IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Secure Resource Allocation for Cooperative OFDMA System with Untrusted AF Relaying

YIFENG JIN[1], XUNAN LI[2], GUOCHENG LV[1], MEIHUI ZHAO[1] AND YE JIN[1].
[1]Peking University, Beijing, China (e-mail: guocheng.lv@pku.edu.cn)
[2]National Computer Network Emergency Response Technical Team Coordination Center of China, Beijing, China (e-mail: lixunan@cert.org.cn)
Corresponding author: Guocheng Lv (e-mail: guocheng.lv@pku.edu.cn).

ABSTRACT In this paper, we consider a cooperative orthogonal frequency division multiple access (OFDMA) system, where a source communicates with multiple users with the help of an untrusted relay. Since we assume no direct links between source and users because of the shadowing effect, the positive secrecy rate of the system cannot be obtained directly. Addressing this issue, we employ the user-aided cooperative jamming method to improve the secrecy performance. With the aim of maximizing the weighted sum secrecy rate, we formulate a joint resource allocation problem of power allocation, subcarrier assignment and subcarrier pairing. By using the alternative optimization and the Lagrange dual method, we solve this non-convex problem efficiently. Furthermore, to reduce the calculation complexity, we propose two suboptimal algorithms. Numerical results are presented to demonstrate the advantage of the proposed algorithms compared with the benchmarks on the secrecy performance. Moreover, we show that our proposed algorithms are more sensitive to user priority weights than benchmarks.

INDEX TERMS Physical layer security, OFDMA, untrusted relay, cooperative jamming, resource allocation.

I. INTRODUCTION

RAPID development of wireless communication systems has caused a lot of attention to the security issues in it, because the broadcast characteristics of the wireless communication system make the confidential signals vulnerable to be eavesdropped [1]. The traditional encryption method uses cryptographic techniques to enhance the security of communication system. However, with the rapid growth of computing power, this upper layer encryption method becomes crackable and insufficient, which makes the research in this field turn to achieve secure communication in the lower layer of system [2]. Hence, the concept of physical layer security came into being. Its basic principle is to achieve secure communication by using the difference between the legal channel and the eavesdropping channel [3]. Compared with traditional encryption methods, the physical layer security method is regarded as the strictest security method, not requiring any key exchange [1], [2].

Orthogonal frequency division multiple access (OFDMA) is a potential physical layer technology that can be used for next generation access networks, such as WiMAX, LTE and beyond [4], [5]. Therefore, physical layer security research in OFDMA has gained considerable attention in recent years. The research scenarios are mainly divided into three cases: 1) Eavesdropper case: all users are assumed to be trustworthy and there are one or more external eavesdroppers trying to decode the confidential information for users [6]–[13]. 2) Untrusted user case: all users are untrustworthy so each user receives data with considering all other users as the potential eavesdroppers [14]–[16]. 3) Untrusted relay case: when the source communicates with users by relay-assisted, there exists another research scenario of physical layer security, where the relay is assumed to be untrustworthy and act as an eavesdropper [17]–[27].

In the untrusted relay case, the authors in [17] proposed a signal-to-noise ratio (SNR) based power allocation scheme to improve system secrecy rate using a single untrusted relay node with single/multiple antennas, and artificial noise emitted by source was employed to combat untrusted relay. The full-duplex untrusted relay in multi-input multi-output (MIMO) scenario was studied in [18] and the authors used secure beamforming to enhance security performance. The

authors in [19] considered the optimal power allocation for secure transmission under an untrusted relay, where user-aid cooperative jamming was employed to achieve positive secrecy rate. Similarly, the user-aid cooperative jamming was used in [20]–[24]. In [20], the authors proposed an optimal power allocation for the relaying network with an untrusted relay. The power allocation for non-orthogonal multiple access (NOMA) system with an untrusted relay is studied in [21]. In [22], the authors considered the power allocation in untrusted relaying networks when multiple wardens exist. A light-weight jamming-resistant scheme for a two-hop network with untrusted relaying was proposed in [23]. In [24], the authors discussed the security-reliability trade-off in cooperative systems with untrusted relaying. The authors in [25] proposed a subcarrier power distribution and time-domain design for a three-hop OFDM system with untrusted relays. The authors in [26] investigated opportunistic secure multiuser scheduling in energy harvesting untrusted relay networks. In [27], the authors proposed a user-pair selection scheme to improve the multiuser cooperative networks with an untrusted relay. However, joint resource allocation in secure cooperative OFDMA system with untrusted relay poses new challenges which have not yet been investigated.

A. MOTIVATION

The study in [28] raised the feasibility issue of resource allocation problem in a secure communication system with untrusted relay, which indicated the resource allocation can greatly improve the secure performance of the system. Hence, we want to extend the research of resource allocation under untrusted relay case to the OFDMA relaying system. User-aid cooperative jamming method is employed in this system to enhance security performance. Thus, the resource allocation problem includes power allocation (source power, relay power and jamming power), subcarrier assignment and subcarrier pairing, which is very complicate and NP-hard. Most previous related researches only considered power allocation in single carrier case, such as [17]–[22]. Hence, the solution cannot be applied to the OFDMA system with multiple subcarriers. The research in [25] studied subcarrier based power allocation in orthogonal frequency division multiplexing (OFDM) system, however, this study used a special three-hop protocol and did not consider subcarrier pairing. Effectively joint utilizing the resource in secure cooperative OFDMA system with untrusted relay raises challenges, which, to the best of our knowledge, has not yet been studied in the literature.

In this paper, we study the joint power allocation, subcarrier assignment and subcarrier pairing for a secure cooperative OFDMA system with an untrusted amplify-and-forward (AF) relay. The object is to maximize the weighted sum secrecy rate of this system subject to individual power constraints of each transmit node.

B. CONTRIBUTION

The major contribution of this paper can be summarized as follows:

(1) We formulate a new resource allocation problem for secure cooperative OFDMA system with untrusted relay to maximize the weighted sum secrecy rate, where the user-aid cooperative jamming method is skillfully employed to combat the untrusted relay and improve the secrecy performance of the system. Unlike many of the previous works in the literature which only explored partial resources, our formulation includes the power allocation, subcarrier assignment and subcarrier pairing altogether in a unified framework.

(2) We propose an effective joint resource allocation algorithm based on alternative optimization and Lagrange dual method to solve the formulated problem. For the problem with individual power constraints, we show that it can be solved by divided into four subproblems which are proved to be convex. Moreover, the complexity of the solution is polynomial in the number of subcarriers and users.

(3) Based on the experience derived from the joint resource allocation algorithm, we further develop two suboptimal algorithms for the problem. They have low complexity and good performance close to the joint resource allocation algorithm.

The rest of the paper is organized as follows. In Section II we introduce the system model and describe the constraints for resource allocation. In Section III, we formulate the problem and present an associated joint resource allocation algorithm. In Section IV, two low complexity suboptimal resource allocation algorithms are presented. In Section V, we demonstrate simulation results to illustrate the performance of the proposed algorithms. Finally this paper is concluded in Section VI.

II. SYSTEM MODEL

We consider a secure cooperative OFDMA system with an untrusted relay as shown in Fig. 1, where a source communicates with M users via the help of an untrusted relay. The relay operates in a time-division half-duplex mode using the AF protocol. All communication nodes are equipped with single antenna. To simplify the shadowing and blocking effect, we assume that there are no direct links between the source and the users. Source-to-relay and relay-to-users channels are considered to be reciprocal, occupying same bandwidth and experiencing frequency-selective fading. Since the system adopts OFDM modulation, each channel is divided logically into N orthogonal subcarriers with flat fading. A central controller, which can be embedded with the source or the users, is assumed to have perfect knowledge of all the channel state information (CSI). The central controller utilizes this information for subcarrier allocation, subcarrier pairing and power allocation.

Herein we assume the relay is service-level trusted but data-level untrusted, which means it performs signal enhancement and forwarding based on AF protocol but acts as an eavesdropper. In order to impair the untrusted relay's

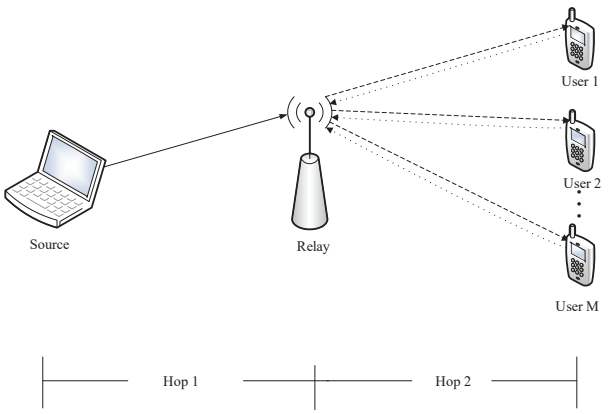

FIGURE 1. Relay assisted cooperative OFDMA system model. Solid lines: signal transmission in the first slot. Dash lines: signal transmission in the second slot. Dotted lines: jamming transmission in the first slot.

eavesdropping ability, user-aid cooperative jamming method is employed in this system. The users act as cooperative jammers to emit artificial jamming signals, which can be fully decoded and completely eliminated by themselves but cannot be decoded by the untrusted relay. Specifically, in order to avoid the interference among the users, each user only emits jamming signals on the specific subcarriers assigned to itself. We allow each user can use multiple subcarriers, while each subcarrier is assigned to at most one user. The subcarriers assigned to one user form the specific user's sub-channel.

The transmission from the source to the users is on a time-frame basis with each frame consisting of multiple OFDM symbols. Each frame transmission is further divided into two time slots. In the first slot, the source transmits the signals on all subcarriers while the relay listens. Meanwhile, the users emit the artificial jamming signals on their respective sub-channels. In the second slot, the source remains silent while the relay amplifies the received signals from the source and the users on a subcarrier basis and forwards them to the users. At the end of each transmission frame, the users combine the received signal from their respective sub-channels and remove the artificial noise before decoding the signals. More specifically, suppose that the i-th subcarrier in the first slot is assigned to the m-th user, the relay receives the confidential signal transmitted from the source and the jamming signal emitted from the m-th user on the i-th subcarrier, amplifies them, and then forwards them to the m-th user on the i'-th subcarrier in the second time slot. Here, the subcarrier index i' may not be as same as i and they form a subcarrier-pair (i, i') and this subcarrier-pair is assigned to the m-th user. It is noteworthy that since each subcarrier has different channel condition, subcarrier pairing can utilize subcarrier diversity to enhance system performance.

Denote the channel coefficients of the source-to-relay channel, the channel from the relay to the m-th user and the channel from the m-th user to the relay on the i-th subcarrier as $h_{i,\mathrm{S}}$, $h_{i,m,\mathrm{R}}$ and $h_{i,m,\mathrm{U}}$, respectively, for $i \in \{1, ..., N\}, m \in \{1, ..., M\}$. Suppose that the subcarrier pair (i, i') is assigned to the m-th user, we further assume that the transmit powers of the source, the relay and the users along this path are $P_{i,\mathrm{S}}$, $P_{i',\mathrm{R}}$ and $P_{i,m,\mathrm{U}}$, respectively. The received signal at the relay on the i-th subcarrier in the first slot can be given by

$$y_{i,1} = \sqrt{P_{i,\mathrm{S}}} h_{i,\mathrm{S}} w_i + \sqrt{P_{i,m,\mathrm{U}}} h_{i,m,\mathrm{U}} z_i + \upsilon_{i,\mathrm{R}}, \quad (1)$$

where w_i and z_i denote symbol of the source's signal and the user's jamming signal on the i-th subcarrier, respectively. $\upsilon_{i,\mathrm{R}}$ denotes the additive white Gaussian noise (AWGN) signal at the relay on the i-th subcarrier and the noise power is σ^2_{R}. The received signal at the m-th user on the i'-th subcarrier in the second slot can be expressed as

$$y_{i',m,2} = \beta_{i,i'} h_{i',m,\mathrm{R}} y_{i,1} + \upsilon_{i',m,\mathrm{U}}, \quad (2)$$

where $\upsilon_{i',m,\mathrm{U}}$ denotes the AWGN signal at the m-th user on the i'-th subcarrier and the noise power is $\sigma^2_{m,\mathrm{U}}$. $\beta_{i,i'}$ denotes the amplification coefficient of the relay on the subcarrier-pair (i, i') and it is default to be

$$\beta_{i,i'} = \sqrt{\frac{P_{i',\mathrm{R}}}{|h_{i,\mathrm{S}}|^2 P_{i,\mathrm{S}} + |h_{i,m,\mathrm{U}}|^2 P_{i,m,\mathrm{U}} + \sigma^2_{\mathrm{R}}}}.$$

Define the effective channel gains as $\alpha_{i,\mathrm{S}} = |h_{i,\mathrm{S}}|^2/\sigma^2_{\mathrm{R}}$, $\alpha_{i',m,\mathrm{R}} = |h_{i',m,\mathrm{R}}|^2/\sigma^2_{m,\mathrm{U}}$ and $\alpha_{i,m,\mathrm{U}} = |h_{i,m,\mathrm{U}}|^2/\sigma^2_{\mathrm{R}}$. Since the z_i is emitted by the m-th user, it can be completely removed by the user. Thus, the achievable transmission rate from the source to the m-th user on the subcarrier-pair (i, i') can be given by

$$\begin{aligned} R^{\mathrm{U}}_{i,i',m} &= \frac{1}{2}\log_2\left(1 + \frac{|h_{i,\mathrm{S}}|^2 P_{i,\mathrm{S}} \beta^2_{i,i'} |h_{i',m,\mathrm{R}}|^2}{\sigma^2_{\mathrm{R}} \beta^2_{i,i'} |h_{i',m,\mathrm{R}}|^2 + \sigma^2_{m,\mathrm{U}}}\right) \\ &= \frac{1}{2}\log_2(1 + \eta_{\mathrm{U}}), \end{aligned} \quad (3)$$

where $\eta_{\mathrm{U}} = \dfrac{\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}}}{1 + \alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}}}$. In (3), the constant coefficient $\dfrac{1}{2}$ accounts for the two time slots in each transmission frame.

The eavesdropping rate at the relay on the i-th subcarrier can be expressed as

$$\begin{aligned} R^{\mathrm{R}}_i &= \frac{1}{2}\log_2\left(1 + \frac{|h_{i,\mathrm{S}}|^2 P_{i,\mathrm{S}}}{\sigma^2_{\mathrm{R}} + |h_{i,m,\mathrm{U}}|^2 P_{i,m,\mathrm{U}}}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}}}{1 + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}}}\right). \end{aligned} \quad (4)$$

Therefore, the secrecy rate from the source to the m-th user on subcarrier-pair (i, i') is formulated as

$$R^{\mathrm{S}}_{i,i',m} = \left(R^{\mathrm{U}}_{i,i',m} - R^{\mathrm{R}}_i\right)^+, \quad (5)$$

where $(x)^+ = max(x, 0)$.

In this paper, we jointly design power allocation, subcarrier assignment and subcarrier pairing to maximize the sum secrecy rate of this system subject to a set of constraints in

the following. Denote $\boldsymbol{t} = \{t_{i,i',m}\} \in \{0,1\}$ as the set of binary variables for subcarrier-pair assignment scheme. In particular, $t_{i,i',m} = 1$ indicates the subcarrier-pair (i,i') is assigned to the m-th user. Since we assume that each subcarrier-pair can be assigned to only one user, $\boldsymbol{t}$ subjects to the following constraint that

$$\sum_{m=1}^{M} t_{i,i',m} = 1, \ \forall i, i'. \tag{6}$$

Denote $\boldsymbol{\phi} = \{\phi_{i,i'}\} \in \{0,1\}$ as the indicator for subcarrier pairing. Specifically, $\phi_{i,i'} = 1$ indicates the i-th subcarrier in the first hop is paired with the i'-th subcarrier in the second hop. Since each subcarrier can be paired with only one subcarrier, $\phi_{i,i'}$ satisfies that

$$\sum_{i=1}^{N} \phi_{i,i'} = 1, \sum_{i'=1}^{N} \phi_{i,i'} = 1, \ \forall i, i'. \tag{7}$$

Denote $\boldsymbol{P} = \{P_{i,\mathrm{S}}, P_{i',\mathrm{R}}, P_{i,m,\mathrm{U}}\}$ as the power allocation scheme set, it satisfies the individual power constraint, which can be expressed as

$$\sum_{i=1}^{N} P_{i,\mathrm{S}} \leq P_{\mathrm{SC}}, \tag{8}$$

$$\sum_{i'=1}^{N} P_{i',\mathrm{R}} \leq P_{\mathrm{RC}}, \tag{9}$$

$$\sum_{i=1}^{N} P_{i,m,\mathrm{U}} \leq P_{m,\mathrm{UC}}, \ \forall m. \tag{10}$$

As such, the total variables to be optimized in our problem are: $\boldsymbol{t} = \{t_{i,i',m}\}$ satisfying (6), $\boldsymbol{\phi} = \{\phi_{i,i'}\}$ satisfying (7), and $\boldsymbol{P} = \{P_{i,\mathrm{S}}, P_{i',\mathrm{R}}, P_{i,m,\mathrm{U}}\}$ satisfying (8), (9) and (10).

III. RESOURCE ALLOCATION FOR SUM SECRECY RATE MAXIMIZATION

In this section, we discuss the joint resource optimization problem for weighted sum secure rate maximization. The problem can be formulated as:

$$\begin{aligned} &\max_{\{\boldsymbol{P},\boldsymbol{\phi},\boldsymbol{t}\}} \sum_{i=1}^{N}\sum_{i'=1}^{N}\sum_{m=1}^{M} l_m \phi_{i,i'} t_{i,i',m} R^{\mathrm{S}}_{i,i',m} \\ &\text{s.}t.\ (6), (7), (8), (9) \ and \ (10), \end{aligned} \tag{11}$$

where l_m is the priority weight factor allocated by the higher layers to the m-th user.

Proposition 1: The secrecy rate $R^{\mathrm{S}}_{i,i',m}$ over a subcarrier-pair is a concave function of the source power $P_{i,\mathrm{S}}$, the relay power $P_{i',\mathrm{R}}$ and the jamming power $P_{i,m,\mathrm{U}}$, respectively. More specifically, the secrecy rate over a subcarrier-pair is monotonically increasing with the relay power and gets maximum when the source power equals $P^{\diamond}_{i,\mathrm{S}}$ and the jamming power equals $P^{\diamond}_{i,m,\mathrm{U}}$, respectively. $P^{\diamond}_{i,\mathrm{S}}$ and $P^{\diamond}_{i,m,\mathrm{U}}$ can be given as

$$\begin{aligned} P^{\diamond}_{i,\mathrm{S}} = &(\alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} \sqrt{(\alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1)} \\ &\cdot \sqrt{\alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}}} - \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} - \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} - 1) \\ &\cdot \frac{1}{\alpha_{i,\mathrm{S}}(\alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + 1)}, \end{aligned} \tag{12}$$

$$\begin{aligned} P^{\diamond}_{i,m,\mathrm{U}} = &(\alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} \sqrt{(\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + 1)} \\ &\cdot \sqrt{(\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}})} + \alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + 1) \\ &\cdot \frac{1}{\alpha_{i,m,\mathrm{U}}(\alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} - 1)}. \end{aligned} \tag{13}$$

Proof: See Appendix A.

Since the optimization problem in (11) is a non-convex combinatorial problem belonging to the class of NP-hard, there is no polynomial time optimal solution possible [29], [30]. It can be observed that the secrecy rate per subcarrier-pair is a concave function of the source power $P_{i,\mathrm{S}}$ for fixed relay power and jamming power $\{P_{i',\mathrm{R}}, P_{i,m,\mathrm{U}}\}$, a concave function of the relay power $P_{i',\mathrm{R}}$ for fixed source power and jamming power $\{P_{i,\mathrm{S}}, P_{i,m,\mathrm{U}}\}$, and also a concave function of the jamming power for fixed source power and relay power $\{P_{i,\mathrm{S}}, P_{i',\mathrm{R}}\}$, as shown in Proposition 1. This motivates us to use the method of alternating optimization (AO) [31] for joint power optimizations and the problem in (11) can be solved by dividing it into one master problem (outer loop) and four subproblems (inner loop) [14]. The first subproblem is the joint allocation of the subcarrier assignment and subcarrier pairing for fixed power allocation. The second subproblem is the source power allocation for fixed other variables. The third subproblem is the relay power allocation for fixed other variables. The fourth subproblem is the jamming power allocation for fixed other variables. In the following subsections, we discuss the four subproblems and solve them in polynomial time complexity.

A. SUBCARRIER ASSIGNMENT AND SUBCARRIER PAIRING FOR FIXED POWER ALLOCATION

The subproblem-1 can be stated as

$$\begin{aligned} &\max_{\{\boldsymbol{\phi},\boldsymbol{t}\}} \sum_{i=1}^{N}\sum_{i'=1}^{N}\sum_{m=1}^{M} l_m \phi_{i,i'} t_{i,i',m} R^{\mathrm{S}}_{i,i',m} \\ &\text{s.}t.\ (6) \ and \ (7), \end{aligned} \tag{14}$$

which is an integer programming problem.

1) Optimal Subcarrier Assignment for Given Subcarrier Pairing

Define D as the set of all possible subcarrier pairings $\boldsymbol{\phi}$ and subcarrier assignment $\boldsymbol{t}$ satisfying (7) and (6), respectively. We first determine the optimal user for a given subcarrier-pair. Suppose (i,i') is one of the valid subcarrier-pair in ϕ, i.e. $\phi_{i,i'} = 1$. It can be easily seen that the optimal user for the subcarrier-pair (i,i') should be the one maximizing the

value of $l_m R^{\mathrm{S}}_{i,i',m}$ in (14), which can be given by

$$t^*_{i,i',m} = \begin{cases} 1, \ m = m(i,i') = \arg\max\limits_{m} l_m R^{\mathrm{S}}_{i,i',m} \\ 0, \ \text{otherwise.} \end{cases} \tag{15}$$

2) Optimal Subcarrier Pairing

Substituting (15) to (14), the optimal problem can be written as

$$\max_{\{\boldsymbol{\phi}\}\in D} \sum_{i=1}^{N}\sum_{i'=1}^{N} \phi_{i,i'} l_m R^{\mathrm{S}}_{i,i'}, \tag{16}$$

where $R^{\mathrm{S}}_{i,i'} = R^{\mathrm{S}}_{i,i',m(i,i')}$. Define an $N \times N$ matrix $\boldsymbol{R} = [R^{\mathrm{S}}_{i,i'}]$, we should pick exactly one element in each row and each column of matrix $\boldsymbol{R}$ to maximize the objective in (16). The subscript of each selected element in $\boldsymbol{R}$ is exactly corresponding to a certain optimal subcarrier-pair (i, i'). This selection is essentially a standard linear assignment problem that can be efficiently solved by the Hungarian method, whose computational complexity is $O(N^3)$. For more details on the Hungarian method, see Appendix B [32].

Let $\pi(i)$ denote the subcarrier index in the second hop paired optimally with subcarrier i in the first hop, for $i \in \{1, ..., N\}$. Then, the optimal subcarrier pairing variable can be expressed as

$$\phi^*_{i,i'} = \begin{cases} 1, \ i' = \pi(i) \\ 0, \ \text{otherwise.} \end{cases} \tag{17}$$

After the above steps, we obtain the optimal solution $\{\boldsymbol{\phi}^*, \boldsymbol{t}^*\}$ for the subproblem-1 in (14). The computational complexity of solving the subproblem-1 is $O(N^3)$.

B. SOURCE POWER ALLOCATION

The subproblem-2 can be stated as

$$\begin{aligned} &\max_{\{P_{i,\mathrm{S}}\}} \sum_{i=1}^{N}\sum_{i'=1}^{N}\sum_{m=1}^{M} l_m R^{\mathrm{S}}_{i,i',m} \\ &\text{s.}t. \ (8), \end{aligned} \tag{18}$$

which is a convex problem because $R^{\mathrm{S}}_{i,i',m}$ is a concave function of $P_{i,\mathrm{S}}$ (cf. Proposition 1). We can easily solve the optimization problem by using Lagrange dual method. The Lagrange dual function of the problem (18) is

$$g(\mu_{\mathrm{s}}) = \max_{P_{i,\mathrm{S}}} L_{\mathrm{s}}(P_{i,\mathrm{S}}, \mu_{\mathrm{s}}). \tag{19}$$

The Lagrangian is

$$\begin{aligned} &L_{\mathrm{s}}(P_{i,\mathrm{S}}, \mu_{\mathrm{s}}) \\ &= \sum_{i=1}^{N}\sum_{i'=1}^{N}\sum_{m=1}^{M} \frac{1}{2} l_m \log_2\left(\frac{a_{\mathrm{s}} P_{i,\mathrm{S}} + b_{\mathrm{s}}}{P^2_{i,\mathrm{S}} + c_{\mathrm{s}} P_{i,\mathrm{S}} + b_{\mathrm{s}}}\right) \\ &+ \mu_{\mathrm{s}}\left(P_{SC} - \sum_{i=1}^{N} P_{i,\mathrm{S}}\right), \end{aligned} \tag{20}$$

where $\mu_{\mathrm{s}} \geq 0$ being the dual variable and

$$\begin{aligned} a_{\mathrm{s}} &= (\alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + 1)(\alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1)/\alpha_{i,\mathrm{S}}, \\ b_{\mathrm{s}} &= (\alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1) \\ &\quad \cdot (\alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1)/\alpha^2_{i,\mathrm{S}}, \\ c_{\mathrm{s}} &= (\alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + 2\alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 2)/\alpha_{i,\mathrm{S}}. \end{aligned}$$

Therefore, the dual optimization problem is expressed by

$$\begin{aligned} &\min_{\mu_{\mathrm{s}}} g(\mu_{\mathrm{s}}) \\ &s.t. \ \mu_{\mathrm{s}} \geq 0. \end{aligned} \tag{21}$$

Since the dual function is inherently convex [33], the dual optimization problem in (21) can be solved by subgradient-based methods with guaranteed convergence. Let $P^*_{i,\mathrm{S}}$ denotes the optimal source power allocation in (19) at a given dual point μ_{s}, then a subgradient of $g(\mu_{\mathrm{s}})$ can be derived as

$$\triangle \mu_{\mathrm{s}} = P_{SC} - \sum_{i=1}^{N} P^*_{i,\mathrm{S}}(\mu_{\mathrm{s}}).$$

The dual variable can be updated as $\mu^{(x+1)}_{\mathrm{s}} = \mu^{(x)}_{\mathrm{s}} + \epsilon^{(x)} \triangle \mu_{\mathrm{s}}$, where the update size $\epsilon^{(x)}$ following the diminishing policy in [34] and x indicates the number of iterations. The subgradient method guarantees that the dual point can converge to the optimal dual variable μ^*_{s} after sufficient iterations, and the corresponding computational complexity is polynomial in the number of dual variable [35].

Applying Karush-Kuhn-Tucher (KKT) conditions [33], we can obtain the optimal source power allocation. After setting the derivative of L_{s} in (20) equal to zero, we obtain a third-order nonlinear equation in $P_{i,\mathrm{S}}$ having the following form

$$A_{\mathrm{s}} P^3_{i,\mathrm{S}} + B_{\mathrm{s}} P^2_{i,\mathrm{S}} + C_{\mathrm{s}} P_{i,\mathrm{S}} + D_{\mathrm{s}} = 0, \tag{22}$$

where

$$\begin{aligned} A_{\mathrm{s}} &= a_{\mathrm{s}}, \\ B_{\mathrm{s}} &= b_{\mathrm{s}} + a_{\mathrm{s}} c_{\mathrm{s}} + \frac{l_m a_{\mathrm{s}}}{2 \ln 2 \mu_{\mathrm{s}}}, \\ C_{\mathrm{s}} &= b_{\mathrm{s}}(a_{\mathrm{s}} + c_{\mathrm{s}}) + \frac{l_m b_{\mathrm{s}}}{2 \ln 2 \mu_{\mathrm{s}}}, \\ D_{\mathrm{s}} &= b^2_{\mathrm{s}} + \frac{l_m b_{\mathrm{s}}(c_{\mathrm{s}} - a_{\mathrm{s}})}{2 \ln 2 \mu_{\mathrm{s}}}. \end{aligned}$$

Since the secrecy rate is a concave function of $P_{i,\mathrm{S}}$ (cf. Proposition 1), depending on μ_{s}, there exists a single positive root $P^{\mathrm{r}}_{i,\mathrm{S}}$ of (21), which satisfies the source power constraint in (8). Since the secrecy rate over a subcarrier-pair reaches maximum when the $P_{i,\mathrm{S}}$ equals to $P^{\diamond}_{i,\mathrm{S}}$ (cf. Proposition 1) without considering the source power constraint, the optimal source power allocation $P^*_{i,\mathrm{S}}$ can be written as

$$P^*_{i,\mathrm{S}} = \begin{cases} P^{\mathrm{r}}_{i,\mathrm{S}}, P^{\mathrm{r}}_{i,\mathrm{S}} \leq P^{\diamond}_{i,\mathrm{S}} \\ P^{\diamond}_{i,\mathrm{S}}, \ \text{otherwise.} \end{cases} \tag{23}$$

Since the dual variable μ_s contains only one optimization variable, the computation complexity of the algorithm is

fixed and is not affected by N and M. Therefore, the computational complexity of solving the subproblem-2 is $O(1)$.

C. RELAY POWER ALLOCATION

The subproblem-3 can be stated as

$$\max_{\{P_{i',\mathrm{R}}\}} \sum_{i=1}^{N}\sum_{i'=1}^{N}\sum_{m=1}^{M} l_m R^{\mathrm{S}}_{i,i',m} \quad \text{s.t. } (9), \tag{24}$$

which is a convex problem because $R^{\mathrm{S}}_{i,i',m}$ is a concave function of $P_{i',\mathrm{R}}$ (cf. Proposition 1). We can solve the optimization problem by using Lagrange dual method. The Lagrange dual function of the problem (24) is

$$g(\mu_{\mathrm{r}}) = \max_{P_{i',\mathrm{R}}} L_{\mathrm{r}}(P_{i',\mathrm{R}}, \mu_{\mathrm{r}}). \tag{25}$$

The Lagrangian is

$$\begin{aligned} &L_{\mathrm{r}}(P_{i',\mathrm{R}}, \mu_{\mathrm{r}}) \\ &= \sum_{i=1}^{N}\sum_{i'=1}^{N}\sum_{m=1}^{M} \frac{1}{2} l_m \log_2\left(\frac{a_{\mathrm{r}} P_{i',\mathrm{R}} + b_{\mathrm{r}}}{c_{\mathrm{r}} P_{i',\mathrm{R}} + d_{\mathrm{r}}}\right) \\ &+ \mu_{\mathrm{r}}\left(P_{\mathrm{R}C} - \sum_{i=1}^{N} P_{i',\mathrm{R}}\right), \end{aligned} \tag{26}$$

where $\mu_{\mathrm{r}} \geq 0$ being the dual variable and

$$\begin{aligned} a_{\mathrm{r}} &= \alpha_{i',m,\mathrm{R}}(\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + 1)(\alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1), \\ b_{\mathrm{r}} &= (\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1)(\alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1), \\ c_{\mathrm{r}} &= \alpha_{i',m,\mathrm{R}}(\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1), \\ d_{\mathrm{r}} &= (\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1)^2. \end{aligned}$$

Similarly, applying KKT conditions, we can obtain the optimal relay power allocation. After setting the derivative of L_{r} in (26) equal to zero, we obtain a second-order nonlinear equation in $P_{i',\mathrm{R}}$ having the following form

$$A_{\mathrm{r}} P^2_{i',\mathrm{R}} + B_{\mathrm{r}} P_{i',\mathrm{R}} + C_{\mathrm{r}} = 0, \tag{27}$$

where

$$\begin{aligned} A_{\mathrm{r}} &= \alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + 1, \\ B_{\mathrm{r}} &= (\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + 2)(\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1)/\alpha_{i',m,\mathrm{R}}, \\ C_{\mathrm{r}} &= (\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1)^2/\alpha^2_{i',m,\mathrm{R}} \\ &\quad - l_m \alpha_{i,\mathrm{S}} P_{i,\mathrm{S}}(\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i,m,\mathrm{U}} P_{i,m,\mathrm{U}} + 1)/(2\ln 2 \mu_{\mathrm{r}} \alpha^2_{i',m,\mathrm{R}}). \end{aligned}$$

Since the secrecy rate is a concave function of $P_{i',\mathrm{R}}$ (cf. Proposition 1), depending on μ_{r}, there exists a single positive root $P^{\mathrm{r}}_{i',\mathrm{R}}$ of (27), which satisfies the relay power constraint in (9). μ_{r} is updated using the subgradient method. Since the secrecy rate over a subcarrier-pair is monotonically increasing with $P_{i',\mathrm{R}}$ (cf. Proposition 1), the optimal relay power allocation $P^{*}_{i',\mathrm{R}} = P^{\mathrm{r}}_{i',\mathrm{R}}$. Similar to subproblem-2, the computational complexity of solving the subproblem-3 is $O(1)$.

D. JAMMING POWER ALLOCATION

The subproblem-4 can be stated as

$$\max_{\{P_{i,m,\mathrm{U}}\}} \sum_{i=1}^{N}\sum_{i'=1}^{N}\sum_{m=1}^{M} l_m R^{\mathrm{S}}_{i,i',m} \quad \text{s.t. } (10), \tag{28}$$

which is also a convex problem because $R^{\mathrm{S}}_{i,i',m}$ is a concave function of $P_{i,m,\mathrm{U}}$(cf. Proposition 1). Similarly, We can solve the optimization problem by using Lagrange dual method. The Lagrange dual function of the problem (28) is

$$g(\mu_{\mathrm{u}}) = \max_{P_{i,m,\mathrm{U}}} L_{\mathrm{u}}(P_{i,m,\mathrm{U}}, \mu_{\mathrm{u}}). \tag{29}$$

The Lagrangian is

$$\begin{aligned} &L_{\mathrm{u}}(P_{i,m,\mathrm{U}}, \mu_{\mathrm{u}}) \\ &= \sum_{i=1}^{N}\sum_{i'=1}^{N}\sum_{m=1}^{M} \frac{1}{2} l_m \log_2\left(\frac{P^2_{i,m,\mathrm{U}} + a_{\mathrm{u}} P_{i,m,\mathrm{U}} + b_{\mathrm{u}}}{P^2_{i,m,\mathrm{U}} + c_{\mathrm{u}} P_{i,m,\mathrm{U}} + d_{\mathrm{u}}}\right) \\ &+ \sum_{m=1}^{M} \mu_{m,\mathrm{U}}\left(P_{m,\mathrm{U}C} - \sum_{i=1}^{N} P_{i,m,\mathrm{U}}\right), \end{aligned} \tag{30}$$

where $\mu_{\mathrm{u}} = (\mu_{1,\mathrm{U}}, ..., \mu_{M,\mathrm{U}}) \succeq 0$ being the vector of the dual variables and

$$\begin{aligned} a_{\mathrm{u}} =& (\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} \\ &+ \alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + 2)/\alpha_{i,m,\mathrm{U}}, \\ b_{\mathrm{u}} =& (\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} \\ &+ \alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + 1)/\alpha^2_{i,m,\mathrm{U}}, \\ c_{\mathrm{u}} =& (2\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + 2)/\alpha_{i,m,\mathrm{U}}, \\ d_{\mathrm{u}} =& (\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + \alpha_{i',m,\mathrm{R}} P_{i',\mathrm{R}} + 1)(\alpha_{i,\mathrm{S}} P_{i,\mathrm{S}} + 1)/\alpha^2_{i,m,\mathrm{U}}. \end{aligned}$$

Similarly, applying KKT conditions, we can obtain the optimal jamming power allocation. After setting the derivative of L_{u} in (30) equal to zero, we obtain a fourth-order nonlinear equation in $P_{i,m,\mathrm{U}}$ having the following form

$$\begin{aligned} &P^4_{i,m,\mathrm{U}} + B_{\mathrm{u}} P^3_{i,m,\mathrm{U}} \\ &= -(C_{\mathrm{u}} P^2_{i,m,\mathrm{U}} + D_{\mathrm{u}} P_{i,m,\mathrm{U}} + E_{\mathrm{u}}), \end{aligned} \tag{31}$$

where

$$\begin{aligned} B_{\mathrm{u}} &= a_{\mathrm{u}} + c_{\mathrm{u}}, \\ C_{\mathrm{u}} &= b_{\mathrm{u}} + d_{\mathrm{u}} + a_{\mathrm{u}} c_{\mathrm{u}} + \frac{l_m}{2\ln 2 \mu_{m,\mathrm{U}}}(a_{\mathrm{u}} - c_{\mathrm{u}}), \\ D_{\mathrm{u}} &= a_{\mathrm{u}} d_{\mathrm{u}} + b_{\mathrm{u}} c_{\mathrm{u}} + \frac{l_m}{2\ln 2 \mu_{m,\mathrm{U}}}(b_{\mathrm{u}} - d_{\mathrm{u}}), \\ E_{\mathrm{u}} &= b_{\mathrm{u}} d_{\mathrm{u}} + \frac{l_m}{2\ln 2 \mu_{m,\mathrm{U}}}(b_{\mathrm{u}} c_{\mathrm{u}} - a_{\mathrm{u}} d_{\mathrm{u}}). \end{aligned}$$

Since the secrecy rate is a concave function of $P_{i,m,\mathrm{U}}$ (cf. Proposition 1), depending on μ_{u}, there exists a single positive root $P^{\mathrm{r}}_{i,m,\mathrm{U}}$ of (31), which satisfies the user power constraint in (10). μ_{u} is updated using the subgradient method. Since the secrecy rate over a subcarrier-pair reaches maximum when the $P_{i,m,\mathrm{U}}$ equals to $P^{\diamond}_{i,m,\mathrm{U}}$ (cf. Proposition 1) without

Algorithm 1 AO based Joint Resource Allocation

Input: $N, M, \sigma_{\mathrm{R}}^2, P_{\mathrm{SC}}, P_{\mathrm{RC}}$
$\{h_{i,\mathrm{S}}\} = \{h_{1,\mathrm{S}}, h_{2,\mathrm{S}}, \ldots, h_{N,\mathrm{S}}\}$
$\{h_{i',m,\mathrm{R}}\} = \{h_{1,1,\mathrm{R}}, h_{1,2,\mathrm{R}}, \ldots, h_{N,M,\mathrm{R}}\}$
$\{h_{i,m,\mathrm{U}}\} = \{h_{1,1,\mathrm{U}}, h_{1,2,\mathrm{U}}, \ldots, h_{N,M,\mathrm{U}}\}$
$\{l_m\} = \{l_1, l_2, \ldots, l_M\}$
$\{\sigma_{m,\mathrm{U}}^2\} = \{\sigma_{1,\mathrm{U}}^2\ \sigma_{2,\mathrm{U}}^2\ \ldots, \sigma_{M,\mathrm{U}}^2\}$
$\{P_{m,\mathrm{UC}}\} = \{P_{1,\mathrm{UC}}, P_{2,\mathrm{UC}}, \ldots, P_{M,\mathrm{UC}}\}$
Output: Optimum set $\{\boldsymbol{P^*}, \boldsymbol{\phi^*}, \boldsymbol{t^*}\}$
The outer loop:
Initialize $P_{i,\mathrm{S}} = P_{\mathrm{SC}}/N, P_{i',\mathrm{R}} = P_{\mathrm{RC}}/N, P_{i,m,\mathrm{U}} = P_{\mathrm{UC}} \cdot M/N$;
for x=1 to ite_{outer} **do**
  Assign subcarrier-pair:
  obtain $\boldsymbol{t}^*$ according to (15);
  obtain $\boldsymbol{\phi}^*$ according to (17);
  Allocate source power:
  for i=1 to ite_{inner} **do**
    initialize μ_{s};
    allocate $P_{i,\mathrm{S}}^*(\mu_{\mathrm{s}})$ according to (23);
    update μ_{s};
  end for
  reallocate $P_{i,\mathrm{S}}^*$ based on $\{\boldsymbol{t}^*, \boldsymbol{\phi}^*\}$.
  Allocate relay power:
  for i=1 to ite_{inner} **do**
    initialize μ_{r};
    allocate $P_{i',\mathrm{R}}^*(\mu_{\mathrm{r}}) = P_{i',\mathrm{R}}^r(\mu_{\mathrm{r}})$according to (27) ;
    update μ_{r};
  end for
  Allocate jamming power:
  for i=1 to ite_{inner} **do**
    initialize μ_{u};
    allocate $P_{i,m,\mathrm{U}}^*(\mu_{\mathrm{u}})$according to (32) ;
    update μ_{u};
  end for
end for
Obtain $\{\boldsymbol{P^*} = \{P_{i,\mathrm{S}}^*, P_{i',\mathrm{R}}^*, P_{i,m,\mathrm{U}}^*\}, \boldsymbol{\phi^*}, \boldsymbol{t^*}\}$;
Calculate the weighted sum secrecy rate.

considering the user power constraint, the optimal jamming power allocation $P_{i,m,\mathrm{U}}^*$ can be written as

$$P_{i,m,\mathrm{U}}^* = \begin{cases} P_{i,m,\mathrm{U}}^{\mathrm{r}}, P_{i,m,\mathrm{U}}^{\mathrm{r}} \leq P_{i,m,\mathrm{U}}^{\diamond} \\ P_{i,m,\mathrm{U}}^{\diamond}, \text{ otherwise.} \end{cases} \tag{32}$$

Suppose the complexity of dual variable μ_{u} updates in the order of M^α, the computational complexity of solving the subproblem-4 is $O(M^\alpha)$.

E. SOLUTION OF THE MASTER PROBLEM

In the above four subsections, we solve the four subproblems respectively. The master problem is solved by AO method. In the outer loop, the AO starts with $\{P_{i,\mathrm{S}}, P_{i',\mathrm{R}}, P_{i,m,\mathrm{U}}\}$ allocated equally, then we optimally solve the four subproblems. This procedure continues either the weighted sum secrecy rate saturates or the outer iteration count exceeds a threshold. Since the weighted sum secrecy rate increases with every inner loop and the function has an upper bound because of the power constrains, the AO method converges, which is also shown in [36], [37]. The whole joint resource allocation (JRA) scheme is given in Algorithm 1. Suppose the iteration count of the outer loop is γ, then the complexity of the JRA algorithm is $O((N^3M^\alpha)^\gamma)$.

Remark: Note that when the number of users approaches infinity, the sum secrecy rate of the system will finally converge to a certain value because the power and bandwidth resource of the system is constrained. However, this value is difficult to derive because the system is too complicated.

IV. TWO LOW COMPLEXITY ALLOCATION ALGORITHMS

In section III we have proposed the AO based resource allocation algorithm, which is not computationally efficient for the large number of users and subcarriers. In this section, we propose two suboptimal algorithms with reduced complexity.

1) Low Complexity Algorithm 1: Sequentially Resource Allocation

The core idea of the Sequentially Resource Allocation (SRA) algorithm is to sequentially optimize the variables of the primal optimization problem in (11) instead of joint optimization, thereby reducing computational complexity. The primal optimization problem was divided into four subproblems and solved by AO in section III. In order to reduce the complexity, we solve the four subproblems sequentially instead. Initially allocating the relay power and jamming power $\{P_{i',\mathrm{R}}, P_{i,m,\mathrm{U}}\}$ equally, we first obtain $\{\boldsymbol{\phi}^*, \boldsymbol{t}^*\}$ by solving the subproblem-1, then we obtain $P_{i,\mathrm{S}}^*$ by solving the subproblem-2, then we obtain $P_{i',\mathrm{R}}^*$ by solving the subproblem-3, finally we obtain $P_{i,m,\mathrm{U}}^*$ by solving the subproblem-4. The SRA scheme is equivalent to the JRA scheme when the iteration of the outer loop is 1. Compared with the JRA algorithm, this suboptimal SRA algorithm does not need to do outer loop. Hence its complexity is $O(N^3M^\alpha)$.

2) Low Complexity Algorithm 2: Suboptimal Joint Resource Allocation

The core idea of the suboptimal joint resource allocation (SJRA) algorithm is to decouple the source power allocation and the relay power allocation with the other resource. The complexity involved in JRA can be reduced by allocating the source and relay power based on channel condition. We assume that the source power and the relay power is distributed proportional to the effective channel gains over

Algorithm 2 Suboptimal Joint Resource Allocation

Input: $N, M, \sigma_{\mathrm{R}}^2, P_{\mathrm{SC}}, P_{\mathrm{RC}}$
$\{h_{i,\mathrm{S}}\} = \{h_{1,\mathrm{S}}, h_{2,\mathrm{S}}, \ldots, h_{N,\mathrm{S}}\}$
$\{h_{i',m,\mathrm{R}}\} = \{h_{1,1,\mathrm{R}}, h_{1,2,\mathrm{R}}, \ldots, h_{N,M,\mathrm{R}}\}$
$\{h_{i,m,\mathrm{U}}\} = \{h_{1,1,\mathrm{U}}, h_{1,2,\mathrm{U}}, \ldots, h_{N,M,\mathrm{U}}\}$
$\{l_m\} = \{l_1, l_2, \ldots, l_M\}$
$\{\sigma_{m,\mathrm{U}}^2\} = \{\sigma_{1,\mathrm{U}}^2\, \sigma_{2,\mathrm{U}}^2\, \ldots, \sigma_{M,\mathrm{U}}^2\}$
$\{P_{m,\mathrm{UC}}\} = \{P_{1,\mathrm{UC}}, P_{2,\mathrm{UC}}, \ldots, P_{M,\mathrm{UC}}\}$
Output: Optimum set $\{\boldsymbol{P^*}, \boldsymbol{\phi^*}, \boldsymbol{t^*}\}$
1: Initialize $P_{i,\mathrm{S}} = P_{\mathrm{SC}}/N, P_{i',\mathrm{R}} = P_{\mathrm{RC}}/N$;
2: **for** i=1 to ite **do**
3: initialize μ_{u};
4: allocate $P_{i,m,\mathrm{U}}^*(\mu_{\mathrm{u}})$ according to (32);
5: obtain $\boldsymbol{t}^*(\mu_{\mathrm{u}})$;
6: obtain $\boldsymbol{\phi}^*(\mu_{\mathrm{u}})$;
7: update μ_{u};
8: **end for**
9: reallocate $P_{i,m,\mathrm{U}}^*$ based on $\{\boldsymbol{t}^*, \boldsymbol{\phi}^*\}$.
10: Obtain $\{\boldsymbol{P^*} = \{P_{i,\mathrm{S}}^*, P_{i',\mathrm{R}}^*, P_{i,m,\mathrm{U}}^*\}, \boldsymbol{\phi^*}, \boldsymbol{t^*}\}$;
11: Calculate the weighted sum secrecy rate.

all subcarriers:

$$P_{i,\mathrm{S}} = \frac{\alpha_{i,\mathrm{S}}}{\sum_{i=1}^{N} \alpha_{i,\mathrm{S}}} \cdot P_{\mathrm{SC}}, \forall i.$$

$$P_{i',\mathrm{R}} = \frac{\sum_{m=1}^{M} \alpha_{i',m,\mathrm{R}}}{\sum_{i'=1}^{N}\sum_{m=1}^{M} \alpha_{i',m,\mathrm{R}}} \cdot P_{\mathrm{RC}}, \forall i'.$$

Then, the optimization problem is to jointly allocate the jamming power, subcarrier pairing and subcarrier assignment. The problem can be stated as

$$\max_{\{P_{i,m,\mathrm{U}}, \boldsymbol{\phi}, \boldsymbol{t}\}} \sum_{i=1}^{N}\sum_{i'=1}^{N}\sum_{m=1}^{M} l_m \phi_{i,i'} t_{i,i',m} R_{i,i',m}^{\mathrm{S}} \qquad (33)$$
$$\text{s.}t.\ (6), (7)\ and\ (10).$$

The mixed integer programming problem can be solved by Lagrange dual method. We first obtain $P_{i,m,\mathrm{U}}^*$ as in (32), then determine subcarrier assignment as in (15), finally we obtain subcarrier pairing using Hungarian method as in (17). The whole SJRA scheme is shown in Algorithm 2. Since the number of dual variable μ_{u} is M, the complexity of SJRA is $O(N^3 M^{\alpha})$.

V. SIMULATION RESULTS

In this section, simulation results are presented to evaluate the performance of the proposed JRA algorithm and the two low complexity scheme (SRA and SJRA).

The Erceg channel model in [38] is employed in our simulation, in which the central frequency is given at 2GHz to emulate a broadband wireless network. We chose Category B, which is hilly terrian with light tree density or flat terrian with moderate-to-heavy tree density. The signal fading follows the Rayleigh distribution without considering shadowing effect. Some of the simulation parameters are summarized in Table 1. For simplicity, we assume the power constraints of the source, relay and all users in (8), (9) and (10) are same. The distribution of users is shown in Fig. 2, where the users are randomly distributed in a square region about 1km × 1km. The center of the square region is on the line formed by the source and the relay and 1km away from the relay.

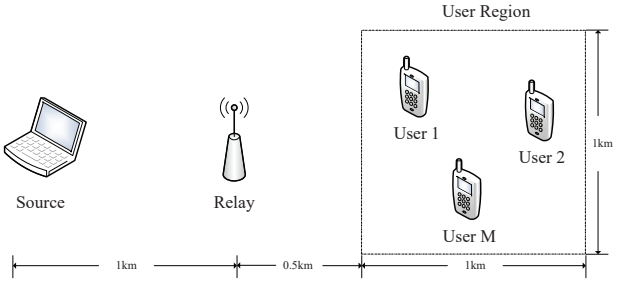

FIGURE 2. User distribution for the setup in Figs. 3, 4, 5, 6 and 7.

TABLE 1. Some Parameters used for simulation

Parameter	Value
Wireless channel band width	1MHz
Noise spectrum density	5.21×10^{-21}W/Hz
Distance between source and relay	1km
Height of source	30m
Height of relay	10m
Height of users	2m

The performance of equal power allocation (EPA) is presented as a benchmark. The EPA scheme obtain the subcarrier paring and subcarrier assignment with allocating the source power, the relay power and the user power equally. The subcarrier assignment is solved by (15) and the subcarrier pairing is solved by (17). The power refinement is employed to equally allocated each user's power by the number of subcarriers assigned to it. The complexity of EPA is $O(N^3)$.

The performance of SNR based allocation proposed in [17] is also presented as another benchmark. The SNR based allocation (SBA) scheme defines a SNR threshold δ. According to [39]–[41], when the eavesdropping SNR of the relay is less than δ, the relay can not decode the received signal and the eavesdropping rate is zero. Then the primal non-convex problem can be simplified to a convex problem, which can be solved by the dual method. The complexity of SBA is $O(N^3(M+1)^{\alpha})$.

Fig. 3 compares the weighted sum secrecy rate achieved by different schemes. The results are based upon average of 200 Monte-Carlo simulations of user distribution. From Fig. 3, we can see that our JRA scheme has the best performance and significantly outperforms the two benchmarks: EPA and SBA. The two low complexity schemes: SRA and SJRA have

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3130067, IEEE Access

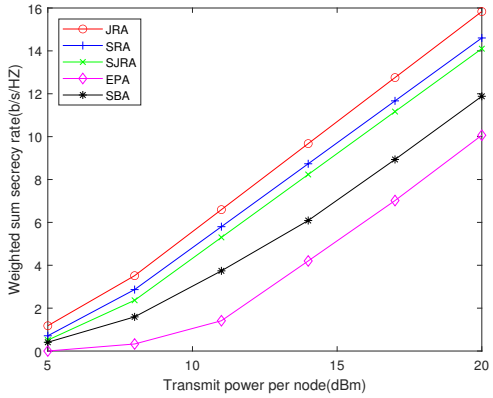

FIGURE 3. Weighted sum secrecy rate versus transmit power per node when N=32 and M=8.

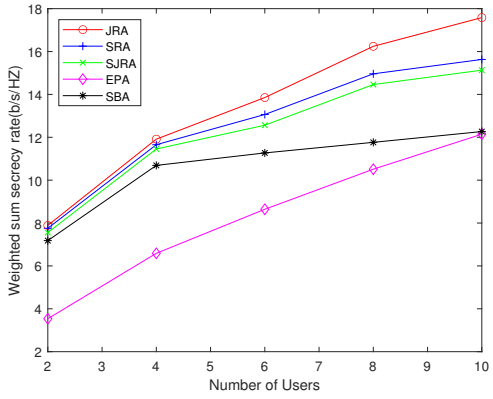

FIGURE 4. Weighted sum secrecy rate versus number of users when N=32 and transmit power per node is 20 dBm.

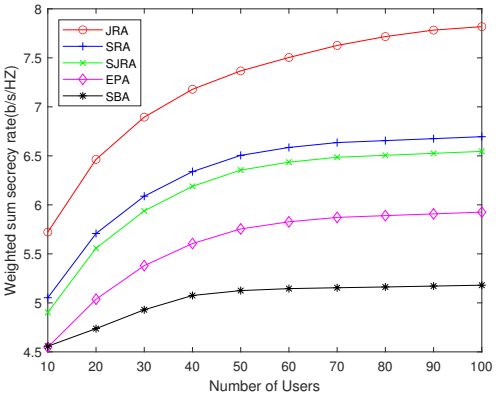

FIGURE 5. Weighted sum secrecy rate versus number of users when N=4 and transmit power per node is 20 dBm.

better performance than benchmarks and their performance is close to JRA. Among the two schemes, the SRA performs slightly better the SJRA with the same complexity, because SRA performs all power optimization while SJRA only performs the jamming power optimization.

Performance of different schemes with number of users M is presented in Fig. 4 and Fig. 5. It indicates that the gap between JRA and other suboptimal schemes increases

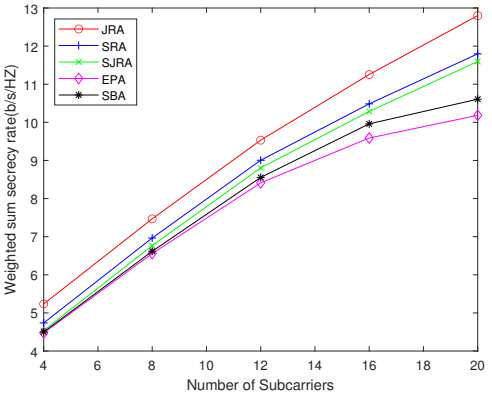

FIGURE 6. Weighted sum secrecy rate versus number of subcarriers when M=8 and transmit power per node is 20 dBm.

with number of users, because when there exist more users, the subcarrier assignment diversity increases and the optimal JRA scheme performs better. Fig. 4 also shows the performance of SBA increases more slowly when the number of users exceeds 4. This is because the eavesdropping SNR increases as the number of users increases, which requires more performance costs to control it below the threshold. This defect does not exist in our proposed algorithms. Fig. 5 shows that when the number of users approaches infinity, the sum secrecy rate of the system will finally converge to a certain value because the power and bandwidth resource of the system is constrained.

Fig. 6 compares the weighted sum secrecy rate achieved by different schemes with respect to the number of subcarriers N. It can be seen that JRA significantly outperforms other schemes and the two low complexity schemes: SRA and SJRA have better performance than benchmarks when the number subcarriers becomes large. Furthermore, due to the limited power and bandwidth resource, the sum secrecy rate of the system will first increase with the growth of the number of subcarriers and finally converge to a value. Therefore, the slope of Fig. 6 will gradually decrease.

Then, the impact of the priority weight of user is discussed. By setting the priority weight of other users to 1, we change the weight of one user and observe the secrecy rate achieved by different algorithms. The simulation result of the weighted secrecy rate of the single user and the weighted sum secrecy rate of the OFDMA system are shown in Fig. 7 and Fig. 8, respectively. It can be seen from Fig. 7 that as the priority weight increasing, the weighted secrecy rate of the single user achieved by JRA increases faster, which indicates that JRA is the most sensitive to the priority weight of user. Under this evaluation standard, the two low complexity schemes are better than the two benchmarks, and SRA is slightly better than SJRA. This is because SJRA only performs the jamming power optimization while SRA optimize all power resources. Fig. 7 shows that the weighted secrecy rate of the user achieved by JRA is lowest when the priority weight of user

is relatively low, because JRA allocates the secrecy rate to other users with higher priority weight in this case. However, the weighted system secrecy rate achieved by JRA is still the highest, as shown in Fig. 8, which indicates the superiority of our algorithms will not disappear as the priority weight of users changes. More Specifically, from Fig. 8, we can see that as the priority weight of one user increases, the weighted sum secrecy rate achieved by different algorithms increases slowly, or even decreases. This is because we allocate a lot of resources to users with higher weights, which may lead to a decrease in the sum rate.

Finally, we discuss the running time of different algorithms, which is shown in Fig. 9. It can be seen that the running time of JRA is the highest and about 9 times the running time of the two low complexity schemes: SRA and SJRA. The extra running time of JRA is brought by AO method and power refinement. The running time of SRA, SJRA and SBA is close because of their calculate complexity is almost the same. EPA has the shortest running time. Particularly, the running time of the fives algorithms are approximately proportional to the third power of the number of subcarriers, which is consistent with the computational complexity we derived.

VI. CONCLUSION

In this paper, we have formulated the subcarrier-pair based resource allocation problem in secure cooperative OFDMA system with untrusted relay, where user-aid jamming method has been employed to enhance system security. We have proposed an effective JRA algorithm based on AO and Lagrange dual method to solve the NP-hard resource allocation problem and the complexity is in polynomial time. To reduce the calculate complexity, we further proposed two suboptimal algorithms: SRA and SJRA. The SRA algorithm reduces complexity by allocating resource sequentially while the SJRA algorithm reduces complexity by decoupling the source power allocation and relay power allocation with other variables. Simulation results have been presented to evaluate the algorithms we have proposed. In simulation, We have shown the performance of JRA is always best. SRA and SJRA significantly outperform the benchmarks with reduced complexity. Specifically, the performance of SRA is slightly better than SJRA.

For the future extension, we will focus on the security-reliability trade-off (SRT) of the cooperative OFDM system with untrusted relays. The SRT shows the trade-off between the security and reliability of the system, which is a very important indicator in secure system. Studying the SRT in the considered OFDMA system with untrusted relaying is an interesting and important problem.

.

APPENDIX A PROOF OF PROPOSITION 1

For simplicity, we replace $R^{\mathrm{S}}_{i,i',m}$ by R^{S}, $P_{i,\mathrm{S}}$ by P_{s}, $P_{i',\mathrm{R}}$ by P_{r}, $P_{i,m,\mathrm{U}}$ by P_{u}, $\alpha_{i,\mathrm{S}}$ by α_{s}, $\alpha_{i',m,\mathrm{R}}$ by α_{r} and $\alpha_{i,m,\mathrm{U}}$ by α_{u} in the proof, respectively.

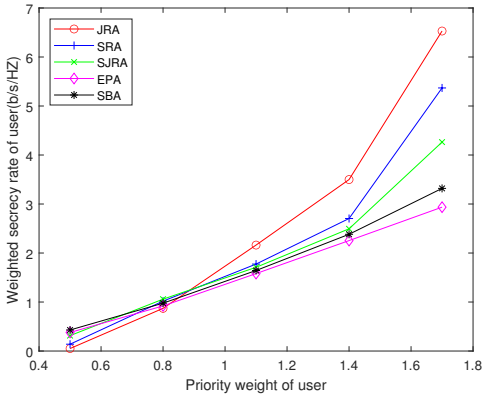

FIGURE 7. Weighted secrecy rate of user versus priority weight of user when N=32, M=8 and transmit power per node is 20 dBm.

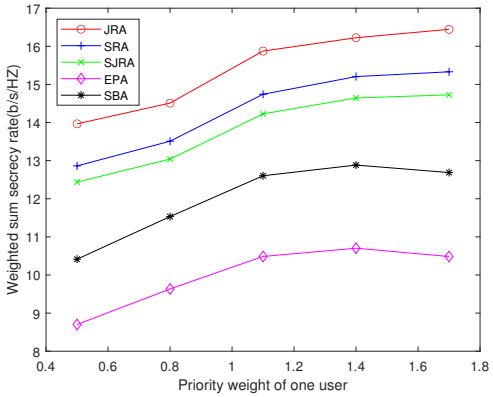

FIGURE 8. Weighted sum secrecy rate versus priority weight of user when N=32, M=8 and transmit power per node is 20 dBm.

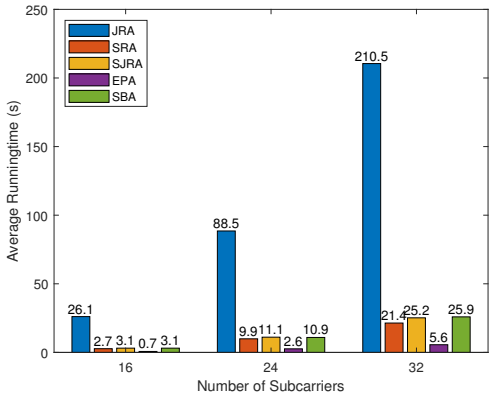

FIGURE 9. Average running time versus number of subcarriers when M=8 and transmit power per node is 20dBm.

1) R^{S} is a concave function of P_{s}

For fixed P_{r} and P_{u}, the secrecy rate R^{S} over a subcarrier-pair can be rewritten as a function of P_{s}:

$$R^{\mathrm{S}}(P_{\mathrm{s}}) = \frac{1}{2}\log_2\left(\frac{a_{\mathrm{s}}P_{\mathrm{s}} + b_{\mathrm{s}}}{P_{\mathrm{s}}^2 + c_{\mathrm{s}}P_{\mathrm{s}} + b_{\mathrm{s}}}\right), P_{\mathrm{s}} \geq 0. \qquad (34)$$

where

$$\begin{aligned} a_{\mathrm{s}} &= (\alpha_{\mathrm{r}} P_{\mathrm{r}} + 1)(\alpha_{\mathrm{u}} P_{\mathrm{u}} + 1)/\alpha_{\mathrm{s}}, \\ b_{\mathrm{s}} &= (\alpha_{\mathrm{r}} P_{\mathrm{r}} + \alpha_{\mathrm{u}} P_{\mathrm{u}} + 1)(\alpha_{\mathrm{u}} P_{\mathrm{u}} + 1)/\alpha_{\mathrm{s}}^2, \\ c_{\mathrm{s}} &= (\alpha_{\mathrm{r}} P_{\mathrm{r}} + 2\alpha_{\mathrm{u}} P_{\mathrm{u}} + 2)/\alpha_{\mathrm{s}}. \end{aligned}$$

Then the first derivative of $R^{\mathrm{S}}(P_{\mathrm{s}})$ is

$$\frac{\partial R^{\mathrm{S}}}{\partial P_{\mathrm{s}}} = \frac{1}{2\ln 2} \frac{-a_{\mathrm{s}} P_{\mathrm{s}}^2 - 2b_{\mathrm{s}} P_{\mathrm{s}} + b_{\mathrm{s}}(a_{\mathrm{s}} - c_{\mathrm{s}})}{(a_{\mathrm{s}} P_{\mathrm{s}} + b_{\mathrm{s}})(P_{\mathrm{s}}^2 + c_{\mathrm{s}} P_{\mathrm{s}} + b_{\mathrm{s}})}. \tag{35}$$

Equating (35) to zero, we obtain

$$P_{\mathrm{s}}^{\diamond} = \frac{-b_{\mathrm{s}} \pm \sqrt{a_{\mathrm{s}}^2 b_{\mathrm{s}} - a_{\mathrm{s}} b_{\mathrm{s}} c_{\mathrm{s}} + b_{\mathrm{s}}^2}}{a_{\mathrm{s}}}. \tag{36}$$

Since $P_{\mathrm{s}} \geq 0$, $P_{\mathrm{s}}^{\diamond} = \frac{-b_{\mathrm{s}} + \sqrt{a_{\mathrm{s}}^2 b_{\mathrm{s}} - a_{\mathrm{s}} b_{\mathrm{s}} c_{\mathrm{s}} + b_{\mathrm{s}}^2}}{a_{\mathrm{s}}}$. It can be easily seen that when $P_{\mathrm{s}} \leq P_{\mathrm{s}}^{\diamond}$, $\frac{\partial R^{\mathrm{S}}}{\partial P_{\mathrm{s}}} \geq 0$, R^{S} increases with P_{s}, when $P_{\mathrm{s}} > P_{\mathrm{s}}^{\diamond}$, $\frac{\partial R^{\mathrm{S}}}{\partial P_{\mathrm{s}}} < 0$, R^{S} decreases with P_{s}. Specially, R^{S} get maximum when $P_{\mathrm{s}} = P_{\mathrm{s}}^{\diamond}$. Since our target is to maximize R^{S}, the domain of P_{s} can be reduced to $[0, P_{\mathrm{s}}^{\diamond}]$.

The second derivative of $R^{\mathrm{S}}(P_{\mathrm{s}})$ is

$$\begin{aligned} \frac{\partial^2 R^{\mathrm{S}}}{\partial P_{\mathrm{s}}^2} = & \frac{1}{2\ln 2 (a_{\mathrm{s}} P_{\mathrm{s}} + b_{\mathrm{s}})^2 (P_{\mathrm{s}}^2 + c_{\mathrm{s}} P_{\mathrm{s}} + b_{\mathrm{s}})^2} \\ & \cdot \big\{ -2(a_{\mathrm{s}} P_{\mathrm{s}} + b_{\mathrm{s}})^2 (P_{\mathrm{s}}^2 + c_{\mathrm{s}} P_{\mathrm{s}} + b_{\mathrm{s}}) \\ & + [a_{\mathrm{s}} P_{\mathrm{s}}^2 + 2b_{\mathrm{s}} P_{\mathrm{s}} - b_{\mathrm{s}}(a_{\mathrm{s}} - c_{\mathrm{s}})] \\ & \cdot [3a_{\mathrm{s}} P_{\mathrm{s}}^2 + 2(b_{\mathrm{s}} + a_{\mathrm{s}} c_{\mathrm{s}}) P_{\mathrm{s}} + b_{\mathrm{s}}(a_{\mathrm{s}} + c_{\mathrm{s}})] \big\}. \end{aligned} \tag{37}$$

When $P_{\mathrm{s}} \leq P_{\mathrm{s}}^{\diamond}$, $a_{\mathrm{s}} P_{\mathrm{s}}^2 + 2b_{\mathrm{s}} P_{\mathrm{s}} - b_{\mathrm{s}}(a_{\mathrm{s}} - c_{\mathrm{s}}) \leq 0$, $\frac{\partial^2 R^{\mathrm{S}}}{\partial P_{\mathrm{s}}^2} \leq 0$. Thus, we prove R^{S} is a concave function of P_{s} when $P_{\mathrm{s}} \in [0, P_{\mathrm{s}}^{\diamond}]$ and gets maximum when $P_{\mathrm{s}} = P_{\mathrm{s}}^{\diamond}$.

2) R^{S} is a concave function of P_{r}

For fixed P_{s} and P_{u}, the secrecy rate R^{S} over a subcarrier-pair can be rewritten as a function of P_{r}:

$$R^{\mathrm{S}}(P_{\mathrm{r}}) = \frac{1}{2} \log_2 \left(\frac{a_{\mathrm{r}} P_{\mathrm{r}} + b_{\mathrm{r}}}{c_{\mathrm{r}} P_{\mathrm{r}} + d_{\mathrm{r}}} \right), P_{\mathrm{r}} \geq 0. \tag{38}$$

where

$$\begin{aligned} a_{\mathrm{r}} &= \alpha_{\mathrm{r}}(\alpha_{\mathrm{s}} P_{\mathrm{s}} + 1)(\alpha_{\mathrm{u}} P_{\mathrm{u}} + 1), \\ b_{\mathrm{r}} &= (\alpha_{\mathrm{s}} P_{\mathrm{s}} + \alpha_{\mathrm{u}} P_{\mathrm{u}} + 1)(\alpha_{\mathrm{u}} P_{\mathrm{u}} + 1), \\ c_{\mathrm{r}} &= \alpha_{\mathrm{r}}(\alpha_{\mathrm{s}} P_{\mathrm{s}} + \alpha_{\mathrm{u}} P_{\mathrm{u}} + 1), \\ d_{\mathrm{r}} &= (\alpha_{\mathrm{s}} P_{\mathrm{s}} + \alpha_{\mathrm{u}} P_{\mathrm{u}} + 1)^2. \end{aligned}$$

Then the first derivative of $R^{\mathrm{S}}(P_{\mathrm{r}})$ is

$$\frac{\partial R^{\mathrm{S}}}{\partial P_{\mathrm{r}}} = \frac{1}{2\ln 2} \frac{a_{\mathrm{r}} d_{\mathrm{r}} - b_{\mathrm{r}} c_{\mathrm{r}}}{(a_{\mathrm{r}} P_{\mathrm{r}} + b_{\mathrm{r}})(c_{\mathrm{r}} P_{\mathrm{r}} + d_{\mathrm{r}})}. \tag{39}$$

Since $a_{\mathrm{r}} d_{\mathrm{r}} - b_{\mathrm{r}} c_{\mathrm{r}} = \alpha_{\mathrm{s}} \alpha_{\mathrm{r}} P_{\mathrm{s}} (\alpha_{\mathrm{u}} P_{\mathrm{u}} + 1)(\alpha_{\mathrm{s}} P_{\mathrm{s}} + \alpha_{\mathrm{u}} P_{\mathrm{u}} + 1)^2 \geq 0$, R^{S} increases with P_{r}.

The second derivative of $R^{\mathrm{S}}(P_{\mathrm{r}})$ is

$$\frac{\partial^2 R^{\mathrm{S}}}{\partial P_{\mathrm{r}}^2} = \frac{1}{2\ln 2} \frac{-(a_{\mathrm{r}} d_{\mathrm{r}} - b_{\mathrm{r}} c_{\mathrm{r}})(2a_{\mathrm{r}} c_{\mathrm{r}} P_{\mathrm{r}} + a_{\mathrm{r}} d_{\mathrm{r}} + b_{\mathrm{r}} c_{\mathrm{r}})}{(a_{\mathrm{r}} P_{\mathrm{r}} + b_{\mathrm{r}})^2 (c_{\mathrm{r}} P_{\mathrm{r}} + d_{\mathrm{r}})^2}. \tag{40}$$

Since $a_{\mathrm{r}} d_{\mathrm{r}} - b_{\mathrm{r}} c_{\mathrm{r}} \geq 0$, $\frac{\partial^2 R^{\mathrm{S}}}{\partial P_{\mathrm{r}}^2} \leq 0$. Thus, we prove R^{S} is a concave function of P_{r} and is monotonically increasing with P_{r}, when $P_{\mathrm{r}} \geq 0$.

3) R^{S} is a concave function of P_{u}

For fixed P_{s} and P_{r}, the secrecy rate R^{S} over a subcarrier-pair can be rewritten as a function of P_{u}:

$$R^{\mathrm{S}}(P_{\mathrm{u}}) = \frac{1}{2} \log_2 \left(1 + \frac{a_{\mathrm{u}} P_{\mathrm{u}} + b_{\mathrm{u}}}{c_{\mathrm{u}} P_{\mathrm{u}}^2 + d_{\mathrm{u}} P_{\mathrm{u}} + e_{\mathrm{u}}} \right), \tag{41}$$

where

$$\begin{aligned} a_{\mathrm{u}} &= \alpha_{\mathrm{u}} \alpha_{\mathrm{s}} P_{\mathrm{s}} (\alpha_{\mathrm{r}} P_{\mathrm{r}} - 1), \\ b_{\mathrm{u}} &= -\alpha_{\mathrm{s}} P_{\mathrm{s}} (\alpha_{\mathrm{s}} P_{\mathrm{s}} + 1), \\ c_{\mathrm{u}} &= \alpha_{\mathrm{u}}^2, \\ d_{\mathrm{u}} &= \alpha_{\mathrm{u}} (2\alpha_{\mathrm{s}} P_{\mathrm{s}} + \alpha_{\mathrm{r}} P_{\mathrm{r}} + 2), \\ e_{\mathrm{u}} &= (\alpha_{\mathrm{s}} P_{\mathrm{s}} + 1)(\alpha_{\mathrm{s}} P_{\mathrm{s}} + \alpha_{\mathrm{r}} P_{\mathrm{r}} + 1). \end{aligned}$$

When $a_{\mathrm{u}} \leq 0$, i.e. $\alpha_{\mathrm{r}} P_{\mathrm{r}} \leq 1$, $R^{\mathrm{S}}(P_{\mathrm{u}}) \leq 0$, the system cannot perform confidential communication. So the $a_{\mathrm{u}} > 0$ must be satisfied. We observe when $P_{\mathrm{u}} < -\frac{b_{\mathrm{u}}}{a_{\mathrm{u}}}$, $R^{\mathrm{S}}(P_{\mathrm{u}}) < 0$, so the domain of P_{u} can be reduced to $[-\frac{b_{\mathrm{u}}}{a_{\mathrm{u}}}, +\infty]$. The first derivative of $R^{\mathrm{S}}(P_{\mathrm{u}})$ is

$$\begin{aligned} \frac{\partial R^{\mathrm{S}}}{\partial P_{\mathrm{u}}} = & \frac{-a_{\mathrm{u}} c_{\mathrm{u}} P_{\mathrm{u}}^2 - 2b_{\mathrm{u}} c_{\mathrm{u}} P_{\mathrm{u}} + a_{\mathrm{u}} e_{\mathrm{u}} - b_{\mathrm{u}} d_{\mathrm{u}}}{2\ln 2 [c_{\mathrm{u}} P_{\mathrm{u}}^2 + (a_{\mathrm{u}} + d_{\mathrm{u}}) P_{\mathrm{u}} + b_{\mathrm{u}} + e_{\mathrm{u}}]} \\ & \cdot \frac{1}{c_{\mathrm{u}} P_{\mathrm{u}}^2 + d_{\mathrm{u}} P_{\mathrm{u}} + e_{\mathrm{u}}}. \end{aligned} \tag{42}$$

Equating (42) to zero, we obtain

$$P_{\mathrm{u}}^{\diamond} = -\frac{b_{\mathrm{u}}}{a_{\mathrm{u}}} \pm \sqrt{\frac{a_{\mathrm{u}}^2 e_{\mathrm{u}} - a_{\mathrm{u}} b_{\mathrm{u}} d_{\mathrm{u}} + b_{\mathrm{u}}^2 c_{\mathrm{u}}}{a_{\mathrm{u}}^2 c_{\mathrm{u}}}}. \tag{43}$$

Since $P_{\mathrm{u}} \geq 0$, $P_{\mathrm{u}}^{\diamond} = -\frac{b_{\mathrm{u}}}{a_{\mathrm{u}}} + \sqrt{\frac{a_{\mathrm{u}}^2 e_{\mathrm{u}} - a_{\mathrm{u}} b_{\mathrm{u}} d_{\mathrm{u}} + b_{\mathrm{u}}^2 c_{\mathrm{u}}}{a_{\mathrm{u}}^2 c_{\mathrm{u}}}}$. It can be easily seen that when $P_{\mathrm{u}} \leq P_{\mathrm{u}}^{\diamond}$, $\frac{\partial R^{\mathrm{S}}}{\partial P_{\mathrm{u}}} \geq 0$, R^{S} increases with P_{u}, when $P_{\mathrm{u}} > P_{\mathrm{u}}^{\diamond}$, $\frac{\partial R^{\mathrm{S}}}{\partial P_{\mathrm{u}}} < 0$, R^{S} decreases with P_{u}. Specially, R^{S} get maximum when $P_{\mathrm{u}} = P_{\mathrm{u}}^{\diamond}$. Since our target is to maximize R^{S}, the domain of P_{u} can be reduced to $[-\frac{b_{\mathrm{u}}}{a_{\mathrm{u}}}, P_{\mathrm{u}}^{\diamond}]$.

The second derivative of $R^{\mathrm{S}}(P_{\mathrm{u}})$ is

$$\frac{\partial^2 R^{\mathrm{S}}}{\partial P_{\mathrm{u}}^2} = \frac{-2c_{\mathrm{u}}(a_{\mathrm{u}}P_{\mathrm{u}}+b_{\mathrm{u}})f_{\mathrm{u}}+g_{\mathrm{u}}h_{\mathrm{u}}}{2\ln 2[c_{\mathrm{u}}P_{\mathrm{u}}^2+(a_{\mathrm{u}}+d_{\mathrm{u}})P_{\mathrm{u}}+b_{\mathrm{u}}+e_{\mathrm{u}}]^2} \cdot \frac{1}{(c_{\mathrm{u}}P_{\mathrm{u}}^2+d_{\mathrm{u}}P_{\mathrm{u}}+e_{\mathrm{u}})^2}, \tag{44}$$

where $f_{\mathrm{u}} = [c_{\mathrm{u}}P_{\mathrm{u}}^2+(a_{\mathrm{u}}+d_{\mathrm{u}})P_{\mathrm{u}}+b_{\mathrm{u}}+e_{\mathrm{u}}](c_{\mathrm{u}}P_{\mathrm{u}}^2+d_{\mathrm{u}}P_{\mathrm{u}}+e_{\mathrm{u}}) > 0$, $g_{\mathrm{u}} = -\{4c_{\mathrm{u}}^2P_{\mathrm{u}}^3+3c_{\mathrm{u}}(a_{\mathrm{u}}+2d_{\mathrm{u}})P_{\mathrm{u}}^2+2[(a_{\mathrm{u}}+d_{\mathrm{u}})d_{\mathrm{u}}+(b_{\mathrm{u}}+c_{\mathrm{u}}+e_{\mathrm{u}})c_{\mathrm{u}}]P_{\mathrm{u}}+(a_{\mathrm{u}}+d_{\mathrm{u}})e_{\mathrm{u}}+(b_{\mathrm{u}}+c_{\mathrm{u}})d_{\mathrm{u}}\} < 0$, $h_{\mathrm{u}} = -a_{\mathrm{u}}c_{\mathrm{u}}P_{\mathrm{u}}^2-2b_{\mathrm{u}}c_{\mathrm{u}}P_{\mathrm{u}}+a_{\mathrm{u}}e_{\mathrm{u}}-b_{\mathrm{u}}d_{\mathrm{u}} \geq 0, \forall P_{\mathrm{u}} \in [0, P_{\mathrm{u}}^{\diamond}]$

When $P_{\mathrm{u}} \in [-\frac{b_{\mathrm{u}}}{a_{\mathrm{u}}}, P_{\mathrm{u}}^{\diamond}]$, $-2c_{\mathrm{u}}(a_{\mathrm{u}}P_{\mathrm{u}}+b_{\mathrm{u}}) \leq 0$, $h_{\mathrm{u}} \geq 0$, so $\frac{\partial^2 R^{\mathrm{S}}}{\partial P_{\mathrm{s}}^2} \leq 0$. Thus, we prove R^{S} is a concave function of P_{u} when $P_{\mathrm{u}} \in [-\frac{b_{\mathrm{u}}}{a_{\mathrm{u}}}, P_{\mathrm{u}}^{\diamond}]$ and gets maximum when $P_{\mathrm{u}} = P_{\mathrm{u}}^{\diamond}$.

Combined the above three subsections, the Proposition 1 is proved.

APPENDIX B THE HUNGARIAN METHOD

The assignment problem deals with assigning machines to tasks, workers to jobs, soccer players to positions, and so on. The goal is to determine the optimum assignment that, for example, minimizes the total cost or maximizes the team effectiveness. The Hungarian algorithm is an easy to understand and easy to use algorithm that solves the assignment problem.

Step 1: Subtract row minimum

For each row, find the lowest element and subtract it from each element in that row.

Step 2: Subtract column minimum

Similarly, for each column, find the lowest element and subtract it from each element in that column.

Step 3: Cover all zeros with a minimum number of lines

Cover all zeros in the resulting matrix using a minimum number of horizontal and vertical lines. If n lines are required, an optimal assignment exists among the zeros. The algorithm stops.

If less than n lines are required, continue with Step 4.

Step 4: Create additional zeros

Find the smallest element (call it k) that is not covered by a line in Step 3. Subtract k from all uncovered elements, and add k to all elements that are covered twice.

REFERENCES

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.

[2] Y. S. Shiu, S. Y. Chang, H. C. Wu, C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, 2011.

[3] A. Wyner, "The wire-tap channel," *Bell Labs Tech J*, vol. 54, no. 8, 1975.

[4] X. Xiao, X. Tao, and J. Lu, "Energy-efficient resource allocation in lte-based mimo-ofdma systems with user rate constraints," *IEEE Trans. Veh. Technol.*, vol. 64, no. 1, pp. 1–1, 2014.

[5] A. Nusairat and X.-Y. Li, "Wimax/ofdma burst scheduling algorithm to maximize scheduled data," *IEEE Trans. Mobile Comput.*, vol. 11, no. 11, pp. 1692–1705, 2012.

[6] T. M. Hoang, A. E. Shafie, D. Costa, T. Q. Duong, and A. Marshall, "Security and energy harvesting for MIMO-OFDM networks," *IEEE Trans. Commun.*, vol. PP, no. 99, pp. 1–1, 2019.

[7] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative jamming for secure ofdm system," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1331–1346, 2018.

[8] Y. Zhang, K. Bai, L. Pang, R. Han, Y. Li, S. Liang, Y. Luan, and G. Ren, "Multi-dimensional resource optimization for incremental af-ofdm systems with rf energy harvesting relay," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 613–627, 2019.

[9] B. Ahuja, D. Mishra, and R. Bose, "Fair subcarrier allocation for securing ofdma in iot against full-duplex hybrid attacker," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2898–2911, 2021.

[10] S.-I. Kim, I.-M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3724–3737, 2015.

[11] A. Jindal and R. Bose, "Resource allocation for secure multicarrier af relay system under total power constraint," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 231–234, 2015.

[12] A. Jindal and R. Bose, "Resource allocation in secure multicarrier af relay system under individual power constraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5070–5085, 2017.

[13] D. Xu and H. Zhu, "Jamming-assisted legitimate eavesdropping and secure communication in multicarrier interference networks," *IEEE Syst J*, pp. 1–12, 2020.

[14] R. Saini, A. Jindal, and S. De, "Jammer-assisted resource allocation in secure ofdma with untrusted users," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1055–1070, 2016.

[15] R. Saini, D. Mishra, and S. De, "Ofdma-based df secure cooperative communication with untrusted users," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 716–719, 2016.

[16] R. Saini, D. Mishra, and S. De, "Novel subcarrier pairing strategy for df relayed secure ofdma with untrusted users," in *IEEE Globecom Workshops, GC Wkshps - Proc.*, 2017, pp. 1–6.

[17] S. Sarma and J. Kuri, "SNR based secure communication via untrusted amplify-and-forward relay nodes using artificial noise," *Wireless Networks*, vol. 24, no. 1, pp. 127–138, 2016.

[18] S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure beamforming for full-duplex mimo two-way untrusted relay systems," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3775–3790, 2020.

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

[20] D. P. Moya Osorio, H. Alves, and E. E. Benitez Olivo, "On the secrecy performance and power allocation in relaying networks with untrusted relay in the partial secrecy regime," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2268–2281, 2020.

[21] L. Lv, H. Jiang, Z. Ding, L. Yang, and J. Chen, "Secrecy-enhancing design for cooperative downlink and uplink NOMA with an untrusted relay," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1698–1715, 2020.

[22] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3737–3749, 2020.

[23] M. Letafati, A. Kuhestani, H. Behroozi, and D. W. K. Ng, "Jamming-resilient frequency hopping-aided secure communication for internet-of-things in the presence of an untrusted relay," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6771–6785, 2020.

[24] A. Kuhestani, A. Mohammadi, and P. L. Yeoh, "Security-reliability trade-off in cyber-physical cooperative systems with non-ideal untrusted relaying," in *IEEE World Forum Internet Things, WF-IoT - Proc*, 2018, pp. 552–557.

[25] Q. Dong and G. Li, "Secure OFDM transmission in wireless networks with untrusted relays," *Int. Conf. Wirel. Commun. Signal Process*, pp. 1–6, 2017.

[26] D. Chen, Y. Cheng, X. Wang, W. Yang, J. Hu, and Y. Cai, "Energy-efficient secure multiuser scheduling in energy harvesting untrusted relay networks," *J COMMUN NETW-S KOR*, vol. 21, no. 4, pp. 365–375, 2019.

[27] B. He, Q. Ni, J. Chen, L. Yang, and L. Lv, "User-pair selection in multiuser cooperative networks with an untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 869–882, 2019.

[28] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

[29] Y. F. Liu and Y. H. Dai, "On the complexity of joint subcarrier and power allocation for multi-user ofdma systems," *IEEE Trans. Signal Process.*, vol. 62, no. 3, pp. 583–596, 2014.
[30] D. Yuan, J. Joung, C. K. Ho, and S. Sun, "On tractability aspects of optimal resource allocation in ofdma systems," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 863–873, 2013.
[31] S. Boyd. (Jun. 2008) Sequential convex programming. [Online]. Available: {http://stanford.edu/class/ee364b/lectures/seq_slides.pdf}
[32] H. W. Kuhn, "The hungarian method for the assignment problem," *Nav Res Logist*, vol. 52, no. 1-2, p. 7–21, 1955.
[33] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
[34] S. Boyd and A. Mutapcic, "Subgradient methods," *notes for EE364, Standford University*, 2003.
[35] W. Chao and H. M. Wang, "Joint relay selection and artificial jamming power allocation for secure df relay networks," in *IEEE Int. Conf. Commun.*, 2014, Conference Proceedings, pp. 819–824.
[36] H. M. Wang, F. Liu, and X. G. Xia, "Joint source-relay precoding and power allocation for secure amplify-and-forward mimo relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1240–1250, 2014.
[37] L. Grippo and M. Sciandrone, "Sciandrone, m.: On the convergence of the block nonlinear gauss-seidel method under convex constraints. oper. res. lett. 26(3), 127-136," *Oper. Res. Lett.*, vol. 26, no. 3, pp. 127–136, 2000.
[38] R. Jain. (Feb. 2007) Channel models: A tutorial. [Online]. Available: {https://www.cse.wustl.edu/~jain/cse574-08/ftp/channel_model_tutorial.pdf}
[39] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, and M. Segal, "Optimization schemes for protective jamming," in *Proc. Int. Symp. Mobile Ad Hoc Networking Comput.*, 2012, Conference Proceedings.
[40] S. Sarma and J. Kuri, "Optimal power allocation for protective jamming in wireless networks: A flow based model," *Comput. Networks*, vol. 81, no. C, pp. 258–271, 2015.
[41] A. L. Swindlehurst, "Fixed sinr solutions for the mimo wiretap channel," in *ICASSP IEEE Int Conf Acoust Speech Signal Process Proc*, 2009, Conference Proceedings.