Improve Physical Layer Security in Cooperative Wireless Network using Distributed Auction Games

Rongqing Zhang*, Lingyang Song*, Zhu Han†, and Bingli Jiao*
*School of Electronics Engineering and Computer Science, Peking University, Beijing, China.
†Electrical and Computer Engineering Department, University of Houston, Houston, TX, USA.

***Abstract*—In this paper, we investigate a cooperative wireless network with jamming-based secure communications, where a friendly jammer can transmit jamming signals to interfere the malicious eavesdropper. We find that the secrecy rate of the source-destination link can be effectively improved with the help of the friendly jammer, and each source intends to obtain optimal jamming power from the friendly jammer to maximize its secrecy rate for data transmission. We then formulate this power allocation problem as an auction game and propose two distributively auction-based power allocation schemes, which are power allocation using Traditional Ascending Clock Auction (ACA-T) and power allocation using Alternative Ascending Clock Auction (ACA-A), considering the friendly jammer as the auctioneer and the sources as the bidders. In addition, we prove that both the proposed schemes can converge in a finite number of iterations. We also prove that the ACA-A scheme is cheat-proof while the ACA-T scheme is not. Finally, simulation results are presented to demonstrate the efficiency of the proposed auction-based schemes in improving secrecy rate of wireless networks.**

I. Introduction

The basic idea of physical layer security is to exploit the physical characteristics of wireless channels to provide secure communications. The security is quantified by *secrecy capacity*, which is defined as the maximum rate of reliable information sent from the source to the intended destination in the presence of eavesdroppers. This line of work was pioneered by Aaron Wyner, who introduced the wiretap channel and established fundamental results of creating perfectly secure communications without relying on private keys [1]. Wyner showed that when the eavesdropper channel is a degraded version of the main channel, the source and the destination can exchange perfectly secure messages at a non-zero rate. In follow-up work, the secrecy capacity of Gaussian wiretap channel was studied [2], and Wyner's approach was extended to the transmission of confidential messages over broadcast channels [3] .

Motivated by the fact that if the source-wiretapper channel has higher channel gain than the source-destination channel, the perfect secrecy capacity will be zero [3], cooperative jamming is considered as a promising approach to improve the secrecy capacity by interfering the eavesdropper with codewords independent of the source messages. For instance, in [5] and [6], several cooperative jamming schemes were investigated for different scenarios. In such cooperative wireless networks with jammers, the network performance of physical layer security depends very much on effective power allocation of jamming signals. To provide an effective and flexible method that studies how the autonomous nodes interact and cooperate with each other for resource allocation, some auction and pricing approaches were therefore proposed in [8]–[11].

In this paper, we investigate how to improve physical layer security in a cooperative scenario, where there is one friendly jammer that can transmit jamming signals to interfere the malicious eavesdropper, as well as several pairs of sources and destinations that want to improve the secrecy rate of their data transmission with the help of the friendly jammer. We find that using a well-chosen amount of jamming power from the friendly jammer, the secrecy rate of a source-destination link can be maximized. In [12], the authors proposed a distributed approach using the share auction by iteratively updating the bids for jamming power allocation in order to optimize the secrecy rate of data transmission. To allocate the jamming power in a distributive and efficient way, we also formulate the power allocation problem as an auction game in which the friendly jammer is the auctioneer and the sources are the bidders. In addition, we propose two power allocation schemes based on auction theory [13], [14], which are power allocation using Traditional Ascending Clock Auction (ACA-T) and power allocation using Alternative Ascending Clock Auction (ACA-A). Then, we investigate some properties of the proposed auction-based power allocation schemes. We prove that both the proposed auction-based schemes can converge in a finite number of iterations. We also prove that the ACA-T scheme is not cheat-proof, while the ACA-A scheme is. Finally, the efficiency of the proposed auction-based schemes are verified by simulations.

The rest of this paper is organized as follows. In Section II, the system model for jammer-assisted secure network is described, and the utilities of the sources and the friendly jammer are formulated. In Section III, two auction-based power allocation schemes are proposed. In Section IV, we investigate some important properties (convergence and cheat-proof) of the proposed auction-based schemes. Simulation results are provided in Section V, and the conclusions are drawn in Section VI.

II. System Model and Problem Formulation

A. System Model

As shown in Fig. 1, we consider a cooperative network consisting of N source nodes, N corresponding destination nodes, one friendly jammer node, and one malicious eavesdropper node, which are denoted by S_i, D_i, $i = 1, 2, \ldots, N$, J, and E, respectively. We denote by $\mathcal{N}$ the set of indices $\{1, 2, \ldots, N\}$. All the nodes here are equipped with a single omni-directional antenna and operate in a half-duplex way, i.e., each node cannot receive and transmit simultaneously. The malicious node always tries to eavesdrop the messages transmitted by the source nodes. The maximum rate of secrecy information

978-1-4244-9920-5/11/$26.00 ©2011 IEEE

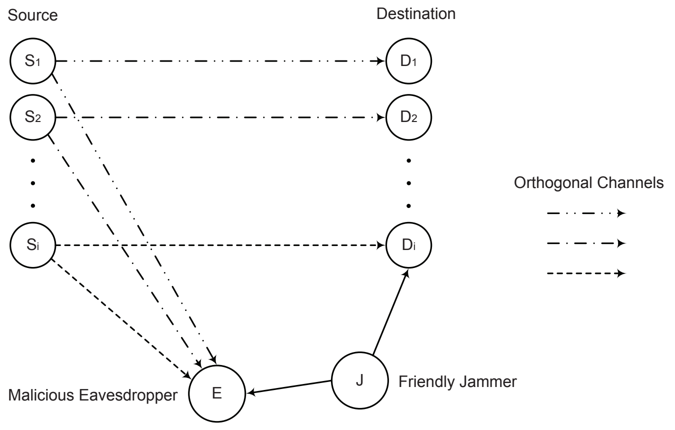

Fig. 1. System model for jammer-assisted secure network.

from the source to its intended destination is defined by the term secrecy capacity, and the secrecy rate we use in this paper is an achievable rate that is smaller than the secrecy capacity.

Suppose source S_i transmits with power p_i, $i \in \mathcal{N}$. The channel gains from source S_i to destination D_i and eavesdropper E are g_{S_i,D_i} and $g_{S_i,E}$, respectively. Friendly jammer J transmits with power p_i^J to help improve the secrecy rate of data transmission from source S_i to destination D_i. The channel gains from friendly jammer J to destination D_i and eavesdropper E are g_{J,D_i} and $g_{J,E}$, respectively. Note that here the channel gains contain the path loss, as well as the Rayleigh fading coefficient with zero mean and unit variance. For simplicity, we assume that the fading coefficients are constant over one slot, and vary independently from one slot to another. The thermal noise power at the destination and eavesdropper nodes is denoted by σ^2. The channel bandwidth is W.

The channel capacity for source S_i to destination D_i, denoted by C_1^i, can be written as

$$C_1^i = W \log \left(1 + \frac{p_i g_{S_i,D_i}}{\sigma^2 + p_i^J g_{J,D_i}} \right). \tag{1}$$

Similarly, the channel capacity for source S_i to malicious eavesdropper E, denoted by C_2^i, can be written as

$$C_2^i = W \log \left(1 + \frac{p_i g_{S_i,E}}{\sigma^2 + p_i^J g_{J,E}} \right). \tag{2}$$

Note that here we assume that there is no interference from the other sources, since different sources transmit their messages to the corresponding destinations in orthogonal channels. Then the secrecy rate for source S_i can be defined as [4]

$$\begin{aligned} C_s^i &= \left(C_1^i - C_2^i \right)^+ \qquad (3) \\ &= W \left[\log \left(1 + \frac{p_i g_{S_i,D_i}}{\sigma^2 + p_i^J g_{J,D_i}} \right) - \log \left(1 + \frac{p_i g_{S_i,E}}{\sigma^2 + p_i^J g_{J,E}} \right) \right]^+, \end{aligned}$$

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

From (1) and (2), we can see that both C_1^i and C_2^i are decreasing and convex functions of jamming power p_i^J, $i \in \mathcal{N}$. However, if C_2^i decreases faster than C_1^i as the jamming power p_i^J increases, C_s^i might increase in a certain region of value p_i^J. But when p_i^J further increases, both C_1^i and C_2^i will approach zero. As a result, C_s^i approaches zero. Then the problems come to whether or not C_s^i can be effectively improved, and how to control the jamming power in a distributed manner. Comparing the expression of C_1^i with that of C_2^i, we can get that if $\frac{g_{J,D_i}}{g_{S_i,D_i}} < \frac{g_{J,E}}{g_{S_i,E}}$, the gain of the secrecy rate will be above zero in a certain region of the jamming power p_i^J. To achieve the improvement, we propose some distributed game theoretical approaches in the following subsections.

B. Source's Utility Function

In this system, we consider source S_i as one of the bidders, $i \in \mathcal{N}$, while friendly jammer J as the auctioneer. The sources submit bids to compete for the jamming power from the friendly jammer, in order to increase the secrecy rate of their own data transmissions. Source S_i can have a performance gain by successfully getting the jamming power p_i^J. However, it needs to pay for the power offered by the friendly jammer, and the payment is determined by the amount of the jamming power and its unit price. Therefore, the utility function of source S_i can be defined as

$$U_i\left(p_i^J, \lambda\right) = \mathcal{G}\left(p_i^J\right) - \mathcal{P}\left(p_i^J, \lambda\right), \tag{4}$$

where $\mathcal{G}\left(p_i^J\right)$ is the performance gain with the jamming power p_i^J, $\mathcal{P}\left(p_i^J, \lambda\right)$ is the cost paid for the friendly jammer, and λ represents the unit price of jamming power asked by the friendly jammer during the auction.

$\mathcal{G}\left(p_i^J\right)$ can be written as

$$\mathcal{G}\left(p_i^J\right) = C_s^i - \tilde{C}_s^i, \tag{5}$$

where C_s^i and $\tilde{C}_s^i$ represent the secrecy rate with and without jamming power, respectively. C_s^i is given in (3), while $\tilde{C}_s^i$ can be obtained by setting $p_i^J = 0$ in (3) as

$$\tilde{C}_s^i = W \left[\log \left(1 + \frac{p_i g_{S_i,D_i}}{\sigma^2} \right) - \log \left(1 + \frac{p_i g_{S_i,E}}{\sigma^2} \right) \right]^+. \tag{6}$$

Generally speaking, the cost paid for the friendly jammer is higher if the jamming power used is larger. Therefore, the cost function $\mathcal{P}\left(p_i^J, \lambda\right)$ should be monotonically increasing with p_i^J. In the literature, due to its simplicity and efficiency, linear pricing is widely used [11]. Then the cost function can be written as

$$\mathcal{P}\left(p_i^J, \lambda\right) = \lambda p_i^J, \tag{7}$$

where the unit price λ is a constant for all the units of jamming power, though it may change in different auction rounds.

From (4), (5), (7), and the expressions of C_s^i in (3) and $\tilde{C}_s^i$ in (6), we can get the utility of source S_i as

$$\begin{aligned} U_i\left(p_i^J, \lambda\right) = W &\left[\log \left(1 + \frac{p_i g_{S_i,D_i}}{\sigma^2 + p_i^J g_{J,D_i}} \right) - \log \left(1 + \frac{p_i g_{S_i,D_i}}{\sigma^2} \right) \right. \\ &\left. - \log \left(1 + \frac{p_i g_{S_i,E}}{\sigma^2 + p_i^J g_{J,E}} \right) + \log \left(1 + \frac{p_i g_{S_i,E}}{\sigma^2} \right) \right] \\ &- \lambda p_i^J, \end{aligned} \tag{8}$$

which is subject to the secrecy rate constraints $C_s^i \geq 0$ and $\tilde{C}_s^i \geq 0$, and transmitting power constraints $0 \leq p_i \leq p_{max}$.

C. Jammer's Utility Function

The friendly jammer charges the sources for the jamming service at a price λ for every unit of jamming power. Provided the maximum power is bounded by p_{max}, we have the utility of friendly jammer J as

$$U_J\left(\{p_i^J\},\lambda\right)=\lambda\sum_i p_i^J, \tag{9}$$
$$\text{s.t.}\quad 0\le\sum_i p_i^J\le p_{max}.$$

Note that there should be a reserve price in the trade, denoted by λ^0, which can be set equal to the average cost of transmitting unit jamming power, i.e., $\lambda^0=\mathcal{C}/p_{max}$, where $\mathcal{C}$ represents the basic cost of sending jamming power at the friendly jammer node. Then, we can easily get if the asking price λ is higher than λ^0, the friendly jammer would always benefit from the trade. Otherwise, it would not participate in the trade.

III. Distributed Auction Games

In this section, we investigate the schemes how the friendly jammer sells the jamming power. Generally speaking, there are two possible approaches, the centralized approach and the distributed approach. In the centralized approach, the friendly jammer knows exactly all the private information of each pair of source and destination as well as the malicious eavesdropper. Thus, the friendly jammer can allocate the jamming power based on the criteria such as maximizing the global secrecy rate or proportional fairness. However, the sources and destinations can be geographically distributed, therefore, it is not feasible for the friendly jammer to collect all the private information of each node in the network. Here we propose two auction-based distributed power allocation schemes, which are power allocation using Traditional Ascending Clock Auction (ACA-T) and power allocation using Alternative Ascending Clock Auction (ACA-A), considering the friendly jammer as the auctioneer and the sources as the bidders. During the auction, the auctioneer first announces an initial price, then the bidders report to the auctioneer their demands at that price, and the auctioneer raises the price until the total demands meet the power supply.

A. ACA-T

In this subsection, the ACA-T scheme based on traditional ascending clock auction [13] is proposed, where each source is allowed to bid any power demand between 0 and p_{max} at every iteration.

As shown in Algorithm I, before the auction, the friendly jammer sets up the iteration index $t=0$, the price step $\delta>0$, as well as the initial asking price λ^0 which is equal to the reserve price given in Subsection II-C, and then announces λ^0 to all the sources. Each source submits its optimal bid $p_{i,0}^J$ by computing

$$\left(p_{i,0}^J,p_{i,0}\right)=\arg\max_{\left(p_i^J,p_i\right)}U_i\left(p_i^J,\lambda^0\right). \tag{10}$$

TABLE I
Algorithm 1: ACA-T

```
1. Given the available jamming power $p_{max}$, price step $\delta > 0$, and iteration index $t = 0$, the friendly jammer initializes the asking price with the reserve price $\lambda^0$.
2. Source $S_i$ computes $\left(p_{i,0}^J, p_{i,0}\right) = \arg\max_{\left(p_i^J,p_i\right)} U_i\left(p_i^J, \lambda^0\right)$ and submits its optimal bid $p_{i,0}^J$.
3. The friendly jammer sums up all the bids from the sources $p_{total,0}^J = \sum_i p_{i,0}^J$ and compares $p_{total,0}^J$ with $p_{max}$:
    * If $p_{total,0}^J \le p_{max}$, the friendly jammer concludes the auction and chooses not to participate in the trade.
    * Else, set $\lambda^{t+1} = \lambda^t + \delta$, $t = t + 1$, and repeat:
        ⋆ The friendly jammer announces $\lambda^t$ to all the sources.
        ⋆ Source $S_i$ computes $\left(p_{i,t}^J, p_{i,t}\right) = \arg\max_{\left(p_i^J,p_i\right)} U_i\left(p_i^J, \lambda^t\right)$ and submits its optimal bid $p_{i,t}^J$.
        ⋆ The friendly jammer sums up all the bids from the sources $p_{total,t}^J = \sum_i p_{i,t}^J$ and compares $p_{total,t}^J$ with $p_{max}$:
            • If $p_{total,t}^J > p_{max}$, set $\lambda^{t+1} = \lambda^t + \delta$, $t = t + 1$, and continue the auction.
            • Else, conclude the auction, set $T = t$, and allocate $p_i^{J\star} = p_{i,T}^J + \frac{p_{i,T-1}^J - p_{i,T}^J}{\sum_i p_{i,T-1}^J - \sum_i p_{i,T}^J}\left(p_{max} - \sum_i p_{i,T}^J\right)$ to source $S_i$.
4. Finally, the utility of source $S_i$ is
    $U_i^\star(p_i^{J\star}, \lambda^T) = \mathcal{G}\left(p_i^{J\star}, p_{i,T}\right) - \lambda^T p_i^{J\star}.$
```

The friendly jammer sums up all the bids from the sources $p_{total,0}^J=\sum_i p_{i,0}^J$ and compares $p_{total,0}^J$ with p_{max}. If $p_{total,0}^J\le p_{max}$, the friendly jammer will conclude the auction and choose not to participate in the trade. Otherwise, the friendly jammer sets $\lambda^{t+1}=\lambda^t+\delta$, $t=t+1$, and announces λ^t to all the sources. Then each source submits its optimal bid $p_{i,t}^J$ again by computing

$$\left(p_{i,t}^J,p_{i,t}\right)=\arg\max_{\left(p_i^J,p_i\right)}U_i\left(p_i^J,\lambda^t\right). \tag{11}$$

Comparing the total bid $p_{total,t}^J=\sum_i p_{i,t}^J$ with the maximal jamming power to be sold, if $p_{total,t}^J>p_{max}$, the friendly jammer continues the auction until $p_{total,t}^J\le p_{max}$. Let the final iteration index be T. As the asking price λ increases discretely every round of the auction, we may have that $p_{total,T}^J<p_{max}$, which does not fully utilize the jamming power. To make sure that $p_{total,T}^J=p_{max}$, we modify $p_{i,T}^J$ by introducing proportional rationing [14]. Therefore, the final allocated jamming power of source S_i can be given as

$$p_i^{J\star}=p_{i,T}^J+\frac{p_{i,T-1}^J-p_{i,T}^J}{\sum_i p_{i,T-1}^J-\sum_i p_{i,T}^J}\left(p_{max}-\sum_i p_{i,T}^J\right), \tag{12}$$

where $\sum_i p_i^{J\star}=p_{max}$.

B. ACA-A

Note that the ACA-T scheme described in Subsection III-A is equivalent to the distributed dual-based optimization approach for Network Utility Maximization (NUM) problem [15], which means that the ACA-T scheme can achieve efficient power allocation. However, as we will prove in the next section, the ACA-T scheme is not cheat-proof. To solve this problem, the ACA-A scheme based on alternative ascending clock auction [14] is proposed.

TABLE II
ALGORITHM 2: ACA-A

```
1. Given the available jamming power $p_{max}$, price step $\delta > 0$, and iteration index $t = 0$, the friendly jammer initializes the asking price with the reserve price $\lambda^0$.
2. Source $S_i$ computes $\left(p_{i,0}^J, p_{i,0}\right) = \arg \max_{\left(p_i^J, p_i\right)} U_i\left(p_i^J, \lambda^0\right)$ and submits its optimal bid $p_{i,0}^J$.
3. The friendly jammer sums up all the bids from the sources $p_{total,0}^J = \sum_i p_{i,0}^J$ and compares $p_{total,0}^J$ with $p_{max}$:
    * If $p_{total,0}^J \le p_{max}$, the friendly jammer concludes the auction and chooses not to participate in the trade.
    * Else, set $\lambda^{t+1} = \lambda^t + \delta$, $t = t + 1$, and repeat:
        ⋆ The friendly jammer announces $\lambda^t$ to all the sources.
        ⋆ Source $S_i$ computes $\left(p_{i,t}^J, p_{i,t}\right) = \arg \max_{\left(p_i^J, p_i\right)} U_i\left(p_i^J, \lambda^t\right)$ and submits its optimal bid $p_{i,t}^J$.
        ⋆ The friendly jammer sums up all the bids from the sources $p_{total,t}^J = \sum_i p_{i,t}^J$ and compares $p_{total,t}^J$ with $p_{max}$:
            • If $p_{total,t}^J > p_{max}$, in this algorithm first compute $L_i^t = \max\left(0, p_{max} - \sum_{j \neq i} p_{j,t}^J\right)$, then set $\lambda^{t+1} = \lambda^t + \delta$, $t = t + 1$, and continue the auction.
            • Else, conclude the auction, set $T = t$, compute $L_i^T = p_{i,T}^J + \frac{p_{i,T-1}^J - p_{i,T}^J}{\sum_i p_{i,T-1}^J - \sum_i p_{i,T}^J}\left(p_{max} - \sum_i p_{i,T}^J\right)$, and allocate $p_i^{J\star} = L_i^T$ to source $S_i$.
4. Finally, the utility of source $S_i$ is
    $U_i^\star\left(p_i^{J\star}, \{\lambda^t\}\right) = \mathcal{G}\left(p_i^{J\star}, p_{i,T}\right) - \mathcal{P}_i^\star$,
   where $\mathcal{P}_i^\star$ is the payment of $S_i$ here and can be expressed as
    $\mathcal{P}_i^\star = \lambda^0 L_i^0 + \sum_{t=1}^T \lambda^t\left(L_i^t - L_i^{t-1}\right)$.
```

As shown in Algorithm II, the procedures of ACA-A are the same as ACA-T except that at every iteration t in ACA-A, the friendly jammer computes the cumulative clinch [14], which is the amount of jamming power that each source is guaranteed to win at iteration t. For source S_i, it can be expressed as

$$L_i^t = \max\left(0, p_{max} - \sum_{j \neq i} p_{j,t}^J\right). \tag{13}$$

Then with the cumulative clinch, the payment from source S_i after the final iteration T is

$$\mathcal{P}(p_i^{J\star}, \{\lambda^t\}) = \lambda^0 L_i^0 + \sum\nolimits_{t=1}^T \lambda^t\left(L_i^t - L_i^{t-1}\right). \tag{14}$$

IV. ANALYSIS OF THE PROPOSED AUCTION GAMES

In this section, we investigate some important properties of the two proposed auction-based power allocation schemes: convergence and cheat-proof.

By differentiating the utility function (8) with respect to p_i^J, we have

$$\frac{\partial U_i}{\partial p_i^J} = -\frac{W\gamma_{S_i,D_i}\gamma_{J,D_i}p_i}{\left(1 + \gamma_{J,D_i}p_i^J\right)\left(1 + \gamma_{S_i,D_i}p_i + \gamma_{J,D_i}p_i^J\right)} + \frac{W\gamma_{S_i,E}\gamma_{J,E}p_i}{\left(1 + \gamma_{J,E}p_i^J\right)\left(1 + \gamma_{S_i,E}p_i + \gamma_{J,E}p_i^J\right)} - \lambda, \tag{15}$$

where $\gamma_{S_i,D_i} \triangleq \frac{g_{S_i,D_i}}{\sigma^2}$, $\gamma_{S_i,E} \triangleq \frac{g_{S_i,E}}{\sigma^2}$, $\gamma_{J,D_i} \triangleq \frac{g_{J,D_i}}{\sigma^2}$, and $\gamma_{J,E} \triangleq \frac{g_{J,E}}{\sigma^2}$, $i \in \mathcal{N}$.

To obtain the optimal solution of jamming power for source S_i, let $\frac{\partial U_i}{\partial p_i^J} = 0$, and then we have

$$\frac{\lambda}{Wp_i} = -\frac{\gamma_{S_i,D_i}\gamma_{J,D_i}}{\left(1 + \gamma_{J,D_i}p_i^J\right)\left(1 + \gamma_{S_i,D_i}p_i + \gamma_{J,D_i}p_i^J\right)} + \frac{\gamma_{S_i,E}\gamma_{J,E}}{\left(1 + \gamma_{J,E}p_i^J\right)\left(1 + \gamma_{S_i,E}p_i + \gamma_{J,E}p_i^J\right)}. \tag{16}$$

Rearranging the above equation, we can get a fourth order polynomial equation as

$$\left(p_i^J\right)^4 + F_{i,3}\left(p_i^J\right)^3 + F_{i,2}\left(p_i^J\right)^2 + F_{i,1}\left(p_i^J\right) + F_{i,0} = 0, \tag{17}$$

where $F_{i,l}$, $l = 0, 1, 2, 3$, are formulae of constants γ_{S_i,D_i}, $\gamma_{S_i,E}$, γ_{J,D_i}, and $\gamma_{J,E}$, as well as variables p_i and λ.

The solution of the quartic (17) can be expressed in closed form, but this is not the primary goal here. The optimal solution to our particular interest can be given as

$$p_i^{J*} = p_i^{J*}\left(\lambda, p_i, \gamma_{S_i,D_i}, \gamma_{S_i,E}, \gamma_{J,D_i}, \gamma_{J,E}\right), \tag{18}$$

which is a function of the asking price λ, the source transmitting power p_i, and other channel parameters. Note that the power constraint $0 \le \sum_i p_i^J \le p_{max}$ in the auction, we can get the optimal strategy for source S_i, $i \in \mathcal{N}$, as

$$p_{i\_opt}^J\left(\lambda, p_i\right) = \min\left(p_{max}, \max\left(p_i^{J*}, 0\right)\right). \tag{19}$$

A. Convergence

In this subsection, we prove that both the proposed auction-based power allocation schemes have the convergence property, i.e., each scheme will conclude in a finite number of iterations.

Theorem 1: The ACA-T and ACA-A schemes will conclude in a finite number of iterations.

Proof: From (16), we can see that if the asking price λ is sufficiently large, the optimal solution of jamming power should be quite small to make sure that the equation holds. Note that the right side of (16) is positive and bounded by a finite number, which can be denoted by M, under the power constraints that $0 \le \sum_i p_i^J \le p_{max}$ and $0 \le p_i \le p_{max}$. Then we can approximately obtain that the optimal solution satisfies

$$p_{i\_opt}^J\left(\lambda\right) = o\left(p_{max}\right), \quad \lambda \to WMp_{max}, \tag{20}$$

where $\alpha(x) = o\left(\beta(x)\right)$ $(x \to a)$ means

$$\lim_{x \to a} \frac{\alpha\left(x\right)}{\beta\left(x\right)} = 0.$$

According to Algorithm I and Algorithm II, we have that the asking price λ increases with a fixed price step $\delta > 0$ until the auction concludes, then λ will become quite a high value with a sufficiently large t. Thus, from (20) we can get that

$$p_{i,t}^J\left(\lambda\right) = o\left(\frac{p_{max}}{N}\right), \quad t \to \frac{WMp_{max}}{\delta}, \tag{21}$$

where N is a finite number and represents the number of sources participating in the auction. Therefore, there exists a finite positive iteration index T, $T < \frac{WMp_{max}}{\delta}$, satisfying the condition that $\sum_{i=1}^N p_{i,T}^J < p_{max}$, which means that the ACA-T and ACA-A auction-based schemes conclude in a finite number of iterations. ■

B. Cheat-Proof

In this subsection, we prove that the ACA-A scheme is cheat-proof while the ACA-T scheme is not. A scheme is cheat-proof, which means that in the scheme reporting true optimal demand at every iteration is a mutually best response for each source.

Theorem 2: The ACA-A scheme is cheat-proof.

Proof: Given that all the other sources report their true optimal demands at every iteration during the auction, the auction will conclude at iteration T_1 if source S_i also reports its true optimal demand at every iteration, while the auction will conclude at iteration T_2 if source S_i does not report its true optimal demand at every iteration. The final utility of source S_i is then denoted by $U_i^{T_1}$ and $U_i^{T_2}$, respectively.

According to Algorithm II, we have

$$\begin{aligned} U_i^{T_j} =& \ \mathcal{G}\left(L_i^{T_j}, p_{i,T_j}\right) - \lambda^0 L_i^0 \\ & - \sum\nolimits_{t=1}^{T_j} \lambda^t \left(L_i^t - L_i^{t-1}\right),\ j \in \{1,2\}, \end{aligned} \tag{22}$$

where the expression of $\mathcal{G}$ is given by (5) and (8).

When δ is sufficiently small, we have

$$L_i^{T_j} = p_{i,T_j}^J = p_{max} - \sum_{k=1,k\neq i}^{N} p_{k,T_j}^J,\ j \in \{1,2\}. \tag{23}$$

- If $T_2 < T_1$, as the asking price increases with the iteration index t, we have $\lambda^{T_1} > \lambda^{T_2}$. Then we can get

$$\begin{aligned} & U_i^{T_1} - U_i^{T_2} \\ =& \ \mathcal{G}\left(L_i^{T_1}, p_{i,T_1}\right) - \mathcal{G}\left(L_i^{T_2}, p_{i,T_2}\right) \\ & - \sum_{t=T_2+1}^{T_1} \lambda^t \left(L_i^t - L_i^{t-1}\right) \\ >& \ \mathcal{G}\left(L_i^{T_1}, p_{i,T_1}\right) - \lambda^{T_1} p_{i,T_1}^J - \mathcal{G}\left(L_i^{T_2}, p_{i,T_2}\right) + \lambda^{T_1} p_{i,T_2}^J \\ =& \ U_i\left(p_{i,T_1}^J, p_{i,T_1}, \lambda^{T_1}\right) - U_i\left(p_{i,T_2}^J, p_{i,T_2}, \lambda^{T_1}\right) \\ \geq& \ 0, \end{aligned} \tag{24}$$

  where the last inequality comes from (11) that $\left(p_{i,T_1}^J, p_{i,T_1}\right) = \arg \max\limits_{\left(p_i^J, p_i\right)} U_i\left(p_i^J, \lambda^{T_1}\right)$.

- If $T_2 \geq T_1$, as the asking price increases with the iteration index t, we have $\lambda^{T_1} \leq \lambda^{T_2}$. Then we can get

$$\begin{aligned} & U_i^{T_1} - U_i^{T_2} \\ =& \ \mathcal{G}\left(L_i^{T_1}, p_{i,T_1}\right) - \mathcal{G}\left(L_i^{T_2}, p_{i,T_2}\right) \\ & + \sum_{t=T_1+1}^{T_2} \lambda^t \left(L_i^t - L_i^{t-1}\right) \\ >& \ \mathcal{G}\left(L_i^{T_1}, p_{i,T_1}\right) - \lambda^{T_1} p_{i,T_1}^J - \mathcal{G}\left(L_i^{T_2}, p_{i,T_2}\right) + \lambda^{T_1} p_{i,T_2}^J \\ =& \ U_i\left(p_{i,T_1}^J, p_{i,T_1}, \lambda^{T_1}\right) - U_i\left(p_{i,T_2}^J, p_{i,T_2}, \lambda^{T_1}\right) \\ \geq& \ 0, \end{aligned} \tag{25}$$

  where the last inequality comes from (11) that $\left(p_{i,T_1}^J, p_{i,T_1}\right) = \arg \max\limits_{\left(p_i^J, p_i\right)} U_i\left(p_i^J, \lambda^{T_1}\right)$.

From (24) and (25), we can obtain that $U_i^{T_1} \geq U_i^{T_2}$. Thus, given that all the other sources report their true optimal demands at every iteration, the best strategy of source S_i is to report its true optimal demand at every iteration. Since all the sources are non-collaborative, reporting true optimal demand at every iteration is a mutually best response for each source. There is no incentive for the sources to cheat since any cheating may lead to a loss in utility. Therefore, the ACA-A scheme is cheat-proof. ■

Theorem 3: The ACA-T scheme is not cheat-proof.

Proof: Given that all the other sources report their true optimal demands at every iteration during the auction, the auction will conclude at iteration T_1 with a price λ^{T_1} and power allocation p_{i,T_1}^J if source S_i also reports its true optimal demand at every iteration, while the auction will conclude at iteration T_2 with a price λ^{T_2} and power allocation p_{i,T_2}^J if source S_i does not report its true optimal demand at every iteration. The final utility of source S_i is then denoted by $U_i^{T_1}$ and $U_i^{T_2}$, respectively.

According to Algorithm I, for any fixed p_i, we have

$$U_i^{T_j} = \ \mathcal{G}\left(p_{i,T_j}^J, p_i\right) - \lambda^{T_j} p_{i,T_j}^J,\ j \in \{1,2\}. \tag{26}$$

Then we can get

$$\begin{aligned} & U_i^{T_1} - U_i^{T_2} \\ =& \ \mathcal{G}\left(p_{i,T_1}^J, p_i\right) - \mathcal{G}\left(p_{i,T_2}^J, p_i\right) - \lambda^{T_1} p_{i,T_1}^J + \lambda^{T_2} p_{i,T_2}^J. \end{aligned} \tag{27}$$

From (27), we cannot guarantee that $U_i^{T_1} > U_i^{T_2}$, since if $\lambda^{T_1} p_{i,T_1}^J - \lambda^{T_2} p_{i,T_2}^J < \mathcal{G}\left(p_{i,T_1}^J, p_i\right) - \mathcal{G}\left(p_{i,T_2}^J, p_i\right)$, then $U_i^{T_1} < U_i^{T_2}$. Therefore, the sources have the incentive not to report their true optimal demands since it can lead to a greater utility, which means that the ACA-T scheme is not cheat-proof. ■

V. Simulation Results

To evaluate the performance of the proposed schemes, we conduct the following simulations. For simplicity and without loss of generality, we consider a communication network with only three pairs of source and destination, in which the sources are located at the coordinate $(-100\text{ m}, 0\text{ m})$, $(-100\text{ m}, 100\text{ m})$, and $(-100\text{ m}, 200\text{ m})$, and the corresponding destinations are located at the coordinate $(100\text{ m}, 0\text{ m})$, $(100\text{ m}, 100\text{ m})$, and $(100\text{ m}, 200\text{ m})$, respectively. The malicious eavesdropper is located at $(100\text{ m}, -100\text{ m})$, while the friendly jammer is located at $(0\text{ m}, -100\text{ m})$. The other simulation parameters are set up as follows: The whole jamming power p_{max} is 0.1 W, which is the same as the source transmitting power constraint; the transmission bandwidth W is 100 KHz; the noise power is $\sigma^2 = -70$ dBm; Rayleigh fading channel is assumed, where the channel gain consists of the path loss and the Rayleigh fading coefficient; the path loss factor is 2; the reserve price λ^0 is 0.001; the price step δ is 0.01 here.

First, we investigate the cheat-proof performance of the ACA-T and ACA-A schemes. Here, we assume that source S_3 reports a false power demand $\tilde{p}_{3,t}^J$ by scaling the true optimal demand $p_{3,t}^J$ with a cheat factor k, i.e., $\tilde{p}_{3,t}^J = \min\left(p_{max}, \max\left(0, kp_{3,t}^J\right)\right)$. In Fig. 2, the final utilities of source S_3 as a function of the cheat factor k in the ACA-T and ACA-A schemes are shown, respectively. We can see that with ACA-T, source S_3 achieves the maximal utility when k is around 0.7. Since the sources are non-collaborative, all the sources have the incentive to report a smaller demand at every iteration. Thus, the ACA-T scheme is not cheat-proof. With ACA-A, we can see that source S_3 achieves the maximal utility

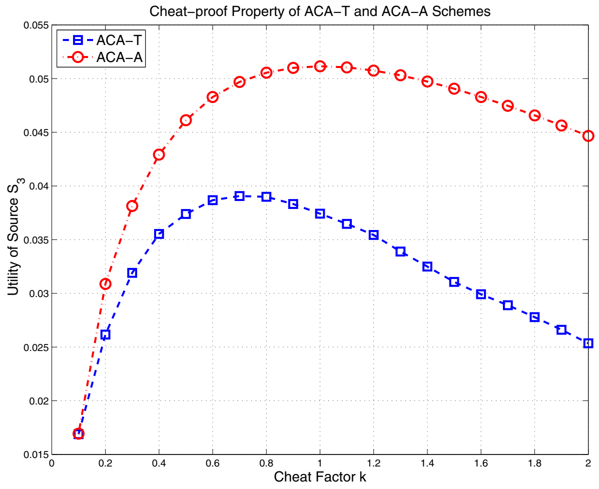

Fig. 2. Cheat-proof property of ACA-T and ACA-A schemes.

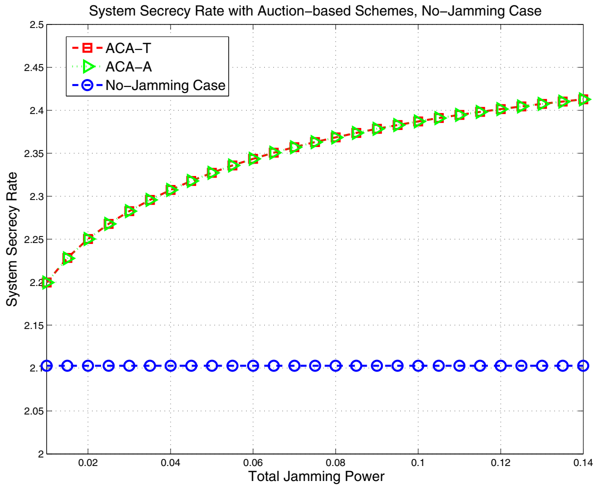

Fig. 3. System secrecy rate with ACA-T and ACA-A schemes as well as no-jamming case.

when $k = 1$, which means that no source has the incentive to cheat since any cheating will lead to a loss in its utility. Thus, the ACA-A scheme is cheat-proof. This simulation result verifies Theorem 2 and Theorem 3.

Then, we investigate the system performance with the two proposed schemes compared to the no-jamming case. In Fig. 3, the system secrecy rate, which is defined as the sum secrecy rate of all the source-destination links, as a function of total jamming power with the ACA-T and ACA-A schemes as well as the no-jamming case is shown, respectively. We can see that with the proposed auction-based schemes allocating the jamming power from the friendly jammer to the sources, the system can effectively obtain a positive performance gain in the secrecy rate compared with the no-jamming case. Furthermore, we can find that ACA-T and ACA-A have almost the same performance in terms of the system secrecy rate. Hence, the system can always achieve efficient jamming power allocation and obtain optimal system secrecy rate with the ACA-T and ACA-A schemes.

VI. Conclusions

In this paper, we have investigated how to improve the secrecy capacity for a cooperative jamming based network with one friendly jammer, one malicious eavesdropper, and several pairs of source and destination. To allocate the jamming power distributively and efficiently, we proposed two auction-based power allocation schemes, i.e., ACA-T and ACA-A, where the friendly jammer behaves as the auctioneer and the sources are the bidders. We proved and verified with simulations that both the proposed schemes can converge in a finite number of iterations, and the ACA-A scheme is cheat-proof which can enforce the selfish and non-collaborative sources to report their true optimal demands at every iteration during the auction, while the ACA-T scheme is not. We also demonstrated that the ACA-T and ACA-A schemes can always achieve efficient jamming power allocation and optimal system secrecy rate.

Acknowledgment

This work was partially supported by the US NSF CNS-0953377, CNS-0905556, and CNS-0910461, and also by the National Nature Science Foundation of China under grant number 60972009 and 61061130561, as well as the National Science and Technology Major Project of China under grant number 2009ZX03003-011, 2010ZX03003-003, 2010ZX03005-003, and 2011ZX03005-002.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[2] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wiretap channel,” *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[3] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[4] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proceedings of IEEE International Symposium on Information Theory*, Seattle, USA, Jul. 2006.
[5] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[6] L. Lai and H. E. Gamal, “The relay-eavesdropper channel: Cooperation for secrecy,” *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[7] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks: Theory, Models and Applications*, in print, Cambridge University Press, UK, 2011.
[8] C. U. Saraydar, N. B. Mandayam, and D. J. Goodman, “Efficient power control via pricing in wireless data networks,” *IEEE Transactions on Communications*, vol. 50, no. 2, pp. 291–303, Feb. 2002.
[9] Y. Wu, B. Wang, K. J. R. Liu, and T. Clancy, “A scalable collusion-resistant multi-winner cognitive spectrum auction game,” *IEEE Transactions on Communications*, vol. 57, no. 12, pp. 3805–3816, Dec. 2009.
[10] Y. Chen, Y. Wu, B. Wang, and K. J. R. Liu, “Spectrum auction games for multimedia streaming over cognitive radio networks,” *IEEE Transactions on Communications*, vol. 58, no. 8, pp. 2381–2390, Aug. 2010.
[11] P. Marbach and R. Berry, “Downlink resource allocation and pricing for wireless networks,” in *Proceedings of IEEE International Conference on Computer Communications*, New York, USA, Jun. 2002.
[12] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, “Improved wireless secrecy rate using distributed auction theory,” in *Proceedings of IEEE International Conference on Mobile Ad-hoc and Sensor Networks*, Wu Yi Mountain, China, Dec. 2009.
[13] V. Krishna, *Auction theory*, Academic Press, USA, 2002.
[14] L. M. Ausubel, “An efficient ascending-bid auction for multiple objects,” *American Economic Review*, vol. 94, no. 5, pp. 1452–1475, May 2004.
[15] D. Palomar and M. Chiang, “A tutorial on decomposition methods for network utility maximization,” *IEEE Journal on Selected Areas in Comunications*, vol. 24, no. 8, pp. 1439–1451, Aug. 2006.