Power Allocation and Partner Selection for Physical Layer Security in OFDM Wireless Networks

Shuanglin Huang[a], Aixia Jing[b] and Jian Xu[c]

School of Information Engineering, Hubei University for Nationalities, EnShi 445000, China

[a]huang-shuanglin@163.com, [b]1273261049@qq.com, [c]3176032@qq.com

Keywords: OFDM, power allocation, physical layer security, wireless network

Abstract. Most orthogonal frequency division multiplexing (OFDM) wireless communication system is poor in secure transmission. Based on user's physical layer security rate requirement, an OFDM system cooperative scheme over multi-relay cooperative communication networks to achieve optimal relay selection and power allocation was proposed in this paper. The proposed approach not only helps the source find the relays at relatively better locations, but also allocate an optimal amount of power among the relays for minimization the source node's payment. In this paper, the uniqueness of the solution was proved. The simulation results showed that although the physical layer security rate was zero while the source node was independent. But when the relay node helped it cooperate to transmit the data, the source node could obtain the physical layer security rate to meet the demand. Furthermore, the more the number of the relay nodes of the participating collaboration, the less the payment of the source node.

1. Introduction

In order to improve the secure performance of OFDM system, the traditional scheme generally employs encryption mechanisms with key to deal with information security. However, the key design, distribution and management based on the traditional encryption mechanisms with key, now are very difficult to realize in wireless network. Due to the increasing demand for wireless communication service and the rapid development of wireless network, information security is faced with greater challenges in wireless network.

Thus, there are few literatures studied how to provide security for OFDM system from the perspective of the physical layer. In literature [1], a differential coding scheme was presented, in which the information transmission of OFDM system has a low probability of intercept. The secrecy capacity of OFDM system was analyzed in the condition of eavesdropping end with different receiver in literature [2-3]. The literature [4] studied how the secrecy rate of OFDM system could reach the maximum through the reasonable power allocation. In [5], two practical physical layer security schemes for the MIMO orthogonal frequency-division multiplexing systems were proposed. For multi-user OFDM system, the resource allocation is the key problem in the physical layer transmission. The literature [6] presented a method of multiuser OFDM system resource allocation scheme restricted in physical layer security, which constructed a multiuser OFDM wiretap channel model from the perspective of information security theory. These studies are security issues in the research of OFDM physical layer, and provide a theoretical guidance for study on the correlation of the future.

However, the scheme given by the reference is only able to obtain the effective physical layer security rate for the harsh conditions. In practical wireless networks, the channel condition of eavesdropping node is more favorable than that of the destination node, which leads to the fact that the physical layer security rate of the two sides of the legal communication can be zero[7-8]. In view of these problems, the source node can seek a trusted relay node cooperative communication, which can obtain considerable cooperative diversity gain.

In this paper, we constructed a wireless system model restricted in physical layer security, which is shown in Figure 1. The model includes an arbitrary pair of source destination nodes, a number of

trusted relay nodes and a eavesdropping node. The eavesdropping node can tap the communication between the source node and the destination node, and the source node can achieve a higher physical layer security rate through the cooperative transmission of multiple relay nodes. In this paper, we propose a distributed power allocation and relay selection algorithm over multi-user cooperative communication networks, which takes explicitly into account the link physical layer security rate requirement of users. The energy consumption cost of relay nodes is jointly minimized and the user's requirement can be satisfied at same time.

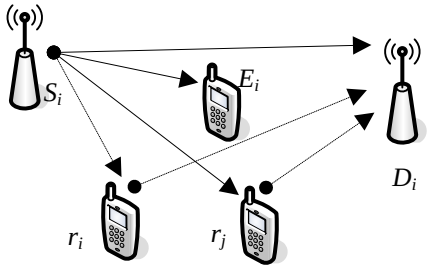

Fig. 1 The system model for cooperative transmission with terminals S_i transmitting to destination D_i.

2. OFDM System Physical Layer Security Model

In Fig.1, there is a source node and destination node pair, which communication is helped by relay nodes with the existence of an eavesdropper. All wireless nodes use the same OFDM modulation and demodulation. The global channel state information of the collaborative user and eavesdropper could be obtained by the sender. The collaboration between source node and relay node was divided into two stages. The carrier of their respective occupation number and the power consumption in each transmitted signal carrier are same as direct transmission (Without the cooperation).

Suppose that the transmission signal vectors are respectively $X_i=[x_{1i}, x_{2i}, , ,x_{Ni}]$, where x_{ki} is the signal of the kth subcarrier. Let $H_{i1}=[h_{i11}, h_{i12}, , , h_{i1N}]$, $H_{i2}=[h_{i21}, h_{i22}, , , h_{i2N}]$ respectively represent the channel gain vectors among node D_i with node S_i and r_i. Accordingly, the additive noise vectors among node D_i with node S_i and r_i is denoted as $W_{i1}=[w_{i11}, w_{i12}, , , w_{i1N}]$ and $W_{i2}=[w_{i21}, w_{i22}, , , w_{i2N}]$. Let $H_{i3}=[h_{i31}, h_{i32}, , , h_{i3N}]$ represent the channel gain vector between node S_i and r_i. And the additive noise vectors between node S_i and r_i is denoted as $W_{i3}=[w_{i31}, w_{i32}, , , w_{i3N}]$. Define the channel between the source node and eavesdropper as a wiretap channel. Let $G_i=[g_{i1}, g_{i2}, , , g_{iN}]$ represent the channel gain vector of the two wiretap channels between eavesdropper and node S_i. The additive noise vectors at the eavesdropper is denoted as $V_i=[v_{i1}, v_{i2}, , , v_{iN}]$. The legitimate destination node receives signal in the specified carrier channel allocated by sender. The signal vectors received at destination nodes D_i can be denoted as $Y_{i1}=[y_{i11}, y_{i12}, , , y_{i1N}]$ and $Y_{i2}=[y_{i21}, y_{i22}, , , y_{i2N}]$. Assuming that the eavesdropper can receive all the information on the transmission carrier, the received signal vector at the eavesdropper can be denoted as $Z=[z_1, z_2, , , z_N]$ in the stage one.

Then, the signal received at the legitimate destination node and the eavesdropper in each carrier can be denoted as:

$$y_{i1k} = x_{ik}h_{i1k} + w_{i1k} \tag{1}$$

$$z_k = x_{ik}g_{ik} + v_{ik} \tag{2}$$

For the single carrier signal, in the first stage, x_{ik} is the message signal from S_i to r_i and destination D_i, then the signal received at the destination node D_i is shown in Eq.(1). And the signal received at the node r_i is given by

$$y_{i3k} = x_{ik}\, h_{i3k} + w_{i3k} \tag{3}$$

In the second stage, r_i amplifies y_{i3k} and relays it to the destination node D_i. Then the signal received at the destination node D_i is shown as

$$\begin{aligned} y_{i2k} &= x_{rik}h_{i2k} + w_{i2k} \\ x_{rik} &= \sqrt{E(x_{rik}^2)}\, y_{i3k} / |y_{i3k}| \end{aligned} \tag{4}$$

Where x_{rik} is just the signal from r_i to destination D_i. Substituting Eq. (3) into Eq. (4), Eq. (4) can be rewrite as Eq. (5).

$$y_{i2k} = \frac{h_{i2k}\sqrt{E(x_{rik}^2)}(x_{ik}\, h_{i3k} + w_{i3k})}{\sqrt{|h_{i3k}|^2\, E(x_{ik}^2) + E(w_{i3k}^2)}} + w_{i2k} \tag{5}$$

So the achieved signal-to-noise ratio (SNR) helped by r_i for S_i to D_i is given by Eq. (6).

$$\lambda_{ik}^r = \frac{|h_{i2k}|^2 |h_{i3k}|^2\, E(x_{rik}^2)E(x_{ik}^2)}{|h_{i3k}|^2\, E(x_{ik}^2)E(w_{i2k}^2) + |h_{i2k}|^2\, E(x_{rik}^2)E(w_{i3k}^2) + E(w_{i3k}^2)E(w_{i2k}^2)} \tag{6}$$

By using maximum signal-to-noise ratio combination scheme to deal with the received signal in the two stages, the effective secrecy rate of node S_i at the D_i is

$$R_{ik}^S = \log(1+\lambda_{ik}^D + \sum_{r\in\{r_1,r_2,...,r_M\}} \lambda_{ik}^r) - \log(1+\lambda_{ik}^E) \tag{7}$$

Where $\lambda_{ik}^D = |h_{ik}|^2\, E(x_{ik}^2)/E(w_{ik}^2)$ is the SNR that results from the direct transmission (DT) from node S_i to D_i and $\lambda_{ik}^E = |g_{ik}|^2\, E(x_{ik}^2)/E(v_{ik}^2)$ is the SNR that results from the direct transmission from node S_i to the eavesdropper.

Thus, the total effective secrecy rate helped by S_j for node S_i at the D_i is given by

$$R_i^S = \sum_{k=1}^{N} R_{ik}^S \tag{8}$$

In practical applications, when the user carries out the key data transmission, the physical layer security rate R_0^S needs to be guaranteed. So, the source node needs to select the most advantageous relay node. The problem is to consider how to minimize the payment of the source node under the constraints of $R_i^S \geq R_0^S$. U_s represent the source node payment, P_{r_m} said the source node to buy r_m relay node for relaying power. By jointly adjusting the transmission power of the relay node, each source node always minimizes its own payment. This is an all relay node power optimization problem, which can be expressed as follows

$$\min_{R_i^S \geq R_0^S} U_s = \sum_{m=1}^{M} P_{r_m} \tag{9}$$

3. Power Allocation Strategy Analysis

This part of the analysis is based on the following assumptions: (1) All channel noise is additive narrow band Gauss white noise, and the noise power density is N_0, and $\sigma^2 = BN_0$; (2) The power allocation on each sub carrier is equal; (3) The channel gain is the same for different sub carriers in the same channel. Under this assumption, the limitation $R_i^S \geq R_0^S$ of the problem (9) can be re-expressed as

$$1+\lambda_{ik}^D + \sum_{r\in\{r_1,r_2,...,r_M\}} \lambda_{ik}^r \geq \lambda_0 \tag{10}$$

In the above formula, $\lambda_0 = 2^{\frac{R_0^S}{NB}+\log(1+\lambda_{ik}^E)}$. Inequality on the right side is a constant, and the left side is associated with the power of each participating cooperative relay nodes. Thus, the problem (9) can be re-expressed as

$$\min U_s = N\sum_{m=1}^{M} P_{r_{mk}}, s.t. 1+\lambda_{ik}^D + \sum_{r\in\{r_1,r_2,...,r_M\}} \lambda_{ik}^r \geq \lambda_0 \tag{11}$$

For the problem (10), we will divide it into two steps to solve. Firstly, we solve it and obtain the optimal power solution of the relays under the condition that the source node's power is a constant. Then, substituting the optimal solutions into (10), the optimal power solution of source node can be obtained by solving a quadratic equation about the power of source node.

Lemma 1: assuming that P_s is a constant, it will have optimal solution $P_r^* = \{P_{r_1}^*, P_{r_2}^*, ..., P_{r_M}^*\}$ for the problem (11). It is satisfied

$$\sum_{m=1}^{M} P_{r_m}^{*} \le \sum_{m=1}^{M} P_{r_m} \tag{12}$$

Proof: For $\lambda(P)$, if we can prove it is a concave function, the global optimal point is the only optimal point. By taking the derivative of $\lambda(P)$ to P_{r_m}, we have

$$\frac{\partial \lambda}{\partial P_{r_m}} = \frac{G_{r_m d} G_{sr_m} P_s \left(G_{sr_m} P_s + \sigma^2 \right)}{\left(P_{r_m} G_{r_m d} + P_s G_{sr_m} + \sigma^2 \right)^2 \sigma^2} > 0 \tag{13}$$

Where $G_{r_m d} = |h_{i1mk}|^2$ and $G_{sr_m} = |h_{i3mk}|^2$. And further,

$$\frac{\partial^2 \lambda}{\partial^2 P_{r_m}} = -G_{r_m d} G_{sr_m} \frac{2 G_{r_m d} G_{sr_m} P_s^2 + 2\sigma^2 G_{r_m d} P_s}{\left(P_{r_m} G_{r_m d} + P_s G_{sr_m} + \sigma^2 \right)^3 \sigma^2} < 0 \tag{14}$$

$$\frac{\partial^2 \lambda}{\partial P_{r_m} P_{r_n}} = 0, (m \ne n) \tag{15}$$

Because P_s is a constant, $\lambda(P)$'s Hessian matrix is a negative definite matrix. So $\lambda(P)$ is a concave function.

4. Simulation Results

The following simulations are based on following assumptions: (*a*) The transmission power for source node is 0.05W and the single subcarrier channel bandwidth W=1Hz when they transmit data independently. (*b*) The path gain for all channels is set at $(7.75\times10^{-3})/d^{3.6}$, where *d* is the distance (in meters) between a transmitter and the corresponding receiver. (*c*) The channel between two nodes is described by the distance between them. All channels are assumed to undergo flat fading and are quasi-static. (*d*) The noise level of the additive white Gaussian noise (AWGN) is 5×10^{-12}W. (*e*) $R_0^S = 1$. We consider a network in which a source node is located at the origin, a destination node is situated 120m east of the source node such that the destination node is located at coordinate (120,0), and a eavesdropper node is existed. For all relay nodes, the maximum transmit power is assumed to be 0.2W.

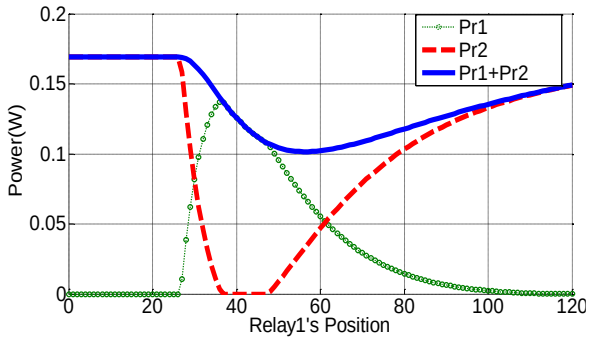

Fig. 2 Two relay case

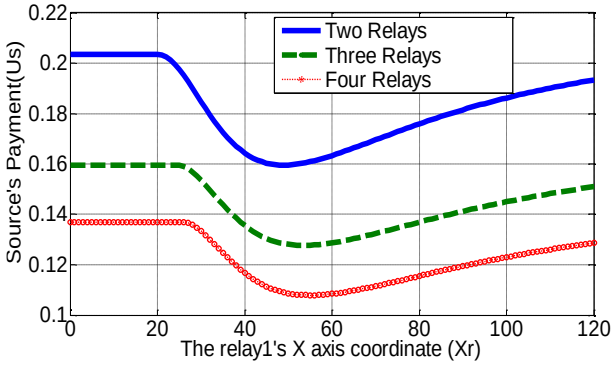

Fig. 3 The effect of position and number of relay on source's payment

The simulation scenario shown in Figure 2 contains a eavesdropper node located at (60, 30), two relay nodes: one relay node r_2 located at (30, 5), and another relay node r_1 that moves along a straight line between (0, 5) and (120, 5).

As the relay node r_1 moves from left to right, we can see that the source node selection and power allocation for relay node r_1 and relay node r_2 from the simulation curve in figure 4. The beginning of the source node does not select the relay node r_1 and only select the relay node R2 to participate in the collaboration (P_{r1}=0); Then the relay node r_1 position becomes better, the source node selects the relay node r_1 and relay node r_2 to participate in the relay cooperation; Then, due to the location of the relay node r_1 becomes better than the relay node r_2, which leads to the relay node r_2 node has not been selected by the source node to participate in the relay Cooperation (P_{r2}=0); Finally, with the relay node r_1 moving to the right, the relay node2 r_1 and r_2 both are selected by source node to participate in the cooperation. The relative size of the power between them reflects the effect of the data transmission to the source node. This whole process reflects the competitive relationship between relay nodes r_1 and r_2.

The simulation scenario shown in Figure 3 contains a eavesdropper node located at (60, 30), two/three/four relay nodes: relay node r_2 located at (30, 5), relay node r_3 located at (50, 5), relay node r_4 located at (80, 5), and relay node r_1 that moves along a straight line between (0, 5) and (120, 5). It can be seen from Figure 6 that the more the number of the relay nodes of the participating collaboration, the less the payment of the source node (equal to the sum of the power of all participating cooperative relay nodes).

5. Conclusion

This paper proposes a payment minimization framework for the joint optimization of the best relay strategy, and the best relay power allocations in a wireless cooperation network. The main objective of this work is to solve source node how to select relay node and how much power is allocated for relays. Furthermore, the power of relay nodes is considered to benefit link data transmission. Not only the payment of source node is minimized but also its link data transmission requirement is satisfied. From the simulations, Source node tends to choose those relays which are located at proper position and are good channel condition, relatively. By emphasizing the physical layer security rate requirement, a margin can be obtained so that data is more likely to be safely, reliably and successfully delivered in unstable wireless channels.

Acknowledgement

This work was supported by the Hubei Province, colleges and universities in the outstanding youth science and technology innovation team plan of china under Grant No. T201512.

References

[1]. Li Zheng, Xia Xianggen. A Distributed Differentially Encoded OFDM Scheme for Asynchronous Cooperative Systems with Low Probability of Interception. IEEE Transactions on Wireless Communications. Vol. 8(2009), p. 3372-3379.

[2]. Renna F, Laurenti N, Poor H V. Physical Layer Secrecy for OFDM Systems. Proceedings of IEEE European Wireless Conference. Lucca, Italy: IEEE Press, 2010, p. 782-789.

[3]. Renna F, Laurenti N, Poor H V. High SNR Secrecy Rates with OFDM Signaling over Fading Channels. Proceedings of the 21st International Symposium on Personal Indoor and Mobile Radio Communications, Istanbul. Turkey: IEEE Press, 2010, p. 2692-2697.

[4]. Jorswieck E, Wolf A. Resource Allocation for the Wire-tap Multi-carrier Broadcast Channel. Proceedings of Int'l Workshop on Multiple Access Communications. Petersburg, Russia, 2008.

[5]. Chih-Yao Wu, Pang-Chang Lan, Ping-Cheng Yeh, et al. Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices. IEEE Journal on Selected Areas in Communications. Vol. 31(2013), p. 1687-1700.
[6]. CHEN Yu-lei, JI Xin-sheng, HUANG Kai-zhi, et al. Resource Allocation Scheme for Physical Layer Security in Multiuser Orthogonal Frequency Division Multiplexing System. Computer Engineering. Vol. 39(2013), p.156-160.
[7]. Chih-Yao Wu, Pang-Chang Lan, Ping-Cheng Yeh, et al. Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices. IEEE Journal on Selected Areas in Communications. Vol. 31(2013), p. 1687 – 1700.
[8]. Hao Li, Xianbin Wang, Yulong Zou. Dynamic Subcarrier Coordinate Interleaving for Eavesdropping Prevention in OFDM Systems. IEEE Communications Letters. Vol. 18(2014), p. 1059-1062.