applied sciences

MDPI

Article

Joint Resource Allocation in Secure OFDMA-Based Networks Taking a Base Station as a Two-Way Relay

Ning Du [1,2,*], Fasheng Liu [1] and Yan Zang [1]

[1] College of Electrical Engineering and Automation, Shandong University of Science and Technology, Qingdao 266590, China; fashengliu@163.com (F.L.); 13122003017@stumail.sdut.edu.cn (Y.Z.)

[2] Department of Mathematics and Information Engineering, Dongchang College of Liaocheng University, Liaocheng 252000, China

* Correspondence: lczhlydn@126.com; Tel.: +86-635-852-0373

Academic Editor: Christos Bouras

Received: 21 March 2017; Accepted: 12 May 2017; Published: 21 May 2017

Abstract: Due to the broadcast nature of wireless media, all nodes in the coverage of a transmitter are capable of capturing its signals, thus wireless transmission is sensitive to wiretapping. Several existing schemes place an emphasis on secrecy rate improvement, under the protocols of amplify-and-forward or decode-and-forward, when there are only relay users in the network. We set up a novel communication model in which normal and two-way relay users coexist in the same cell, taking the base station as a relay. Our objective is to maximize the total secrecy rate, taking subcarrier pairing, subcarrier assignment and power allocation into account, when there is one eavesdropper in one cell of the cellular network. Although this problem is very intricate, we reformulate it as a convex optimization problem by means of Lagrange duality. In order to reduce the computational complexity, equal power allocation is proposed. Lastly, the experimental results show the proposed resource allocation scheme can obtain a higher secrecy rate than traditional schemes.

Keywords: secrecy rate; two-way relay; joint resource allocation

1. Introduction

Security refers to the system resistance ability facing man-made threats such as wiretaps, attacks or tampering in the process of data transmission. With the continuous development of communication technology, security has become a main factor to measure the reliability of a communication system [1]. Due to the broadcasting characteristics of a wireless channel, the mobility of the wireless terminal and the instability of transportation, wireless communication systems are facing more security threats than traditional cable communication systems. Thus, communication privacy and information security in a wireless network has become an important factor demanding more attention, especially in fields such as military and national security. The purpose of secure communication is to ensure that legitimate users can receive source point information, while it prevents eavesdroppers in wireless networks from obtaining information [2]. The physical safety design is from the viewpoint of information theory, and makes good use of the physical characteristics of a wireless channel to achieve the purpose of transmitting information safely; such design ideas have attracted more and more attention from researchers.

Collaborative communication, for example, with the enrichment of physical layer transmission technology and physical security features, has been paid more and more attention [3]. In collaborative communication, the source point not only can broadcast information directly to the destination node, but can also complete information transmission to the destination node through the assistance of relay nodes, which use diversity gain to effectively overcome multipath fading and improve system performance. However, due to the broadcast feature of a wireless transmission environment,

the eavesdropper not only can steal information through the link between itself and source point, but also can acquire information through the link between the relay node and eavesdropper, thus increasing the likelihood of information leakage and threatening the security of the system. How to design node collaboration solutions and resource allocation strategies to ensure secure communication to prevent eavesdropping on legal information in the physical layer has become the research focus in collaborative communication in recent years [4]. Joint relay and jammer selection for secure two-way relay networks was put forward by Chen [5]. Cooperating relays were used to improve the wireless physical layer security by Dong [6]. Secure resource allocation and scheduling was put forward by D. Ng [7] in Orthogonal Frequency Division Multiple Access (OFDMA) decode-and-forward relay networks. Under the premise of ensuring secrecy rate for primary users in cognitive radio networks, power allocation, time allocation, and relay selection problem [8] were investigated. For cases when there are one or more eavesdroppers [9], a different relay cooperation scheme was put forward to ensure safe communication between the source and the destination node. In particular, a cooperative jamming scheme was presented for a two-hop relay network [10]. Considering the limited power of the relay, a kind of cooperative jamming strategy coordination strategy was put forward in which each relay sends a weighted disturbance signal in order to reduce the eavesdropper channel quality [11]. Secure communications with untrusted secondary nodes in cognitive radio networks were put forward by H. Jeon [12]. In cognitive radio networks, a kind of relay selection scheme was put forward for physical layer [13]. Diversity techniques were used to improve physical layer security in wireless communications [14]. For the Multiple-Input Multiple-Output (MIMO) channel with a multiple antenna eavesdropper, the secrecy rate optimization problem was investigated by K. Cumanan [15]. In order to improve the secrecy rate, robust beamforming technology [16] was used in systems with wireless information and power transfer. When there was an untrusted intermediate relay, the system sum secrecy rate, in which cell-edge mobile stations transmit confidential messages to the base station, was maximized by means of power allocation [17]. When a multi-antenna base station simultaneously communicated with multiple potentially malicious users in the presence of randomly located external eavesdroppers, the achievable secrecy rate was studied [18]. A cognitive relay selection algorithm was put forward for secure communication in cognitive decode-and-forward relay networks against eavesdropping [19]. When there was a sophisticated multiple antenna eavesdropper and a multiple antenna transmitter, transmit antenna selection was used in the physical layer security scheme [20]. Secure transmission in two-hop amplify-and-forward untrusted relay networks was investigated, taking power allocation into account [21]. Opportunistic multi-hop routing [22] which adopted the best of multiple receivers to forward each packet was suggested to improve throughput for a wireless network, the model of which had multiple nodes. Our model takes one base station as a relay, which is different from the scenario with multiple relays. The problem of selecting the optimal constrained candidate set was considered in the opportunistic routing paradigm [23], which also took into account of the network scenario with multiple candidate nodes. However, these two schemes place an emphasis on a routing algorithm, which is different from our objective that puts an emphasis on physical security.

Several existing schemes merely lay an emphasis on either Amplify and Forward (AF) or Decode and Forward (DF) relay to improve the secrecy rate. However, these schemes do not take normal users into account in one cell that transmits and receives information in traditional way. Our objective is to maximize the total secrecy rate by means of joint power allocation, subcarrier pairing and subcarrier assignment, when one cell has both relay users and normal users in the OFDMA network taking the base station as a two-way relay. In the next section, the system model is set up. In Section 3, the optimization problem is solved using the dual method. In Section 4, the experiments are conducted in order to test the performance of the proposed scheme. In the last section, some conclusions are given.

2. System Model

In the proposed model, there is one eavesdropper node, and there are normal users marked as $\psi = \{T_1, T_2, ..., T_K\}$ in one cell who exchange information with corresponding users in another cell.

At the same time, there are paired users marked as $\Gamma = \{(A_1, B_1), (A_2, B_2), ..., (A_M, B_M)\}$ who exchange information with each other taking the base station as a relay. M and K represent the number of paired and normal users, respectively. The OFDMA channel has N number of subcarriers marked as $\mathrm{N} = \{1, 2, ..., N\}$. To avoid interference, each subcarrier pair can only be assigned to one normal user or one paired user in the uplink and downlink. Each normal user or paired user can occupy more than one pair of subcarriers. Here, we give an example to explain the adopted communication protocol as shown in Figure 1. In the first time slot, the paired users (A_1, B_1) send information to the base station over the i-th subcarrier simultaneously, $i \in \mathrm{N}$; the normal user in the cell transmits information to normal user in another adjacent cell through the base station over the i'-th subcarrier, $i' \in \mathrm{N}$. In the second time slot, the base station amplifies the received signal from the paired user A_1 and B_1 and forwards it to B_1 and A_1 over the j-th subcarrier, $j \in \mathrm{N}$; the normal user in the cell receives information from the normal user in another adjacent cell through the base station over the j'-th subcarrier, $j' \in \mathrm{N}$. Suppose subcarrier i and j are assigned to the m-th paired users in the first and second time slot, respectively. Since nodes A_1 and B_1 know their own transmitted symbols, they can subtract the back-propagating self-interference [24]. In the first time slot, the received signal over subcarrier i at the base station is:

$$y_R^i = \sqrt{P_{A_m}^i} h_{A_m,R}^i x_{A_m,i} + \sqrt{P_{B_m}^i} h_{B_m,R}^i x_{B_m,i} + n_{R,i}. \tag{1}$$

where $i \in$, $x_{A_m,i}$ and $x_{B_m,i}$ are the transmitted complex Gaussian signal with a mean of zero and a variance of 1 on subcarrier i from A_m and B_m respectively; $P_{A_m}^i$ and $P_{B_m}^i$ are the transmit power of A_m and B_m over subcarrier i; $h_{A_m,R}^i$ and $h_{B_m,R}^i$ are the channel gain over subcarrier i from A_m and B_m to the base station, respectively; $n_{R,i}$ is Additive White Gaussian Noise (AWGN) at the base station over subcarrier i with a mean of zero and a variance of σ^2, $m \in \{1, 2, ..., M\}$. It is assumed that all the channel state information in the network is perfectly known at the central controller, which can be embedded within the base station or the user [25]. The purpose of perfect channel status information is to provide a performance reference for a real system. The received signal at the eavesdropper over subcarrier i is:

$$y_E^i = \sqrt{P_{A_m}^i} h_{A_m,E}^i x_{A_m,i} + \sqrt{P_{B_m}^i} h_{B_m,E}^i x_{B_m,i} + n_{E,i}. \tag{2}$$

where $h_{A_m,E}^i$ and $h_{B_m,E}^i$ are the channel gain over subcarrier i from A_m and B_m to the eavesdropper, respectively; $n_{E,i}$ is Additive White Gaussian Noise at the eavesdropper over subcarrier i with a mean of zero and a variance of σ^2. In the second time slot, the base station amplifies the received signal and broadcasts the signal on subcarrier j with amplification factor $\beta_{m,i}$ and transmit power $P_{R,(A_m,B_m)}^j$.

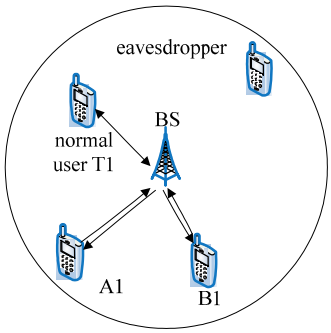

Figure 1. System model.

$$\beta_{m,i} = \frac{\sqrt{P_{R,(A_m,B_m)}^j}}{\alpha} = \frac{\sqrt{P_{R,(A_m,B_m)}^j}}{P_{A_m}^i |h_{A_m,R}^i|^2 + P_{B_m}^i |h_{B_m,R}^i|^2 + \sigma^2}. \tag{3}$$

$\alpha = P^i_{A_m}|h^i_{A_m,R}|^2 + P^i_{B_m}|h^i_{B_m,R}|^2 + \sigma^2$, the received signal at A_m and B_m over subcarrier j in the second time slot are $y^{i,j}_{A_m}$ and $y^{i,j}_{B_m}$ respectively.

$$y^{i,j}_{A_m} = \sqrt{P^j_{R,(A_m,B_m)}}g^j_{A_m}y^i_R/\alpha + n_{A_m,j}$$
$$y^{i,j}_{B_m} = \sqrt{P^j_{R,(A_m,B_m)}}g^j_{B_m}y^i_R/\alpha + n_{B_m,j}$$

Substituting y^i_R into the above two equations, we get:

$$\begin{aligned} y^{i,j}_{A_m} &= \sqrt{P^j_{R,(A_m,B_m)}}g^j_{A_m}\left(\sqrt{P^i_{A_m}}h^i_{A_m,R}x_{A_m,i} + \sqrt{P^i_{B_m}}h^i_{B_m,R}x_{B_m,i} + n_{R,i}\right)/\alpha + n_{A_m,j} \\ &= \sqrt{P^j_{R,(A_m,B_m)}}g^j_{A_m}\sqrt{P^i_{A_m}}h^i_{A_m,R}x_{A_m,i}/\alpha + \sqrt{P^j_{R,(A_m,B_m)}}g^j_{A_m}\sqrt{P^i_{B_m}}h^i_{B_m,R}x_{B_m,i}/\alpha \\ &+ \sqrt{P^j_{R,(A_m,B_m)}}g^j_{A_m}n_{R,i}/\alpha + n_{A_m,j} \end{aligned} \tag{4}$$

and

$$\begin{aligned} y^{i,j}_{B_m} &= \sqrt{P^j_{R,(A_m,B_m)}}g^j_{B_m}\left(\sqrt{P^i_{A_m}}h^i_{A_m,R}x_{A_m,i} + \sqrt{P^i_{B_m}}h^i_{B_m,R}x_{B_m,i} + n_{R,i}\right)/\alpha + n_{B_m,j} \\ &= \sqrt{P^j_{R,(A_m,B_m)}}g^j_{B_m}\sqrt{P^i_{A_m}}h^i_{A_m,R}x_{A_m,i}/\alpha + \sqrt{P^j_{R,(A_m,B_m)}}g^j_{B_m}\sqrt{P^i_{B_m}}h^i_{B_m,R}x_{B_m,i}/\alpha \\ &+ \sqrt{P^j_{R,(A_m,B_m)}}g^j_{B_m}n_{R,i}/\alpha + n_{B_m,j} \end{aligned} \tag{5}$$

$g^j_{A_m}$ and $g^j_{B_m}$ are the downlink channel gain over subcarrier j from the base station to A_m and B_m respectively; $n_{A_m,j}$ and $n_{B_m,j}$ are Additive White Gaussian Noise over subcarrier j at A_m and B_m with a mean of zero and a variance of σ^2. The received signal on subcarrier j at the eavesdropper in the second time slot is $y^{i,j}_E = \sqrt{P^j_{R,(A_m,B_m)}}g^j_{R,E}y^i_R/\alpha + n_{E,j}$. Substituting y^i_R into this equation, we get:

$$\begin{aligned} y^{i,j}_E &= \sqrt{P^j_{R,(A_m,B_m)}}g^j_{R,E}\left(\sqrt{P^i_{A_m}}h^i_{A_m,R}x_{A_m,i} + \sqrt{P^i_{B_m}}h^i_{B_m,R}x_{B_m,i} + n_{R,i}\right)/\alpha + n_{E,j} \\ &= \sqrt{P^j_{R,(A_m,B_m)}}g^j_{R,E}\sqrt{P^i_{A_m}}h^i_{A_m,R}x_{A_m,i}/\alpha + \sqrt{P^j_{R,(A_m,B_m)}}g^j_{R,E}\sqrt{P^i_{B_m}}h^i_{B_m,R}x_{B_m,i}/\alpha \\ &+ \sqrt{P^j_{R,(A_m,B_m)}}g^j_{R,E}n_{R,i}/\alpha + n_{E,j} \end{aligned} \tag{6}$$

$g^j_{R,E}$ is the channel gain between the base station and the eavesdropper over subcarrier j and $n_{E,j}$ is Additive White Gaussian Noise at the eavesdropper over subcarrier j with a mean of zero and a variance of σ^2. According to the fact that the secrecy capacity of a Gaussian wiretap channel is the difference between the main channel and the wiretap channel [26], we can conclude that the achievable secure rate for A_m and B_m is:

$$R^{i,j}_{\text{sec},m} = \left[R^{i,j}_{A_m} + R^{i,j}_{B_m} - R^{i,j}_E\right]^+. \tag{7}$$

$$R^{i,j}_{A_m} = \frac{1}{2}\log\left(1 + SNR^{i,j}_{A_m}\right). \tag{8}$$

$$R^{i,j}_{B_m} = \frac{1}{2}\log\left(1 + SNR^{i,j}_{B_m}\right). \tag{9}$$

$$R^{i,j}_E = \frac{1}{2}\log\det(\boldsymbol{I} + \boldsymbol{H}_E\boldsymbol{H}^H_E\boldsymbol{Q}^{-1}_E). \tag{10}$$

$R^{i,j}_{A_m} + R^{i,j}_{B_m}$ is the main channel capacity between the paired user and the base station, $R^{i,j}_E$ is the wiretap channel capacity when the eavesdropper is wiretapping the communication process between the paired user and the base station, $[x]^+ = \max\{0, x\}$, and $\boldsymbol{I}$ is a unit vector.

$$\boldsymbol{H}_E = \begin{bmatrix} \sqrt{P^i_{A_m}}h^i_{A_m,E} & \sqrt{P^i_{B_m}}h^i_{B_m,E} \\ \sqrt{P^j_{R,(A_m,B_m)}}g^j_{R,E}\sqrt{P^i_{A_m}}h^i_{A_m,R}/\alpha & \sqrt{P^j_{R,(A_m,B_m)}}g^j_{R,E}\sqrt{P^i_{B_m}}h^i_{B_m,R}/\alpha \end{bmatrix} \tag{11}$$

$$\boldsymbol{Q}_E = \sigma^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 + P^j_{R,(A_m,B_m)} |g^j_{R,E}|^2/\alpha^2 \end{bmatrix} \tag{12}$$

$$\begin{aligned} SNR^{i,j}_{A_m} &= \frac{P^j_{R,(A_m,B_m)} |g^j_{A_m}|^2 P^i_{B_m} |h^i_{B_m,R}|^2/\alpha^2}{\left(P^j_{R,(A_m,B_m)} |g^j_{A_m}|^2/\alpha^2 + 1\right)\sigma^2}, \\ SNR^{i,j}_{B_m} &= \frac{P^j_{R,(A_m,B_m)} |g^j_{B_m}|^2 P^i_{A_m} |h^i_{A_m,R}|^2/\alpha^2}{\left(P^j_{R,(A_m,B_m)} |g^j_{B_m}|^2/\alpha^2 + 1\right)\sigma^2} \end{aligned} \tag{13}$$

$$\begin{aligned} &\det(\boldsymbol{I} + \boldsymbol{H}_E \boldsymbol{H}_E^H \boldsymbol{Q}_E^{-1}) \\ &= \frac{P^i_{A_m} P^i_{B_m} (|h^i_{A_m,E}|^2 |h^i_{B_m,R}|^2 + |h^i_{B_m,E}|^2 |h^i_{A_m,R}|^2) + \sigma^2 (P^i_{A_m} |h^i_{A_m,E}|^2 + P^i_{B_m} |h^i_{B_m,E}|^2 + P^i_{A_m} |h^i_{A_m,R}|^2 + P^i_{B_m} |h^i_{B_m,R}|^2)}{\sigma^4} \\ &- \frac{P^i_{A_m} P^i_{B_m} 2\mathrm{Re}\left\{h^i_{A_m,E} (h^i_{B_m,E})^* (h^i_{A_m,R})^* h^i_{B_m,R}\right\}}{\sigma^4} + 1. \end{aligned} \tag{14}$$

Substituting the above equations into (7), the achievable secure rate for the paired user is expressed as:

$$\begin{aligned} &R^{i,j}_{\mathrm{sec},m} \\ &= \frac{1}{2} \log \left\{ \frac{\left(P^j_{R,(A_m,B_m)} |g^j_{A_m}|^2/\alpha^2 + 1\right)\sigma^2 + P^j_{R,(A_m,B_m)} |g^j_{A_m}|^2 P^i_{B_m} |h^i_{B_m,R}|^2/\alpha^2}{\left(P^j_{R,(A_m,B_m)} |g^j_{A_m}|^2/\alpha^2 + 1\right)} \right. \\ &\left. \cdot \frac{\left(P^j_{R,(A_m,B_m)} |g^j_{B_m}|^2/\alpha^2 + 1\right)\sigma^2 + P^j_{R,(A_m,B_m)} |g^j_{B_m}|^2 P^i_{A_m} |h^i_{A_m,R}|^2/\alpha^2}{\left(P^j_{R,(A_m,B_m)} |g^j_{B_m}|^2/\alpha^2 + 1\right)} \right\} \\ &- \frac{1}{2} \log \left\{ P^i_{A_m} P^i_{B_m} (|h^i_{A_m,E}|^2 |h^i_{B_m,R}|^2 + |h^i_{B_m,E}|^2 |h^i_{A_m,R}|^2) + \sigma^2 (P^i_{A_m} |h^i_{A_m,E}|^2 + P^i_{B_m} |h^i_{B_m,E}|^2 \right. \\ &\left. + P^i_{A_m} |h^i_{A_m,R}|^2 + P^i_{B_m} |h^i_{B_m,R}|^2) - P^i_{A_m} P^i_{B_m} 2\mathrm{Re}\left\{h^i_{A_m,E} (h^i_{B_m,E})^* (h^i_{A_m,R})^* h^i_{B_m,R}\right\} + \sigma^4 \right\} \end{aligned} \tag{15}$$

The achievable secure rate for the normal user T_k, $k \in \{1, 2, ..., K\}$ is:

$$R^{i,j}_{\mathrm{sec},T_k} = \left[R^{i,j}_{T_k,R} - R^{i,j}_{T_k,E}\right]^+. \tag{16}$$

$$R^{i,j}_{T_k,R} = \frac{1}{4} \left\{ \log\left(1 + \frac{|h^i_{T_k,R}|^2 P^i_{T_k}}{\sigma^2}\right) + \log\left(1 + \frac{|g^j_{R,T_k}|^2 P^j_{R,T_k}}{\sigma^2}\right) \right\} \tag{17}$$

$$R^{i,j}_{T_k,E} = \frac{1}{4} \left\{ \log\left(1 + \frac{|h^i_{T_k,E}|^2 P^i_{T_k}}{\sigma^2}\right) + \log\left(1 + \frac{|g^j_{R,E}|^2 P^j_{R,T_k}}{\sigma^2}\right) \right\} \tag{18}$$

$R^{i,j}_{T_k,R}$ is the main channel capacity between the normal user and the base station, $R^{i,j}_{T_k,E}$ is the wiretap channel capacity when the eavesdropper is wiretapping the communication process between the normal user and the base station, $h^i_{T_k,R}$ and g^j_{R,T_k} are the uplink and downlink channel gains between the normal user T_k and the base station over subcarrier i and j respectively; $h^i_{T_k,E}$ is the channel gain between the normal user T_k and the eavesdropper over subcarrier i. $P^i_{T_k}$ is the uplink transmit power from the normal user T_k to the base station and P^i_{R,T_k} is the downlink transmit power from the base station to the normal user T_k over subcarrier i. We define two indicator functions to represent subcarrier assignment and subcarrier pairing. $\pi_{i,j} = 1$ or $\eta_{i,j} = 1$ means that the uplink subcarrier i is paired with the downlink subcarrier j for the normal user or the paired users; otherwise, $\pi_{i,j} = 0$ or $\eta_{i,j} = 0$. $\rho^{i,j}_k = 1$ or $\rho^{i,j}_m = 1$ means that the uplink subcarrier i and the downlink subcarrier j are assigned to the k-th normal user or the m-th paired users; otherwise, $\rho^{i,j}_k = 0$ or $\rho^{i,j}_m = 0$. In the cellular network that has paired and normal users, we can realize secrecy communication without information leakage [26], if the information transmission rate is less than the maximum secrecy

rate. Firstly, we need to investigate the problem of maximizing the total secrecy rate for paired and normal users in one cell by means of subcarrier assignment, subcarrier pairing and power allocation. This primary optimization problem can be expressed as:

$$\begin{aligned}
&\underset{\boldsymbol{\pi},\boldsymbol{\rho},\boldsymbol{\eta},\boldsymbol{P}}{\text{maxmize}}\left(\sum_{k=1}^{K}\sum_{i=1}^{N}\sum_{j=1}^{N}\pi_{i,j}\rho_k^{i,j}R_{\text{sec},T_k}^{i,j}+\sum_{m=1}^{M}\sum_{i=1}^{N}\sum_{j=1}^{N}\eta_{i,j}\rho_m^{i,j}R_{\text{sec},m}^{i,j}\right).\\
&\text{s.t.}\sum_{j=1}^{N}\left(\sum_{m=1}^{M}P_{R,(A_m,B_m)}^{j}+\sum_{k=1}^{K}P_{R,T_k}^{j}\right)\le P_{totalB}.\\
&\rho\in\{0,1\},\ \eta\in\{0,1\}.\\
&\sum_{T_k\in\Psi}\rho_k^{i,j}+\sum_{(A_m,B_m)\in\Gamma}\rho_m^{i,j}=1,\forall i\in 1,2,...,N;k=1,2,...,K;m=1,2,...,M.\\
&\sum_{T_k\in\Psi}\rho_k^{i,j}+\sum_{(A_m,B_m)\in\Gamma}\rho_m^{i,j}=1,\forall j\in 1,2,...,N;k=1,2,...,K;m=1,2,...,M.
\end{aligned}\tag{19}$$

$\boldsymbol{\pi}=\{\pi_{i,j}\}$ and $\boldsymbol{\eta}=\{\eta_{i,j}\}$ are the sets of all possible subcarrier pairings; $\boldsymbol{\rho}=\{\rho_k^{i,j},\rho_m^{i,j}\}$ is the set of all possible subcarrier-user assignments; and $\boldsymbol{P}=\{P_{R,T_k}^{j},P_{R,(A_m,B_m)}^{j}\}$ is the set of all possible power allocations for the given subcarrier pairing and subcarrier assignment, which satisfies $P_{R,T_k}^{j}\ge 0$, $P_{R,(A_m,B_m)}^{j}\ge 0$ for $\pi_{i,j}\rho_k^{i,j}=1$, $\eta_{i,j}\rho_m^{i,j}=1$ and $P_{R,T_k}^{j}=0$, $P_{R,(A_m,B_m)}^{j}=0$ for $\pi_{i,j}\rho_k^{i,j}=0$, $\eta_{i,j}\rho_m^{i,j}=0$. This is a mixed integer programming problem, the solving process of which is very complicated. However, we can relax $\rho\in[0,1]$ and $\eta\in[0,1]$ to get the near the optimal solution. In the next section, the dual method is used to solve this optimization problem.

3. Problem Solution

After relaxing $\rho\in[0,1]$ and $\eta\in[0,1]$, we can see that all constraints of problem (19) are affine and the target function is concave, therefore the Slater's condition is satisfied. This optimization problem can be solved by the Lagrange dual method with a zero duality gap [27]. Because the dual function is always concave and the constraints are convex [27], the primary problem is transformed into convex optimization. λ is the dual variable associated with the total power constraints at the base station. The Lagrange dual function for (19) is:

$$g(\lambda)=\underset{\boldsymbol{\pi},\boldsymbol{\rho},\boldsymbol{P}}{\text{maxmize}}L(\boldsymbol{\pi},\boldsymbol{\eta},\boldsymbol{\rho},\boldsymbol{P},\lambda)\tag{20}$$

This is a maximization problem, and is solved in three phases step-by-step using convex optimization.

$$\begin{aligned}
&L(\boldsymbol{\pi},\boldsymbol{\eta},\boldsymbol{\rho},\boldsymbol{P},\lambda)\\
&=\sum_{k=1}^{K}\sum_{i=1}^{N}\sum_{j=1}^{N}\pi_{i,j}\rho_k^{i,j}R_{\text{sec},T_k}^{i,j}+\sum_{m=1}^{M}\sum_{i=1}^{N}\sum_{j=1}^{N}\eta_{i,j}\rho_m^{i,j}R_{\text{sec},m}^{i,j}-\lambda\cdot\sum_{j=1}^{N}\left(\sum_{m=1}^{M}P_{R,(A_m,B_m)}^{j}+\sum_{k=1}^{K}P_{R,T_k}^{j}\right)+\lambda P_{totalB}\\
&=\sum_{j=1}^{N}\sum_{k=1}^{K}\sum_{i=1}^{N}(\pi_{i,j}\rho_k^{i,j}R_{\text{sec},T_k}^{i,j}-\lambda\cdot P_{R,T_k}^{j})+\sum_{j=1}^{N}\sum_{m=1}^{M}\sum_{i=1}^{N}(\eta_{i,j}\rho_m^{i,j}R_{\text{sec},m}^{i,j}-\lambda\cdot P_{R,(A_m,B_m)}^{j})+\lambda P_{totalB}\\
&=\sum_{j=1}^{N}L_{j,k}(\pi_{i,j},\rho_k^{i,j},P_{R,T_k}^{j},\lambda)+\sum_{j=1}^{N}L_{j,m}(\eta_{i,j},\rho_m^{i,j},P_{R,(A_m,B_m)}^{j},\lambda)+\lambda P_{totalB}
\end{aligned}\tag{21}$$

$$L_{j,k}(\pi_{i,j},\rho_k^{i,j},P_{R,T_k}^{j},\lambda)=\sum_{i=1}^{N}\sum_{k=1}^{K}(\pi_{i,j}\rho_k^{i,j}R_{\text{sec},T_k}^{i,j}-\lambda\cdot P_{R,T_k}^{j})\tag{22}$$

$$L_{j,m}(\eta_{i,j},\rho_m^{i,j},P_{R,(A_m,B_m)}^{j},\lambda)=\sum_{i=1}^{N}\sum_{m=1}^{M}(\eta_{i,j}\rho_m^{i,j}R_{\text{sec},m}^{i,j}-\lambda\cdot P_{R,(A_m,B_m)}^{j}).\tag{23}$$

The dual problem can be expressed as:

$$\begin{aligned} &\underset{\lambda}{\text{minmize}} g(\lambda). \\ &\text{s.t. } \lambda \geq 0 \end{aligned} \tag{24}$$

This is a convex optimization problem, which can be solved by the sub-gradient method with guaranteed convergence [28]. The derived sub-gradient of $g(\lambda)$ is:

$$\begin{aligned} \Delta\lambda &= P_{totalB} - \sum_{j=1}^{N}\left(\sum_{m=1}^{M}\widehat{P}^{j}_{R,(A_m,B_m)} + \sum_{k=1}^{K}\widehat{P}^{j}_{R,T_k}\right) \\ \lambda^{(l+1)} &= \lambda^{(l)} + \varepsilon^{(l)}\Delta\lambda \end{aligned} \tag{25}$$

ε is the step size in the l-th iteration; $\widehat{\rho}^{i,j}_{k}$ and $\widehat{\rho}^{i,j}_{m}$ are the optimal power allocations at the dual point, which can be found in the following step.

Step 1. For fixed $\pi_{i,j} = 1$ and $\rho^{i,j}_{k} = 1$, according to Karush-Kuhn-Tucker condition, the solution is the non-negative real root of the quadratic function.

$$\begin{aligned} &\left[4\lambda(\ln 2)|g^{j}_{R,T_k}|^2|g^{j}_{R,E}|^2\right]\left(P^{j}_{R,T_k}\right)^2 + \left[4\lambda\sigma^2(\ln 2)[|g^{j}_{R,T_k}|^2 + |g^{j}_{R,E}|^2]\right]P^{j}_{R,T_k} \\ &+4\lambda(\ln 2)\sigma^4 - \sigma^2\left(|g^{j}_{R,T_k}|^2 - |g^{j}_{R,E}|^2\right) = 0 \end{aligned} \tag{26}$$

The solution is:

$$\begin{aligned} \widehat{P}^{j}_{R,T_k} &= \frac{\sqrt{\left[|g^{j}_{R,T_k}|^2 - |g^{j}_{R,E}|^2\right]^2 16\lambda^2\sigma^4(\ln 2)^2 - 16\lambda(\ln 2)|g^{j}_{R,T_k}|^2|g^{j}_{R,E}|^2\sigma^2[|g^{j}_{R,T_k}|^2 - |g^{j}_{R,E}|^2]}}{8\lambda(\ln 2)|g^{j}_{R,T_k}|^2|g^{j}_{R,E}|^2} \\ &- \frac{\sigma^2}{2|g^{j}_{R,T_k}|^2|g^{j}_{R,E}|^2} \end{aligned} \tag{27}$$

For fixed $\eta_{i,j} = 1$ and $\rho^{i,j}_{m} = 1$, by solving $\frac{dR^{i,j}_{\text{sec},m}}{dP^{j}_{R,(A_m,B_m)}} = 0$, we can obtian the optimal solution $\widehat{P}^{j}_{R,(A_m,B_m)}$ expressed as a non-negative real root of the quartic function.

$$\begin{aligned} &a\left(P^{j}_{R,(A_m,B_m)}\right)^4 + b\left(P^{j}_{R,(A_m,B_m)}\right)^3 + c\left(P^{j}_{R,(A_m,B_m)}\right)^2 + dP^{j}_{R,(A_m,B_m)} + e = 0. \\ &a = 2\lambda(\ln 2)\Big[\sigma^8|g^{j}_{A_m}|^4|g^{j}_{B_m}|^4 + \sigma^6 P^{i}_{A_m}|h^{i}_{A_m,R}|^2|g^{j}_{A_m}|^4|g^{j}_{B_m}|^4 \\ &+P^{i}_{B_m}\sigma^6|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^4|g^{j}_{B_m}|^4 + \sigma^4 P^{i}_{A_m}P^{i}_{B_m}|h^{i}_{A_m,R}|^2|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^4|g^{j}_{B_m}|^4\Big] \\ &b = 2\lambda(\ln 2)\big\{[2\sigma^4\alpha^2|g^{j}_{A_m}|^2 + \sigma^2\alpha^2 P^{i}_{B_m}|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^2]\cdot[\sigma^4|g^{j}_{B_m}|^4 + \sigma^2 P^{i}_{A_m}|h^{i}_{A_m,R}|^2|g^{j}_{B_m}|^4] \\ &+[2\sigma^4\alpha^2|g^{j}_{B_m}|^2 + \sigma^2\alpha^2 P^{i}_{A_m}|h^{i}_{A_m,R}|^2|g^{j}_{B_m}|^2]\cdot[\sigma^4|g^{j}_{A_m}|^4 + \sigma^2 P^{i}_{B_m}|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^4\big\} \\ &c = 2\lambda(\ln 2)\big\{[\sigma^8\alpha^4|g^{j}_{B_m}|^4 + \sigma^6\alpha^4 P^{i}_{A_m}|h^{i}_{A_m,R}|^2|g^{j}_{B_m}|^4 + \sigma^8\alpha^4|g^{j}_{A_m}|^4 + \sigma^6\alpha^4 P^{i}_{B_m}|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^4] \\ &+[2\sigma^4\alpha^2|g^{j}_{B_m}|^2 + \sigma^2\alpha^2 P^{i}_{A_m}|h^{i}_{A_m,R}|^2|g^{j}_{B_m}|^2]\cdot[2\sigma^4\alpha^2|g^{j}_{A_m}|^2 + \sigma^2\alpha^2 P^{i}_{B_m}|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^2]\big\} \\ &-\sigma^6\alpha^2 P^{i}_{B_m}|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^2|g^{j}_{B_m}|^4 - \sigma^4\alpha^2 P^{i}_{A_m}P^{i}_{B_m}|h^{i}_{A_m,R}|^2|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^2|g^{j}_{B_m}|^4 \\ &-\sigma^6\alpha^2 P^{i}_{A_m}|h^{i}_{A_m,R}|^2|g^{j}_{A_m}|^4|g^{j}_{B_m}|^2 - \sigma^4\alpha^2 P^{i}_{A_m}P^{i}_{B_m}|h^{i}_{A_m,R}|^2|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^4|g^{j}_{B_m}|^2 \\ &d = 2\lambda(\ln 2)[2\sigma^8\alpha^6|g^{j}_{B_m}|^2 + \sigma^6\alpha^6 P^{i}_{A_m}|h^{i}_{A_m,R}|^2|g^{j}_{B_m}|^2 + 2\sigma^8\alpha^6|g^{j}_{A_m}|^2 + \sigma^6\alpha^6 P^{i}_{B_m}|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^2 \\ &-2\sigma^6\alpha^4 P^{i}_{B_m}|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^2|g^{j}_{B_m}|^2 - 2\sigma^4\alpha^4 P^{i}_{A_m}P^{i}_{B_m}|h^{i}_{A_m,R}|^2|h^{i}_{B_m,R}|^2|g^{j}_{A_m}|^2|g^{j}_{B_m}|^2 \\ &-2\sigma^6\alpha^4 P^{i}_{A_m}|h^{i}_{A_m,R}|^2|g^{j}_{A_m}|^2|g^{j}_{B_m}|^2 \end{aligned} \tag{28}$$

$$e = 2\lambda(\ln 2)[2\sigma^8\alpha^6|g^j_{B_m}|^2 + \sigma^6\alpha^6 P^i_{A_m}|h^i_{A_m,R}|^2|g^j_{B_m}|^2 + 2\sigma^8\alpha^6|g^j_{A_m}|^2 + \sigma^6\alpha^6 P^i_{B_m}|h^i_{B_m,R}|^2|g^j_{A_m}|^2]$$
$$-\sigma^6\alpha^6 P^i_{B_m}|h^i_{B_m,R}|^2|g^j_{A_m}|^2 - \sigma^6\alpha^6 P^i_{A_m}|h^i_{A_m,R}|^2|g^j_{B_m}|^2$$

Step 2. In the above step, we achieve the optimal $\widehat{P}^j_{R,T_k}$ and $\widehat{P}^j_{R,(A_m,B_m)}$. For the given subcarrier pairing strategy $\pi_{i,j} = 1$, $\eta_{i,j} = 1$, the subcarrier assignment can be expressed as:

$$\max_{\pi,\rho}\left\{\sum_{j=1}^{N} L_{j,k}(\pi_{i,j}, \rho^{i,j}_k, \widehat{P}^j_{R,T_k}, \lambda) + \sum_{j=1}^{N} L_{j,m}(\eta_{i,j}, \rho^{i,j}_m, \widehat{P}^j_{R,(A_m,B_m)}, \lambda) + \lambda P_{totalB}\right\} \tag{29}$$

The solution is:

$$\widehat{\rho}^{i,j}_k = \begin{cases} 1, & k = k(i,j) = \underset{k}{\operatorname{argmax}}\left(L_{j,k}(\pi_{i,j}, \rho^{i,j}_k, \widehat{P}^j_{R,T_k}, \lambda) + L_{j,m}(\eta_{i,j}, \rho^{i,j}_m, \widehat{P}^j_{R,(A_m,B_m)}, \lambda)\right) \\ 0, & otherwise \end{cases}. \tag{30}$$

$$\widehat{\rho}^{i,j}_m = \begin{cases} 1, & m = m(i,j) = \underset{m}{\operatorname{argmax}}\left(L_{j,k}(\pi_{i,j}, \rho^{i,j}_k, \widehat{P}^j_{R,T_k}, \lambda) + L_{j,m}(\eta_{i,j}, \rho^{i,j}_m, \widehat{P}^j_{R,(A_m,B_m)}, \lambda)\right) \\ 0, & otherwise \end{cases} \tag{31}$$

Step 3. For the given $\widehat{P}^j_{R,T_k}$, $\widehat{P}^j_{R,(A_m,B_m)}$, $\widehat{\rho}^{i,j}_k$ and $\widehat{\rho}^{i,j}_m$, the subcarrier pairing is expressed as:

$$\max_{\pi}\left\{\sum_{j=1}^{N} (L_{j,k}(\pi_{i,j}, \widehat{\rho}^{i,j}_k, \widehat{P}^j_{R,T_k}, \lambda) + L_{j,m}(\eta_{i,j}, wide\hat{\rho}^{i,j}_m, \widehat{P}^j_{R,(A_m,B_m)}, \lambda))\right\}. \tag{32}$$

Inserting $\widehat{P}^j_{R,T_k}$ and $\widehat{P}^j_{R,(A_m,B_m)}$ into Equations (15) and (16), we get $\widehat{R}^{i,j}_{\mathrm{sec},m}$ and $\widehat{R}^{i,j}_{\mathrm{sec},T_k}$. Formula (32) can be expressed as:

$$\text{maxmize} \sum_{i=1}^{N}\sum_{j=1}^{N} \pi_{i,j}\hat{R}^{i,j}_{\mathrm{sec},T_k} + \sum_{i=1}^{N}\sum_{j=1}^{N} \eta_{i,j}\widehat{R}^{i,j}_{\mathrm{sec},m} - \lambda\left(\sum_{j=1}^{N} (\hat{P}^j_{R,T_k} + \widehat{P}^j_{R,(A_m,B_m)})\right). \tag{33}$$

So, we only need to maximize:

$$\sum_{i=1}^{N}\sum_{j=1}^{N} \pi_{i,j}\widehat{R}^{i,j}_{\mathrm{sec},T_k} + \sum_{i=1}^{N}\sum_{j=1}^{N} \eta_{i,j}\widehat{R}^{i,j}_{\mathrm{sec},m} \tag{34}$$

We define two profit matrices $[\widehat{R}^{i,j}_{\mathrm{sec},m}]_{N\times N}$ and $[\widehat{R}^{i,j}_{\mathrm{sec},T_k}]_{N\times N}$. In order to maximize (34), we need to pick elements in the two profit matrices to make the sum of profits maximization. This is obviously a standard linear assignment problem [27], which can be efficiently solved by the Hungarian method.

4. Simulation Results and Discussion

In order to verify the effectiveness of the proposed algorithm, computer simulations are carried out. The path-loss exponent is set to 3, and the adopted wireless broadband frequency selective fading channel model is Stanford University Interim-6, each channel of which is a six-tap channel. The first tap follows Ricean distribution, while the other five taps follow Rayleigh distribution. There is only one eavesdropper in one cell. All the users are deployed 40 m away from the base station and the eavesdropper is 200 m away from the base station. The noise power σ^2 is -119 dBm. There are two simulation scenarios.

(1) Two normal users and two paired users with 32 subcarriers
(2) Four normal users and four paired users with 64 subcarriers

The relation between secrecy spectral efficiency and base station transmitting power is shown in Figure 2 when all the users have the same transmitting power of 2 dBm over all subcarriers in the uplink. The equal power allocation method means to allocate equal power to all users, which is less complicated than the proposed scheme. For the conventional scheme, there is no subcarrier pairing or subcarrier assignment.

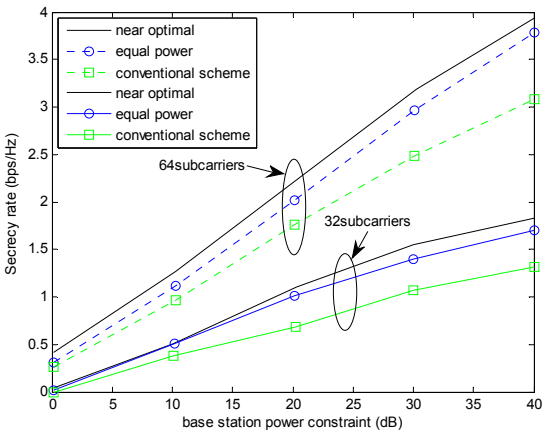

Figure 2. Secrecy spectral efficiency versus base station transmitting power.

It can be seen that the total secrecy spectral efficiency rises with the increase of transmitting power. The total secrecy spectral efficiency under the condition with 48 subcarriers is higher than the secrecy spectral efficiency under the condition with 32 subcarriers. This is because the second scenario with 48 subcarriers has more users, which can increase the signal-to-noise ratio. The relation between secrecy spectral efficiency and user transmitting power is shown in Figure 3, when the base station has a transmitting power of 20 dBm. It can be seen that the secrecy spectral efficiency rises with the increase of user signal-to-noise ratio. The proposed scheme has the largest secrecy spectral efficiency. The equal power allocation method almost has the same secrecy spectral efficiency as the proposed scheme when the number of subcarriers is small at a low signal-to-noise ratio. When the signal-to-noise ratio is about 43 dB, the secrecy spectral efficiency tends to be stable. This is because the capacity of the wiretap channel grows with the increase of user signal-to-noise ratio. From Equation (15), we can see that the mean value of the secrecy spectral efficiency is a constant for fixed power at the base station, which is relevant to the channel characteristics.

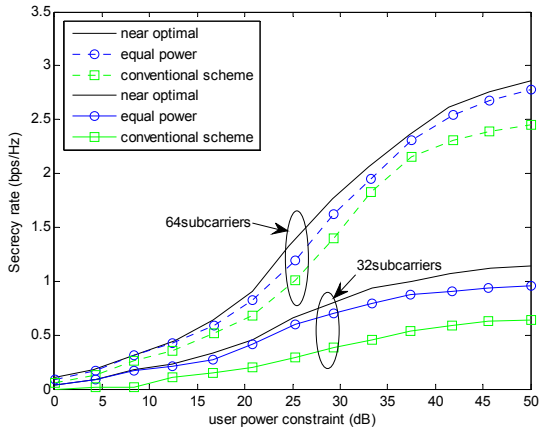

Figure 3. Secrecy spectral efficiency versus user transmitting power.

5. Conclusions and Future Research

We have set up the mathematical model to maximize the total secrecy rate when paired and normal users coexists in one cell. We take into account the joint optimization problem consisting of subcarrier pairing, subcarrier assignment and power allocation. The optimization problem belongs to mixed integer programming, which is very complicated. We solve this problem in a dual domain and put forward the equal power allocation method to reduce the calculation complexity. Simulation results show that the proposed scheme can improve the secrecy rate compared to conventional schemes, and the secrecy spectral efficiency tends to be stable at a high signal-to-noise ratio, because the mean value of the secrecy spectral efficiency is a constant for fixed power at the base station. As the user power reaches infinity, the average secrecy spectral efficiency expressed as Equation (15) can be worked out according to channel statistical characteristics. Recently, related issues in cooperative communication, such as wireless resource allocation, relay selection, physical-layer security, energy harvesting and the relationship between nodes, have triggered a great deal of research interest. Based on these research topics, we further investigate some key technologies of cooperative communication. In the future, we will take into account the possibility of an eavesdropper with multiple antennas. However, the perfect channel state information only makes sense in a slowly changing environment. In actual wireless links, due to a series of uncertain factors such as channel estimation error, quantization error and feedback delay, it is difficult to obtain full channel state information. Therefore, it is very important to establish the optimization model of partial channel status information for the application of the actual system in our future research.

Acknowledgments: The authors would like to express their acknowledgement for the support from the Natural Science Foundation of Shandong Province in China (ZR2015FL028), Science and Technology Plan Project of the Educational Department of Shandong Province of China (No. J16LI12) and project of the 13th five-year planning of education science in Shandong Province (Joint resource allocation research in OFDMA relay network based on convex optimization).

Author Contributions: Ning Du conceived and designed the experiments; Ning Du analyzed the data and wrote the paper; Yan Zang performed the experiments; and Fansheng Liu provided some suggestions and revised the paper.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. Wang, X.; Tao, M.; Mo, J.; Xu, Y. Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 693–702. [CrossRef]
2. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Di Renzo, M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [CrossRef]
3. Yang, Y.; Li, Q.; Ma, W.K.; Ge, J.; Ching, P.C. Cooperative secure beamforming for AF relay networks with multiple eavesdroppers. *IEEE Signal Process. Lett.* **2013**, *20*, 35–38. [CrossRef]
4. Li, Q.; Yang, Y.; Ma, W.K.; Lin, M.; Ge, J.; Lin, J. Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks. *IEEE Trans. Signal Process.* **2015**, *63*, 206–220. [CrossRef]
5. Chen, J.C.; Zhang, R.Q.; Song, L.Y.; Han, Z.; Jiao, B.L. Joint Relay and Jammer Selection for Secure Two-Way Relay Networks. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 310–320. [CrossRef]
6. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888. [CrossRef]
7. Ng, D.; Lo, E.; Schober, R. Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 3528–3540. [CrossRef]
8. Mokari, N.; Parsaeefard, S.; Saeedi, H.; Azmi, P. Cooperative Secure Resource Allocation in Cognitive Radio Networks with Guaranteed Secrecy Rate for Primary Users. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1058–1073. [CrossRef]

9. Li, J.; Petropulu, A.P.; Weber, S. On cooperative relaying schemes for wireless physical layer security. *IEEE Trans. Signal Process.* **2011**, *59*, 4985–4997. [CrossRef]
10. Huang, J.; Swindlehurst, A.L. Cooperative jamming for secure communications in MIMO relay networks. *IEEE Trans. Signal Process.* **2011**, *59*, 4871–4884. [CrossRef]
11. Zheng, G.; Choo, L.C.; Wong, K.K. Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Trans. Signal Process.* **2011**, *59*, 1317–1322. [CrossRef]
12. Jeon, H.; McLaughlin, S.; Kim, I.M.; Ha, J. Secure communications with untrusted secondary nodes in cognitive radio networks. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1790–1805. [CrossRef]
13. Sakran, H.; Shokair, M.; Nasr, O.; EI-Rabaie, S.; EI-Azm, A. Proposed relay selection scheme for physical layer security in cognitive radio networks. *IET Commun.* **2012**, *6*, 2676–2687. [CrossRef]
14. Zou, Y.; Zhu, J.; Wang, X.; Leung, V. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Netw.* **2015**, *29*, 42–48. [CrossRef]
15. Cumanan, K.; Ding, Z.; Sharif, B.; Tian, G.; Leung, K.K. Secrecy rate optimizations for a MIMO secrecy channel with a multiple antenna eavesdropper. *IEEE Trans. Veh. Technol.* **2014**, *63*, 1678–1690. [CrossRef]
16. Ng, D.W.K.; Lo, E.S.; Schober, R. Robust beamforming for secure communication in systems with wireless information and power transfer. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 4599–4615. [CrossRef]
17. Jiang, W. Joint Power Allocation at the Base Station and the Relay for Untrusted Relay Cooperation OFDMA Network. *Int. J. Antennas Propag.* **2015**, *2015*, 1–15. [CrossRef]
18. Geraci, G.; Singh, S.; Andrews, J.; Yuan, J.; Collings, I. Secrecy rates in broadcast channels with confidential messages and external eavesdroppers. *IEEE Trans. Wirel. Commun.* **2013**, *13*, 2931–2943.
19. Liu, Y.; Wang, L.; Duy, T.T.; Elkashlan, M.; Duong, T.Q. Relay selection for security enhancement in cognitive relay networks. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 46–49. [CrossRef]
20. Alves, H.; Souza, R.D.; Debbah, M.; Bennis, M. Performance of transmit antenna selection physical layer security schemes. *IEEE Signal Process. Lett.* **2012**, *19*, 372–375. [CrossRef]
21. Wang, L.; Elkashlan, M.; Huang, J.; Tran, N.H.; Duong, T.Q. Secure transmission with optimal power allocation in untrusted relay networks. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 289–292. [CrossRef]
22. Biswas, S.; Morris, R. ExOR: Opportunistic Multi-Hop Routing for Wireless Networks. In Proceedings of the 2005 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Philadelphia, PA, USA, 22–26 August 2005; pp. 133–144.
23. Cacciapuoti, A.S.; Caleffi, M.; Paura, L. Optimal Constrained Candidate Selection for Opportunistic Routing. In Proceedings of the GLOBECOM 2010, Miami, FL, USA, 6–10 December 2010.
24. Rankov, B.; Wittneben, A. Spectral efficient protocols for half-duplex fading relay channels. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 379–389. [CrossRef]
25. Li, X.; Zhang, Q.; Zhang, G.; Qin, J. Joint Power Allocation and Subcarrier Pairing for Cooperative OFDM AF Multi-Relay Networks. *IEEE Commun. Lett.* **2013**, *17*, 872–875.
26. Leung-Yan-Cheong, S.K.; Hellman, M.E. The Gaussian wiretap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [CrossRef]
27. Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: New York, NY, USA, 2004.
28. Tao, M.; Liang, Y.C.; Zhang, F. Resource allocation for delay differentiated traffic in multiuser OFDM systems. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2190–2201.