Article

Joint Resource Allocation in Secure OFDM Two-Way Untrusted Relay System

Yifeng Jin [1], Xunan Li [2], Guocheng Lv [1,*], Meihui Zhao [1] and Ye Jin [1]

1 School of Electronics, Peking University, Beijing 100871, China; jinyifeng@pku.edu.cn (Y.J.); meihui_zhao@pku.edu.cn (M.Z.); jinye@pku.edu.cn (Y.J.)
2 National Computer Network Emergency Response Technical Team Coordination Center of China, Beijing 100029, China; lixunan@cert.org.cn
* Correspondence: lv.guocheng@pku.edu.cn

Abstract: The security issue of wireless communication is a common concern because of its broadcast nature, especially when the relay becomes an eavesdropper. In the orthogonal frequency division multiplexing (OFDM) relay system, when the relay is untrusted, the security of the system faces serious threats. Although there exist some resource allocation schemes in a single-carrier system with untrusted relaying, it is difficult to apply them to the multi-carrier system. Hence, a resource allocation scheme for the multi-carrier system is needed. Compared to the one-way relay system, a two-way relay system can improve the data transmission efficiency. In this paper, we consider joint secure resource allocation for a two-way cooperative OFDM system with an untrusted relay. The joint resource allocation problem of power allocation and subcarrier pairing is formulated to maximize the sum secrecy rate of the system under individual power constraints. To solve the non-convex problem efficiently, we propose an algorithm based on the alternative optimization method. The proposed algorithm is evaluated by simulation results and compared with the benchmarks in the literature. According to the numerical results, in a high signal-to-noise ratio (SNR) scenario, the proposed algorithm improves the achievable sum secrecy rate of the system by more than 15% over conventional algorithms.

Keywords: physical layer security; OFDM two-way system; untrusted relay; joint resource allocation

1. Introduction

Due to the broadcast nature of wireless communication, the threats of eavesdropping and information leakages have increased sharply and the security issue becomes a common concern. The traditional encryption technology uses cryptographic methods in the upper layer of the system, which is crackable and insufficient with the rapid growth of computing power. Therefore, secure communication in the lower layer of the system has been studied and the physical layer security has become a frontier research. Unlike cryptographic methods, the principle of physical layer security technology is to use the difference between the legal channel and the eavesdropping channel to achieve secure communication of the system, which is also its advantage [1,2]. The concept of physical layer security is first introduced by Wyner in a one-hop communication system [3]. With the wide application of relays, many researchers have extended this technology to relay systems [4–7]. In order to utilize the limited resource of the communication system to maximize the secrecy rate, efficient resource allocation is essential in physical layer security.

The two-way relay communication systems has attracted much attention in the past few years due to its ability in combating the half-duplex constraint of relay nodes and improving the data transmission efficiency [8–10]. Due to the advantages of physical layer security, many studies on two-way cooperative communication systems have considered security issue from a physical layer perspective. The research scenarios can be divided into two cases: (1) External eavesdropper [11,12], in which an illegitimate eavesdropper

that does not belong to the network tries to decode the confidential information, and (2) untrusted relay [13–19], in which the relay is assumed to be untrustworthy and acts as an eavesdropper.

In the two-way untrusted relay system, the physical security was first studied in [13], in which the authors proved this system can achieve secure communication without external friendly jammer. The authors in [14] employed artificial noise and studied power allocation in the two-way untrusted relay system with channel estimation errors. Ref. [15] studied the power allocation in the two-way system with multiple untrusted relays. In the two-way untrusted relay system with multi-antenna, the authors in [16] proposed a joint beamforming and suboptimal power allocation scheme to maximize the sum secrecy rate of the system. The problem of optimal power allocation for two-way untrusted relaying networks with an external jammer was examined in [17]. In [18], the authors studied secure relay selection for two-way untrusted relaying networks. Secure beamforming for full-duplex multiple-input–multiple-output (MIMO) two-way untrusted relay systems was considered in [19]. In other scenarios, the authors in [20] proposed machine learning techniques to conserve the position confidentiality of roaming position-based services (PBSs) users. In [21], the authors proposed a whale optimization algorithm to solve the resource allocation problem in an Internet of Things (IoT) system to reduce the total communication cost.

The above related works are all based on the single-carrier system, so the resources that need to be allocated in the system are the transmission power only. In two-way relay assisted orthogonal frequency division multiplexing (OFDM) systems, channel gains of one subcarrier in one hop differ from another hop, and system capacity can be maximized by subcarrier pairing and power allocation [22]. The joint resource allocation in the secure OFDM one-way system was studied in some previous works [23–25]; however, due to the differences in system models, the existing resource allocation schemes cannot be applied in an OFDM two-way untrusted relay system. A summary of related work is presented in Table 1. To the best of the authors' knowledge, secure resource allocation jointly considering subcarrier pairing and power allocation for a two-way cooperative OFDM system with untrusted relaying has not been studied in the literature.

Table 1. A summary of related works.

Reference	Algorithm	Year	Pros and Cons
[7]	SNR-based approach	2016	- Easy implementation - Unable to find optimal solution
[16]	Iterative algorithm	2018	- Obtain better solutions - High complexity
[17]	Derivative algorithm	2018	- Low complexity - Only suitable for univariate problems
[23]	Fractional programming algorithm	2019	- Obtain better solutions - Only suitable for fractional problems
[25]	Dual algorithm	2021	- Low complexity - Only suitable for convex problems

In this paper, our main innovation is to study the secure resource allocation jointly considering subcarrier pairing and power allocation for a two-way cooperative OFDM system with untrusted relaying, including constructing the system model, formulating the optimization problem, and proposing an effective algorithm to solve the non-convex

problem. Our goal is to achieve the secure communication in the OFDM two-way communication system with untrusted relaying. We use resource allocation to enhance the security performance of the system by maximizing the sum secrecy rate of the system under individual power constraints of each transmit node. The key idea of our resource allocation algorithm is to decouple the non-convex optimization problem into several brief subproblems and relax them to convex ones.

The major contribution of this paper are twofold:

1. We introduce a two-way cooperative OFDM system with an untrusted relay and formulate the resource allocation problem to maximize the sum secrecy rate under individual power constraints, which include the subcarrier pairing and power allocation.

2. To solve the problem, we propose a joint resource allocation algorithm based on alternative optimization method. The problem is solved by divided into four subproblems. In particular, we show that the complexity of the solution is polynomial in the number of subcarriers. According to the numerical results, in a high signal-to-noise ratio (SNR) scenario, the proposed algorithm improves the achievable sum secrecy rate of the system by more than 15% over conventional algorithms.

The remainder of this paper is organized as follows. Section 2 describes the system model and derives the formulation of the sum secrecy rate. Section 3 formulates the optimization problem and presents an efficient joint resource allocation algorithm based on alternative optimization (AO). Section 4 demonstrates the simulation results to illustrate the performance of the proposed algorithm. Finally, this paper is concluded in Section 5.

2. System Model

We consider a two-way cooperative OFDM system with untrusted relaying, as shown in Figure 1, where two users, denoted as A and B, wish to exchange confidential information via an untrusted relay R. The two-way relay operates in a half-duplex mode using the amplify-and-forward (AF) protocol. All communication nodes are assumed to be equipped with a single antenna. We assume that there are no direct links between A and B due to the long distance between them. The users-to-relay channels are considered to be reciprocal, occupying the same bandwidth and experiencing frequency-selective fading. Each OFDM channel is composed of N orthogonal subcarriers.

Particularly, the relay is assumed trusted at the service level and untrusted at the data level, as in [26]. Service-level trust entails following the AF protocol as expected. This involves for relays to feedback true CSI, adapt their power according to system schedule, and forward the amplified version of received signal without modification. Since the relay is data-level untrusted, the source imposes security constraints on relays. This is to prevent the untrusted relay from extracting useful information from its received signal.
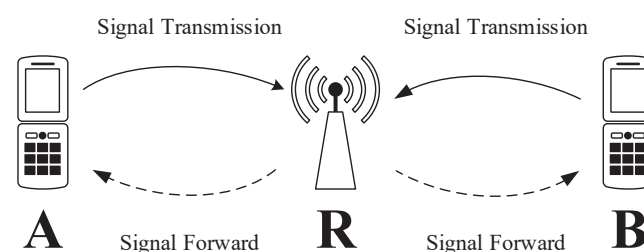

Figure 1. An OFDM two-way system with an untrusted relay. Solid lines: signal transmission on subcarriers in the first slot. Dashed lines: signal forward transmission on subcarriers in the second slot.

The transmission from the users to the relay is on a timeframe basis with each frame consisting of multiple OFDM symbols. Each frame is further divided into two time slots. In the first time slot, both A and B send signals to R simultaneously on all subcarriers. We

denote the channel coefficients of A to R and B to R on the i-th subcarrier as $h_{i,A}$ and $h_{i,B}$, respectively, for $i \in \{1, ..., N\}$. We further assume that the transmit powers of A and B on the i-th subcarrier are $P_{i,A}$ and $P_{i,B}$, respectively. Then, the received signal at R on the i-th subcarrier in the first time slot can be given by

$$y_{i,R} = \sqrt{P_{i,A}} h_{i,A} w_{i,A} + \sqrt{P_{i,B}} h_{i,B} w_{i,B} + n_{i,R}, \tag{1}$$

where $w_{i,A}$ and $w_{i,B}$ denote symbol of A and B's signal on the i-th subcarrier, respectively. $n_{i,R}$ denotes the additive white Gaussian noise (AWGN) signal at the relay on the i-th subcarrier and the noise power is σ_n^2.

In the second time slot, R amplifies the received signals $y_{i,R}$ on the i-th subcarrier with a constant gain and forwards them to both A and B on the i'-th subcarrier. Note that the subcarrier index i' may not be as same as i and they form a subcarrier pair (i, i'), and each subcarrier in A to R is paired with only one subcarrier in B to R. Since each subcarrier has different channel gains, subcarrier pairing can utilize subcarrier diversity to enhance system performance. We denote the transmit power of R on the i'-th subcarrier as $P_{i',R}$. Let $\beta_{i,i'}$ represent the power gain at R to normalize the power of the signal transmitted, i.e.,

$$\beta_{i,i'} = \frac{P_{i',R}}{|h_{i,A}|^2 P_{i,A} + |h_{i,B}|^2 P_{i,B} + \sigma_R^2}. \tag{2}$$

Following that, the received signal at A and B from R on the i'-th subcarrier in the second time slot can be given by

$$y_{i',A} = \sqrt{\beta_{i,i'}} \sqrt{P_{i,A}} h_{i',A} h_{i,A} w_{i,A} + \sqrt{\beta_{i,i'}} \sqrt{P_{i,B}} h_{i',A} h_{i,B} w_{i,B} + \sqrt{\beta_{i,i'}} h_{i',A} n_{i,R} + n_{i',A}, \tag{3}$$

and

$$y_{i',B} = \sqrt{\beta_{i,i'}} \sqrt{P_{i,A}} h_{i',B} h_{i,A} w_{i,A} + \sqrt{\beta_{i,i'}} \sqrt{P_{i,B}} h_{i',B} h_{i,B} w_{i,B} + \sqrt{\beta_{i,i'}} h_{i',B} n_{i,R} + n_{i',B}, \tag{4}$$

where $n_{i',A}$ and $n_{i',B}$ denote the AWGN at A and B on the i'-th subcarrier with variances σ_n^2. Assuming that both user A and B can perfectly estimate the channel state information (CSI) for channels $h_{i',A}$ and $h_{i,B}$, the self-interference terms can be eliminated perfectly at both users (first term in (3) and second term in (4)). Therefore, the received signal at A and B can be expressed as

$$y_{i',A} = \sqrt{\beta_{i,i'}} \sqrt{P_{i,B}} h_{i',A} h_{i,B} w_{i,B} + \sqrt{\beta_{i,i'}} h_{i',A} n_{i,R} + n_{i',A}, \tag{5}$$

$$y_{i',B} = \sqrt{\beta_{i,i'}} \sqrt{P_{i,A}} h_{i',B} h_{i,A} w_{i,A} + \sqrt{\beta_{i,i'}} h_{i',B} n_{i,R} + n_{i',B}. \tag{6}$$

Then, the resultant SNR at A and B on the subcarrier pair (i, i') can be represented as

$$\gamma_{i,i',A} = \frac{\beta_{i,i'} P_{i,B} |h_{i',A}|^2 |h_{i,B}|^2}{\beta_{i,i'} |h_{i',A}|^2 \sigma_n^2 + \sigma_n^2} = \frac{\alpha_{i,B} \alpha_{i',A} P_{i,B} P_{i',R}}{\alpha_{i,A} P_{i,A} + \alpha_{i,B} P_{i,B} + \alpha_{i',A} P_{i',R} + 1}, \tag{7}$$

and

$$\gamma_{i,i',B} = \frac{\beta_{i,i'} P_{i,A} |h_{i',B}|^2 |h_{i,A}|^2}{\beta_{i,i'} |h_{i',B}|^2 \sigma_n^2 + \sigma_n^2} = \frac{\alpha_{i,A} \alpha_{i',B} P_{i,A} P_{i',R}}{\alpha_{i,A} P_{i,A} + \alpha_{i,B} P_{i,B} + \alpha_{i',B} P_{i',R} + 1}, \tag{8}$$

where $\alpha_{i,A} = |h_{i,A}|^2 / \sigma_n^2$ and $\alpha_{i,B} = |h_{i,B}|^2 / \sigma_n^2$ are effective channel coefficients. Then, the transmission rate at A and B on the subcarrier pair (i, i') can be expressed as $R_{i,i',A} = \frac{1}{2} \log_2(1 + \gamma_{i,i',A})$ and $R_{i,i',B} = \frac{1}{2} \log_2(1 + \gamma_{i,i',B})$, respectively.

As mentioned before, the relay is considered to be untrusted and tries to eavesdrop on the confidential signal. The untrusted relay employs successive the interference cancellation

(SIC) method to decode the mixed signal, which requires the relay to decode one user's signal and remove it from the mixed signals before decoding another user's signal. This creates two situations that we need to discuss separately: (1) The SIC is successful, which means the relay successfully decodes one user's signal. In this case, the relay will not experience interference while it decodes another user's signal. Since the signal will weaken in the transmission of relay forward to the user, the eavesdropping rate of relay must be greater than the transmission rate of the user, so the system cannot achieve secure communication and the resource allocation is meaningless. (2) The SIC is unsuccessful, then the untrusted relay decodes one of the users' signals by treating the other user as noise, which is called the single-user decode mode [27]. In this case, the resource allocation can achieve secure communication of the system. Therefore, in the following derivation, the untrusted relay adopts the single-user decode mode. The eavesdropping rate at R on A and B over the i-th subcarrier can be computed from (1) and is given by

$$R_{i,\mathrm{RA}} = \frac{1}{2} \log_2(1 + \frac{P_{i,\mathrm{B}}|h_{i,\mathrm{B}}|^2}{P_{i,\mathrm{A}}|h_{i,\mathrm{A}}|^2 + \sigma_{\mathrm{n}}^2}) = \frac{1}{2} \log_2(1 + \frac{\alpha_{i,\mathrm{B}}P_{i,\mathrm{B}}}{\alpha_{i,\mathrm{A}}P_{i,\mathrm{A}} + 1}), \tag{9}$$

and

$$R_{i,\mathrm{RB}} = \frac{1}{2} \log_2(1 + \frac{P_{i,\mathrm{A}}|h_{i,\mathrm{A}}|^2}{P_{i,\mathrm{B}}|h_{i,\mathrm{B}}|^2 + \sigma_{\mathrm{n}}^2}) = \frac{1}{2} \log_2(1 + \frac{\alpha_{i,\mathrm{A}}P_{i,\mathrm{A}}}{\alpha_{i,\mathrm{B}}P_{i,\mathrm{B}} + 1}). \tag{10}$$

Therefore, the sum secrecy rate of the system on subcarrier pair (i, i') can be formulated as

$$R_{i,i'}^{\mathrm{S}} = (R_{i,i',\mathrm{A}} - R_{i,\mathrm{RA}})^+ + (R_{i,i',\mathrm{B}} - R_{i,\mathrm{RB}})^+, \tag{11}$$

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

In this paper, our aim is to jointly design the resource allocation scheme of power allocation and subcarrier pairing to maximize the sum secrecy rate of the system, with the constraints of individual power budgets per node. We define $\boldsymbol{P} = \{P_{i,\mathrm{A}}, P_{i,\mathrm{B}}, P_{i',\mathrm{R}}\}$ as the set of power allocation scheme, and it satisfies the individual power constraints, which are

$$\sum_{i=1}^{N} P_{i,\mathrm{A}} \leq P_{\mathrm{A}}, \tag{12}$$

$$\sum_{i=1}^{N} P_{i,\mathrm{B}} \leq P_{\mathrm{B}}, \tag{13}$$

$$\sum_{i'=1}^{N} P_{i',\mathrm{R}} \leq P_{\mathrm{R}}, \tag{14}$$

where P_{A}, P_{B}, and P_{R} denote the transmitting power budgets on the user A, the user B, and the relay R, respectively.

In addition to the power constraints, the system must also satisfy the subcarrier pairing constraint that guarantees that each subcarrier is paired strictly with one subcarrier. We define $\boldsymbol{\rho} = \{\rho_{i,i'}\}$ as the set of subcarrier pairing scheme; $\rho_{i,i'} = 1$ indicates that the i-th subcarrier in the first slot is paired with the i'-th subcarrier in the second slot. The subcarrier pairing constraint can be given by

$$\sum_{i'=1}^{N} \rho_{i,i'} = 1, \ \forall i, \quad \sum_{i=1}^{N} \rho_{i,i'} = 1, \ \forall i', \tag{15}$$

3. Resource Allocation for Sum Secrecy Rate Maximization

The optimization problem can be formulated as

$$\max_{\{P,\rho\}} \sum_{i=1}^{N} \sum_{i'=1}^{N} \rho_{i,i'} R_{i,i'}^{S} \tag{16}$$

$$\text{s.t. } \sum_{i=1}^{N} P_{i,A} \leq P_A, \sum_{i=1}^{N} P_{i,B} \leq P_B, \sum_{i'=1}^{N} P_{i',R} \leq P_R,$$

$$\sum_{i'=1}^{N} \rho_{i,i'} = 1, \ \forall i, \sum_{i=1}^{N} \rho_{i,i'} = 1, \ \forall i'.$$

The optimization problem in (16) is a non-convex mixed-integer programming, which is NP-hard. Since there exist four optimization variables, i.e., $P_{i,A}$, $P_{i,B}$, $P_{i',R}$, and $\rho_{i,i'}$ in (16), we can decompose the primal problem into four subproblems by using the alternating optimization (AO) method, which is widely used in research related to resource allocation [28–30]. In the AO method, the optimal resource allocation scheme of the optimization problem is obtained by solving the subproblems in sequence, which are discussed in the following subsections.

3.1. Power Allocation Scheme for User A

Assuming that the other optimization variables, i.e., $P_{i,B}$, $P_{i',R}$, and $\rho_{i,i'}$, are given, and we define the i' as the given subcarrier index in the second time slot paired with the i-th subcarrier in the first time slot, then the subproblem of power allocation for user A can be given as

$$\max_{\{P_{i,A}\}} \sum_{i=1}^{N} R_{i,i'}^{S} \tag{17}$$

$$\text{s.t. } \sum_{i=1}^{N} P_{i,A} \leq P_A,$$

which is still a non-convex problem. Since most of the impact caused by the power allocation for the user A is reflected in the transmission rate from the user A to the user B and the eavesdropping rate at R on B, we can approximate the optimization problem in (17) as

$$\max_{\{P_{i,A}\}} \sum_{i=1}^{N} (R_{i,i',B} - R_{i,RB}). \tag{18}$$

$$\text{s.t. } \sum_{i=1}^{N} P_{i,A} \leq P_A.$$

Proposition 1. *The optimization problem in (18) is convex.*

Proof. See Appendix A. □

Therefore, we can solve the convex problem in (18) by dual method [31]. We denote $\lambda_A \geq 0$ as the dual variable associated with the power constraints in the user A. The dual function can be defined as

$$g(\lambda_A) = \max_{P_{i,A}} L_A(P_{i,A}, \lambda_A), \tag{19}$$

where the Lagrangian is

$$L_A(P_{i,A}, \lambda_A) = \sum_{i=1}^{N} \frac{1}{2} \log_2 \left(\frac{a_A P_{i,A} + b_A}{P_{i,A}^2 + c_A P_{i,A} + b_A} \right) + \lambda_A \left(P_A - \sum_{i=1}^{N} P_{i,A} \right), \tag{20}$$

where a_A, b_A and c_A are coefficients determined by the channel gains as

$$a_A = (\alpha_{i',B} P_{i',R} + 1)(\alpha_{i,B} P_{i,B} + 1)/\alpha_{i,A},$$
$$b_A = (\alpha_{i',B} P_{i',R} + \alpha_{i,B} P_{i,B} + 1)(\alpha_{i,B} P_{i,B} + 1)/\alpha_{i,A}^2,$$
$$c_A = (\alpha_{i',B} P_{i',R} + 2\alpha_{i,B} P_{i,B} + 2)/\alpha_{i,A}.$$

Computing the dual function $g(\lambda_A)$ requires us to determine the optimal $P_{i,A}$ at the given dual variable λ_A. In the following we present the derivations in detail.

3.1.1. Optimizing the Primal Variables $P_{i,A}$ for Given λ_A

By applying Karush–Kuhn–Tucker (KKT) conditions [32], we can obtain the optimal power allocation scheme $P_{i,A}^*(\lambda_A)$. Specifically, $P_{i,A}^*(\lambda_A)$ is the non-negative real root of the following cubic equation:

$$A_A P_{i,A}^3 + B_A P_{i,A}^2 + C_A P_{i,A} + D_A = 0, \tag{21}$$

where A_A, B_A, C_A, and D_A are coefficients determined by the channel gains and the dual variable λ_A as

$$A_A = a_A,$$
$$B_A = b_A + a_A c_A + a_A/(2 \ln 2 \lambda_A),$$
$$C_A = b_A(a_A + c_A) + b_A/(2 \ln 2 \lambda_A),$$
$$D_A = b_A^2 + b_A(c_A - a_A)(2 \ln 2 \lambda_A).$$

Then the dual function can be further written as

$$g(\lambda_A) = \max_{P_{i,A}^*} L_A(P_{i,A}^*, \lambda_A), \tag{22}$$

3.1.2. Optimizing the Dual Variable λ_A

After computing $g(\lambda_A)$, we now solve the standard dual optimization problem which is

$$\min_{\lambda_A} g(\lambda_A) \tag{23}$$
$$\text{s.t. } \lambda_A \geq 0.$$

Since the dual function is always convex [32], the dual optimization problem in (23) can be solved by subgradient-based methods with global convergence. The subgradient of $g(\lambda_A)$ can be derived as

$$\triangle \lambda_A = P_A - \sum_{i=1}^{N} P_{i,A}^*(\lambda_A). \tag{24}$$

The dual variable can be updated as $\lambda_A^{(l+1)} = \lambda_A^{(l)} + \epsilon^{(l)} \triangle \lambda_A$, where l is the number of iterations and $\epsilon^{(l)}$ is the diminishing update step size to guarantee the convergence of the subgradient method.

3.2. Power Allocation Scheme for User B

Keeping the given and obtained variables, i.e., $P_{i,A}^*$, $P_{i',R}$, and $\rho_{i,i'}$, the subproblem of power allocation for user B can be given as

$$\max_{\{P_{i,B}\}} \sum_{i=1}^{N} R_{i,i'}^{S} \tag{25}$$

$$\text{s.t. } \sum_{i=1}^{N} P_{i,B} \leq P_B,$$

which is still a non-convex problem. Since most of the impact caused by the power allocation for the user B is reflected in the transmission rate from the user B to the user A and the eavesdropping rate at R on A, we can approximate the optimization problem in (25) as

$$\max_{\{P_{i,B}\}} \sum_{i=1}^{N} (R_{i,i',A} - R_{i,RA}), \tag{26}$$

$$\text{s.t. } \sum_{i=1}^{N} P_{i,B} \leq P_B.$$

Proposition 2. *The optimization problem in (26) is convex.*

Proof. See Appendix B. □

Therefore, the subproblem in (26) can be similarly solved as problem in (18) by the dual method. We denote $\lambda_B \geq 0$ as the dual variable associated with the power constraints in the user B. After similar derivations, $P_{i,B}^*(\lambda_B)$ is the non-negative real root of the following cubic equation:

$$A_B P_{i,B}^3 + B_B P_{i,B}^2 + C_B P_{i,B} + D_B = 0, \tag{27}$$

where A_B, B_B, C_B, and D_B are coefficients determined by the channel gains and the dual variable λ_B as

$$A_B = a_B,$$
$$B_B = b_B + a_B c_B + a_B / (2 \ln 2 \lambda_B),$$
$$C_B = b_B (a_B + c_B) + b_B / (2 \ln 2 \lambda_B),$$
$$D_B = b_B^2 + b_B (c_B - a_B)(2 \ln 2 \lambda_B),$$

where a_B, b_B and c_B are coefficients determined by the channel gains as

$$a_B = (\alpha_{i',A} P_{i',R} + 1)(\alpha_{i,A} P_{i,A} + 1) / \alpha_{i,B},$$
$$b_B = (\alpha_{i',A} P_{i',R} + \alpha_{i,A} P_{i,A} + 1) \cdot (\alpha_{i,A} P_{i,A} + 1) / \alpha_{i,B}^2,$$
$$c_B = (\alpha_{i',A} P_{i',R} + 2\alpha_{i,A} P_{i,A} + 2) / \alpha_{i,B}.$$

The dual variable λ_B can be obtained by subgradient-based methods with global convergence as the solution of the problem in (23).

3.3. Power Allocation Scheme for Relay R

Keeping the given and obtained variables, i.e., $P_{i,A}^*$, $P_{i,B}^*$, and $\rho_{i,i'}$, the subproblem of power allocation for relay R can be given as

$$\max_{\{P_{i',R}\}} \sum_{i=1}^{N} R_{i,i'}^{S} \tag{28}$$

$$\text{s.t. } \sum_{i'=1}^{N} P_{i',R} \leq P_{R}.$$

Proposition 3. *The optimization problem in (28) is convex.*

Proof. See Appendix C. □

Therefore, the subproblem in (28) can be similarly solved as the problem in (18) by the dual method. We denote $\lambda_R \geq 0$ as the dual variable associated with the power constraints in the relay R. After similar derivations, $P_{i',R}^*(\lambda_R)$ is the non-negative real root of the following quartic equation:

$$A_R P_{i',R}^4 + B_R P_{i',R}^3 + C_R P_{i',R}^2 + D_R P_{i',R} + E_R = 0, \tag{29}$$

where $A_R, B_R, C_R,$ and D_R are coefficients determined by the channel gains and the dual variable λ_R as

$$
\begin{aligned}
A_R &= a_R, \\
B_R &= b_R + a_R d_R, \\
C_R &= c_R(a_R + 1) + b_R d_R - (a_R d_R - b_R)/(2 \ln 2 \lambda_R), \\
D_R &= c_R(b_R + d_R) - (a_R - 1) c_R / (\ln 2 \lambda_R), \\
E_R &= c_R^2 - c_R(b_R - d_R)(2 \ln 2 \lambda_R),
\end{aligned}
$$

where $a_R, b_R, c_R,$ and d_R are coefficients determined by the channel gains as

$$
\begin{aligned}
a_R &= (\alpha_{i,A} P_{i,A} + 1)(\alpha_{i,B} P_{i,B} + 1), \\
b_R &= (\alpha_{i',A}(\alpha_{i,B} P_{i,B} + 1) + \alpha_{i',B}(\alpha_{i,A} P_{i,A} + 1))(\alpha_{i,A} P_{i,A} + \alpha_{i,B} P_{i,B} + 1)/(\alpha_{i',A} \alpha_{i',B}), \\
c_R &= (\alpha_{i,A} P_{i,A} + \alpha_{i,B} P_{i,B} + 1)^2/(\alpha_{i',A} \alpha_{i',B}), \\
d_R &= (\alpha_{i',A} + \alpha_{i',B})(\alpha_{i,A} P_{i,A} + \alpha_{i,B} P_{i,B} + 1)/(\alpha_{i',A} \alpha_{i',B}).
\end{aligned}
$$

The dual variable λ_R can be obtained by subgradient-based methods with global convergence as the solution of the problem in (23).

3.4. Subcarrier Pairing Scheme

Keeping the obtained variables $P_{i,A}^*$, $P_{i,B}^*$, and $P_{i',R}^*$, we next determine the subcarrier pairing scheme, which is

$$\max_{\{\rho\}} \sum_{i=1}^{N} \sum_{i'=1}^{N} \rho_{i,i'} R_{i,i'}^{S} \tag{30}$$

$$\text{s.t. } \sum_{i'=1}^{N} \rho_{i,i'} = 1, \ \forall i, \ \sum_{i=1}^{N} \rho_{i,i'} = 1, \ \forall i',,$$

which is an integer programming. Defining a $N \times N$ cost matrix $\boldsymbol{R} = [R_{i,i'}^S], \forall i, i' \in \{1, ...N\}$, the solution of problem (30) is finding an optimal assignment of N elements in the cost matrix to maximize the cost. The subscript of each selected element in $\boldsymbol{R}$ is corresponding to the subcarrier-pair (i, i'), where the row represents the subcarrier index i and the column

represents the subcarrier index i'. Particularly, this selection is a standard linear assignment problem and we can solve it by the Hungarian method [33] with $O((N^3)$ complexity. We define $\mu(i)$ as the optimal subcarrier index in the second slot paired with subcarrier i in the first slot, and the optimal subcarrier pairing variable can be given by

$$\rho_{i,i'}^* = \begin{cases} 1, & i' = \mu(i) \\ 0, & \text{otherwise.} \end{cases} \tag{31}$$

The $\mu(i)$ is obtained by the Hungarian method and (31) is the subcarrier mapping pattern, where the subcarrier mapping scale is $N \times N$. For more details on the Hungarian method, see Appendix D.

3.5. Alternating Optimization

In the above subsections, the subproblems are solved and the corresponding optimization variables are obtained. Then, we use the AO method to solve the primal optimization problem of joint resource allocation in (16). The initial variable values for the algorithm are $P_{i,A} = P_A/N, P_{i,B} = P_B/N, P_{i',R} = P_R/N, i' = i, \forall i, i' \in \{1, ..., N\}$. Then, in the first loop, we obtain $P_{i,A}^*, P_{i,B}^*, P_{i,R}^*$ and $\rho_{i,i'}^*$ by solving the subproblems sequentially. Note that when solving a subproblem, the solution of the previous subproblem is used as its initial variable value. In the next loop, the initial power allocation and subcarrier pairing scheme inherit the results in the previous loop. The loop ends when the iteration count exceeds a threshold. The whole resource allocation algorithm is given in Algorithm 1. The flowchart of the proposed algorithm is shown in Figure 2.

Since the sum secrecy rate of the system increases after each loop and has an upper bound due to the limited power budgets, the sum secrecy rate achieved by the AO algorithm finally converges. Defining the iteration count as γ, the complexity of the AO algorithm is $O((N^{3\gamma})$.

Algorithm 1 Proposed algorithm for problem (16)

1: Initialize $P_{i,A} = P_A/N, P_{i,B} = P_B/N, P_{i',R} = P_R/N, i' = i, \forall i, i' \in \{1, ..., N\}$;
2: Initialize μ_A, μ_B, μ_R;
3: **for** x=1 to γ **do**
4:     **Power Allocation for User** A**:**
5:     **repeat**
6:     obtain $P_{i,A}^*(\mu_A)$ using (21);
7:     update μ_A;
8:     **until** μ_A converges.
9:     **Power Allocation for User** B**:**
10:     **repeat**
11:     obtain $P_{i,B}^*(\mu_B)$ using (27);
12:     update μ_B;
13:     **until** μ_B converges.
14:     **Power Allocation for Relay** R**:**
15:     **repeat**
16:     obtain $P_{i',R}^*(\mu_R)$ using (29);
17:     update μ_R;
18:     **until** μ_R converges.
19:     **Subcarrier Pairing:**
20:     obtain ρ^* according to (31);
21: **end for**
22: Obtain $\{\boldsymbol{P}^* = \{P_{i,A}^*, P_{i,B}^*, P_{i',R}^*\}, \boldsymbol{\rho}^* = \{\rho_{i,i'}^*\}$.
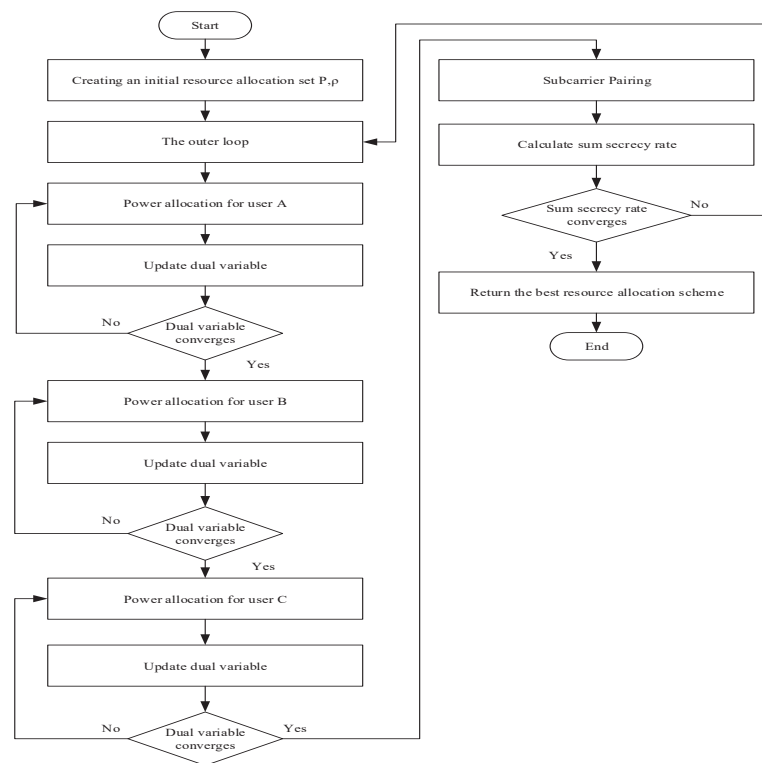

Figure 2. Flowchart of the proposed algorithm.

Remark 1. *There are only two cases for the respective secrecy rate of the user* A *and* B*: both 0 or both positive. Particularly, in this optimization algorithm, if $P_{i,A} = 0$, then $P_{i,B} = 0$, and vice versa. This is because when $P_{i,A} = 0$, according to* (9)*, there is no interference to the relay eavesdropping on user* A*. Therefore, the $R^{S}_{i,i',A} = 0$, which means that user* B *does not need to allocate power on the i-th subcarrier, i.e., $P_{i,B} = 0$.*

4. Simulation Results

In simulation, the signal fading follows the Rayleigh distribution. For simplicity, the power constraints of the users and relay are assumed to be the same. The distance between user A and B is 2 km, and the relay is located at the center of their connection. Three degraded benchmarks, namely, the channel-based power allocation with subcarrier pairing (CBA with SP), equal power allocation with subcarrier pairing (EPA with SP), and equal power allocation without subcarrier pairing (EPA without SP), are considered for comparisons. Since the computational complexity of the algorithms is a polynomial of the number of subcarriers, the sorting scale of the simulation depends on the number of subcarriers, and we perform simulations with subcarriers ranging from 4 to 32.

The CBA with SP algorithm first allocates power according to the equivalent channel coefficient of each subcarrier, with more power allocated to subcarriers with better channels. Then, the algorithm uses the Hungarian method for subcarrier pairing. Differently, the EPA with SP algorithm first allocates power equally on subcarriers and then uses the Hungarian method for subcarrier pairing. The EPA without SP algorithm only allocates power equally on subcarriers, where the subcarrier index for pairing is the same, i.e., $i = i'$.

Two conventional algorithms are also presented for comparison. The first algorithm is the SNR-based allocation (SBA) scheme proposed in [7]. This algorithm defines an SNR threshold and assumes that when the eavesdropping SNR of the relay is less than the threshold, the untrusted relay cannot decode the confidential signals, so the eavesdropping rate is 0. Then, the primal non-convex problem can be simplified to a convex problem. The second algorithm is the derivative algorithm (DA) proposed in [17]. This algorithm

splits the primal multiple-variable problem into several univariate problems and obtains the solution of these problems by derivation.

In all resource allocation schemes, a central controller acts as service provider, which is assumed to have perfect knowledge of all CSI. The users, as service requesters, provide their own power budgets and CSI to the service provider, and the service provider utilizes this information for subcarrier pairing and power allocation in order to ensure secure communication for users.

The sum secrecy rate achieved by different algorithms is shown in Figure 3. The numerical results are based on average of 200 Monte Carlo simulations. We can see that the proposed algorithm achieves higher sum secrecy rate than the three benchmarks. In a high SNR regime, the proposed algorithm improves the achievable sum secrecy rate of the system by more than 15% over the three degraded benchmarks and two conventional algorithms. Figure 3 also shows that the CBA algorithm performs better than the EPA algorithm, which indicates that the subcarrier pairing can effectively improve secrecy performance of the system. The SBA algorithm has the worst performance, because in the two-way untrusted relay system, the small eavesdropping SNR of the relay will result in the decrease of the transmission rate of the users. Hence, the sum secrecy rate of the system will also be reduced. The performance of the DA algorithm is between the CBA algorithm and the EBA algorithm, because the optimization problem is non-convex and the DA algorithm is only suitable for convex problems.
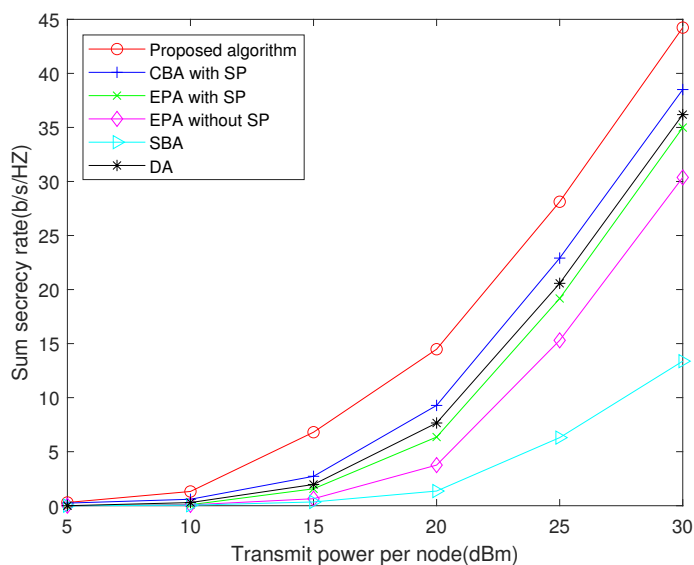

Figure 3. Sum secrecy rate versus transmit power per node when $N = 16$.

Figure 4 compares the sum secrecy rate achieved by different algorithms with respect to the number of subcarriers. It can be seen that the proposed algorithm significantly outperforms other schemes, especially with more subcarriers. This is because the conventional algorithms in benchmarks cannot make efficient use of the diversity of subcarriers. Furthermore, since the power and bandwidth of the system are limited, the sum secrecy rate will increase with the growth of the number of subcarriers at first, and finally converge. Therefore, the slope of Figure 4 will gradually decrease.
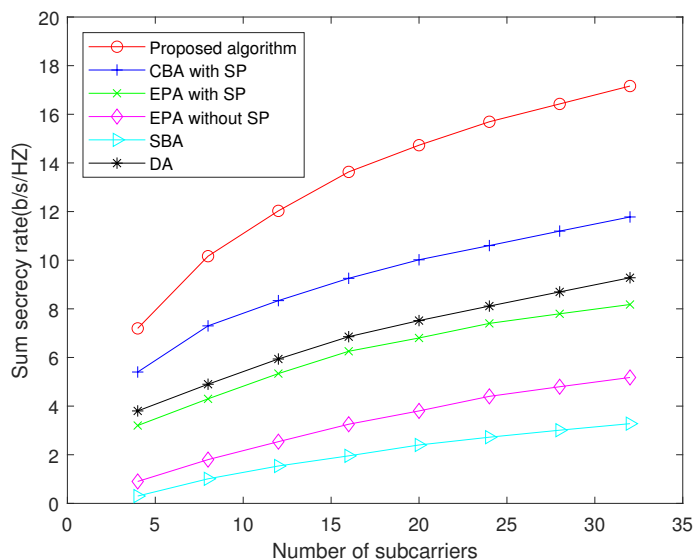
Figure 4. Sum secrecy rate versus number of subcarriers when transmit power per node is 20 dBm.

Figure 5 shows the power allocation scheme on different subcarriers by the proposed algorithm. The corresponding effective channel coefficients of subcarriers are presented in Table 2. It can be seen that for the same subcarrier, if $P_A = 0$, then $P_B = 0$, which proves our remark in Section 3. We can also see that the proposed algorithm tends to allocate more power to subcarriers with similar channel gains on A to R and B to R. This is because the untrusted relay decodes one of the users' signals by treating the other user as noise. Therefore, the allocated power on the subcarrier with similar channel gains on A to R and B to R can more effectively reduce the eavesdropping rate and increase the sum secrecy rate.

Table 2. Effective channel coefficients of simulation in Figure 5.

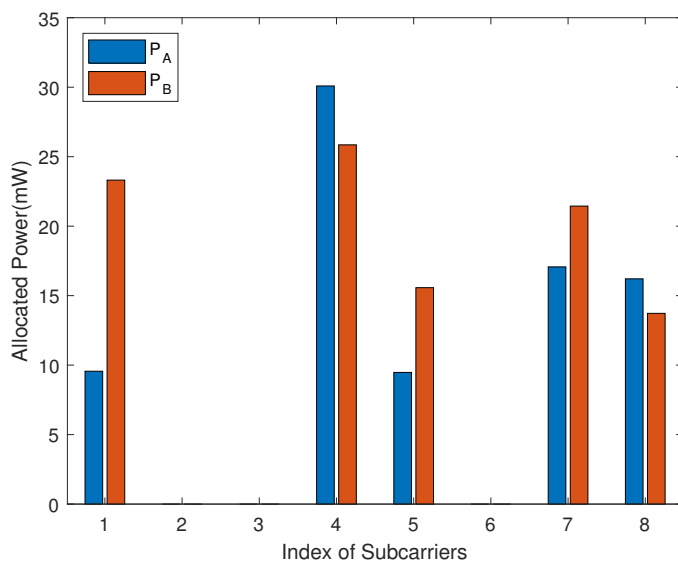| i	1	2	3	4	5	6	7	8
$\alpha_{i,A}$	2.51	0.80	0.10	1.16	0.72	0.22	1.50	0.45
$\alpha_{i,B}$	0.80	0.27	1.34	1.15	0.39	0.83	0.80	0.59

Figure 5. Allocated power versus index of subcarriers when transmit power per node is 20 dBm; $N = 8$.

Figure 6 compares the sum secrecy rate achieved by different algorithms with respect to the distance from the user to the relay. The proposed algorithm has better performance than algorithms in the benchmarks at any location of the relay. Particularly, from Figure 6, it can be seen that the sum secrecy rate achieved by all algorithms reaches the maximum when the distance from the relay R to the user A is 1 km, i.e., the distance from A to R is equal to the distance from B to R. This is because when the distances from A to R and B to R are closer, the channel fading parameters of the subcarriers on A to R and B to R become similar. As mentioned above, the allocated power on the subcarrier with similar channel gains on A to R and B to R can more effectively reduce the eavesdropping rate and increase the sum secrecy rate. Therefore, the sum secrecy rate of the system increases as the distances between the relay and the two users become closer.
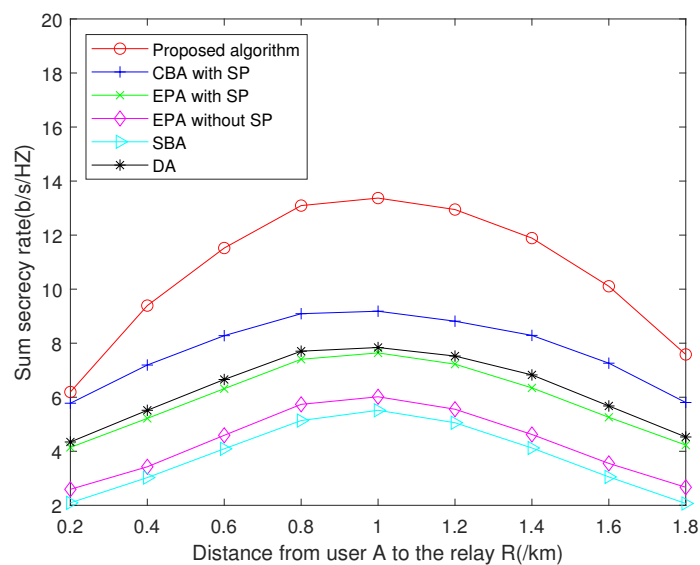

Figure 6. Sum secrecy rate versus distance from user A to the relay R when $N = 16$ and transmit power per node is 20 dBm.

Particularly, when the untrusted relay is not cooperative and could alter the power to undermine the strategy, the proposed algorithm can still effectively allocate resource, because the power allocation of the untrusted relay is decoupled from the primal problem in the proposed algorithm. Therefore, the proposed algorithm still works well with the variation of the relay power. In Figure 7, we limit the user's power to 20 dBm, and the untrusted relay can alter its transmit power. Since the untrusted relay is not cooperative, it will always allocate power equally to each subcarrier. Figure 7 compares the sum secrecy rate achieved by different algorithms in this scenario. It can be seen that our proposed algorithm has the best performance, which also confirms our analysis.
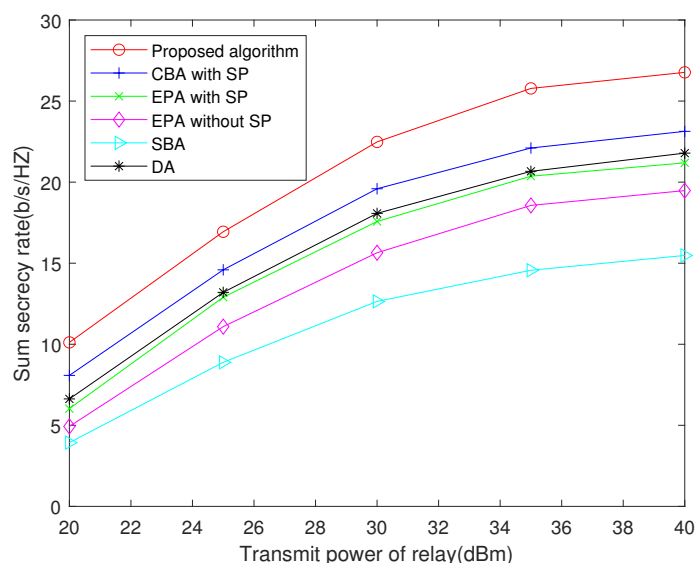
Figure 7. Sum secrecy rate versus transmit power of relay R when $N = 16$ and transmit power of user nodes is 20 dBm.

5. Conclusions

In this paper, we introduced an OFDM two-way untrusted relay system and formulated a subcarrier-pair-based secure resource allocation problem to maximize the sum secrecy rate of the system. A joint resource allocation algorithm based on the AO method was proposed to solve the non-convex optimization problem. We show that the primal NP-hard problem can be solved in polynomial time by decomposing into several subproblems. Furthermore, we show that in this system, there is no situation where one user can achieve secure communication and another user cannot. The simulation results show that the proposed algorithm outperforms other existing algorithms significantly, especially in a high-SNR regime with more subcarriers.

For the future extension, we will consider the smart untrusted relay in the OFDM two-way communication system. This means the relay can use pilot spoofing to alternate channel estimates, masquerading the eavesdropping channel as in [34], so the CSI is imperfect. Effective channel estimators should be used to combat the pilot spoofing attacks.

Author Contributions: Conceptualization, Y.J. (Yifeng Jin) and X.L.; methodology, Y.J. (Yifeng Jin) and X.L.; software, Y.J. (Yifeng Jin); validation, Y.J. (Yifeng Jin); formal analysis, Y.J. (Yifeng Jin); investigation, Y.J. (Yifeng Jin) and X.L.; resources, Y.J. (Yifeng Jin); data curation, Y.J. (Yifeng Jin) and M.Z.; writing—original draft preparation, Y.J. (Yifeng Jin); writing—review and editing, X.L., G.L., M.Z. and Y.J. (Ye Jin); visualization, Y.J. (Yifeng Jin); supervision, G.L. and Y.J. (Ye Jin); project administration, G.L. and Y.J. (Ye Jin); funding acquisition, G.L. and Y.J. (Ye Jin). All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to confidentiality.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

OFDM	Orthogonal frequency division multiple
AF	Amplify and forward
MIMO	Multiple-input–multiple output
AWGN	Additive white Gaussian noise
CSI	Channel state information
SNR	Signal-to-noise ratio
AO	Alternating optimization
CBA	Channel-based power allocation
SP	Subcarrier pairing
EPA	Equal power allocation

Appendix A

For simplicity, we replace $R_{i,i',A}^S$ by R_a, $R_{i,i',B}^S$ by R_b, $R_{i,i'}^S$ by R_s, $P_{i,A}$ by P_a, $P_{i',R}$ by P_r, $P_{i,B}$ by P_b, $\alpha_{i,A}$ by α_a, $\alpha_{i',A}$ by $\alpha_{a'}$, $\alpha_{i,B}$ by α_b, and $\alpha_{i',B}$ by $\alpha_{b'}$ in the proof, respectively.

(1) When $R_b = 0$, R_b is a concave function of P_a.

(2) When $R_b > 0$, it can be rewritten as

$$R_b(P_a) = \frac{1}{2}\log_2\left(\frac{a_a P_a + b_a}{P_a^2 + c_a P_a + b_a}\right), \tag{A1}$$

where

$$a_a = (\alpha_{b'} P_r + 1)(\alpha_b P_b + 1)/\alpha_a,$$
$$b_a = (\alpha_{b'} P_r + \alpha_b P_b + 1)(\alpha_b P_b + 1)/\alpha_a^2,$$
$$c_a = (\alpha_{b'} P_r + 2\alpha_b P_b + 2)/\alpha_a.$$

It can be calculated that when $0 < P_a < P_a^\diamond$, $\frac{\partial R_b}{\partial P_a} > 0$, when $P_a > P_a^\diamond$, $\frac{\partial R_b}{\partial P_a} < 0$, where

$$P_a^\diamond = \frac{-b_a \pm \sqrt{a_a^2 b_a - a_a b_a c_a + b_a^2}}{a_a}. \tag{A2}$$

Since our target is to maximize R_b, the optimal solution P_a^* will always satisfy $P_a^* \leq P_a^\diamond$. Hence, the domain of P_a can be reduced to $[0, P_a^\diamond]$. The optimization problem in (18) is equivalent to the problem below, which can be given by

$$\max_{\{P_{i,A}\}} \sum_{i=1}^{N} (R_{i,i',B} - R_{i,RB}). \tag{A3}$$

$$\text{s.t. } \sum_{i=1}^{N} P_{i,A} \leq P_S, \ P_{i,A} \leq P_{i,A}^\diamond, \forall i.$$

The second derivative of $R^S(P_s)$ is

$$\frac{\partial^2 R_b}{\partial P_a^2} = \frac{1}{2\ln 2(a_a P_a + b_a)^2(P_a^2 + c_a P_a + b_a)^2}$$
$$\cdot \left\{-2(a_a P_a + b_a)^2(P_a^2 + c_a P_a + b_a)\right.$$
$$+ [a_a P_a^2 + 2b_a P_a - b_a(a_a - c_a)]$$
$$\left.\cdot [3a_a P_a^2 + 2(b_a + a_a c_a)P_a + b_a(a_a + c_a)]\right\}. \tag{A4}$$

When $P_a \leq P_a^\diamond$, $a_a P_a^2 + 2b_a P_a - b_a(a_a - c_a) \leq 0$, $\dfrac{\partial^2 R_b}{\partial P_a^2} \leq 0$. Thus, we prove R_b is a concave function of P_a when $P_a \in [0, P_a^\diamond]$. Therefore, the problem in (A3) is convex and the optimization problem in (18) is also convex.

Appendix B

Substituting R_b with R_a, P_a with P_b, α_a with α_b, α_b with α_a, and $\alpha_{b'}$ with $\alpha_{a'}$, the proof of Proposition 2 is exactly the same as the proof of Proposition 1.

Appendix C

(1) When $R_a > 0$ and $R_b > 0$, R_s can be rewritten as:

$$R_s(P_r) = \underbrace{\frac{1}{2}\log_2(1+\gamma_a)}_{R_{s1}} + \underbrace{\frac{1}{2}\log_2(1+\gamma_b)}_{R_{s2}} - C, \tag{A5}$$

where C denotes the eavesdropping rate of relay, which is constant when P_a and P_b is given.

The second derivative of the first part of $R_s(P_r)$ is

$$\frac{\partial^2 R_{s1}}{\partial P_r^2} = \frac{1}{2\ln 2} \frac{-(a_r d_r - b_r c_r)(2a_r c_r P_r + a_r d_r + b_r c_r)}{(a_r P_r + b_r)^2 (c_r P_r + d_r)^2}, \tag{A6}$$

where

$$a_r = \alpha_{b'}(\alpha_a P_a + 1)(\alpha_b P_b + 1),$$
$$b_r = (\alpha_a P_a + \alpha_b P_b + 1)(\alpha_b P_b + 1),$$
$$c_r = \alpha_{b'}(\alpha_a P_a + \alpha_b P_b + 1),$$
$$d_r = (\alpha_a P_a + \alpha_b P_b + 1)^2.$$

Since $a_r d_r - b_r c_r \geq 0$, $\dfrac{\partial^2 R_{s1}}{\partial P_r^2} \leq 0$. Similarly, we can prove $\dfrac{\partial^2 R_{s2}}{\partial P_r^2} \leq 0$. Hence, $\dfrac{\partial^2 R_s}{\partial P_r^2} \leq 0$.

(2) When $R_a > 0$ and $R_b = 0$, $R_s = R_{s1} - C$, $\dfrac{\partial^2 R_s}{\partial P_r^2} \leq 0$.

(3) When $R_a = 0$ and $R_b > 0$, $R_s = R_{s2} - C$, $\dfrac{\partial^2 R_s}{\partial P_r^2} \leq 0$.

(4) When $R_a = 0$ and $R_b = 0$, $R_s = 0$, $\dfrac{\partial^2 R_s}{\partial P_r^2} = 0$.

Therefore, we prove R_s is a concave function of P_r and the optimization problem in (28) is convex.

Appendix D. The Hungarian Method

The assignment problem's goal is to determine the optimum assignment that, e.g., minimizes the total cost. The Hungarian algorithm is an effective algorithm that solves the assignment problem.

In: a $N \times N$ matrix, named cost matrix.

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. Debbah, M. Mobile Flexible Networks: The Challenges Ahead. In Proceedings of the 2008 International Conference on Advanced Technologies for Communications, Hanoi, Vietnam, 6–9 October 2008.
2. Liang, Y.; Poor, H.V.; Shamai, S. *Information Theoretic Security*; Now Foundations and Trends: Hanover, MA, USA, 2010.
3. Wyner, A. The Wire-Tap Channel. *Bell Labs. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
4. Yuan, C.; Tao, X.; Ni, W.; Li, N.; Liu, R.P. Joint Power Allocation and Beamforming for Overlaid Secrecy Transmissions in MIMO-OFDM Channels. *IEEE Trans. Veh. Technol.* **2020**, *69*, 10019–10032. [CrossRef]
5. Lv, L.; Jiang, H.; Ding, Z.; Yang, L.; Chen, J. Secrecy-Enhancing Design for Cooperative Downlink and Uplink NOMA With an Untrusted Relay. *IEEE Trans. Commun.* **2020**, *68*, 1698–1715. [CrossRef]
6. Ju, Y.; Wang, H.; Pei, Q.; Wang, H.M. Physical Layer Security in Millimeter Wave DF Relay Systems. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 5719–5733. [CrossRef]
7. Sarma, S.; Kuri, J. SNR based secure communication via untrusted amplify-and-forward relay nodes using artificial noise. *Wirel. Netw.* **2016**, *24*, 127–138. [CrossRef]
8. Li, H.; Zhao, X. Joint Resource Allocation for OFDM-Based Cognitive Two-Way Multiple AF Relays Networks With Imperfect Spectrum Sensing. *IEEE Trans. Veh. Technol.* **2018**, *67*, 6286–6300. [CrossRef]
9. Jia, X.; Zhang, C.; Kim, I.M. Optimizing Wireless Powered Two-Way Communication System With EH Relays and Non-EH Relays. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11248–11252. [CrossRef]
10. Ju, M.; Yang, H.C. Optimum Design of Energy Harvesting Relay for Two-Way Decode-and-Forward Relay Networks Under Max–Min and Max-Sum Criterions. *IEEE Trans. Commun.* **2019**, *67*, 6682–6697. [CrossRef]
11. Zhang, H.; Xing, H.; Cheng, J.; Nallanathan, A.; Leung, V.C.M. Secure Resource Allocation for OFDMA Two-Way Relay Wireless Sensor Networks Without and With Cooperative Jamming. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1714–1725. [CrossRef]
12. Zhong, B.; Zhang, Z. Secure full-duplex two-way relaying networks with optimal relay selection. *IEEE Commun. Lett.* **2017**, *21*, 1123–1126. [CrossRef]
13. Zhang, R.; Song, L.; Han, Z.; Jiao, B. Physical Layer Security for Two-Way Untrusted Relaying With Friendly Jammers. *IEEE Trans. Veh. Technol.* **2012**, *61*, 3693–3704. [CrossRef]
14. Gong, L.; Ding, X.; Zhu, Q.; Zhou, N. Cooperative Interference and Power Allocation in a Bidirectional Untrusted Relay Network With Channel Estimation Errors. *IEEE Access* **2018**, *6*, 50950–50958. [CrossRef]
15. Wang, D.; Bai, B.; Chen, W.; Han, Z. Secure Green Communication via Untrusted Two-Way Relaying: A Physical Layer Approach. *IEEE Trans. Commun.* **2016**, *64*, 1861–1874. [CrossRef]
16. Mekkawy, T.; Yao, R.; Tsiftsis, T.A.; Xu, F.; Lu, Y. Joint Beamforming Alignment With Suboptimal Power Allocation for a Two-Way Untrusted Relay Network. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2464–2474. [CrossRef]
17. Kuhestani, A.; Mohammadi, A.; Yeoh, P.L. Optimal Power Allocation and Secrecy Sum Rate in Two-Way Untrusted Relaying Networks With an External Jammer. *IEEE Trans. Commun.* **2018**, *66*, 2671–2684. [CrossRef]
18. Mekkawy, T.; Yao, R.; Qi, N.; Lu, Y. Secure Relay Selection for Two Way Amplify-and-Forward Untrusted Relaying Networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11979–11987. [CrossRef]
19. Zhao, S.; Liu, J.; Shen, Y.; Jiang, X.; Shiratori, N. Secure Beamforming for Full-Duplex MIMO Two-Way Untrusted Relay Systems. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3775–3790. [CrossRef]
20. Sangaiah, A.K.; Medhane, D.V.; Han, T.; Hossain, M.S.; Muhammad, G. Enforcing Position-Based Confidentiality With Machine Learning Paradigm Through Mobile Edge Computing in Real-Time Industrial Informatics. *IEEE Trans. Ind. Inf.* **2019**, *15*, 4189–4196. [CrossRef]
21. Sangaiah, A.K.; Hosseinabadi, A.A.R.; Shareh, M.B.; Bozorgi Rad, S.Y.; Zolfagharian, A.; Chilamkurti, N. IoT Resource Allocation and Optimization Based on Heuristic Algorithm. *Sensors* **2020**, *20*, 539. [CrossRef]
22. Zhang, H.; Liu, Y.; Tao, M. Resource Allocation with Subcarrier Pairing in OFDMA Two-Way Relay Networks. *IEEE Commun. Lett.* **2012**, *1*, 61–64. [CrossRef]
23. Li, R.; Wang, L.; Tao, X.; Song, M.; Han, Z. Generalized Benders Decomposition to Secure Energy-Efficient Resource Allocation for Multiuser Full-Duplex Relay Cooperative Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 10728–10741. [CrossRef]
24. Jin, Y.; Li, X.; Lv, G.; Zhao, M.; Jin, Y. Secure Resource Allocation for Cooperative OFDMA System With Untrusted AF Relaying. *IEEE Access* **2021**, *9*, 156818–156830. [CrossRef]
25. Yuan, C.; Tao, X.; Ni, W.; Li, N.; Jamalipour, A.; Liu, R.P. Optimal Power Allocation for Superposed Secrecy Transmission in Multicarrier Systems. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1332–1346. [CrossRef]
26. Khodakarami, H.; Lahouti, F. Link Adaptation with Untrusted Relay Assignment: Design and Performance Analysis. *IEEE Trans. Commun.* **2013**, *61*, 4874–4883. [CrossRef]
27. Tekin, E.; Yener, A. The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming. *IEEE Trans. Inf. Theory* **2008**, *54*, 2735–2751. [CrossRef]

28.   Zhao, W.; Wang, S. Resource Allocation for Device-to-Device Communication Underlaying Cellular Networks: An Alternating Optimization Method. *IEEE Commun. Lett.* **2015**, *19*, 1398–1401. [CrossRef]

29.   Huang, W.; Si, Q.; Jin, M. Alternating Optimization Based Low Complexity Hybrid Precoding in Millimeter Wave MIMO Systems. *IEEE Commun. Lett.* **2020**, *24*, 635–638. [CrossRef]

30.   Pham, T.M.; Farrell, R.; Tran, L.N. Revisiting the MIMO Capacity With Per-Antenna Power Constraint: Fixed-Point Iteration and Alternating Optimization. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 388–401. [CrossRef]

31.   Boyd, S.; Mutapcic, A. Subgradient Methods. In *Notes for EE364;* Standford University: Stanford, CA, USA, 2003.

32.   Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: Cambridge, UK, 2004.

33.   Kuhn, H.W. The Hungarian method for the assignment problem. *Nav. Res. Logist.* **1955**, *52*, 7–21. [CrossRef]

34.   Darsena, D.; Gelli, G.; Iudice, I.; Verde, F. Design and Performance Analysis of Channel Estimators Under Pilot Spoofing Attacks in Multiple-Antenna Systems. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3255–3269. [CrossRef]