EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Joint subcarrier and power allocation for physical layer security in cooperative OFDMA networks

An Wang, Jin Chen, Yueming Cai*, Chunxiao Cai, Wendong Yang and Yunpeng Cheng

Abstract

In this paper, a joint subcarrier and power allocation algorithm is proposed to improve the physical layer security in cooperative orthogonal frequency division multiple access (OFDMA) networks, where several source-destination pairs and one untrusted relay are involved. The relay is friendly and intends to help these pairs to enhance their communications. However, it may be overheard by a malicious eavesdropper at the same time. To optimize the joint subcarrier and power allocation with low complexity, we divide the optimization problem into two simpler subproblems. Firstly, the subcarriers are assigned to the source-destination pairs by employing the dual approach under the assumption that the relay power is equally allocated to all the subcarriers. Then, the relay power is allocated to the subcarriers based on the alternative ascending clock auction mechanism. In addition, we prove that the two subproblems can converge after a finite number of iterations. We also find that the proposed auction is cheat-proof and, thus, can avoid the cheating behaviors in the auction process. Numerical results demonstrate that our proposed algorithm can effectively improve the system sum secrecy rate, and the convergence performance is also desirable.

Keywords: Cooperative OFDMA; Resource allocation; Dual; Auction; Physical layer security

1 Introduction

Cooperative relaying with orthogonal frequency division multiple access (OFDMA) has recently emerged as a promising technology to achieve the virtual spatial diversity in the wireless networks, which has been adopted in the fourth-generation mobile communication standard. However, the broadcast nature of wireless communication makes it difficult to ensure reliable and secure message transmission in the presence of passive eavesdroppers. Consequently, physical layer security has aroused growing attention during the recent years. The basic idea of physical layer security is to exploit the physical characteristics of the wireless channels to guarantee secure communication. Physical layer security is quantified by the secrecy capacity, which was pioneered by Wyner in [1]. He also points out that the condition for secure communication is that the secrecy capacity is larger than zero.

Motivated by the fact that careful resource management can remarkably ameliorate the performance of cooperative OFDMA networks, resource allocation has been extensively employed to tackle the challenges of physical layer security [2-8]. In [2], the source and relay power allocation problem is considered in a two-hop wireless relay network, where the secrecy rate is improved through choosing proper amount of power to transmit jamming signals for both the source and the relay. In [3], an outage probability-based power distribution algorithm between data and artificial noise is proposed to improve physical layer security in the multiple-input-single-output system.

Taking the multiuser communications scenario into consideration, the distributed resource management approaches are more desired. Game theory offers a novel perspective and an effective mathematical tool to investigate the interactions among rational players [9]. Recently, the distributed game approaches have been widely employed to develop distributed and flexible resource management mechanisms in order to avoid the

*Correspondence: caiym@vip.sina.com
Institute of Communications Engineering, PLA University of Science and Technology, Nanjing, China

© 2013 Wang et al.; licensee Springer. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/2.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

high complexity and excessive energy consumption of centralized methods [4-8,10,11]. In [4], Han et al. investigated the interaction among the source and the friendly jammers to increase the secrecy capacity using the Stackelberg game. Physical layer security is also improved by utilizing jamming power allocation for the two-way untrusted relaying based on the Stackelberg game in [5]. In [6], the coalitional game is employed to enhance the physical layer security. Auction game [12] has been widely investigated as an efficient tool for resource allocation, such as in [7,10], and [11]. In [7], the physical layer security is ameliorated using two auctions: the traditional ascending clock auction (ACA-T) and the alternative ascending clock auction (ACA-A). The literature mentioned above mostly focus on the power allocation (the relay's or the jammer's power). However, effective subcarrier assignment can also improve the performance of the OFDMA systems, which has not drawn sufficient attention [8]. In [8], the authors formulated an analytical framework for subcarrier and power allocation in a downlink OFDMA-based broadband network with coexistence of secure users and normal users. The average aggregate information rate of all the normal users was maximized via dual decomposition while maintaining an average secrecy rate for each secure user.

In this paper, a cooperative OFDMA network is considered, where there exist several source-destination pairs and one untrusted relay. The case of untrusted relaying in physical layer security has been investigated in the previous literature [13-15]. The untrusted relay in this paper is friendly and intends to help these user pairs to enhance their communications, which is different from the traditional ones in [13]. It is untrusted because it may be overheard by a malicious eavesdropper at the same time. Moreover, the eavesdropper can just passively listen to the relay, and it is not capable of disturbing the normal communication process. As a result, we can try to improve the physical layer security of the network by jointly optimizing the subcarrier and relay power allocation policies. To avoid the high complexity resulting from the optimal joint subcarrier and power allocation, we decompose it into two simpler subproblems instead. Firstly, the subcarriers are assigned to the source-destination pairs by employing the dual approach under the assumption that the relay power is equally allocated to all the subcarriers. Then, the relay power is allocated to the subcarriers according to the ACA-A mechanism. In the proposed auction game, the relay is modeled as the auctioneer and the subcarriers are regarded as the bidders. However, due to the fact that the subcarriers are not entities, it is the corresponding sources that submit the bids instead of the subcarriers. The main contribution of this paper can be summarized as follows:

- A novel joint subcarrier and power allocation algorithm is proposed to improve the physical layer security for the cooperative OFDMA networks. This algorithm reduces the complexity of optimal joint resource allocation and can ensure all the users' secrecy rate effectively.
- A non-convergent infinite series is designed to ensure the convergence of the proposed dual-based subcarrier assignment algorithm. For the proposed ACA-A-based power allocation algorithm, we prove the existence of the equilibrium and the cheat-proof property.

The rest of the paper is organized as follows. System model and the assumptions are introduced in Section 2. Detailed description of the dual-based subcarrier assignment is presented in Section 3. Section 4 describes the ACA-A-based power allocation and investigates some properties of the proposed auction, including the convergence performance and the cheat-proof property. Section 5 shows and discusses the simulation results, and it is followed by the conclusion in Section 6.

2 System model

As shown in Figure 1, we consider a cooperative OFDMA network which consists of M source-destination pairs, denoted by S_m and D_m, $m \in \mathcal{M} = \{1, \ldots, M\}$, and one untrusted relay denoted by R. The relay intends to help these user pairs to enhance their communications. It is untrusted because it may be overheard by a malicious eavesdropper at the same time. Moreover, the eavesdropper can just passively listen to the relay, and it is not capable of disturbing the normal communication process. Such communication scenario can be easily found in the distributed wireless sensor networks. For example, some sensor nodes in a cluster intend to deliver secret messages to other sensors via a fusion center (FC) node. However, the FC node maybe passively eavesdropped by malicious users.

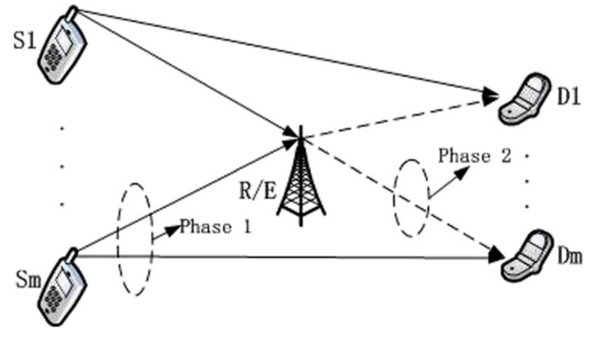

Figure 1 System model.

We assume that all the source-destination pairs share the total N available subcarriers, and each subcarrier n, $n \in \mathcal{N} = \{1, \ldots, N\}$, can only be exclusively allocated to one user pair. Assume that the instantaneous channel state information (CSI) of any user pair is perfectly known at the corresponding source node. For the broadband channel model, we consider the slow and flat Rayleigh fading and long path loss. For the nth subcarrier, the channel coefficients between the source S_m and the destination D_m, between the source S_m and the relay R, and between the relay R and the destination D_m are denoted by $h^n_{d,m}$, $h^n_{a,m}$, and $h^n_{b,m}$, respectively. For the long path loss, a path loss exponent β is assumed. Without loss of generality, we assume that the thermal noise at each node is independent and has the same variance σ^2.

We assume that all the nodes operate in the half-duplex mode, and the untrusted relay employs the amplify-and-forward strategy. We take the mth source-destination pair, for example, to describe the communication process. For the mth user pair, the complete transmission process can be divided into two phases. In phase 1, the source S_m broadcasts its data to the relay R and its intended destination D_m. During phase 2, the relay R amplifies its received signal to the destination D_m. We also assume that the destination can perfectly combine the signals received from the source and the relay.

According to [16], the mutual information between the source S_m and the destination D_m on the nth subcarrier, denoted by $I^n_{d,m}$, can be written as

$$I^n_{d,m} = \log_2 \left(1 + \frac{p_s \left| h^n_{d,m} \right|^2}{\sigma^2} + \frac{p_s \left| h^n_{a,m} \right|^2 p^n_m \left| h^n_{b,m} \right|^2}{\sigma^2 \left(\sigma^2 + p_s \left| h^n_{a,m} \right|^2 + p^n_m \left| h^n_{b,m} \right|^2 \right)} \right) \tag{1}$$

where p_s is the transmit power of the source, and p^n_m is the power that the relay allocates to the mth user pair on the nth subcarrier. In this paper, we just focus on the relay power allocation and simply assume that all the source nodes transmit with the same power p_s, $0 \leq p_s \leq p_{\max}$, where $p_{\max}$ is the peak power of all the nodes in the network.

Similarly, the mutual information between the source S_m and the eavesdropper (i.e., the untrusted relay R) on the nth subcarrier, denoted by $I^n_{e,m}$, can be written as

$$I^n_{e,m} = I^n_{r,m} = \log_2 \left(1 + \frac{p_s \left| h^n_{a,m} \right|^2}{\sigma^2} \right) \tag{2}$$

If the high SNR scenario is assumed, according to [1], the secrecy rate of the mth pair on the nth subcarrier can be expressed as

$$\begin{aligned} \mathrm{RS}^n_m &= \left(I^n_{d,m} - I^n_{e,m} \right)^+ \\ &= \left(\log_2 \left(\frac{\left| h^n_{d,m} \right|^2}{\left| h^n_{a,m} \right|^2} + \frac{p^n_m \left| h^n_{b,m} \right|^2}{p_s \left| h^n_{a,m} \right|^2 + p^n_m \left| h^n_{b,m} \right|^2} \right) \right)^+ \end{aligned} \tag{3}$$

where $(x)^+$ represents $\max\{x, 0\}$.

If we let $A^n_m = \frac{\left| h^n_{d,m} \right|^2}{\left| h^n_{a,m} \right|^2}$ and $B^n_m = \frac{p_s \left| h^n_{a,m} \right|^2}{\left| h^n_{b,m} \right|^2}$, then we can rewrite the secrecy rate RS^n_m as

$$\mathrm{RS}^n_m = \left(\log_2 \left(A^n_m + \frac{p^n_m}{B^n_m + p^n_m} \right) \right)^+ \tag{4}$$

In this paper, our primary goal is to maximize the available secrecy rate through careful resource allocation approaches. Joint subcarrier and power allocation is carefully considered to meet the secure requirements of the cooperative OFDMA network. As we know, the optimal subcarrier and power allocation is an NP-hard problem and will become extremely complex as the number of subcarriers gets large. For simplicity, we divide the original optimization problem into two progressive subproblems, that is, the subcarrier assignment and power allocation are separately optimized. Firstly, we assign the subcarriers using the dual approach under the assumption that the relay power is equally allocated to all the subcarriers. After that, the relay power is allocated to the subcarriers according to the ACA-A mechanism. The distributed auction can not only reduce the complexity of solving the power allocation problem but also can ensure all the users' secrecy rate. Therefore, the auction-based power allocation can effectively avoid the high complexity and the unfairness, which are both the drawbacks of the centralized methods. In the following two sections, the dual-based subcarrier assignment and the ACA-A-based power allocation are respectively introduced.

3 Dual-based subcarrier assignment

As illustrated above, our first task is to assign the subcarriers to the source-destination pairs. Here, we can express the subcarrier assignment by the binary assignment variables c^n_m. If $c^n_m = 1$, it implies that the nth subcarrier is assigned to the mth source-destination pair; and if $c^n_m = 0$, otherwise. Also, the binary assignment variables form the subcarrier assignment matrix $\mathbf{C}_{N \times M}$. As a result, we can treat the subcarrier assignment problem as a 0-1 integer programming problem.

The goal of this section is to find the optimal subcarrier assignment policies to maximize the system sum secrecy rate while satisfying the minimum secrecy rate constraints. As a result, the optimization problem for the subcarrier assignment can be formulated as follows:

$$\begin{aligned} &\text{maximize} && RS = \sum_{m=1}^{M}\sum_{n=1}^{N} c_m^n RS_m^n \\ &\text{subject to} && (5a) \sum_{m=1}^{M} c_m^n \le 1, \forall \mathrm{n} \\ &&& (5b)\, c_m^n \in \{0,1\}, \forall m, \mathrm{n} \\ &&& (5c) \sum_{n=1}^{N} c_m^n RS_m^n \ge \overline{RS}_m, \forall m \end{aligned} \tag{5}$$

where RS is the system sum secrecy rate and is the optimization goal in this paper. The constraints 5a) and 5b) are used to guarantee that each subcarrier can only be exclusively assigned to one user pair, and the last constraint 5c) indicates that the secrecy rate of each user pair must be larger than a predefined threshold to ensure the secure communication.

It is not difficult to find that the optimization problem defined in (5) satisfies the time-sharing condition which was introduced in [17], that is, the objective function is concave and the constraint 5c) is convex given that RS_m^n is concave in p_m^n and that the integral preserves concavity. As a result, we can employ the dual approach to solve the subcarrier assignment problem, and the duality gap becomes asymptotically zero for a large enough number of subcarriers.

We firstly derive the Lagrangian function of the optimization problem as

$$\begin{aligned} L(\mathbf{C}, \boldsymbol{\lambda}) &= \sum_{m=1}^{M}\sum_{n=1}^{N} c_m^n \mathrm{RS}_m^n + \sum_{m=1}^{M} \lambda_m \left(\sum_{n=1}^{N} c_m^n \mathrm{RS}_m^n - \overline{\mathrm{RS}}_m \right) \\ &= \sum_{m=1}^{M} (1+\lambda_m) \sum_{n=1}^{N} c_m^n \mathrm{RS}_m^n - \sum_{m=1}^{M} \lambda_m \overline{\mathrm{RS}}_m \end{aligned} \tag{6}$$

where $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, \ldots, \lambda_m]^T$ is the vector of dual variables for the constraints. Therefore, the Lagrangian dual function can be obtained [18]:

$$\mathrm{g}(\boldsymbol{\lambda}) = \begin{cases} \max\limits_{\mathbf{C}} L(\mathbf{C}, \boldsymbol{\lambda}) \\ \text{s.t.} \quad \sum\limits_{m=1}^{M} c_m^n \le 1, \forall \mathrm{n} \\ \qquad c_m^n \in \{0,1\}, \forall m, \mathrm{n} \end{cases} \tag{7}$$

Accordingly, the dual problem of the original problem can be expressed as

$$\min_{\boldsymbol{\lambda} \ge 0} \mathrm{g}(\boldsymbol{\lambda}) \tag{8}$$

By dual decomposition, we can remove the coupling among the subcarriers and then the dual problem $\mathrm{g}(\boldsymbol{\lambda})$ can be decomposed into N independent subproblems at each subcarrier. For the nth subcarrier, the optimization problem is

$$\begin{aligned} &\text{maximize} && L_n(\mathbf{C^n}) = \sum_{m=1}^{M} (1+\lambda_m) c_m^n \mathrm{RS}_m^n \\ &\text{subject to} && \sum_{m=1}^{M} c_m^n \le 1, c_m^n \in \{0,1\}, \forall m \end{aligned} \tag{9}$$

where $\mathbf{C^n}$ is the vector of c_m^n on the nth subcarrier, whose elements are all zero except for one non-zero entry. The optimal solution for (9) can be written as

$$c_m^n = \begin{cases} 1, m = m^* = \arg\max\limits_{m} (1+\lambda_m) \mathrm{RS}_m^n \\ 0, \text{otherwise} \end{cases} \tag{10}$$

The dual problem can be solved by the subgradient method [18]. The dual variables $\boldsymbol{\lambda}$ are updated in parallel as follows:

$$\lambda_m(t{+}1) = \left[\lambda_m(t) + \alpha(t) \left(\overline{\mathrm{RS}}_m - \sum_{n=1}^{N} c_m^n(t) \mathrm{RS}_m^n(t) \right) \right]^+ \tag{11}$$

where t is the iteration number, and $\alpha(t)$ represents the proper step sizes. The above update is guaranteed to converge to the optimal dual variables as long as the step sizes follow a diminishing step size rule.

Theorem 1. *[19] If* $\sum\limits_{t} \alpha(t) \to \infty$ *and* $\alpha(t) \to 0$ *as* $t \to \infty$*, then the optimizing goal can converge to the optimal value.*

According to Theorem 1, the optimal solution can be obtained as long as we design a non-convergent infinite series $\alpha(t)$, whose items decrease to zero as the iteration number goes to infinite. Therefore, in this paper, we let $\alpha(t) = \frac{1}{t}$ and the optimal solution can be achieved.

Finally, the dual-based subcarrier assignment algorithm can be summarized as follows:

(S1) Initialize $\boldsymbol{\lambda}(0)$. The user pairs feedback RS_m and CSI to the relay.
(S2) Given $\boldsymbol{\lambda}(t)$, for each subcarrier n, the relay

(a) calculates the secrecy rate $\mathrm{RS}_{m,t}^n$,
(b) solves the assignment variables $c_{m,t}^n$ according to (eq10),
(c) broadcasts the subcarrier assignment matrix $\mathbf{C}_t$ of this iteration to all the sources.

(S3) The sources update the dual variables $\boldsymbol{\lambda}(t)$ according to (11) and then set $t = t + 1$.
(S4) Return to (S2) until convergence is reached.

4 ACA-A-based power allocation

In Section 3, all the subcarriers have been carefully assigned to the user pairs based on the dual approach. The following key issue is how to allocate the available relay power efficiently to all the subcarriers in a distributed way. In this paper, we adopt the ACA-A mechanism [12] to optimize the relay power allocation to improve the system sum secrecy rate. On one hand, the distributed auction can reduce the complexity of solving the power allocation problem. On the other hand, the auction can also ensure the competitive fairness among all the bidders, and thus, all the users' secrecy rate can be guaranteed.

In the proposed ACA-A model, we try to maximize the secrecy rate on each subcarrier, and finally the system sum secrecy rate is maximized. Taking the structure of the cooperative OFDMA network into consideration, we define the auction elements as follows: the good for sale is the total relay power, the relay is the auctioneer, and the subcarriers are the bidders. However, the subcarriers are not authentic entities and are not capable of reporting its optimal demands to the auctioneer in the auction process, but we should notice that the relay has broadcasted the final subcarrier assignment matrix to all the sources in the former step, which implies that each source knows which subcarriers belong to it. As a result, it is the corresponding source node that interacts with the relay instead of the subcarrier in the auction process. Therefore, although we model the subcarriers as the bidders, it is actually the sources that participate in the auction.

In the proposed ACA-A model, each subcarrier competes for the relay power in order to increase its own secrecy rate. However, each subcarrier has to pay the relay for the power. The payment is determined by the amount of power it buys and the unit price. Accordingly, we define the utility function of the nth subcarrier as

$$U_m^n\left(p_m^n,\mu\right)=\mathrm{RS}_m^n\left(p_m^n\right)-\mathcal{P}\left(p_m^n,\mu\right) \tag{12}$$

where $\mathcal{P}\left(p_m^n,\mu\right)$ denotes the cost paid for the relay, and μ is the unit price of the relay power asked by the relay in the auction. The cost function $\mathcal{P}\left(p_m^n,\mu\right)$ should be monotonically increasing with p_m^n, which means that the cost will be higher if the relay power that one subcarrier buys is larger. In this paper, for simplicity and efficiency, we adopt the linear cost function [20] defined as

$$\mathcal{P}\left(p_m^n,\mu\right)=\mu p_m^n \tag{13}$$

Having defined the utility functions of the bidders, now, we turn to the auctioneer. The relay charges the subcarriers for the relay power to maximize its own profits. The auctioneer's profit should be similar with the bidder's cost function, which increases with the power consumption and the unit price. This paper mainly focuses on the bidders' profit and the increase of the secrecy rate. As a result, we just establish a simple and linear utility function for the relay [7] defined as

$$\begin{aligned}&U_r\left(\left\{p_m^n\right\},\mu\right)=\mu\sum_{m=1}^{M}\sum_{n=1}^{N}p_m^n\\&\text{subject to}\quad 0\le\sum_{m=1}^{M}\sum_{n=1}^{N}p_m^n\le p_{\max}\end{aligned} \tag{14}$$

We can easily see that the relay's utility function is monotonically increasing with the unit price μ and the total power consumption $\sum_{m=1}^{M}\sum_{n=1}^{N}p_m^n$. We should note that there should be a reserve price μ^0 in the trade, which is set equal to the average cost of transmitting unit power, i.e., $\mu^0=\mathcal{C}\text{ost}/p_{\max}$, where $\mathcal{C}$ost denotes the basic cost of the relay. Then, we can always keep the relay in the trade if the asking price μ is larger than μ^0. In the next subsection, the ACA-A-based power allocation algorithm is carried out and analyzed in detail.

4.1 ACA-A-based power allocation algorithm

The detailed steps of the proposed ACA-A-based power allocation algorithm are summarized as follows:

```
(S1) Given the available relay power $p_{\max}$, the price step $\delta>0$ and the iteration index $t=0$. The relay initializes the asking price with the reserve price $\mu^0$ and broadcasts it to all the sources.
(S2) For each subcarrier $n$, its corresponding source $S_m$ computes $p_{m,0}^n=\arg\max_{p_m^n}U_m^n\left(p_m^n,\mu^0\right)$ and submits its optimal bid $p_{m,0}^n$ to the relay.
(S3) The relay sums up all the bids from the sources $p_{\text{total},0}=\sum_{n=1}^{N}\sum_{m=1}^{M}p_{m,0}^n$ and compares it with $p_{\max}$:
    (1) If $p_{\text{total},0}\le p_{\max}$, the relay concludes the auction and chooses to quit the trade.
    (2) Else, update $\mu^{t+1}=\mu^t+\delta$, $t=t+1$, and repeat:
        (a) The relay announces $\mu^t$ to all the sources.
        (b) For each subcarrier $n$, its corresponding source $S_m$ computes $p_{m,t}^n=\arg\max_{p_m^n}U_m^n\left(p_m^n,\mu^t\right)$ and submits its optimal bid $p_{m,t}^n$ to the relay.
        (c) The relay sums up all the bids from the sources $p_{\text{total},t}=\sum_{n=1}^{N}\sum_{m=1}^{M}p_{m,t}^n$ and compares it with $p_{\max}$:
```

- If $p_{\text{total},t} > p_{\max}$, first compute $\mathrm{F}_{m,t}^{n} = \left(p_{\max} - \sum\limits_{i \neq m} \sum\limits_{j \neq n} p_{i,t}^{j}\right)^{+}$, then set $\mu^{t+1} = \mu^{t} + \delta$, $t = t + 1$ and continue the auction.
- Else, set $T = t$ and compute $\mathrm{F}_{m,T}^{n} = p_{m,T}^{n} + \frac{p_{m,T-1}^{n} - p_{m,T}^{n}}{\sum\limits_{m}\sum\limits_{n} p_{m,T-1}^{n} - \sum\limits_{m}\sum\limits_{n} p_{m,T}^{n}} \left(p_{\max} - \sum\limits_{m}\sum\limits_{n} p_{m,T}^{n}\right)$, conclude the auction and allocate $p_{m}^{n^*} = \mathrm{F}_{m,T}^{n}$ to the nth subcarrier.

(S4) Finally, the utility of the nth subcarrier is $U_{m}^{n^*}\left(p_{m}^{n^*}, \mu^{T}\right) = \mathrm{RS}_{m}^{n}(p_{m}^{n^*}) - \mathcal{P}(p_{m}^{n^*}, \mu^{T})$, where $\mathcal{P}^*(p_{m}^{n^*}, \mu^{T})$ is the payment of the nth subcarrier and can be expressed as
$\mathcal{P}(p_{m}^{n^*}, \mu^{T}) = \mu^{0}\mathrm{F}_{m,0}^{n} + \sum\limits_{t=1}^{T} \mu^{t}\left(\mathrm{F}_{m,t}^{n} - \mathrm{F}_{m,t-1}^{n}\right)$.

We can easily see that the cost function used above is different from that defined in (13). We give a special explanation here. If the cost function (13) is adopted, we call the auction the ACA-T, which is not cheat-proof. To overcome the drawback of the ACA-T, we adopt the ACA-A instead, which can lead to the same power allocation policies [7]. Different from the ACA-T, in each iteration of the ACA-A, the relay needs to calculate the cumulative clinch [21], which is the amount of power that each subcarrier is guaranteed to win in the iteration. For the nth subcarrier, the cumulative clinch can be expressed as

$$\mathrm{F}_{m,t}^{n} = \left(p_{r} - \sum_{i \neq m}\sum_{j \neq n} p_{i,t}^{j}\right)^{+} \tag{15}$$

Then, the payment of the nth subcarrier after the final iteration T is

$$\mathcal{P}(p_{m}^{n^*}, \mu^{T}) = \mu^{0}\mathrm{F}_{m,0}^{n} + \sum_{t=1}^{T} \mu^{t}\left(\mathrm{F}_{m,t}^{n} - \mathrm{F}_{m,t-1}^{n}\right) \tag{16}$$

In every iteration of the proposed ACA-A-based power allocation algorithm, each subcarrier needs to compute the optimal bid $p_{m,t}^{n} = \arg\max\limits_{p_{m}^{n}} U_{m}^{n}\left(p_{m}^{n}, \mu^{t}\right)$. Differentiating the utility function in (12) with respect to p_{m}^{n} and setting it to zero, we have

$$\frac{\partial U_{m}^{n}}{\partial p_{m}^{n}} = \frac{1}{\ln 2} \cdot \frac{B_{m}^{n}}{\left(A_{m}^{n}+1\right) p_{m}^{n2} + B_{m}^{n}\left(2A_{m}^{n}+1\right) p_{m}^{n} + A_{m}^{n}B_{m}^{n}2} - \mu = 0 \tag{17}$$

$$\left(A_{m}^{n}+1\right) p_{m}^{n2} + B_{m}^{n}\left(2A_{m}^{n}+1\right) p_{m}^{n} + A_{m}^{n}B_{m}^{n2} - \frac{B_{m}^{n}}{\mu \ln 2} = 0 \tag{18}$$

By solving (18), we can easily obtain the optimal bid p_{m}^{n*} and then compare it with the constraints, we can get

$$p_{m}^{n*} = \min(p_{\max}, \max(p_{m}^{n*}, 0)) \tag{19}$$

4.2 Properties of the ACA-A-based power allocation algorithm

In this subsection, we analyze some properties of the proposed ACA-A-based power allocation algorithm: the existence of the equilibrium and the cheat-proof property. The cheat-proof property implies that the cheating behaviors can be effectively avoided in the auction process. If an auction is cheat-proof, it means that in every iteration, the mutually best response of each bidder is to submit its true optimal bid rather than any other bid value. Therefore, no bidder has the incentive to cheat in the auction procedure because any cheating will lead to the loss of its ultimate utility value.

Theorem 2. *The proposed ACA-A-based power allocation algorithm converges after a finite number of iterations and exists at least one equilibrium point.*

Proof. Rearrange (17) and we obtain the following equation

$$\frac{\left|h_{a,m}^{n}\right|^{2}}{\ln 2\left|h_{b,m}^{n}\right|^{2}} \cdot \frac{1}{\left(A_{m}^{n}+1\right) p_{m}^{n2} + B_{m}^{n}\left(2A_{m}^{n}+1\right) p_{m}^{n} + A_{m}^{n}B_{m}^{n2}} = \frac{\mu}{p_{s}} \tag{20}$$

From (20), we can see that if the unit price μ is large enough, the optimal power has to be sufficiently small to keep the equation holding. It is obvious that the left side of (18) is positive and bounded by a finite number K. Here, we assume that the left side is always smaller than a finite number under all the constraints. Then, we can approximately conclude that the optimal power satisfies

$$\lim_{\mu \to Kp_{s}} \frac{p_{m}^{n*}}{p_{\max}} = 0 \tag{21}$$

According to the ACA-A algorithm, the unit price μ increases with a fixed price step $\delta > 0$ until the auction concludes. Therefore, with a sufficiently large t, the unit price μ will be quite high. So, we have

$$\lim_{t \to Kp_{s}/\delta} \frac{p_{m}^{n*}}{p_{\max}/N} = 0 \tag{22}$$

Therefore, there exists a finite positive iteration index T, $T < Kp_{s}/\delta$, satisfying the condition $\sum\limits_{n=1}^{N}\sum\limits_{m=1}^{M} p_{m,T}^{n} < p_{\max}$. So, we can conclude that the proposed ACA-A algorithm converges after a finite number of iterations and exists at least one equilibrium point. Therefore, Theorem 2 is proved. □

Theorem 3. *The proposed ACA-A-based power allocation algorithm is cheat-proof and no bidder cheats in the auction.*

Proof. Here, we assume that if all the bidders are honest and report their true bid values in the auction procedure, the auction concludes after T_1 iterations. If all the other bidders are honest except that one bidder n submits $kp_m^n\,(k > 0, k \neq 1)$ instead of the optimal power p_m^n in each iteration, we assume that the auction concludes after T_2 iterations. The ultimate utility values of the bidder n are denoted by U_{m,T_1}^n and U_{m,T_2}^n, respectively. According to the ACA-A algorithm, we have

$$\begin{aligned} U_{m,T_j}^n = {} & \mathrm{RS}_m^n\left(\mathrm{F}_{m,T_j}^n\right) - \mu^0 \mathrm{F}_{m,0}^n \\ & - \sum_{t=1}^{T_j} \mu^t \left(\mathrm{F}_{m,t}^n - \mathrm{F}_{m,t-1}^n\right), j \in \{1,2\} \end{aligned} \tag{23}$$

When the fixed price step δ is sufficiently small, we have

$$\mathrm{F}_{m,T_j}^n = p_{m,T_j}^n = p_{\max} - \sum_{i \neq m} \sum_{j \neq n} p_{i,T_j}^j, j \in \{1,2\} \tag{24}$$

There are two cases here:

1. If $T_2 < T_1$, then $\mu^{T_2} < \mu^{T_1}$, and we have

$$\begin{aligned} U_{m,T_1}^n - U_{m,T_2}^n = {} & \mathrm{RS}_m^n\left(\mathrm{F}_{m,T_1}^n\right) - \mathrm{RS}_m^n\left(\mathrm{F}_{m,T_2}^n\right) \\ & - \sum_{t=T_2+1}^{T_1} \mu^t \left(\mathrm{F}_{m,t}^n - \mathrm{F}_{m,t-1}^n\right) \\ & > \mathrm{RS}_m^n\left(\mathrm{F}_{m,T_1}^n\right) - \mu^{T_1} p_{m,T_1}^n \\ & - \mathrm{RS}_m^n\left(\mathrm{F}_{m,T_2}^n\right) + \mu^{T_1} p_{m,T_2}^n \\ & = U_m^n\left(p_{m,T_1}^n, \mu^{T_1}\right) - U_m^n\left(p_{m,T_2}^n, \mu^{T_1}\right) \\ & \geq 0 \end{aligned} \tag{25}$$

2. If $T_2 \geq T_1$, then $\mu^{T_2} \geq \mu^{T_1}$, and we have

$$\begin{aligned} U_{m,T_1}^n - U_{m,T_2}^n = {} & \mathrm{RS}_m^n\left(\mathrm{F}_{m,T_1}^n\right) - \mathrm{RS}_m^n\left(\mathrm{F}_{m,T_2}^n\right) \\ & + \sum_{t=T_1+1}^{T_2} \mu^t \left(\mathrm{F}_{m,t}^n - \mathrm{F}_{m,t-1}^n\right) \\ & \geq \mathrm{RS}_m^n\left(\mathrm{F}_{m,T_1}^n\right) - \mu^{T_1} p_{m,T_1}^n \\ & - \mathrm{RS}_m^n\left(\mathrm{F}_{m,T_2}^n\right) + \mu^{T_1} p_{m,T_2}^n \\ & = U_m^n\left(p_{m,T_1}^n, \mu^{T_1}\right) - U_m^n\left(p_{m,T_2}^n, \mu^{T_1}\right) \\ & \geq 0 \end{aligned} \tag{26}$$

From (25) and (26), we can conclude that $U_{m,T_1}^n \geq U_{m,T_2}^n$ always holds in both cases. As a result, if all the other bidders submit their true optimal bid values, the best response of the bidder n is also to report its true optimal bid value at every iteration. In other words, to submit the optimal bid is the mutually best response for all the bidders. In such auction, no bidder intends to cheat in the auction procedure, and any cheating may lead to the loss of its ultimate utility value. Therefore, the proposed that ACA-A algorithm is cheat-proof, and Theorem 3 is proved. □

5 Simulation results and discussions

In this section, some simulation results done on the MATLAB platform are carried out to verify the performance of our proposed joint subcarrier and power allocation algorithm in this paper. The simulation assumptions and parameters are set up as follows [7]. We assume that there are totally M source-destination pairs randomly locating around the untrusted relay. These source-destination pairs share the total N available subcarriers. All the source nodes transmit with the power $p_s = 1$ W. For all the channels, a slow and flat Rayleigh fading environment with unitary power is assumed, where the channel coefficients consist of the Rayleigh fading and the long path loss; the path loss factor is $\beta = 2$. The thermal noise variance at each node is $\sigma^2 = 10^{-12}$ W. We set the reserve price μ^0 to 0.1 and set the price step δ to 0.01 in the simulation.

At the very beginning, we verify that our proposed that joint subcarrier and power allocation algorithm can actually ameliorate the physical layer security for the cooperative OFDMA network. In Figures 2 and 3, four different algorithms are simulated respectively:

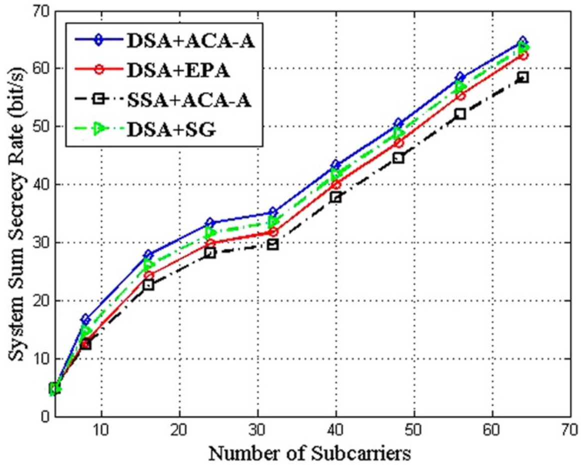

Figure 2 System sum secrecy rate versus number of subcarriers ($M = 4$).

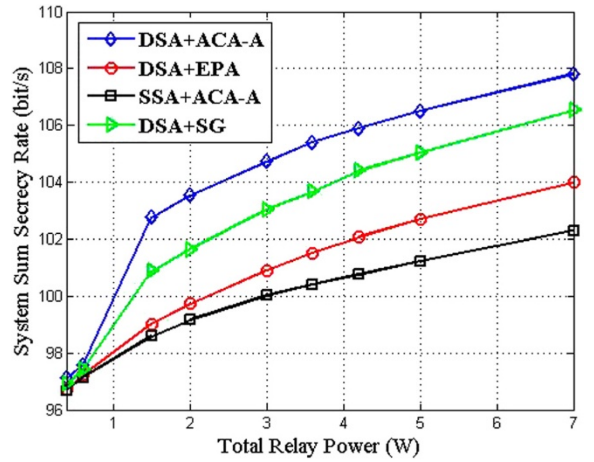

Figure 3 System sum secrecy rate versus total relay power ($M = 4$,$N = 64$).

- *DSA+ACA-A*. This represents our proposed joint subcarrier and power allocation algorithm in this paper.
- *DSA+EPA*. The subcarriers are assigned to the user pair based on the dual approaches [22], and the relay power is equally allocated to all the subcarriers.
- *SSA+ACA-A*. In this algorithm, the subcarriers are randomly assigned to the pairs, and the relay power is allocated using the ACA-A mechanism [7].
- *DSA+SG*. This means the dual-based subcarrier assignment and the Stackelberg game-based relay power allocation in [4].

Figure 2 depicts the relationship between the system sum secrecy rate and the number of subcarriers, and Figure 3 shows how the system sum secrecy rate changes with the total relay power. From Figures 2 and 3, we can easily draw the following conclusions:

Table 1 Number of iterations of the dual-based subcarrier assignment algorithm

Number of subcarriers	Iteration times
4	50
8	29
16	78
24	71
32	59
40	79
48	79
56	76
64	72

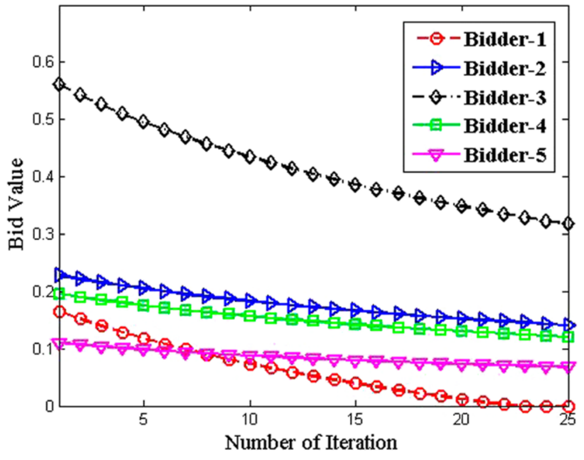

Figure 4 Bid value change versus number of iterations ($M = 4, N = 128$).

- Our proposed 'DSA+ACA-A' algorithm can far outperform the other algorithms as the number of the subcarriers and the total relay power increase. This implies that physical layer security can be meliorated through felicitous subcarrier and power allocation in this paper.
- In the Stackelberg game-based power allocation algorithm, the information exchange indeed includes the optimal power and the optimal price. In each iteration of our proposed ACA-A-based power allocation algorithm, each source needs to submit the optimal bid, and the relay only needs to broadcast the updated price. The two game-based algorithms could both improve the physical layer security with less information exchange. This implies that our proposed power allocation algorithm can achieve better performance than the Stackelberg game-based

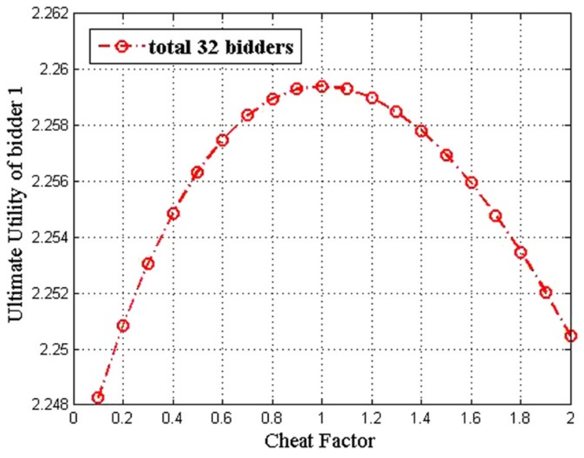

Figure 5 Ultimate utility of bidder 1 versus cheat factor ($N = 32$).

algorithm with almost the same information exchange.

- We can also find that the security performance of the system will become much worse when the subcarriers are randomly allocated or the power is equally allocated. The simulation results demonstrate that the subcarrier assignment and power allocation are both very important to the improvement of the physical layer security. More importantly, we can conclude that joint resource management far outperforms the separate subcarrier assignment or power allocation.

Next, we evaluate the convergence behavior of the proposed dual-based subcarrier assignment algorithm and the ACA-A-based power allocation algorithm, respectively. Table 1 lists the number of iterations of the DSA algorithm when the number of the available subcarriers is different. We can see that the number of iteration always lie between 20 and 80 no matter what the number of the subcarriers is. The complexity of the DSA algorithm is quite acceptable in practice. Figure 4 shows how the bid value of each bidder changes in the auction procedure of the ACA-A algorithm. The iteration process will not stop until the sum of the absolute value of the bid value change in the adjoining iterations is less than 10^{-4}. We can find that the iteration stops within about 25 times while the number of the bidders is 128. Therefore, our proposed ACA-A-based power allocation algorithm has a desirable convergence performance and can converge within a finite number of iterations.

Finally, we examine the cheat-proof property of our proposed ACA-A mechanism. In our simulation, the 32 bidders' case is considered and the bidder 1 submits a false bid $\hat{p}^n_{m,t}$ by scaling the true bid $p^n_{m,t}$ with a positive cheat factor k, namely $\hat{p}^n_{m,t} = k \cdot p^n_{m,t}$. In Figure 5, the relationship between the ultimate utility value of the bidder 1 and the cheat factor value is presented. It is obvious that the ultimate utility value of the bidder 1 is maximized when the cheat factor k equals 1, which indicates that no bidder has the incentive to cheat in the auction procedure because any cheating behavior will lead to a loss in its ultimate utility value. Therefore, the cheat-proof property of our proposed ACA-A mechanism is verified.

6 Conclusion

In this paper, we develop a joint subcarrier and power allocation algorithm to improve physical layer security in cooperative OFDMA networks. Specifically, we assign the subcarriers to the source-destination pairs by utilizing the dual approach under the assumption that the power is equally allocated to all the subcarriers. Then, the relay power is allocated to the subcarriers according to the ACA-A mechanism. We prove that both of the subproblems can converge in a finite number of iterations. We also found that the proposed auction is cheat-proof and, thus, can avoid cheating behaviors in the auction process. Numerical results also demonstrate that our proposed algorithm can effectively increase the system sum secrecy rate.

Physical layer security is a potential supplement for the cryptographic methods and an effective technique to achieve perfect secrecy rate against eavesdropping. In the future, we will try to develop more effective and simpler resource allocation algorithms for the cooperative OFDMA networks to gain the capabilities against eavesdropping.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This study is supported by the National Natural Science Foundation of China (no. 61001107), the China Postdoctoral Science Foundation under grant no. 2013T60912, and the Jiangsu Provincial Natural Science Foundation of China under grant no. BK2013105.

Received: 4 December 2012 Accepted: 9 July 2013
Published: 18 July 2013

References

1. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
2. L Dong, H Yousefi' zadeh, H Jafarkhani, Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper. Paper presented at the IEEE ICC, Kyoto, Japan, 5–9 June 2011
3. N R-Zurita, M Ghogho, D McLernon, Outage probability based power distribution between data artificial noise for physical layer security. IEEE Signal Process. Lett. **19**(2), 71–74 (2012)
4. Z Han, N Marina, M Debbah, A Hjotrungnes, Physical layer security game: interaction between source, eavesdropper, and friendly jammer. EURASIP J. Wireless Commun. and Netw.-Special Issue on Wireless Phys. Layer Security. **2009**(11), 445–453 (2009)
5. R Zhang, L Song, Z Han, B Jiao, Physical layer security for two-way untrusted relaying with friendly jammers. IEEE Trans. Veh. Technol. **61**(8), 3693–3704 (2012)
6. W Saad, Z Han, T Basar, A Hjorungnes, Physical layer security: coalitional games for distributed cooperation. Paper presented at the seventh international symposium on modeling and optimization in mobile, ad hoc, and wireless networks, Seoul, South Korea, 23–27 June 2009
7. R Zhang, L Song, Z Han, B Jiao, Improve physical layer security in cooperative wireless network using distributed auction games. Paper presented at the IEEE INFOCOM WKSHPS , Shanghai, China, 15 April 2011
8. X Wang, M Tao, J Mo, Y Xu, Power and subcarrier allocation for physical-layer security in of DMA-based broadband wireless networks. IEEE T. Inf. Foren. Sec. **6**(3), 693–702 (2011)
9. G Owen, *Game Theory, 3rd edition* (Academic, Salt Lake City, 2001)
10. J Huang, Z Han, HV Chiang, Poor, Auction-based resource allocation for cooperative communications. IEEE J. Select. Areas Commun. **26**(7), 1226–1237 (2008)
11. J Huang, RA Berry, ML Honig, Auction-based spectrum sharing. ACM Mobile Netw. Appl. J. **11**(3), 405–418 (2006)
12. V Krishna, *Auction Theory, 2nd edition* (Academic Press, Salt Lake City, 2009)
13. X He, A Yener, Cooperation with an untrusted relay: A secrecy perspective. IEEE Trans. Inf. Theory **56**(8), 3807–3827 (2010)
14. He X, A Yener, Two-hop secure communication using an untrusted relay: A case for cooperative jamming. Paper presented at the IEEE GLOBECOM , New Orleans, LO, 30 November–4 December 2008
15. R Zhang, L Song, Z Han, B Jiao, M Debbah, Physical layer security for two way relay communications with friendly jammers. Paper presented at IEEE GLOBECOM , Miami, FL, 6–10 December 2010
16. CW Sung, KK Leung, A generalized framework for distributed power control in wireless networks. IEEE Trans. Inf. Theory **51**(7), 2625–2635 (2005)

17. W W Yu, R Lui, Dual methods for nonconvex spectrum optimization of multicarrier systems. IEEE Trans. Commun. **54**(7), 1310–1322 (2006)
18. S Boyd, L Vandenberghe, *Convex Optimization* (Cambridge University Press, London, 2004)
19. L Wolsey, *Integer Programming* (Wiley-Interscience Publication, San Francisco, 1998)
20. P Marbach, R Berry, Downlink resource allocation and pricing for wireless networks. IEEE INFOCOM. **3**, 1470–1479 (2002)
21. LM Ausubel, An efficient ascending-bid auction for multiple objects. Am. Eco. Rev. **94**(5), 1452–1475 (2004)
22. D Zhang, Y Wang, J Lu, Qos aware relay selection and subcarrier allocation in cooperative OFDMA systems. IEEE Commun. Lett. **14**(4), 294–296 (2010)

doi:10.1186/1687-1499-2013-193
Cite this article as: Wang *et al.*: **Joint subcarrier and power allocation for physical layer security in cooperative OFDMA networks.** *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:193.

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Immediate publication on acceptance
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com