Secure Algorithm via Hybrid Relaying Scheme and Resource Allocation for OFDM Networks

Xianwen Zhou, Pinyi Ren(✉), and Qinghe Du

School of Electronic and Information Engineering, Xi'an Jiaotong University,
Xi'an 710049, China
zhou19910225@stu.xjtu.edu.cn, {pyren,duqinghe}@mail.xjtu.edu.cn

Abstract. Due to its high spectrum efficiency, strong ability to resist multipath fading, OFDM networks is widely applied in various wireless communication systems. However, physical layer security is also an important problem in OFDM networks. By using relay nodes, the secrecy outage probability can be reduced since relay nodes could increase freedoms of optimization for the cooperative OFDM networks. By optimizing multiple variables, which includes adaptive hybrid relaying scheme, relay selection, and resource allocation, we propose the secure algorithm which aims at minimizing the secrecy outage probability of multiuser in cooperative OFDM networks. To achieve this goal, we establish an optimization problem including multiple optimization variables. Then, we convert the optimization problem into a graph theory problem. Simulation results show that the secure algorithm can significantly reduce the secrecy outage probability of multiuser in cooperative OFDM networks.

Keywords: Physical layer security · Hybrid relaying scheme
Resource allocation · Cooperative OFDM networks

1 Introduction

Due to its high spectrum efficiency, strong ability to resist multipath fading, the Orthogonal Frequency Division Multiplexing (Orthogonal Frequency Division Multiplexing, OFDM) technology is widely applied in various wireless communication systems. Because people pay more and more attention to information security, physical layer security also becomes a critical issue in OFDM networks. In [1], Shannon pointed out that complete secret communication can be realized by means of "one word one secret" when the wiretap channel and the legitimate channel are not differential channels. Then, a degraded wiretap channel was proposed in the discrete memoryless channel by Wyner in [2] which considers a more general situation. However, when legitimate receiver's channel state information is worse than the eavesdropper's channel state information, secrecy rate is zero. To overcome this problem, in [3–8], the author uses cooperative relay communication technology to strengthen secure communication of legal receivers.

B. Li et al. (Eds.): ChinaCom 2017, LNICST 237, pp. 283–291, 2018.
https://doi.org/10.1007/978-3-319-78139-6_29

Due to the relay technology advantages in the physical layer security, in [9–12], the author found that the cooperative OFDM networks could achieve the maximal secrecy throughput by resource allocation. However, sometimes secrecy throughput is inappropriate in some scenes which hopes secrecy outage probability of multiuser in cooperative OFDM networks is low. Furthermore, secrecy performance is poor when a single relay protocol is used. To address the problem, in [13–16], some adaptive hybrid relaying scheme is proposed.

To address the problems of above, we consider a scenario consisting of a base station, multiple relay nodes, multiple users, and a passive eavesdropper. And in this paper, we define secrecy outage probability of multiuser as performance indicator in cooperative OFDM network which considers user's scheduling fairness, and a adaptive hybrid relaying scheme which switches between Amplify-and-Forward protocol (AF) and Decode-and-Forward protocol (DF) for multiple relays is proposed.

In this paper, our goal is to reduce the secrecy outage probability of multiuser in cooperative OFDM networks by optimizing multiple variables, which includes adaptive hybrid relaying scheme, relay selection, resource allocation. Here, the relaying scheme includes Decode-and-Forward protocol (DF) and Amplify-and-Forward protocol (AF). To order to achieve the above goal, we establish a multi-variable optimization problem. Then, we convert the optimization problem into a graph theory problem. Lastly, numerical results illustrate that the proposed algorithm have better secrecy outage probability performance.

The rest of this paper is organized as follows. Section 2 introduces the system model. Section 3 focuses on the optimization for secrecy outage probability of multiuser in cooperative OFDM networks. Section 4 shows the numerical results. Finally, Sect. 5 offers conclusions.

2 System Model

As illustrated in Fig. 1, In this paper, we consider a cooperative OFDM network which consists of a base station (S), K relays (R), a passive eavesdropper (Eve) and N users (d(1), $\cdots$, d(N)), the OFDM network has M available subcarriers ($N \leq M$). Each node has a single antenna, and operates in half-duplex mode. We call s-d pairs between base station and multiple users under different subcarrier. Due to channel fading, let's assume that there are no direct transmission links between S and d(n) or Eve. We define the channel coefficient on subcarrier m from S to R, from R to d(n) and from R to Eve as h_{sr}^{m}, $\mathrm{h}_{rd(n)}^{m}$ and h_{re}^{m}, respectively. We assume that N_0 is the Gaussian noise variance, and channels are subjected to quasi-static flat fading. Finally, we assume that each node knows the full channel state information (CSI).

The cooperative relay transmission between each user pair is divided into two slots. In the process of cooperative transmission, the first transmission time-slot and second transmission time-slot use the same subcarrier by resource allocation. To improve performance of secrecy outage probability, a adaptive hybrid relaying

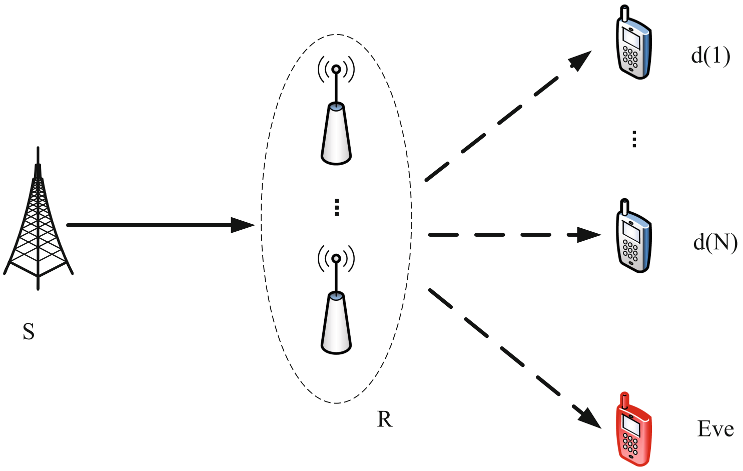

Fig. 1. System model.

scheme which switches between AF and DF for the relays is proposed. In such a adaptive hybrid relaying scheme, a relay could choose between AF and DF according to its own decoding ability.

3 Optimization Problem Description and Optimal Solution

3.1 Optimization Problem Description

The problem which we will solve is that in a multiple relays and multiuser cooperative OFDM network, how we jointly select its relaying transmission scheme, relay selection and resource allocation to minimize the secrecy outage probability of multiuser. To order to build the optimization problem effectively, the binary integral variables $\rho_n^i\left(r,m\right)$ represent a user's joint selection strategy. Concretely speaking, $\rho_n^i\left(r,m\right)=1$ means that the nth user selects the r relay and the i relaying transmission scheme, and the first transmission time-slot and second transmission time-slot use the same subcarrier m. Finally, the variables $R_n^i\left(r,m\right)$ represent the secrecy rate which the nth user can obtain under the strategy of $\rho_n^i\left(r,m\right)$.

In such a adaptive hybrid relaying scheme, a relay could choose between AF and DF according to its own decoding ability. when the decoding ability of the relay node is strong, the DF relay protocol is used. Otherwise, the AF relay protocol is used instead. We show the achievable secrecy rate of using DF or AF protocol as follows.

(1) Amplify-and-Forward Relay Mode (AFM): When the relaying nodes are very far from the base station, the relays's decoding ability may become low. The AF relaying scheme may obtain a greater secrecy rate for users. In the

cooperative transmission process, the base station sends the information to the selected relay r on subcarrier m in the first time-slot. Then, the relay node r amplifies its received signals and sends them to the user n on subcarrier m in the second time-slot. The secrecy rate of AF relaying scheme can be expressed as follows,

$$R_n^1(r,m) = \frac{1}{2}\left\{\begin{array}{c} \log_2\left(1+\frac{\gamma_0^2|h_{sr}^m|^2\left|h_{rd(n)}^m\right|^2}{\gamma_0|h_{sr}^m|^2+\gamma_0\left|h_{rd(n)}^m\right|^2+1}\right) \\ -\log_2\left(1+\frac{\gamma_0^2|h_{sr}^m|^2|h_{re}^m|^2}{\gamma_0|h_{sr}^m|^2+\gamma_0|h_{re}^m|^2+1}\right) \end{array}\right\}^+ \tag{1}$$

where $\{\cdot\}^+$ is defined as $\{\cdot\}^+=\max(\cdot,\,0)$ and $\gamma_0 = \frac{P_S}{N_0} = \frac{P_R}{N_0} = \text{SNR}$.

(2) Decode-and-Forward Relay Mode (DFM): When the relaying nodes are very close to the base station, the relays's decoding ability may become high, The DF relaying scheme may obtain a greater secrecy rate for users. Similar to the AF relay protocol, when relay nodes use DF relay protocol, the base station sends the information to the selected relay r on subcarrier m in the first time-slot. Then, the relay decodes the received signal and forwards the decoded signal to the destination user n on subcarrier m in the second time-slot. The secrecy rate of DF relaying scheme can be expressed as follows,

$$R_n^2(r,m) = \frac{1}{2}\left\{\begin{array}{c} \min\left\{\log_2\left(1+\gamma_0|h_{sr}^m|^2\right),\right. \\ \left.\log_2\left(\frac{1+\gamma_0\left|h_{rd(n)}^m\right|^2}{1+\gamma_0|h_{re}^m|^2}\right)\right\} \end{array}\right\}^+ \tag{2}$$

where $\{\cdot\}^+$ is defined as $\{\cdot\}^+=\max(\cdot,\,0)$ and $\gamma_0 = \frac{P_S}{N_0} = \frac{P_R}{N_0} = \text{SNR}$.

In this article, we want to reduce the secrecy outage probability of multiuser. An interruption occurs to a user pair when its secrecy rate is smaller than the secrecy outage threshold R. We define 0–1 binary variable to represent the secrecy outage of multiuser. The expression of secrecy interruption of user pair can be expressed as follows,

$$I_n^i(r,m) = \begin{cases} 0, \rho_n^i(r,m)R_n^i(r,m) \geq R \\ 1, \rho_n^i(r,m)R_n^i(r,m) < R \end{cases} \tag{3}$$

Next, we could obtain the secrecy outage probability of multiuser F as follows,

$$F = \frac{1}{N}\sum_{n=1}^{N}\sum_{i=1}^{Q}\sum_{r=0}^{K}\sum_{m=1}^{M} I_n^i(r,m) \tag{4}$$

which Q means different relaying scheme. Concretely speaking, Q = 1 means that the user uses AF relaying scheme, and Q = 2 means that the user uses DF relaying scheme.

To avoid interference among multiuser, A subcarrier can only be assigned to one user for transmitting information. The specific restrictions are expressed as follows,

$$\sum_{n=1}^{N}\sum_{i=1}^{Q}\sum_{r=0}^{K}\rho_n^i(r,m) \leq 1, m=1,2,\cdots,M \tag{5}$$

Each user can only select a relay forwarding strategy for each information transmission and the user works on the same subcarrier in the first and second transmission time-slot. The specific restrictions are represented as follows:

$$\sum_{i=1}^{Q}\sum_{r=0}^{K}\sum_{m=1}^{M}\rho_n^i(r,m) \leq 1,n{=}1,2,\cdots,N \tag{6}$$

In summary, the optimization problem of minimizing the secrecy outage probability of multiuser in cooperative OFDM networks could be represented as follows,

$$\begin{aligned} &\min_{\rho_n^i(r,m)} \tfrac{1}{N} \sum_{n=1}^{N}\sum_{i=1}^{Q}\sum_{r=0}^{K}\sum_{m=1}^{M} I_n^i(r,m)a \\ &s.t. \begin{cases} \sum\limits_{n=1}^{N}\sum\limits_{i=1}^{Q}\sum\limits_{r=0}^{K} \rho_n^i(r,m) \leq 1,m{=}1,2,\cdots,M \\ \sum\limits_{i=1}^{Q}\sum\limits_{r=0}^{K}\sum\limits_{m=1}^{M} \rho_n^i(r,m) \leq 1,n{=}1,2,\cdots,N \\ \rho_n^i(r,m) \in \{0,1\} \end{cases} \end{aligned} \tag{7}$$

In order to minimize the secrecy outage probability of multiple users in cooperation OFDM network, each user can not simply decide which relay node, relaying scheme, subcarrier to select according to user's own secrecy rate, but should be to find a optimal strategy which could minimize the secrecy outage probability of multiuser in whole cooperative OFDM network.

3.2 Optimal Solution

We find that the above established optimization problem is an integer programming problem through analysis. There are four optimization variables which includes relay nodes, relay forwarding strategy, user selection and available subcarrier. Decision sets include a total of 2^{NQKM} decision choice. Therefore, if we use the exhaustive search to solve the optimal solution, the time complexity of the solution is 2^{NQKM}. In order to reduce the computational complexity, we must find an efficient algorithm to solve the above optimization problem. In the following optimization solution, we find that the Hungarian algorithm could effectively solve the above integer programming problem. Through analysis, we could find that each user could only select one relay and one subcarrier in first and second time-slot. This characteristic implies that the optimization problem could indeed be transformed into a integer programming problem.

As illustrated in Fig. 2, in order to use graph theory to solve the optimization problem, we must construct a bipartite graph $G = (V \cup U, E)$. Firstly, we use set $V = \{(s, d(n)) \,|1 \leq n \leq N\}$ to represent all possible user pairs, and set $U = \{(i, r, m) \,|1 \leq i \leq Q, 0 \leq r \leq K, 1 \leq m \leq M\}$ to represent user's all possible joint strategies. The strategy $u \in U$ shows that a user selects relay protocol i, relay node r and transmits on subcarrier m during the first and second time-slots. If the user pair $v \in V$ has a greater secrecy rate than the secrecy outage threshold R under the strategy $u \in U$. We use one edge $e \in E$ to connected

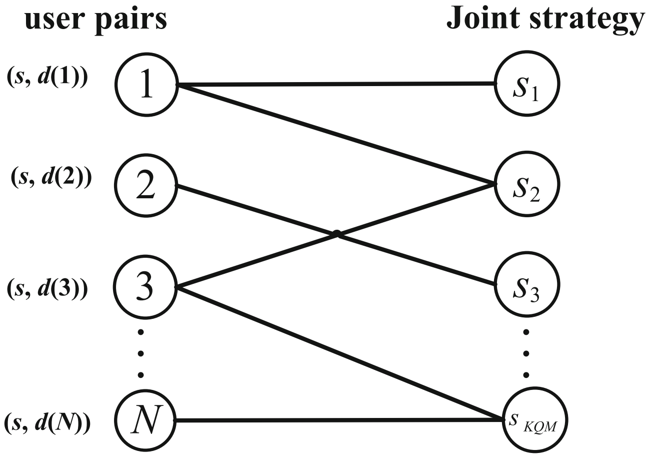

Fig. 2. The constructed bipartite graph.

vertex v with u. The set of all edges in graph G is E. When we have completed the abstract construction of the bipartite graph $G = (V \cup U, E)$. Then, the original optimization problem can be transformed into graph theory and solved equivalently by Hungarian algorithm.

The key of the proposed optimal solution is the equivalent transformation from parametric programming to the max-matching problem. When the bipartite graph G is constructed, the Hungary algorithm could effectively solve the above integer programming problem for G [17,18]. The optimization solution is expressed as Algorithm 1.

Algorithm 1. Find the optimal relaying scheme and resource allocation

```
1: First, we should construct the bipartite graph G.
2: Then, we use the Hungarian algorithm to obtain a max-matching T.
3: The $|T|$ is maximum number of users without occurring secrecy interruption. Therefore, the minimal secrecy outage probability of multiuser in the cooperative OFDM network is $1 - |T|/N$.
```

4 Numerical Results

In the end, the numerical results are given to demonstrate the performance of the proposed algorithm which hopes to minimize secrecy outage probability of multiuser in the cooperative OFDM network. The simulation parameters are given as follows. We fix base station at point (0, 0), relay nodes, multi-users, and the passive eavesdroppers are randomly distributed in a two-dimensional 1×1 rectangular plane. The simulation mainly considers small scale fading. The number of users are $\mathrm{N} = 20$ and there are $\mathrm{M} = 20$ available subcarriers in the cooperative OFDM network. The numerical simulation is performed over 1000 independent Rayleigh channel realizations totally.

Figure 3 gives the secrecy outage probability of multiuser under different SNR conditions. And in this simulation, we set up the number of relay nodes K = 6, secrecy outage threshold R = 1 bit/s/Hz. From the simulation result of Fig. 3, it can be seen that the proposed joint algorithm can achieve a lower secrecy outage probability of multiuser under different SNR conditions compared to AF or DF relay protocol. Figure 3 also shows that under different SNR conditions, the best transmission mode is hybrid relay protocol. The relay nodes can automatically switch according to according to its own decoding ability, so the proposed algorithm compared to the AF or DF relaying protocol has a lower the performance of secrecy outage probability.

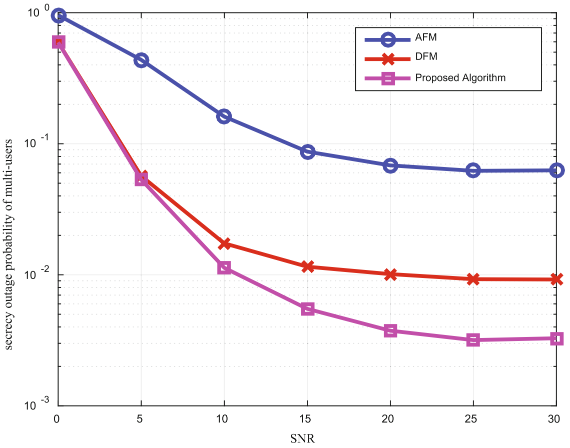

Fig. 3. Secrecy outage probability of multi-users under different SNR.

Figure 4 gives the secrecy outage probability of multiuser under different secrecy outage threshold R, And in this simulation, we set up the number of relay nodes K = 6, SNR = 5 dB. From the simulation result of Fig. 4, it can be seen that the proposed algorithm has better secrecy outage probability performance than AFM or DFM, and secrecy outage probability increases with the increasing of secrecy outage threshold R.

Figure 5 gives the secrecy outage probability of multiuser under different number of relay nodes, And in this simulation, we set up SNR = 10 dB, secrecy outage threshold R = 1 bit/s/Hz. From the simulation result of Fig. 5, it can be seen that the proposed algorithm has better secrecy outage probability performance than AFM or DFM, and secrecy outage probability decreases with the increasing of number of relay nodes. This is because, with the increasing of number of relay nodes, the channel state condition between base station and user is better, so secrecy outage probability of multiuser is lower with the increasing of number of relay nodes.

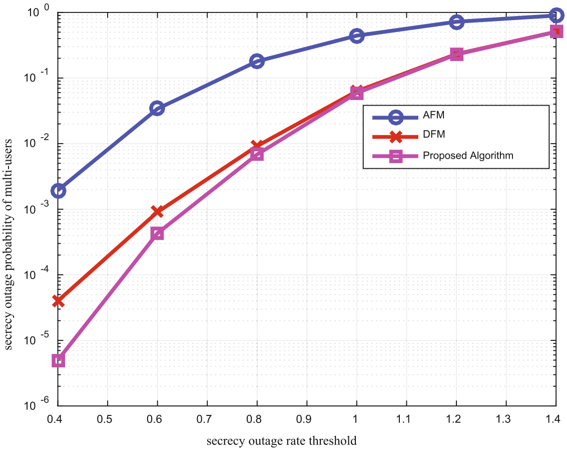

Fig. 4. Secrecy outage probability of multi-users under different secrecy outage threshold.

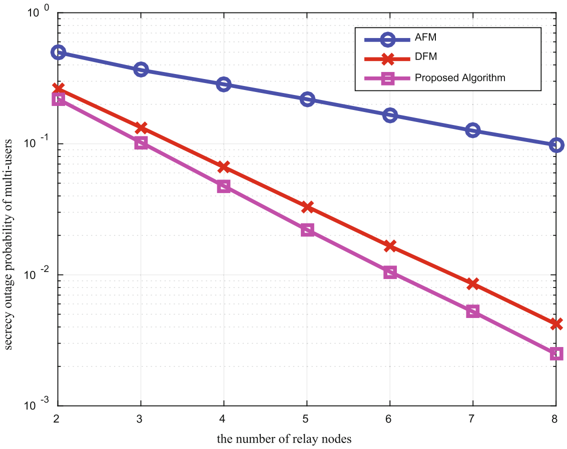

Fig. 5. Secrecy outage probability of multi-users under different number of relay nodes.

5 Conclusions

In this paper, we propose a secure algorithm towards minimizing the secrecy outage probability of multiuser in cooperative OFDM network. Firstly, To order to achieve the above goal, we establish a multi-variable optimization problem. Then, we convert the optimization problem into a graph theory problem. Lastly, numerical results illustrate that the proposed algorithm has a lower secrecy outage probability.

References

1. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
2. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
3. Li, J., Petropulu, A.P., Weber, S.: Optimal cooperative relaying schemes for improving wireless physical layer security. IEEE Trans. Sig. Process. **59**(10), 4985–4997 (2011)
4. Yang, Y., Li, Q., Ma, W.K., Ge, J.: Cooperative secure beamforming for AF relay networks with multiple eavesdroppers. IEEE Sig. Process. Lett. **20**(1), 35–38 (2013)
5. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Improving wireless physical layer security via cooperating relays. IEEE Trans. Sig. Process. **58**(3), 1875–1888 (2010)
6. Goeckel, D., Vasudevan, S., Towsley, D., Adams, S.: Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks. IEEE J. Sel. Areas Commun. **29**(10), 2067–2076 (2011)
7. Gamal, H.E., Lai, L.: The relay-eavesdropper channel: cooperation for secrecy. In: IEEE International Symposium on Information Theory, pp. 931–935 (2012)
8. Mo, J., Tao, M., Liu, Y.: Relay placement for physical layer security: a secure connection perspective. IEEE Commun. Lett. **16**(6), 878–881 (2012)
9. Cai, C., Cai, Y., Wang, R., Yang, W.: Resource allocation for physical layer security in cooperative OFDM networks. In: IEEE International Conference on Wireless Communications Signal Processing, pp. 1–5 (2015)
10. Jeong, C., Kim, I.M.: Optimal power allocation for secure multicarrier relay systems. IEEE Trans. Sig. Process. **59**(11), 5428–5442 (2011)
11. Ng, D.W.K., Lo, E.S., Schober, R.: Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks. IEEE Trans. Wirel. Commun. **10**(10), 3528–3540 (2011)
12. Cai, C., Cai, Y., Yang, W.: Subcarrier allocation for physical-layer security in cooperative OFDMA networks. IEICE Trans. Commun. **94**(12), 3387–3390 (2011)
13. Divya, T., Gurrala, K.K., Das, S.: Performance analysis of hybrid decode-amplify-forward (HDAF) relaying for improving security in cooperative wireless network. In: Communication Technologies, pp. 682–687 (2015)
14. Chen, H., Liu, J., Zhai, C., Zheng, L.: Performance analysis of SNR-based hybrid decode-amplify-forward cooperative diversity networks over rayleigh fading channels. In: Wireless Communications and Networking Conference, pp. 1–6 (2010)
15. Duong, T.Q., Zepernick, H.: Hybrid decode-amplify-forward cooperative communications with multiple relays. IEEE Trans. Sig. Process. 273–278 (2009)
16. Duong, T.Q., Zepernick, H.J.: On the performance gain of hybrid decode-amplify-forward cooperative communications. EURASIP J. Wirel. Commun. Netw. **2009**, 1–10 (2009)
17. Chen, H. Ren, P., Sun, L., Du, Q.: A joint optimization of transmission mode selection and resource allocation for cognitive relay networks. In: 2013 IEEE International Conference on Communications (ICC), pp. 2852–2856 (2013)
18. Koide, T., Kubo, H., Watanabe, H.: A study on the tie-set graph theory and network flow optimization problems. Int. J. Circ. Theory Appl. **32**(6), 447–470 (2004)