^B \frac{p_{i,1}^{\star B}\left(p_i^R(t)\right)}{\sum_{i\in\mathcal{N}^\circ(t)} p_{i,1}^{\star B}\left(p_i^R(t)\right)} \mathbb{I}\left\{\sum_{i\in\mathcal{N}^\circ(t)} p_{i,1}^{\star B}\left(p_i^R(t)\right) > P^B\right\} + p_{i,1}^{\star B}\left(p_i^R(t)\right)\mathbb{I}\left\{\sum_{i\in\mathcal{N}^\circ(t)} p_{i,1}^{\star B}\left(p_i^R(t)\right) \leqslant P^B\right\}, \tag{17}$$

where $p_{i,1}^{\star B}(p_i^R(t))$ is defined in Theorem 4. From (16) and (17), one can find that UR equally allocates its power to the accessed MS at t and the BS power allocation is based on proportional rule. In particular, if $\sum_{i\in\mathcal{N}^\circ(t)} p_{i,1}^{\star B}(p_i^R(t)) \leqslant P^B$, then the obtained jamming power for MS-i ($i \in \mathcal{N}^\circ(t)$) is $p_{i,1}^{\star B}$; otherwise, its jamming power is in proportion to $p_{i,1}^{\star B}(p_i^R(t))/\sum_{i\in\mathcal{N}^\circ(t)} p_{i,1}^{\star B}(p_i^R(t))$. The access control scheme for this new suboptimal algorithm is the same as Algorithm 5. To sum up, we have another suboptimal algorithm (Algorithm 7) which is summarized as below.

Algorithm 7 (equal relay power allocation and optimal proportional jamming power allocation (EROptPJam)).

Step 1. Initialize $t = 0$ and $\mathcal{N}^\circ(t) = \mathcal{N}$.

Step 2. Perform relay and jamming power allocation based on (16) and (17), respectively; then we have $p_i^B(t)$ and $p_i^R(t)$ and go to Step 3.

Step 3. Calculate the system sum (general) secrecy rate $\sum_{i\in\mathcal{N}^\circ(t)} R_i^\circ(p_i^B(t), p_i^R(t))$ and if $\sum_{i\in\mathcal{N}^\circ(t)} R_i^\circ(p_i^B(t), p_i^R(t)) > \sum_{i\in\mathcal{N}^\circ(t-1)} R_i^\circ(p_i^B(t-1), p_i^R(t-1))$, then let $\mathcal{N}^\circ(t) = \mathcal{N}^\circ(t) \setminus i^\star$ and $t = t + 1$; go to Step 2, where $i^\star = \arg\min_{i\in\mathcal{N}^\circ(t)} R_i^\circ(t)$; otherwise, the algorithm is finished.

One can note that the complexity of Algorithm 7 is significantly lower. This is because we do not need to perform any power iteration but just calculate the jamming power $p_{i,1}^{\star B}$ by (14) for given relay power allocation. Therefore, it is of no doubt that Algorithm 7 has lower complexity but experiences worse performance than Algorithm 5.

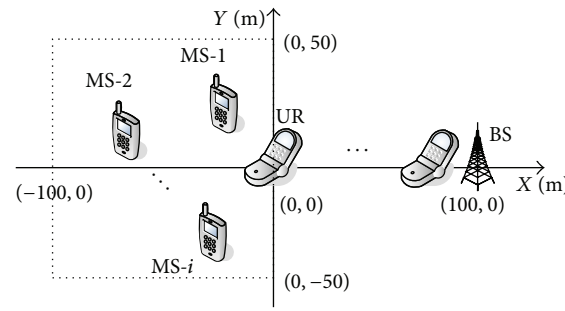

Figure 2: The simulated network configuration.

4. Simulations Results

In this section, we present simulation results to demonstrate the performance of all proposed algorithms. Our simulation scenario is shown in Figure 2, where the BS is located at (100 m, 0 m), and multiple MS are randomly distributed over the dashed rectangle region where the X coordinate is limited from −100 m to 0 m, and the Y coordinate ranges from 50 m to −50 m. The Y coordinate of the UR is fixed at 0 m, while its X coordinate varies from 0 m to 100 m. The simulation scenario and parameters' setting are similar to those in [31, 32]. The channel gains are $\eta(0.0097/d^\tau)^{1/2}$, where d is the distance between any two nodes, for example, BS and UR, or MS and UR, and the path-loss exponent is $\tau = 4$; η represents fading and is taken here as $\eta \sim \mathcal{CN}(0, 1)$. In the simulation, the noise variance is $\sigma^2 = 10^{-8}$ W and $\varepsilon = 10^{-5}$ is the convergence threshold of the proposed alternatively optimization algorithms. In order to better understand the performance of our proposed algorithms, two other benchmark schemes are introduced as follows.

JoPowerOpt (Joint Power Constraint-Based Alternating Optimization) [33]. This algorithm is based on joint BS and UR power constraint. In other words, the system has power constraint $P^R + P^B = P$. The procedure of this algorithm is similar to OptROptJam. It is obvious that, with joint power constraint, system can obtain better performance for its ability to balance power usage between jamming and relay [34].

ExJoPowerOpt (Extension of Joint Power Constraint-Based Alternating Optimization) [33]. This algorithm extends JoPowerOpt to the scenario with individual power constraint. The main idea is that when JoPowerOpt is convergent, we separately check the conditions of BS power constraint P^B and UR power constraint P^R; if both of them are satisfied, then ExJoPowerOpt is over; otherwise, let $P = P - \Delta P$ and repeat JoPowerOpt, where ΔP is a small positive constant.

4.1. General Secrecy Rate. In this section, we plot the MS (e.g., MS-i) general secrecy rate $R_i^\circ(p_i^B, p_i^R)$ as a function of relay power p_i^R and jamming power p_i^B, and the result is shown in Figure 3. BS is located at (100 m, 0 m), and UR is located at (10 m, 0 m), and MS-i is located at (−90 m, 5 m). The

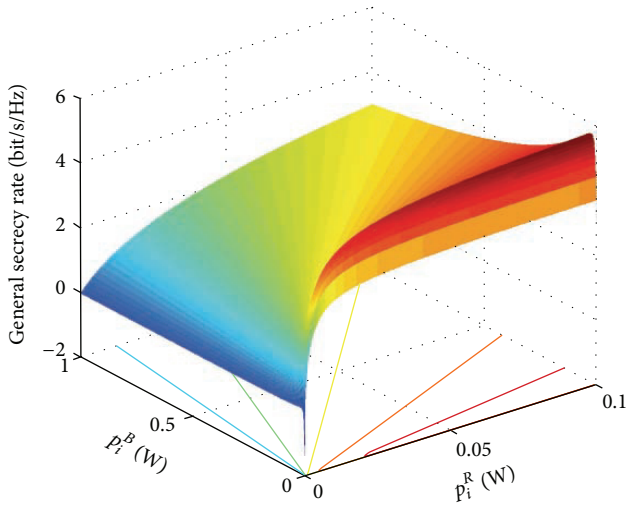

FIGURE 3: General secrecy rate as a function of relay power and jamming power.

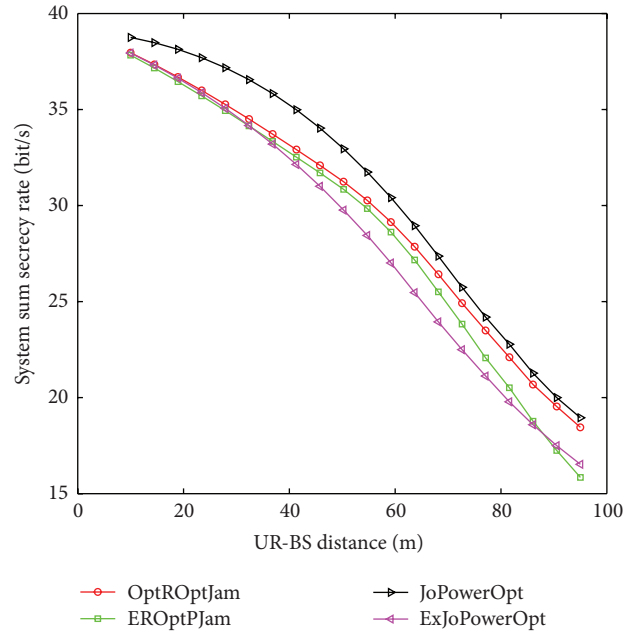

FIGURE 4: System sum secrecy rate versus UR-BS distance.

transmission power of MS-i is $p_i^S = 0.1$ W. From Figure 3, we can observe that, for given jamming power p_i^B, $R_i^\circ(p_i^B, p_i^R)$ is an increasing and concave function of p_i^R, while, for given p_i^R, the convexity of $R_i^\circ(p_i^B, p_i^R)$ with respect to p_i^B depends on the value of p_i^R. If p_i^R is too small, then $R_i^\circ(p_i^B, p_i^R)$ is a concave function of p_i^B. When p_i^R becomes larger, then $R_i^\circ(p_i^B, p_i^R)$ is quasi-concave of p_i^B. This is consistent with our theoretic analysis. In addition, from Figure 3, we can find that if the relay power is too small, that is, the necessary condition (6) in Lemma 1 is not satisfied, then MS-i obtains negative general secrecy rate. (In fact, the negative general secrecy rate has no physical meaning and it is introduced for convenient illustration. Herein, the negative general secrecy rate denotes the zero value of secrecy rate.)

4.2. Performance under Different System Parameters. In this section, we evaluate the performance of the proposed algorithms under different UR positions, number of MS, and the available BS and UR power.

We first evaluate the system performance under different UR positions and the results are presented in Figures 4–6. In the simulation, the UR is initially placed at (80 m, 0 m) and moves to (5 m, 0 m) along a line. Therefore, UR moves away from nearby the BS to far from the BS. The power constraints are $P^B = 2.0$ W at BS and $P^R = 1.5$ W at UR. The number of MS in the system is $N = 15$, and the transmit power of each MS is $p^S = p_i^S = 0.2$ W, $\forall i \in \mathcal{N}$. Figure 4 illustrates the achievable system sum secrecy rate versus the UR-BS distance. It is clear that the attained secrecy rates are decreasing functions of UR-BS distance. This result can be attributed to three factors: (i) the decrease of multiple MS access gain (this can be explained by Lemma 1 and verified in Figure 5; we know that when UR moves away from BS, the number of successively accessed MS decrease); (ii) the decrease of BS jamming efficiency (if UR-BS distance increases, then the channel conditions between UR and BS become worse); (iii) the increase eavesdropping ability of UR (if UR moves away from BS, then the channel conditions between UR and MS become better).

From Figure 4, one can note that the algorithm JoPowerOpt outperforms other three algorithms in the performance of system sum secrecy rate. However, we must highlight that JoPowerOpt is based on the scenario with joint power constraint. Thus, it is impractical for realistic system, and it is introduced just for performance comparison. The algorithm OptROptJam takes the second place, while the performance gap between JoPowerOpt and OptROptJam is small when UR is far away from the BS and it becomes larger if UR is closer to BS. Finally, this performance gap decreases if UR is nearby the BS. The increase of this performance gap is due to the fact that joint power constraint-based algorithm has the ability to balance power usage between relay and jamming. Thus, it can result in higher efficiency in resource usage, while the decrease of performance gap owes to the channel degradation between MS and UR, especially if UR is very close to BS. Moreover, in Figure 4, one can observe that the performance gap between OptROptJam and EROptPJam/ExJoPowerOpt is large when UR is far away from BS and then is reduced when UR moves to BS. In fact, the reasons for performance gap reduction for EROptPJam and ExJoPowerOpt are similar: when UR moves towards BS, all channels between MS and UR are going to be bad and the channel gains between UR and BS are going to be the same. Therefore, with the movement of UR, the optimal proportional jamming is then equal to the optimal jamming, and the performance of optimal relay power allocation is approximated by equal relay power allocation. From this figure, one can note that the performance gain by optimal relay power allocation (or optimal jamming power allocation) is only little when UR is close to BS.

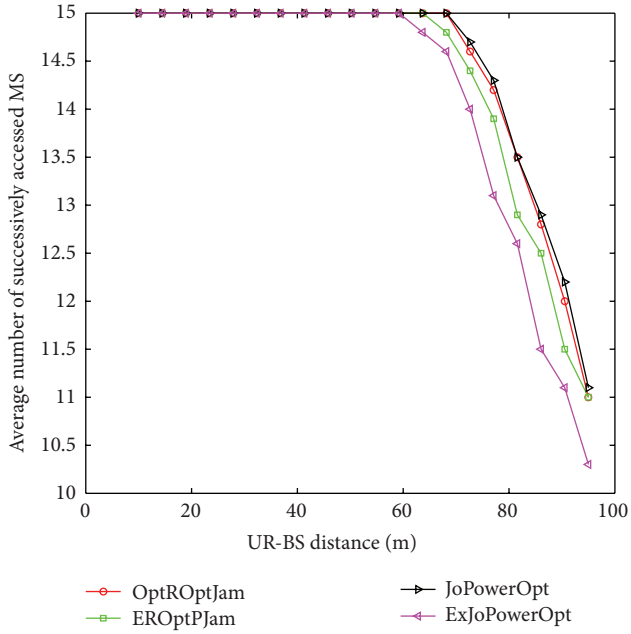

Figure 5: Number of successively accessed MS versus UR-BS distance.

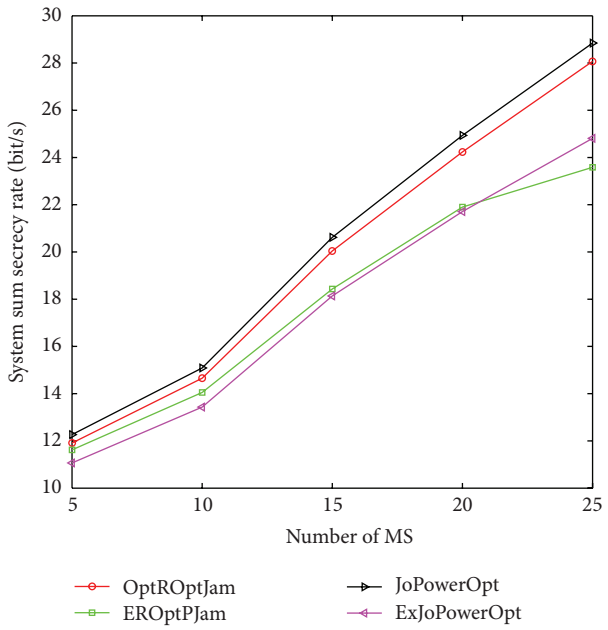

Figure 7: System sum secrecy rate versus number of MS.

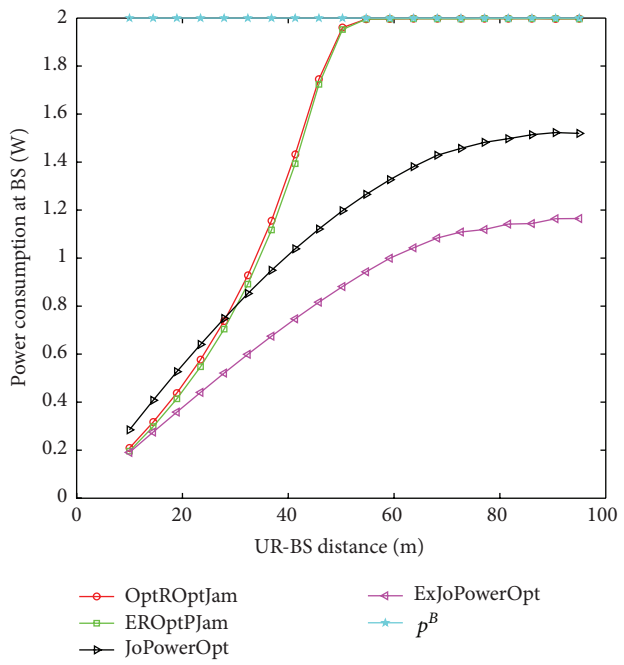

Figure 6: Total power consumption at BS versus UR-BS distance.

Figure 6 shows how BS power consumption is varying with UR-BS distance. One can observe that, for all proposed algorithms, the total jamming power consumption at BS increases if UR moves away from BS. This increase is consistent with intuitive and theoretic analysis; that is, the BS jamming efficiency is high when UR is close to BS (better channel conditions between UR and BS) and it is low if UR is far away from the BS (worse channel conditions between UR and BS). In Figure 6, we see that if UR-BS distance is larger than 50 m, the algorithms OptROptJam and EROptPJam render the BS to use its whole available power to jam, while if UR-BS distance keeps decreasing, then the total jamming power consumption at BS is sharply reduced. By Figure 6, it is not difficult to uncover the reasons why algorithm ExJoPowerOpt attains worse system sum secrecy rate performance. If the UR is far away from the BS, the jamming power consumption of ExJoPowerOpt is about 1.5 W (right now, the jamming power consumption of ExJoPowerOpt is the same as JoPowerOpt). Because we have $P = P^B + P^R = 3.5$ W, about 2 W ($> P^R = 1.5$ W) power is allocated to UR to perform relay. We know that, except the joint power constraint, algorithm ExJoPowerOp should also satisfy the individual power constraint at BS and UR as well. This indicates that we need to perform $P = P - \Delta$ until the power allocated to UR is not larger than 1.5 W. This procedure finally renders the total used jamming power at BS less than 1.2 W. This power is smaller than that used by JoPowerOpt. Hence, it experiences some performance loss.

We then analyze the system performance under different MS numbers, and the results are depicted in Figures 7 and 8. The simulation is done with the parameters $P^B = 2.0$ W, $P^R = 1.5$ W, and UR is located at (10 m, 0 m). From Figure 7, we see that the system sum secrecy rates are increasing if the number of MS becomes larger. The improvement of secrecy rate can be attributed to the multiple MS access gain (i.e., see Figure 8). In other words, the more MS in the system leads to the higher efficiency. If the number of MS is few, we note that the performance gaps among these four algorithms are small. If the number of MS increases, the performance gap between JoPowerOpt and OptROptJam is still not too much but JoPowerOpt always outperforms OptROptJam, while the performance gap between OptROptJam/JoPowerOpt and

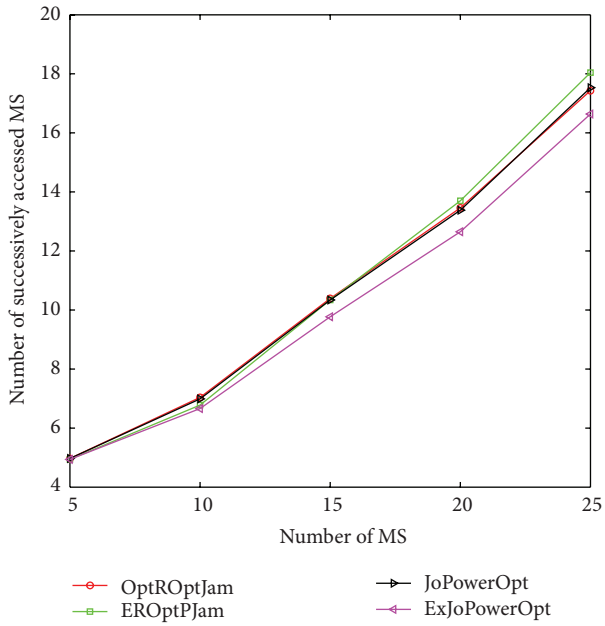

Figure 8: Number of successively accessed MS number versus number of MS.

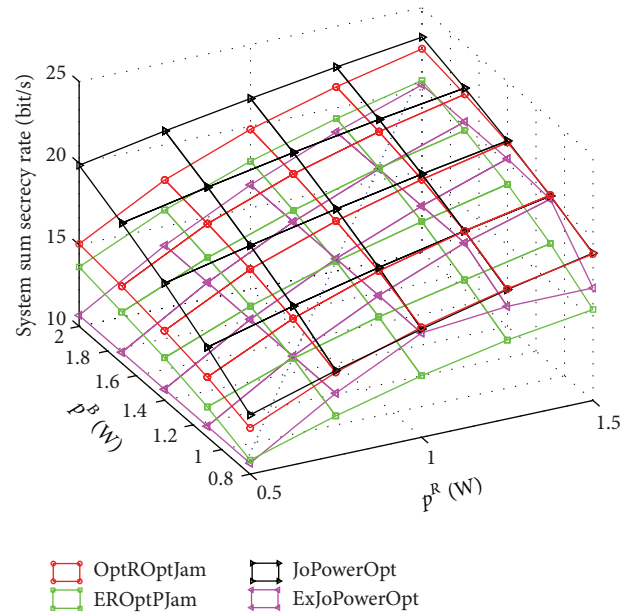

Figure 9: System sum secrecy rate versus UR and BS total power.

EROptPJam/ExJoPowerOpt becomes larger as the number of MS increases. For EROptPJam, the increase of performance gap is due to its equal relay power allocation rule. For ExJoPowerOpt, individual power constraints limit its performance. In addition, depending on the number of MS, EROptPJam obtains better secrecy rate performance when the MS number is small, and ExJoPowerOpt dominates EROptPJam if the number of MS becomes larger. From this simulation result, one can note that if the MS number is large, we should optimize both relay and jammer power to obtain better system performance; if the MS number is only a few, the suboptimal algorithm EROptPJam is enough. From Figure 8, although the number of successively accessed MS increases when the number of MS becomes larger, one can find that the number of MS be rejected by the system increases as well, while ExJoPowerOpt always accesses the least MS among these algorithms.

At last, how system sum secrecy rate is affected by available UR and BS power is analyzed, and the result is shown in Figure 9. The number of MS in the system is $N = 15$, and UR is located at (10 m, 0 m). Available power at BS is varying from 0.8 W to 2.0 W and total power at UR is varying in [0.5 W, 1.5 W]. From Figure 9, we can find that the secrecy rates of OptROptJam, EROptPJam, and JoPowerOpt are all increasing functions of available UR and BS power. In fact, the conclusion that the system sum secrecy rate is an increasing function of relay power is consistent with theoretic analysis (in the proof of Theorem 3). Also, since the UR is located at 90 m far away from the BS, from Figure 6, we know that the increase of jamming power still can improve the system secrecy rate performance. Although the increasing of UR power will significantly improve the obtained secrecy rate for ExJoPowerOpt, if the UR power is small, the secrecy rate for ExJoPowerOpt seems to remain unchanged with the increase of BS power. In other words, right now the system secrecy rate is restricted by the UR power (for its individual power constraint requirements). Additionally, in Figure 9, one can see that JoPowerOpt always attained the highest secrecy rate, and OptROptJam takes the second place. This performance difference has been explained in Figure 4. For EROptPJam and ExJoPowerOpt and the given power matrix plane (formulated by the UR and BS power), if we define a diagonal line (the blue dashed line in Figure 9) from point (0.5 W, 0.8 W) to point (1.5 W, 2.0 W), then ExJoPowerOpt obtained better performance on the right side and EROptPJam achieves higher secrecy rate on the other side. This result can be explained as that, due to the additional individual power constraint, the secrecy rate performance of ExJoPowerOpt is more sensitive to the unbalance of available UR and BS power.

5. Conclusion

In this work, based on the DBJ secure communication protocol [18], joint BS and UR power allocation to maximize system sum secrecy rate is discussed for the untrusted relay cooperation OFDMA network. We develop the joint power optimization problem and our analysis indicates that the joint power allocation is equivalent to joint MS access control and power allocation. By problem relaxation and using the dual alternating optimization approach, two suboptimal MS access control and power allocation algorithms are proposed, that is, the algorithms OptROptJam and EROptPJam. The former is iteration-based algorithm and we have proved its convergence, while the complexity of this algorithm is $\mathcal{O}(N^3 \log_2(\lambda^*/\varepsilon) \log_2(\xi^*/\varepsilon))$. The later can be implemented without any iteration and it has the complexity of $\mathcal{O}(N^2)$. Two

other benchmark schemes are introduced for performance comparison. These two benchmark algorithms both have the approximate complexity of $\mathcal{O}(N^2\log_2(\lambda^*/\varepsilon))$. Our simulation results indicate that (i) the benchmark scheme JoPowerOpt always has the best secrecy rate performance. However, it is based on joint BS and UR power constraint. Thus, it is useless for realistic system; (ii) our proposed algorithm OptROptJam takes the second place in secrecy rate performance. At some UR and BS power region, if the UR is far away from BS, the performance gap between JoPowerOpt and OptROptJam is only little; (iii) the secrecy rate performance of both ExJoPowerOpt and EROptPJam depends on particular system parameters. Additionally, if UR is close to BS or the number of MS is small, the performance gap between JoPowerOpt/OptROptJam and ExJoPowerOpt/EROptPJam is negligible.

Appendices

A. Proof of Lemma 1

First, condition (6) can be directly derived from the positive secrecy rate condition $R_i > 0$. Based on (6), it is easy to obtain the following relationship:

$$P^R \geqslant \sum_{i\in\mathcal{N}} p_i^R > \sum_{i\in\mathcal{N}} p_{i,\text{th}}^R > \sum_{i\in\mathcal{N}} \frac{1}{\gamma_i^{RB}}. \tag{A.1}$$

The last strict inequality comes from the fact that no direct link exists between BS and MS and then zero jamming power always leads to zero secrecy rate. In order to obtain positive secrecy rate we must have $p_i^B > 0, \forall i \in \mathcal{N}$.

B. Proof of Proposition 2

Let $\mathcal{F}_{\text{OP2}}$ and $\mathcal{F}_{\text{OP3}}$ denote the feasible region of OP2 and OP3, respectively. Then we have $\mathcal{F}_{\text{OP2}} = \{(\mathcal{N}^\circ, \mathbf{p}^R, \mathbf{p}^B) \mid \mathcal{N}^\circ \subseteq \mathcal{N}, (\mathbf{p}^R, \mathbf{p}^B) \text{ satisfies (8b) and (8c)}\}$ and $\mathcal{F}_{\text{OP3}} = \{(\mathcal{N}^\circ, \mathbf{p}^R, \mathbf{p}^B) \mid \mathcal{N}^\circ \subseteq \mathcal{N}, (\mathbf{p}^R, \mathbf{p}^B) \text{ satisfies (8b)}\}$. It is obvious that $\mathcal{F}_{\text{OP2}} \subseteq \mathcal{F}_{\text{OP3}}$ and $\mathcal{S}_{\text{OP3}} \in \mathcal{F}_{\text{OP3}}$.

In order to prove this proposition, we should first prove $\mathcal{S}_{\text{OP3}} \in \mathcal{F}_{\text{OP2}}$. In other words, the optimal solution of OP3 is in the feasible region of OP2. Because both the feasible access subsets of OP2 and OP3 are the subset of $\mathcal{N}$, then $\mathcal{N}^\star_{\text{OP3}}$ must be in the feasible access subset of OP2. Moreover, we have $\mathcal{F}_{\text{OP2}} \subseteq \mathcal{F}_{\text{OP3}}$. Hence, in order to have $\mathcal{S}_{\text{OP3}} \in \mathcal{F}_{\text{OP2}}$, it is equivalent to proving that, for $\forall i \in \mathcal{N}^\star_{\text{OP3}}$, we have $0 < p_{i,\text{th}}^{\star R}(p_{i,\text{OP3}}^{\star B}) < p_{i,\text{OP3}}^{\star R}$ and $p_{i,\text{OP3}}^{\star B} > 0$. In the following, we use contradiction approach to finish this proof. At first, we assume that $\exists i \in \mathcal{N}^\star_{\text{OP3}}$ lets one of the following four cases be true.

Case 1. If $p_{i,\text{OP3}}^{\star B} = 0$ and $p_{i,\text{OP3}}^{\star R} = 0$, then we have $[R_i^B(p_{i,\text{OP3}}^{\star B}, p_{i,\text{OP3}}^{\star R}) - R_i^R(p_{i,\text{OP3}}^{\star B})] = \log(1) - \log(1 + p_i^S\gamma_i^{SR}) < 0$.

Case 2. If $p_{i,\text{OP3}}^{\star B} = 0$ and $p_{i,\text{OP3}}^{\star R} > 0$, then we have $[R_i^B(p_{i,\text{OP3}}^{\star B}, p_{i,\text{OP3}}^{\star R}) - R_i^R(p_{i,\text{OP3}}^{\star B})] = \log(1 + p_i^S p_{i,\text{OP3}}^{\star R}\gamma_i^{SR}\gamma_i^{RB}/(1 + p_i^S\gamma_i^{SR} + p_{i,\text{OP3}}^{\star R}\gamma_i^{RB})) - \log(1 + p_i^S\gamma_i^{SR}) < 0$.

Case 3. If $p_{i,\text{OP3}}^{\star B} > 0$ and $p_{i,\text{OP3}}^{\star R} = 0$, then we have $[R_i^B(p_{i,\text{OP3}}^{\star B}, p_{i,\text{OP3}}^{\star R}) - R_i^R(p_{i,\text{OP3}}^{\star B})] = \log(1) - \log(1 + p_i^S\gamma_i^{SR}/(1 + p_{i,\text{OP3}}^{\star B}\gamma_i^{BR})) < 0$.

Case 4. If $p_{i,\text{OP3}}^{\star B} > 0$ and $0 < p_{i,\text{OP3}}^{\star R} \leqslant p_{i,\text{th}}^{\star R}(p_{i,\text{OP3}}^{\star B})$, then based on Lemma 1 we have $[R_i^B(p_{i,\text{OP3}}^{\star B}, p_{i,\text{OP3}}^{\star R}) - R_i^R(p_{i,\text{OP3}}^{\star B})] = \log(1 + p_i^S p_{i,\text{OP3}}^{\star R}\gamma_i^{SR}\gamma_i^{RB}/(1 + p_i^S\gamma_i^{SR} + p_{i,\text{OP3}}^{\star R}\gamma_i^{RB} + p_{i,\text{OP3}}^{\star B}\gamma_i^{BR})) - \log(1 + p_i^S\gamma_i^{SR}/(1 + p_{i,\text{OP3}}^{\star B}\gamma_i^{BR})) \leqslant 0$.

Therefore, for $\forall i \in \mathcal{N}^\star_{\text{OP3}}$, if $(p_{i,\text{OP3}}^{\star B}, p_{i,\text{OP3}}^{\star R})$ does not satisfy the condition that $0 < p_{i,\text{th}}^{\star R}(p_{i,\text{OP3}}^{\star B}) < p_{i,\text{OP3}}^{\star R}$ and $p_{i,\text{OP3}}^{\star B} > 0$, then MS-$i$ obtains negative secrecy rate (without considering the triviality case). By solving the outer subproblem of OP3, we can remove this MS (i.e., MS-i) from the system and render an increase of the system sum secrecy rate even without power reallocation. This violates the assumption that $\mathcal{S}_{\text{OP3}}$ is the optimal solution for OP3. Thus, we must have $\mathcal{S}_{\text{OP3}} \in \mathcal{F}_{\text{OP2}}$.

In fact, under the conclusion that $\mathcal{S}_{\text{OP3}} \in \mathcal{F}_{\text{OP2}}$, OP3 is equivalent to OP2. Then, $\mathcal{S}_{\text{OP3}}$ is the optimal solution for OP3 indicating that it is also the optimal solution for OP2.

C. Proof of Theorem 3

For given $\mathcal{N}^\circ$ and $\mathbf{p}^{\star B}$, it is obvious that constraint (10b) is convex. Thus, our focus is on the objective function. For $\sum_{i\in\mathcal{N}^\circ} R_i^\circ(p_i^{\star B}, p_i^R)$ or $R_i^\circ(p_i^{\star B}, p_i^R)$, we have the following: (i) $\partial\sum_{i\in\mathcal{N}^\circ} R_i^\circ(p_i^{\star B}, p_i^R)/\partial p_i^R = \partial R_i^\circ(p_i^{\star B}, p_i^R)/\partial p_i^R > 0$ and (ii) $\partial^2 R_i^\circ(p_i^{\star B}, p_i^R)/\partial(p_i^R)^2 < 0$ and $\partial^2 R_i^\circ(p_i^{\star B}, p_i^R)/\partial p_i^R\partial p_j^R = 0$, $j \neq i$. Hence, the objective function is an increasing function of p_i^R, $\forall i \in \mathcal{N}^\circ$, and it is also concave with respect to $\mathbf{p}^{\star R}$. Therefore, OP4 is a convex programming. Introducing Lagrangian coefficient λ, corresponding to the constraint in (10b), the Lagrangian associated with OP4 is as follows:

$$L\left(\mathbf{p}^{\star B}, \mathbf{p}^R, \lambda\right) = \sum_{i\in\mathcal{N}^\circ} R_i^\circ\left(p_i^{\star B}, p_i^R\right) + \lambda\left(P^R - \sum_{i\in\mathcal{N}^\circ} p_i^R\right). \tag{C.1}$$

The KKT conditions [30] can be written as

$$\frac{\partial R_i^\circ\left(p_i^{\star B}, p_i^R\right)}{\partial p_i^R} - \lambda = 0, \quad \forall i \in \mathcal{N}^\circ \tag{C.2}$$

$$\lambda\left(P^R - \sum_{i\in\mathcal{N}^\circ} p_i^R\right) = 0 \tag{C.3}$$

$$\lambda \geqslant 0. \tag{C.4}$$

Substituting the expansion of $\partial R_i^\circ(p_i^{\star B}, p_i^R)/\partial p_i^R$ into (C.2) and after some transformations, then the optimal relay power for MS i satisfies the following quadratic equation:

$$A_i\left(p_i^R\right)^2 + B_i\left(p_i^R\right) + C_i = 0. \tag{C.5}$$

Since $A_i > 0$ and $B_i > 0$, $\forall i \in \mathcal{N}^\circ$, then it is not difficult to prove that the nonnegative solution of the above quadratic

equation is (11). As mentioned earlier, the objective function is an increasing function of p_i^R, $\forall i \in \mathcal{N}^\circ$. Thus, the optimal Lagrangian coefficient $\lambda^\star$ satisfies $\lambda^\star > 0$ and (C.3); that is, $\sum_{i\in\mathcal{N}^\circ} p_i^{\star R} = P^R$; otherwise, that is, $\sum_{i\in\mathcal{N}^\circ} p_i^{\star R} < P^R$ and it is possible to increase the objective function value by allocating the remainder relay power $P^R - \sum_{i\in\mathcal{N}^\circ} p_i^{\star R}$ to any MS in $\mathcal{N}^\circ$ without violating the power constraint. As the optimization problem in hand is convex, the Lagrangian coefficient λ can be calculated using Newton method or the interior point method such that the KKT condition in (C.3) is satisfied.

D. Proof of Theorem 4

For the first part of (1), we know that the condition $\sum_{i\in\mathcal{N}^\circ} p_{i,1}^{\star B} \leqslant P^B$ could be true under two cases: (i) for $\forall i \in \mathcal{N}^\circ$ we have $p_i^{\star R}\gamma_i^{RB} > 1$ and $\sum_{i\in\mathcal{N}^\circ} p_{i,1}^{\star B}(p_i^{\star R}) \leqslant P^B$. In other words, for MS-i, $\forall i \in \mathcal{N}^\circ$, the optimal jamming power that can maximize its (general) secrecy rate is $p_{i,1}^{\star B}$; also the sum of MS (in $\mathcal{N}^\circ$) jamming power requirement is less than or equal to the available power at BS. Under this situation, BS has no reasons not to allocate the optimal jamming power $p_{i,1}^{\star B}$ to these MS; otherwise, the system (general) secrecy rate will not be maximized; (ii) $|\mathcal{N}^\circ| = 1$ and $p_i^{\star R}\gamma_i^{RB} \leqslant 1$; that is to say, we have only one MS in the system and the allocated relay power for this MS is too small. Then, our previous analysis indicated that the (general) secrecy rate of this MS is an increasing function of p_i^B and the optimal jamming strategy is $p_i^{\star B} = p_{i,1}^{\star B} = P^B$. In addition, we can note that, no matter which case the system belongs to, we always have $\xi^\star = 0$. Thus, we have the first part of (1).

Now we prove the second part of (1), in which the condition $\sum_{i\in\mathcal{N}^\circ} p_{i,1}^{\star B}(p_i^{\star R}) > P^B$ is true. One can note that this condition could be true under three cases: (i) for $\forall i \in \mathcal{N}^\circ$, we have $p_i^{\star R}\gamma_i^{RB} > 1$ and $\sum_{i\in\mathcal{N}^\circ} p_{i,1}^{\star B}(p_i^{\star R}) > P^B$; (ii) $\exists i \in \mathcal{N}^\circ$ let $p_i^{\star R}\gamma_i^{RB} \leqslant 1$ and $\exists j \in \mathcal{N}^\circ$ let $p_j^{\star R}\gamma_j^{RB} > 1$, $j \neq i$; (iii) for $\forall i \in \mathcal{N}^\circ$, we have $p_i^{\star R}\gamma_i^{RB} \leqslant 1$ and $|\mathcal{N}^\circ| > 1$. As mentioned earlier, no matter which case is true for the system, the optimal solution of OP5 must satisfy (15). According to the value of $p_i^{\star R}\gamma_i^{RB}$, the solution of (15) can be separately discussed as follows:

(S1) If $p_i^{\star R}\gamma_i^{RB} \leqslant 1$ ($\forall i \in \mathcal{N}^\circ$), then from (13) we know that $\partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B|_{p_i^B=0} = \xi_{\text{th}} = \gamma_i^{RB}(\alpha_i - 1)((\beta_i(\alpha_i + \beta_i - 2) + 1)/\alpha_i\beta_i(\alpha_i + \beta_i - 1)) > 0$ and $\partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B|_{p_i^B=\infty} = 0$, where $\alpha_i = 1 + p_i^S\gamma_i^{SR}$, $\beta_i = 1 + p_i^{\star R}\gamma_i^{RB}$. Moreover, it is easy to verify that $\partial^2 R_i^\circ(p_i^B, p_i^{\star R})/\partial(p_i^B)^2 < 0$, which indicates that $\partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B$ is a monotonic decreasing function of p_i^B and takes the maximum ξ_{th} at $p_i^B = 0$. Following these properties of $\partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B$, we know that the solution of (15) under $p_i^{\star R}\gamma_i^{RB} \leqslant 1$ may have two subcases: (S1-1) if $\xi < \xi_{\text{th}}$, then (15) has unique real positive root and if we let it be $p_{i,2}^{\star B}$, then $|\mathcal{X}_i| = 1$ and $p_i^{\star B} = p_{i,2}^{\star B}$; (S1-2) if $\xi \geqslant \xi_{\text{th}}$, then (15) has no real positive root and $\mathcal{X}_i = \Phi$; then $p_i^{\star B} = 0$.

(S2) If $p_i^{\star R}\gamma_i^{RB} > 1$ ($\forall i \in \mathcal{N}^\circ$), then from (13) we know that $\partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B > 0$ in $p_i^B \in [0, p_{i,1}^{\star B})$ and $\partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B < 0$ in $p_i^B \in (p_{i,1}^{\star B}, \infty)$. Therefore, if $p_{i,2}^{\star B}$ is the real positive root of (15) for $\xi > 0$, then we have $0 < p_{i,2}^{\star B} < p_{i,1}^{\star B}$. In order to check the number of real positive root of (15), substituting (13) into (15) and after some simplifications, then we have the following quartic equation:

$$H_{i,4}\left(p_i^B\right)^4 + H_{i,3}\left(p_i^B\right)^3 + \left(H_{i,2}\xi - D_i\right)\left(p_i^B\right)^2 + \left(H_{i,1}\xi - E_i\right)p_i^B + H_{i,0}\xi - F_i = 0. \tag{D.1}$$

Let $\theta_i = p_i^S\gamma_i^{SR}p_i^{\star R}\gamma_i^{RB}$; then $H_{i,4} = (\gamma_i^{RB})^3/(\alpha_i - 1)$, $H_{i,3} = (\gamma_i^{RB})^2[3\alpha_i + 2\beta_i + \theta_i - 1]/(\alpha_i - 1)$, $H_{i,2} = \gamma_i^{RB}[\alpha_i + (\alpha_i + 1)(2(\alpha_i + \beta_i - 1) + \theta_i) + \alpha_i\beta_i(\alpha_i + \beta_i - 1)]/(\alpha_i - 1)$, $H_{i,1} = [\alpha_i(2(\alpha_i + \beta_i - 1) + \theta_i) + \alpha_i\beta_i(\alpha_i + \beta_i - 1)(1 + \alpha_i)]/(\alpha_i - 1)$, $H_{i,4} = [\alpha_i^2\beta_i(\alpha_i + \beta_i - 1)]/\gamma_i^{BR}(\alpha_i - 1)$. Since we have $H_{i,j} > 0$, $\forall j = 0, \ldots, 4$, $E_i > 0$ and $F_i > 0$. Furthermore, the condition $p_i^{\star R}\gamma_i^{RB} > 1$ indicates that $D_i < 0$ and $H_{i,2}\xi - D_i > 0$ (we have used the condition $\xi \geqslant 0$); then using the *Descartes rule of sign*, the number of positive root of (D.1) at most is two. More precisely, if $H_{i,1}\xi - E_i < 0$ and $H_{i,0}\xi - F_i > 0$, then the number of positive roots of (D.1) at most is two; if $H_{i,1}\xi - E_i \geqslant 0$ and $H_{i,0}\xi - F_i < 0$, or $H_{i,1}\xi - E_i < 0$ and $H_{i,0}\xi - F_i = 0$, then the number of positive roots of (D.1) at most is one; if $H_{i,1}\xi - E_i \geqslant 0$ and $H_{i,0}\xi - F_i \geqslant 0$, then the number of positive roots of (D.1) is zero. If we define the set of real positive root of (D.1) be $\mathcal{X}_i(\xi)$ for given ξ (for $i \in \mathcal{N}^\circ$) and thus $\mathcal{X}_i(\xi) = \{p_{i,2}^{\star B}(\xi) \mid p_{i,2}^{\star B}(\xi) > 0,\ \partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B|_{p_{i,2}^{\star B}(\xi)} - \xi = 0\}$. Then, we may have $|\mathcal{X}_i(\xi)| = 2$, or $|\mathcal{X}_i(\xi)| = 1$, or $|\mathcal{X}_i(\xi)| = 0$.

(S2-1) For the case $|\mathcal{X}_i(\xi)| = 2$, let $\mathcal{X}_i(\xi) = \{p_{i,2_1}^{\star B}, p_{i,2_2}^{\star B}\}$. Without loss of generality, we further assume that $0 < p_{i,2_1}^{\star B} < p_{i,2_2}^{\star B} < p_{i,1}^{\star B}$. Since $\partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B > 0$ for $p_i^B \in [0, p_{i,1}^{\star B})$, $R_i^\circ(p_i^B, p_i^{\star R})$ is an increasing function for $p_i^B \in [0, p_{i,1}^{\star B})$. Then, we have $R_i^\circ(p_{i,2_2}^{\star B}, p_i^{\star R}) > R_i^\circ(p_{i,2_1}^{\star B}, p_i^{\star R})$ and then $\widetilde{p}_i^{\star B} = p_{i,2_2}^{\star B}$. Therefore, $\widetilde{p}_i^{\star B} = \arg\max_{p_{i,2}^{\star B}\in\mathcal{X}_i(\xi)} p_{i,2}^{\star B}$ is the optimal solution.

(S2-2) For the case $|\mathcal{X}_i(\xi)| = 1$, we have $\mathcal{X}_i(\xi) = \{p_{i,2}^{\star B}\}$ and then $p_{i,2}^{\star B}$ is the optimal solution.

(S2-3) For the case $|\mathcal{X}_i(\xi)| = 0$, we have $\mathcal{X}_i(\xi) = \Phi$. Therefore, the real positive root set of (D.1) is null and $\widetilde{p}_i^{\star B} = 0$.

From the KKT conditions, we know that, at the optimal solution $\xi^\star, \{p_i^{\star B} : \forall i \in \mathcal{N}^\circ\}$, the BS power constraint must be satisfied. Thus, $\xi^\star$ takes the value to have $\sum_{i\in\mathcal{N}^\circ} p_i^{\star B}(p_i^{\star R}, \xi) = P^B$. To sum up, we have conclusion (1).

For conclusion (2), we only need to prove that $\widetilde{p}_i^{\star B}(\xi)$ is a decreasing function of ξ, $\forall i \in \mathcal{N}^\circ$. Similarly, according to the value of $p_i^{\star R}\gamma_i^{RB}$, it can be separately discussed as follows:

(S1) If $p_i^{\star R}\gamma_i^{RB} \leqslant 1$ ($\forall i \in \mathcal{N}^\circ$), then our previous analysis indicated that $\partial R_i^\circ(p_i^B, p_i^{\star R})/\partial p_i^B$ is a decreasing

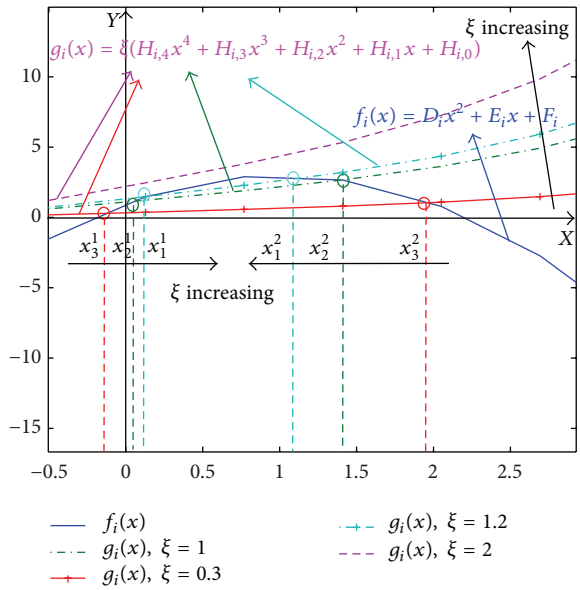

FIGURE 10: The legend of $f_i(p_i^B)$ and $g_i(p_i^B)$, where we use x to denote variable p_i^B.

function in $p_i^B \in (0, \infty)$. Thus, with the increase of ξ, the solution of $\partial R_i^{\circ}(p_i^B, p_i^{\star R})/\partial p_i^B = \xi$ will decrease. Therefore, $p_{i,2}^{\star B}(\xi)$ or $\widetilde{p}_i^{\star B}(\xi)$ is a decreasing function of ξ.

(S2) If $p_i^{\star R}\gamma_i^{RB} > 1$ $(\forall i \in \mathcal{N}^{\circ})$, rigorously proving that $\widetilde{p}_i^{\star B}(\xi)$ is a decreasing function of ξ is difficult and we leverage a legend to finish this proof. First, we define following two functions:

$$f_i\left(p_i^B\right) = D_i\left(p_i^B\right)^2 + E_i p_i^B + F_i$$
$$g_i\left(p_i^B\right) = \xi\left(H_{i,4}\left(p_i^B\right)^4 + H_{i,3}\left(p_i^B\right)^3 + H_{i,2}\left(p_i^B\right)^2 + H_{i,1}p_i^B + H_{i,0}\right). \quad \text{(D.2)}$$

Then, we know that the solution of (D.1) is the X-coordinate of the cross-point of $f_i(p_i^B)$ and $g_i(p_i^B)$. The real positive solution of (D.1) is the X-coordinate of the cross-point in the interval $(0, \infty)$. For $f_i(p_i^B)$, we have $D_i < 0$, $E_i > 0$, and $F_i > 0$. For $g_i(p_i^B)$, we have $H_{i,j} > 0$, $\forall j = 0, \ldots, 4$, and $\xi > 0$ (the condition $\xi = 0$ is omitted for no sense). Then, we plot the instances of these two functions in Figure 10 (where we use x to denote the variable p_i^B), in which we have taken four different values of ξ; that is, $\xi = 0.3$, $\xi = 1$, $\xi = 1.2$, and $\xi = 2$. From these two functions, we know that, with the increase of ξ, for example, $0.3 \to 1 \to 1.2 \to 2$, both $g_i(p_i^B)$ and its first derivative will increase in $(0, \infty)$, while the tendency of $f_i(p_i^B)$ will remain unchanged. Then, from Figure 10, we can note that the X-coordinates of the cross-points of these two functions in interval $(0, \infty)$ under different values of ξ are $x_3^2|_{\xi=0.3} \to (x_2^1, x_2^2)|_{\xi=1} \to (x_1^1, x_1^2)|_{\xi=1.2} \to \Phi|_{\xi=2}$. This is consistent with our previous analysis. That is to say, under the condition $p_i^{\star R}\gamma_i^{RB} > 1$, the number of real positive roots of (D.1) would be two or one or zero. Moreover, from Figure 10, we can find that $x_3^2 > x_2^2 > x_1^2$ and $x_2^1 < x_1^1$. Therefore, with the increase of ξ, $\widetilde{p}_i^{\star B}$ defined by $\widetilde{p}_i^{\star B} = \arg\max_{p_{i,2}^{\star B} \in \mathcal{X}_i} p_{i,2}^{\star B}$ will decrease, and the term $\arg\min_{p_{i,2}^{\star B} \in \mathcal{X}_i} p_{i,2}^{\star B}$ increases. It is clear that the decrease and increase of these two terms will be equal if ξ reaches a certain value (let it be ξ°). If ξ keeps increasing (larger than ξ°), the operator arg will give feedback as zero. Thus we have the conclusion for the case $p_i^{\star R}\gamma_i^{RB} > 1$.

E. Proof of Proposition 6

For OP3 with given $\mathcal{N}^{\circ}$, we can observe that (i) the alternative relay and jamming power optimization belongs to the nonlinear Gauss-Seidel (GS) method where the optimization vector is only partitioned into two component vectors [29, 33–38]; (ii) both the relay and jamming power optimization has the unique solution for giving the other. Therefore, the alternating optimization can surely converge [37]. For the access control procedure, the termination condition is that the system sum (general) secrecy rate is not increasing. Thus, it is obvious that the access control is convergent for no more than N times of MS remove. Also, the convergence of alternative power optimization and access control scheme are not affected by each other. Hence, Algorithm 5 always has a limit point. Moreover, both the alternative power optimization and access control result in nondecreasing objective values. The access control scheme promises that all accessed MS can achieve positive secrecy rate (i.e., the limit point generated by Algorithm 5 is in the feasible region of OP2). Then, the limit point generated by Algorithm 5 is at least a suboptimal solution for OP2.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by Fundamental Research Funds for the Central Universities (CDJXS11162236).

References

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[3] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 29–40, 2013.

[4] J. Ni, Z. Fei, C. Xing, D. Zhao, N. Wang, and J. Kuang, "Secrecy balancing over two-user MISO interference channels

with rician fading," *International Journal of Antennas and Propagation*, vol. 2013, Article ID 546260, 7 pages, 2013.

[5] X. Zhou, L. Song, and Y. Zhang, Eds., *Physical Layer Security in Wireless Communications*, CRC Press, 2013.

[6] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1132–1138, Urbana Champaign, Ill, USA, September 2008.

[7] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 68–73, 2004.

[8] H. Halabian, A. Zainaldin, and I. Lambadaris, "Optimal joint resource allocation and power control in bidirectional relaying networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4520–4535, 2014.

[9] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 359–368, 2012.

[10] M. Lin, J. Ge, Y. Yang, and Y. Ji, "Joint cooperative beamforming and artificial noise design for secrecy sum rate maximization in two-way AF relay networks," *IEEE Communications Letters*, vol. 18, no. 2, pp. 380–383, 2014.

[11] W. Liu, D. Tan, and G. Xu, "Low complexity power allocation and joint relay-jammer selection in cooperative jamming DF relay wireless secure networks," in *Proceedings of the IEEE International Conference on Anti-Counterfeiting, Security and Identification (ASID '13)*, pp. 1–5, Shanghai, China, October 2013.

[12] C. Wang and H.-M. Wang, "Joint relay selection and artificial jamming power allocation for secure DF relay networks," in *Proceedings of the IEEE International Conference on Communication Workshops (ICC '14)*, pp. 819–824, IEEE, Sydney, Australia, June 2014.

[13] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[14] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[15] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[16] 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.

[17] 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, 2010.

[18] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, Article ID 305146, 13 pages, 2009.

[19] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2012.

[20] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2536–2550, 2013.

[21] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[22] J. Huang and A. L. Swindlehurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," in *Proceedings of the 47th Asilomar Conference on Signals, Systems, and Computers (ACSSC '13)*, pp. 1555–1559, Pacific Grove, Calif, USA, November 2013.

[23] 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.

[24] X.-Y. Li, L. Jin, and K.-Z. Huang, "A physical layer security transmission mechanism based on joint channel characteristics in relay system," in *Proceedings of the IEEE 14th International Conference on Communication Technology (ICCT '12)*, pp. 599–603, Chengdu, China, November 2012.

[25] H. Jeon, S. W. McLaughlin, I.-M. Kim, and J. Ha, "Secure communications with untrusted secondary nodes in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 1790–1805, 2014.

[26] 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.

[27] R. Bassily, E. Ekrem, X. He et al., "Cooperative security at the physical layer: a summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, 2013.

[28] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Communications Letters*, vol. 3, no. 3, pp. 289–292, 2014.

[29] W. Zhang, U. Mitra, and M. Chiang, "Optimization of amplify-and-forward multicarrier two-hop transmission," *IEEE Transactions on Communications*, vol. 59, no. 5, pp. 1434–1445, 2011.

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

[31] J. Zou and H. Xu, "Auction-based power allocation for multiuser two-way relaying networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 31–39, 2013.

[32] B. Wang, Z. Han, and K. J. R. Liu, "Distributed relay selection and power control for multiuser cooperative communication networks using stackelberg game," *IEEE Transactions on Mobile Computing*, vol. 8, no. 7, pp. 975–990, 2009.

[33] W.-H. Jiang and W.-J. Feng, "Joint relay and base station power control in the downlink for untrust-relay based cooperation cell network," Reports, 2014.

[34] I. Hammerstrom and A. Wittneben, "Power allocation schemes for amplify-and-forward MIMO-OFDM relay links," *IEEE Transactions on Wireless Communications*, vol. 6, no. 8, pp. 2798–2802, 2007.

[35] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1714–1727, 2013.

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

[37] L. Grippo and M. Sciandrone, "On the convergence of the block nonlinear Gauss-Seidel method under convex constraints," *Operations Research Letters*, vol. 26, no. 3, pp. 127–136, 2000.

[38] Y. Ma, A. Liu, and Y. Hua, "A dual-phase power allocation scheme for multicarrier relay system with direct link," *IEEE Transactions on Signal Processing*, vol. 62, no. 1, pp. 5–16, 2014.