Forty-Ninth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 28 - 30, 2011

Recruiting Multi-Antenna Transmitters as Cooperative Jammers: An Auction-Theoretic Approach

Igor Stanojev and Aylin Yener
The Pennsylvania State University
University Park, PA 16802
ixs11@psu.edu, yener@ee.psu.edu

***Abstract*—This paper proposes and investigates a distributed mechanism that motivates otherwise non-cooperative terminals to participate as cooperative jammers assisting a source-destination pair that communicates over a wireless medium, in the presence of an eavesdropper from whom the communicated messages need to be kept secret. The cooperation incentive is provided by an opportunity for potential jammers, possibly equipped with multiple antennas, to utilize the spectrum belonging to the ongoing secure transmission for their own data traffic. A fully decentralized framework is put forth through a competition of potential cooperative jammers for spectrum access by trying to make the jamming offer that most improves the secrecy rate of the source-destination pair. Effective arbitration of cooperative jamming is performed using auction theory, with the source in the role of the auctioneer, and the jammers acting as bidders. The proposed scheme can be alternatively seen as a practical basis for the implementation of cognitive radio networks operating according to the property-rights model, i.e., spectrum leasing.**

I. Introduction

Protecting confidential message transmission from malicious eavesdropping is a necessity in many communications scenarios. In his pioneering work [1], Shannon applied the concept of mutual information as a measure of information secrecy. Assuming that the eavesdropper obtains the same signal as the legitimate receiver, Shannon arrived at a somewhat pessimistic conclusion that the legitimate parties need to share a secret key of the same rate as the communicated message in order to perfectly conceal it from the eavesdropper. In [2], Wyner formally defined the wiretap channel and showed that a more practical scheme without secret key is indeed possible, guaranteeing a positive secrecy rate provided that the eavesdropper's channel is degraded respective to that of the legitimate receiver. Reference [3] considered the general discrete memoryless wiretap channel, and the secrecy capacity for reliable communication revealing no information to the eavesdropper, was established. The Gaussian wiretap channel was studied in [4].

Among different communication channels, the broadcast nature of the wireless medium makes it particularly susceptible to malicious eavesdropping. A number of studies on more complex wireless scenarios, such as the multiuser and multi-antenna models, exists in literature [5]-[14]. Of particular interest to this work is the *cooperative jamming* paradigm [5], wherein it was recognized that the broadcast property of the wireless medium can also be exploited to improve the secrecy rates. In particular, cooperative jamming prescribes creating judicious interference through deployment of cooperative jammers transmitting noise [5] [6] or structured codewords [12] [15] [16], so as to impair the eavesdropper's ability to decode the confidential information and thus increase secure communication rates between legitimate parties. This approach, however, requires deployment of dedicated and/or altruistic jamming nodes, willing to unconditionally utilize their resources for the communications they do not benefit from [6] [16], which may not be realistic for scenarios involving mobile stations with limited batteries.

Motivated by this fact, a scheme was recently proposed in [17] to demonstrate that jammers can be recruited to provide significant improvements of secrecy rates even when the assumption of altruistic or dedicated jammers is alleviated. Following the lines of the *spectrum leasing* paradigm [18], incentive for potential cooperative jammers is provided through an opportunity to use the spectrum belonging to the ongoing secret transmission for the traffic of their own data. This mechanism is facilitated through dividing the spectrum and orthogonalizing the transmission of the cooperative jammers own data to the secure communication that takes place between the source and the destination with the assistance of the cooperative jammer. The Stackelberg leader-follower game-theoretic framework is used to model and analyze this system.

Implementing multiple transmissions through a spectrum division is known to be a suboptimal approach. On this line, in this paper we shall consider a scenario where the legitimate parties and the cooperative jammers communicate *simultaneously*. To facilitate such a scenario, the nodes which can serve as cooperative jammers are possibly equipped with multiple antennas, and thus capable of leveraging spatial dimension for simultaneous noise and data transmission to multiple receivers, namely their destination, the destination involved in the secure transmission and the eavesdropper, under the constraint of maintaining the agreed level of jamming service. A fully decentralized framework is put forth through a competition of potential jammers for spectrum access by trying to make the jamming offer that most improves the secrecy rate of confidential communication. Effective arbitration of cooperative jamming is performed using auction theory, with

978-1-4577-1818-2/11/$26.00 ©2011 IEEE

the source and the jammers acting as the auctioneer and bidders, respectively. Due to its many advantageous properties, as discussed in Section III, we employ the sealed-bid second-price, i.e., the Vickrey auction [19] and analyze the proposed scheme performance in equilibrium.

It is also noted that the proposed solution can be alternatively applied as a practical implementation framework for cognitive radio networks operating according to property-rights model [18]. The role of the primary node is played by the source transmitting a confidential message and that of the secondary by the jamming nodes. The retribution for spectrum access from secondary to primary nodes is in the form of cooperative jamming to the primary secure transmission, thus avoiding the regulatory issues or money transactions that commonly hinder the implementation of the property-rights concept.

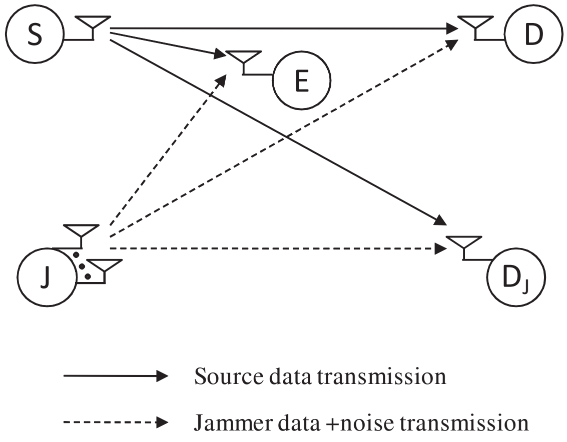


Figure 1. System model with a single potential jammer.

II. System Model

In this section, we provide the general description of the proposed scheme and the overview of the relevant parameters.

A. Model Overview

The model of interest consists of a source S communicating with a destination D in the presence of an eavesdropper E from whom the communication must be kept secret. Moreover, N nodes J_k, $k = 1, ..., N$, have data to transmit towards their intended receivers $\mathrm{D}_{\mathrm{J},k}$ and can act as potential cooperative jammers for the S-D secure communication, as illustrated in Fig. 1 for $N = 1$. Potential jammers are equipped with M_k antennas, $M_k = 1, 2, ..$, while all the remaining terminals are single-antenna. The source S is willing to employ a cooperative jamming service from a node J_k, if it is potentially helpful to increase its secrecy rate. Simultaneously, the awarded jammer is allowed to exploit the source's bandwidth for transmission of its own data, under the constraint of maintaining the jamming level agreed upon during the auction phase, as detailed later.

In line with the wiretapping channel model with cooperative jamming [6], the jamming is performed via noise transmission. To accommodate for simultaneous noise and data transmission, a single-antenna jammer J dedicates a fraction of its transmission power for the transmission of the noise stream, and the remaining power for its data. In case of a multi-antenna potential jammer, it can also exploit spatial dimension and apply beamforming methods. A potential jammer is interested in providing the cooperative jamming solely in order to attain the opportunity to transmit its own traffic with as much rate as possible, as will be elaborated in Section IV-A.

A potential jammer may use the secrecy rate of the S-D communication assisted by its jamming as a bid to be submitted to the source to enable the auction-based assignment of the jammed transmission. This also implies that the potential jammers avail information about the channel parameters impacting the source's secrecy rate, as detailed in Section IV-C. It is noted that any multiple-access scheme can be employed to ensure the collision-free bid submissions. Having collected all the bids from the jammers, the source decides to assign the jammer that offered the highest jamming-assisted source's secrecy rate, if the latter is larger than the source's 'reserve price', i.e., the source's secrecy rate with no jamming.

B. Physical Layer Parameters

The channel gains between nodes are modeled as independent complex Gaussian random variables. The channel gains between node S and nodes D, E and $\mathrm{D}_{\mathrm{J},i}$ are denoted as h_{SD}, h_{SE} and $h_{\mathrm{SD_J},k}$, respectively, while the $M_k \times 1$ vectors of channel gains between node J_k and nodes D, E and $\mathrm{D}_{\mathrm{J},k}$ are denoted as $\boldsymbol{h}_{\mathrm{J}_k\mathrm{D}}$, $\boldsymbol{h}_{\mathrm{J}_k\mathrm{E}}$ and $\boldsymbol{h}_{\mathrm{J}_k}$, where M_k is the J_k's number of antennas and $k = 1, .., N$. Average transmission powers for the source S and the jammer J_k are P_S and P_{J_k}, respectively. The independent additive white Gaussian noise variance for each link is σ^2. Throughout the paper we assume signaling using Gaussian codebooks and the cooperative jamming in the form of Gaussian noise.

III. Auction-Theoretic Preliminaries

To provide a framework for distributed resource allocation where potential jammers are competing for bandwidth access, the jammers are modeled as rational and selfish entities, interested solely in maximizing their own utilities, as detailed in Section IV-A. The scenario at hand can be conveniently investigated in the framework of auction theory [20] [21]. This section provides a brief overview of the fundamental game- and auction-theoretic concept of dominant strategy equilibrium (DSE) [20], essential to the outcome of the Vickrey auction, and the Vickrey auction [19] itself. It is noted that the Vickrey auction is applied here due to its convenient properties [19], as detailed in Section III-B, but the concepts presented in this work are not constrained to Vickrey principles and can be applied using any type of auction.

A. Auctions and Dominant Strategy Equilibrium

Auction theory provides means to identify meaningful operational points corresponding to equilibrium states for the competitive decision processes. Identifying such equilibrium points can be used to predict the system behavior and to allow its design. Following standard game-theoretic definitions, an equilibrium point defines a set of bidders', i.e., selfish and rational players' in the game-theoretic jargon [20], strategies from which no bidder has incentive to unilaterally deviate. Several equilibrium solutions may be defined with different robustness properties with respect to the information that a certain bidder is assumed to know regarding the other bidders. Here, we are interested in the dominant strategy equilibrium, DSE, a concept that poses the strictest requirement in terms of robustness: DSE strategies are required to remain preferable to every bidder, i.e., jammer, irrespective of the amount of information available on other bidders [20].

DSE have thus two essential properties: on one hand, they provide a reliable prediction of the system behavior due to the robustness feature mentioned above; on the other hand, they enable implementation with no requirement for exchanging information regarding other jammers' types. In other words, the DSE solution requires that strategy for a jammer is the *best response* against any number of other bidders, their parameters and chosen strategies. Notice that this strategy is chosen by a rational bidder even if the other players don't exercise rational behavior [20].

While finding a DSE solutions for a general class of auctions is generally prohibitive, for Vickrey auctions, also known as sealed-bid second-price auctions, solution can be typically found.

B. Background on Vickrey Auction

In sealed-bid second-price auctions, i.e., Vickrey auctions [19], the bidding item is awarded to the highest bidder at the price of the second highest bid, i.e., at the price of the highest losing bid. The most attractive property of Vickrey auction is its 'truth telling nature': namely, a dominant strategy for each bidder is to report to the auctioneer its evaluation of the bidding item truthfully. In particular, [19] defines truthful bidding as bidding with the "price at which a bidder would be on the margin of indifference as to whether he obtains the article or not,..., a highest amount he could afford to pay without incurring a net loss". To provide a brief intuition on the truthful bidding property of Vickrey auctions, notice that if bidding less than the value of indifference, the bidder can only reduce his chance of winning while not affecting the price it would pay if he was the winner. On the other hand, if bidding with a value larger than that of indifference, the chance of winning increases but only if yielding an unprofitable or unfeasible outcome. As a consequence, implementation of a dominant strategy for Vickrey auctions at each bidder requires no information on the other bidders' strategies or their evaluations of the bidding item, as this knowledge would not impact the truthful bidding strategy, i.e., the DSE strategy.

The Vickrey model generally results in an efficient goods allocation, as reported in [19]-[23], almost identical to that of a classic English first-price ascending auction [22] [23]. Attractive properties of Vickrey auctions have also inspired related research within the wireless community. The work in [18], most related to the one at hand, was already discussed in Section I. Furthermore, [24] exploits Vickrey auction to determine the optimum partner selection in a self-configuring cooperative network. Vickrey auction was implemented in [25] to design a wireless network model that combats selfishness and enforces cooperation among nodes. In [26], an algorithm based on the Vickrey auction was applied to the problem of fair allocation of a wireless fading channel. As a final remark, we notice that Vickrey auctions can be vulnerable to malicious behavior of the auctioneer, e.g., the 'lying auctioneer' issue, and the bidders, e.g., the bidder collusion issue, and appropriate mechanisms should be applied for its protection; see, e.g., [27] for a related discussion.

IV. System Performance in DSE

In this section, we first define the utility of a potential jammer in Section IV-A. Relation between the source's secrecy rate assisted by cooperative jamming and the assisting jammer's data rate is analyzed in Section IV-B. This relation is used to find the dominant strategy equilibrium and the auction outcome under Vickrey rule in Section IV-C.

A. Jammer's Strategies and Goal

A potential jammer is interested in cooperative jamming solely to attain the opportunity to transmit its own traffic with as much rate as possible. Denoting the information rate achievable by the kth jammer, if it is selected by the source, as $R_{\mathrm{J},k}$, the consequent jamming-assisted secrecy rate of the source S as $R_{\mathrm{S},k}$ and the source's secrecy rate without cooperative jamming, i.e., its reserve price, as R'_{S}, that jammer's utility can be formulated as:

$$u_k = R_{\mathrm{J},k} \cdot 1\left(R_{\mathrm{S},k} = \max\left(R'_{\mathrm{S}}, R_{\mathrm{S},i=1,..,N}\right)\right), \qquad (1)$$

where the indicator function $1(\cdot)$ equals 1 or 0 according to whether its argument is satisfied or not, respectively. The definition (1) says that, if the jammer J_k wins the auction, he accrues an utility equal to $R_{\mathrm{J},k}$, whereas otherwise the utility is zero. It will be shown in the following subsection that (1) reflects a trade-off for a bidder J_k between maximizing its transmission rate $R_{\mathrm{J},k}$ and the probability of being selected for transmission by providing the largest bid $R_{\mathrm{S},k}$.

B. Source Secrecy Rate R_{S} versus Jammer Data Rate R_{J}

1) Single-Antenna Jammer: For a single-antenna jammer, the only available degree of freedom, i.e., its strategy, is the fraction of its available power it will dedicate to jamming, denoted as α_k, with $0 \leq \alpha_k \leq 1$. Thus, the power $\alpha_k P_{\mathrm{J}_k}$ is used for transmitting the noise and $(1-\alpha_k)P_{\mathrm{J}_k}$ is dedicated for its data transmission. Focusing on a single jammer and dropping its index for clarity, the source's secrecy rate and

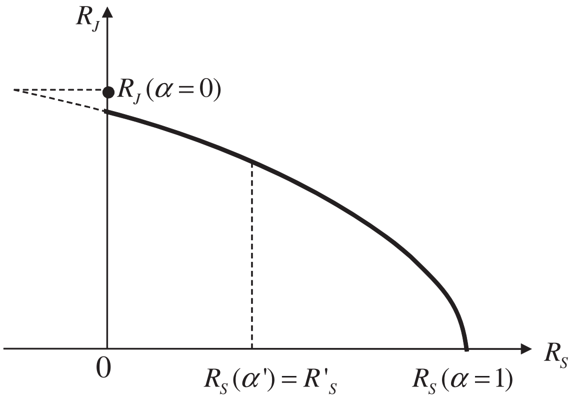


Figure 2. Dependence $R_{\mathrm{S}} - R_{\mathrm{J}}$ (solid line)

the jammer data transmission rate read, respectively [6]:

$$
\begin{aligned}
R_{\mathrm{S}} \; &= \; \left[\log_2\left(1+\frac{|h_{\mathrm{SD}}|^2 P_{\mathrm{S}}}{\sigma^2+|h_{\mathrm{JD}}|^2 P_{\mathrm{J}}}\right) - \right. \\
&\qquad \left. \log_2\left(1+\frac{|h_{\mathrm{SE}}|^2 P_{\mathrm{S}}}{\sigma^2+\alpha\,|h_{\mathrm{JE}}|^2 P_{\mathrm{J}}}\right)\right]^{+} \qquad (2) \\
R_{\mathrm{J}} \; &= \; \log_2\left(1+\frac{(1-\alpha)\,|h_{\mathrm{J}}|^2 P_{\mathrm{J}}}{\sigma^2+|h_{\mathrm{S}}|^2 P_{\mathrm{S}}+\alpha\,|h_{\mathrm{J}}|^2 P_{\mathrm{J}}}\right), \qquad (3)
\end{aligned}
$$

where $[x]^{+} = \max(0,x)$. Notice that the destination D experiences interference induced by an entire power P_{J}, while the eavesdropper is impaired only by αP_{J}, both scaled by appropriate power channel gains. On the other hand, interference at $\mathrm{D_J}$ entails the jammer's noise transmission αP_{J}, as well as the source's transmission P_{S}. Recall that we consider the worst-case scenario [6], wherein the eavesdropper is the only node that can attempt to decode any data transmission, while the destinations D and $\mathrm{D_J}$ treat transmissions other than their intended one as interference. Moreover, the reserve price R'_{S} is given by (2) with $P_{\mathrm{J}} = 0$.

It is easily seen from (2) that the source secrecy rate is a non-decreasing function of α, and strictly increasing for $R_{\mathrm{S}} > 0$, while the jammer's data rate in (3) decreases with α. Recalling (1), this also reflects a trade-off for J_k between maximizing its transmission rate, which calls for small α, and the probability of being selected for transmission by providing the largest bid in the form of secrecy rate, which calls for large α. The function R_{J} is thus a monotonically decreasing function of R_{S}, as also depicted in Fig. 2 where each point corresponds to a unique fraction α. For the illustration purpose, the dashed lines for $R_{\mathrm{S}} < 0$ are obtained ignoring the $[\cdot]^{+}$ operator in (2). The point corresponding to α' on Fig. 2 is determined as the solution of $R_{\mathrm{S}}(\alpha') = R'_{\mathrm{S}}$, i.e., it is the fraction of P_{J} that would yield the secrecy rate in the absence of jammer. Consequently, the legibility of a jammer participation in auction is conditioned with $\alpha' < 1$. The fraction α' for $R'_{\mathrm{S}} > 0$ is easily derived using (2) as:

$$
\begin{aligned}
\alpha'|_{R'_{\mathrm{S}}>0} = &\left(\sigma^2+|h_{\mathrm{SE}}|^2 P_{\mathrm{S}}\right)|h_{\mathrm{JD}}|^2 |h_{\mathrm{SD}}|^2 P_{\mathrm{S}} \cdot \qquad (4) \\
&\Big(|h_{\mathrm{JE}}|^2 |h_{\mathrm{SE}}|^2 P_{\mathrm{S}}\left(\sigma^2+|h_{\mathrm{JD}}|^2 P_{\mathrm{J}}+|h_{\mathrm{SD}}|^2 P_{\mathrm{S}}\right) - \\
&|h_{\mathrm{JE}}|^2 |h_{\mathrm{JD}}|^2 |h_{\mathrm{SD}}|^2 P_{\mathrm{J}} P_{\mathrm{S}}\Big)^{-1},
\end{aligned}
$$

while, for $R'_{\mathrm{S}} = 0$, it is given as

$$
\alpha'|_{R'_{\mathrm{S}}=0} = \frac{|h_{\mathrm{SE}}|^2 P_{\mathrm{S}}(\sigma^2+|h_{\mathrm{JD}}|^2 P_{\mathrm{J}}) - \sigma^2 |h_{\mathrm{SD}}|^2 P_{\mathrm{S}}}{|h_{\mathrm{JE}}|^2 P_{\mathrm{J}}\, |h_{\mathrm{SD}}|^2 P_{\mathrm{S}}}. \quad (5)
$$

2) Multi-Antenna Jammer: For a multi-antenna jammer, the strategy is given by the pair $(\boldsymbol{w}_N, \boldsymbol{w}_D)$ of the $M \times 1$ beamforming vector gains for the noise and data stream, respectively, with $P_{\mathrm{J}} = \|\boldsymbol{w}_N\|^2 + \|\boldsymbol{w}_D\|^2$. The source's secrecy rate and a potential jammer's data rate now read:

$$
\begin{aligned}
R_{\mathrm{S}} \; &= \; \left[\log_2\left(1+\frac{|h_{\mathrm{SD}}|^2 P_{\mathrm{S}}}{\sigma^2+|(\boldsymbol{w}_N+\boldsymbol{w}_D)^H \boldsymbol{h}_{\mathrm{JD}}|^2}\right) - \right. \\
&\qquad \left. \log_2\left(1+\frac{|h_{\mathrm{SE}}|^2 P_{\mathrm{S}}}{\sigma^2+\left|\boldsymbol{w}_N^H \boldsymbol{h}_{\mathrm{JE}}\right|^2}\right)\right]^{+} \qquad (6) \\
R_{\mathrm{J}} \; &= \; \log_2\left(1+\frac{\left|\boldsymbol{w}_D^H \boldsymbol{h}_{\mathrm{J}}\right|^2}{\sigma^2+|h_{\mathrm{S}}|^2 P_{\mathrm{S}}+\left|\boldsymbol{w}_N^H \boldsymbol{h}_{\mathrm{J}}\right|^2}\right), \qquad (7)
\end{aligned}
$$

where $(\cdot)^H$denotes the Hermitian transpose.

In order to determine the best strategy available to a jammer when deciding on $\boldsymbol{w}_N$ and $\boldsymbol{w}_D$, we exploit results of [28], where a general system with multiple multiple-antenna transmitters and multiple single-antenna receivers was discussed. Each receiver has utility, not to be confused with (1), that increases with the power of received signal from its intended transmitter and decreases with the power of signal received from an unintended transmitter. Relying on the paradigm of *gain regions* [28], it was shown that the *Pareto optimal utility region*, that is the region corresponding to the set of operating points where utility of one receiver cannot be further improved without simultaneously degrading performance of at least one of the remaining receivers, has to satisfy the following conditions on transmitting beamforming gains $\boldsymbol{w}_i$, for each transmitter i:

$$
\begin{aligned}
\boldsymbol{w}_i \; &= \; p_i \sqrt{P_i}\, \boldsymbol{v}_{max}\left(\sum_{l=1}^{n} e_{i,l} \lambda_{i,l} \boldsymbol{h}_{i,l} \boldsymbol{h}_{i,l}^H\right) \qquad (8) \\
\sum_{l=1}^{n} \lambda_{i,l} \; &= \; 1, \; p_i, \lambda_{i,l} \in [0,1], \qquad (9)
\end{aligned}
$$

where n is the number of receivers, the value $e_{i,l} \in \{-1, 1\}$ depends on whether the lth receiver is intended for a transmitter i or not, $e_{i,l} = 1$ and $e_{i,l} = -1$, respectively, $\boldsymbol{h}_{i,l}$ is the channel vector gain from transmitter i to receiver l, $\boldsymbol{v}_{max}(\mathbf{Z})$ is the eigenvector of matrix $\mathbf{Z}$ corresponding to its largest eigenvalue, i.e., the principal eigenvector of $\mathbf{Z}$, and P_i is the transmitting power of transmitter i. Conditions (8)-(9) can be further simplified by setting the power-control parameter $p_i = 1$ and $p_i = 0$ if the largest eigenvalue of matrix $\sum_{l=1}^{n} e_{i,l}\lambda_{i,l}\boldsymbol{h}_{i,l}\boldsymbol{h}_{i,l}^H$ is positive or negative, respectively [28].

To apply the concept of [28] to the model of interest herein, rates (6) and (7) are chosen as the receivers' utilities and the jammer is modeled as two M-antenna transmitters, one transmitting the noise with a beamforming vector $\boldsymbol{w}_N$ and another transmitting data with $\boldsymbol{w}_D$, with $P_{\mathrm{J}} = \|\boldsymbol{w}_N\|^2 + \|\boldsymbol{w}_D\|^2$ [28]. For the former one, intended receiver is the eavesdropper E and the unintended receivers are D and $\mathrm{D_J}$, while for the latter one, intended receiver is $\mathrm{D_J}$ and the unintended receiver is D, as seen in (6) and (7). We also recognize that the utility, in terms of [28], of the destination D and eavesdropper E can be merged into R_{S} given by (6), as also suggested by [28], while the utility of the jammer's destination $\mathrm{D_J}$ is given by R_{J} in (7). Thus, exploiting (8)-(9), the resulting Pareto region $R_{\mathrm{S}} - R_{\mathrm{J}}$ must satisfy the following conditions:

$$\boldsymbol{w}_N = \sqrt{\alpha P_{\mathrm{J}}}\boldsymbol{v}_{max}\Big(\lambda_1 \boldsymbol{h}_{\mathrm{JE}}\boldsymbol{h}_{\mathrm{JE}}^H - \lambda_2 \boldsymbol{h}_{\mathrm{JD}}\boldsymbol{h}_{\mathrm{JD}}^H - (1-\lambda_1-\lambda_2)\,\boldsymbol{h}_{\mathrm{J}}\boldsymbol{h}_{\mathrm{J}}^H\Big) \quad (10)$$

$$\boldsymbol{w}_D = \sqrt{(1-\alpha)P_{\mathrm{J}}}\boldsymbol{v}_{max}(-\lambda_3 \boldsymbol{h}_{\mathrm{JD}}\boldsymbol{h}_{\mathrm{JD}}^H + (1-\lambda_3)\boldsymbol{h}_{\mathrm{J}}\boldsymbol{h}_{\mathrm{J}}^H) \quad (11)$$

$$\alpha, \lambda_i \in [0,1], i = 1,2,3, \quad \lambda_1 + \lambda_2 \leq 1. \quad (12)$$

Notice that there is no need for power-control for the vector $\boldsymbol{w}_D$ in (11) as the largest eigenvalue of the matrix $-\lambda_3 \boldsymbol{h}_{\mathrm{JD}}\boldsymbol{h}_{\mathrm{JD}}^H + (1-\lambda_3)\boldsymbol{h}_{\mathrm{J}}\boldsymbol{h}_{\mathrm{J}}^H$ is always positive [28], while the power-control for the vector $\boldsymbol{w}_N$ in (10) is implicitly controlled by α. The Pareto region obtained with (10)-(12) results in a region $R_{\mathrm{S}} - R_{\mathrm{J}}$ that has a similar shape as that of a single antenna jammer in Fig. 2, with the extreme rates $R_{\mathrm{S}}(\alpha = 1)$ and $R_{\mathrm{J}}(\alpha = 0)$ generally increased. Notice that, unlike for a single-antenna case, here a jammer is always able to enhance the performance of the secure S-D link, for example, by applying a zero-force beamforming vector that would create no interference at the destination D [28].

C. Dominant Strategy Equilibrium under Vickrey Mechanism

Here we investigate DSE solutions for the model at hand when the Vickrey auction mechanism is used.

1) Single-Antenna Jammer: As elaborated in Section IV-B1, for a single-antenna jammer to be legible for placing the bid, $\alpha' < 1$ needs to be satisfied, where α' is defined in (4) and (5). Under the Vickrey, i.e., the second-price auction rule, the DSE bidding strategy is to bid with the indifference value $R_{\mathrm{S}}^* = R_{\mathrm{S}}(\alpha^* = 1)$, i.e., to dedicate all transmission power to the artificial noise transmission. This can be explained using a similar argument as in Section III-B: choosing $\alpha < 1$ would yield a smaller secrecy rate $R_{\mathrm{S}}(\alpha)$ than R_{S}^*, and thus a reduced chance of winning the auction, i.e., attaining the spectrum access for transmission of its data, while not affecting the second-best price $\hat{R}_{\mathrm{S}}$ it would pay if it was the winner. Bidding with larger R_{S} than R_{S}^* would increase the chance of winning, but only if yielding an unfeasible outcome.

Recovering the jammers' indices and assuming that there is a jammer that bids with $R_{\mathrm{S},k}^* > R_{\mathrm{S}}'$, the auction winner is $\hat{k} = \mathrm{argmax}_{i=1,..,N}(R_{\mathrm{S},i}^*)$. The winner has to provide the second-best rate, i.e., $\hat{R}_{\mathrm{S},\hat{k}} = \max_{j\neq\hat{k}}(R_{\mathrm{S},j}^*, R_{\mathrm{S}}')$. The data rate obtained by the winning jammer is $\hat{R}_{\mathrm{J},\hat{k}} = R_{\mathrm{J},\hat{k}}(\hat{\alpha}_{\hat{k}})$, where $\hat{\alpha}_{\hat{k}}$ is the solution of $R_{\mathrm{S},\hat{k}}(\hat{\alpha}_{\hat{k}}) = \hat{R}_{\mathrm{S},\hat{k}}$. Applying this equality to (2) we get:

$$\hat{\alpha}_{\hat{k}} = -\frac{\sigma^2}{\left|h_{\mathrm{J}_{\hat{k}}\mathrm{E}}\right|^2 P_{\mathrm{J}_{\hat{k}}}} + 2^{\hat{R}_{\mathrm{S},\hat{k}}}\frac{\left(\sigma^2 + \left|h_{\mathrm{J}_{\hat{k}}\mathrm{D}}\right|^2 P_{\mathrm{J}_{\hat{k}}}\right)\left(\sigma^2 + \left|h_{\mathrm{J}_{\hat{k}}\mathrm{E}}\right|^2 P_{\mathrm{J}_{\hat{k}}} + \left|h_{\mathrm{SE}}\right|^2 P_{\mathrm{S}}\right)}{\left|h_{\mathrm{J}_{\hat{k}}\mathrm{E}}\right|^2 P_{\mathrm{J}_{\hat{k}}}\left(\sigma^2 + \left|h_{\mathrm{J}_{\hat{k}}\mathrm{D}}\right|^2 P_{\mathrm{J}_{\hat{k}}} + \left|h_{\mathrm{SD}}\right|^2 P_{\mathrm{S}}\right)}. \quad (13)$$

Notice that the DSE and (13) imply that a bidding jammer requires the knowledge of source's parameters, namely P_{S}, h_{SE}, h_{SD}. On the other hand, a jammer requires no knowledge of any parameters related to other bidding jammers, which is in line with Vickrey principles and the nature of the DSE. Finally, if there was no jammer $k = 1,..,N$ providing $R_{\mathrm{S},k}^* > R_{\mathrm{S}}'$, the source transmits with no jamming assistance.

2) Multi-Antenna Jammer: Following a similar reasoning as for the single antenna-jammer in Section IV-C1, the bid in the DSE for a multiple-antenna jammer is obtained by dedicating all transmission power to noise transmission. Recalling (10)-(12), the DSE is thus the solution of optimization problem:

$$\begin{gathered} R_{\mathrm{S}}^* = \max R_{\mathrm{S}}(\boldsymbol{w}_N, \boldsymbol{w}_D) \quad (14) \\ s.t.\ \boldsymbol{w}_N = \sqrt{P_{\mathrm{J}}}\boldsymbol{v}_{max}\Big(\lambda \boldsymbol{h}_{\mathrm{JE}}\boldsymbol{h}_{\mathrm{JE}}^H - (1-\lambda)\boldsymbol{h}_{\mathrm{JD}}\boldsymbol{h}_{\mathrm{JD}}^H\Big) \\ \boldsymbol{w}_D = 0 \\ \lambda \in [0,1], \end{gathered}$$

where $R_{\mathrm{S}}(\boldsymbol{w}_N, \boldsymbol{w}_D)$ is given by (6). No power-control is required for $\boldsymbol{w}_N$ as the largest eigenvalue of the matrix $\lambda \boldsymbol{h}_{\mathrm{JE}}\boldsymbol{h}_{\mathrm{JE}}^H - (1-\lambda)\boldsymbol{h}_{\mathrm{JD}}\boldsymbol{h}_{\mathrm{JD}}^H$ is always positive.

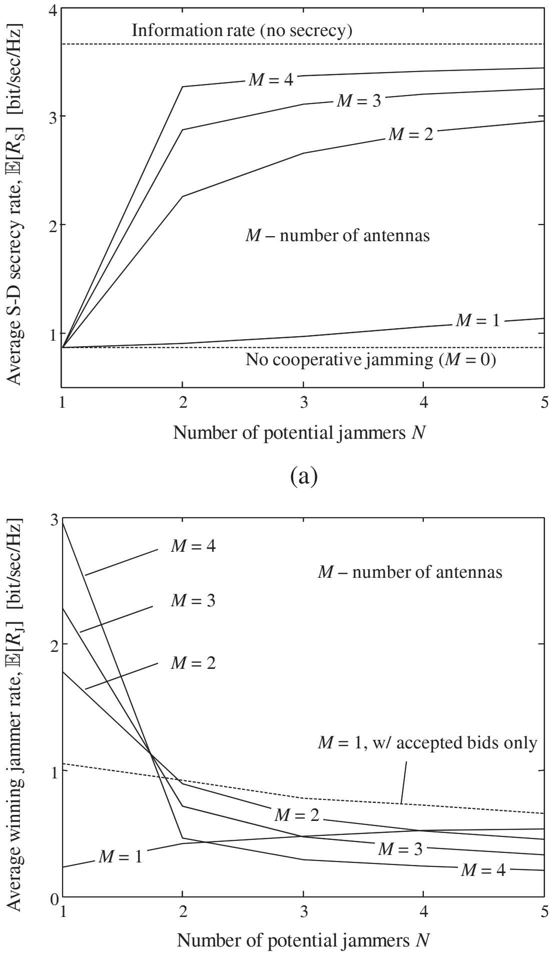
Recovering the jammers' indices and assuming that there is a jammer that bids with $R_{\mathrm{S},k}^* > R_{\mathrm{S}}'$, the auction winner is $\hat{k} = \mathrm{argmax}_{i=1,..,N}(R_{\mathrm{S},i}^*)$. The rate that the winner has to provide to the source is the second-best bidding rate, i.e., $\hat{R}_{\mathrm{S},\hat{k}} = \max_{j\neq\hat{k}}(R_{\mathrm{S},j}^*, R_{\mathrm{S}}')$. The data rate $\hat{R}_{\mathrm{J},\hat{k}}$ obtained by the winning jammer is then the solution of the following optimization problem:

$$\begin{gathered} \hat{R}_{\mathrm{J},\hat{k}} = \max R_{\mathrm{J},\hat{k}}(\boldsymbol{w}_N, \boldsymbol{w}_D) \quad (15) \\ s.t.\ R_{\mathrm{S},\hat{k}}(\boldsymbol{w}_N, \boldsymbol{w}_D) = \hat{R}_{\mathrm{S},\hat{k}} \\ \text{and conditions (10)-(12) hold,} \end{gathered}$$

where $R_{\mathrm{S},\hat{k}}(\boldsymbol{w}_N, \boldsymbol{w}_D)$ and $R_{\mathrm{J},\hat{k}}(\boldsymbol{w}_N, \boldsymbol{w}_D)$ are given in (6) and (7), respectively. Finally, if there were no bid satisfying $R_{\mathrm{S},k}^* > R_{\mathrm{S}}'$, no jamming assistance would be provided to the source, and the latter transmits with the secrecy rate R_{S}'.

V. Numerical Results

This section provides some insights into the proposed cooperative jamming via the auction-based spectrum leasing scheme using numerical results. The source's secrecy rate and the winning cooperative jammer data rate in DSE, averaged over channel realizations, $\mathbb{E}[R_{\mathrm{S}}]$ and $\mathbb{E}[R_{\mathrm{J}}]$ are illustrated in Fig. 3-(a) and Fig. 3-(b), respectively, as a function of the number of potential jamming nodes N, for different number of antennas $M_k = M$ and parameters $P_{\mathrm{S}}/\sigma^2 = P_{\mathrm{J}_k}/\sigma^2 = 10$ dB, $k = 1, .., N$, with power channel gains for each link equal to 0 dB. The benefits for both the secrecy rate and the chosen jammer's data rate with the proposed scheme are clearly visible. Fig. 3-(a) confirms that the secrecy rate increases with number of potential jammers N and the number of jammer's transmitting antenna M. For $M = 1$ the benefits are relatively small, as the jammers are often not legible for auction, i.e., $\alpha'_k < 1$ is not satisfied. Notice that for $N = 1$, there is no improvement of the source's secrecy rate, as the second-best bid is in fact source's reserve price, i.e., its secrecy rate with no cooperative jamming assistance. As expected, Fig. 3-(b) shows that the winning jammer's rate decreases with N, due to competitiveness of the scheme; this conclusion holds also for $M = 1$, if only the scenarios resulting in successful spectrum lease are considered. Interestingly, increasing number of antennas M leads to decreased jammer's rate for $N \geq 2$. Namely, large M leads to the second-price secrecy rate relatively close to the source's information rate, and the winning jammer has to dedicate most of its resources to the noise transmission for jamming the eavesdropper.



(a)

(b)

Figure 3. Averaged secrecy rate $\mathbb{E}[R_{\mathrm{S}}]$ and winning cooperative jammer's information rate $\mathbb{E}[R_{\mathrm{J}}]$ versus the number of potential cooperative jammers.

VI. Concluding Remarks

This paper has demonstrated that the cooperative jamming paradigm for secure communications in wireless channel is implementable even when the jamming nodes are not willing to altruistically assist the secure communication. The proposed scheme involves multiple-antenna jammers and relies on an auction-theoretic framework and, implicitly, on the spectrum leasing concept. Numerical results corroborate the performance improvements for all involved entities, despite their selfish nature. Future work includes considering the vector channel extension by deploying multiple antennas at all nodes.

References

[1] C. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. Journal*, vol. 28, no. 4, pp. 656-715, Sep. 1949.

[2] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] I. Csiszar and J. Komer, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wire-tap Channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[5] E. Tekin and A. Yener, "The Gaussian Multiple Access Wire-Tap Channel: Wireless Secrecy and Cooperative Jamming," in *Proc. Inf. Theory Applications Workshop*, San Diego, CA, Jan. 2007.

[6] E. Tekin and A. Yener, "The General Gaussian Multiple Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, June 2008.

[7] E. Tekin and A. Yener, "Achievable Rates for the General Gaussian Multiple Access Wire-Tap Channel with Collective Secrecy," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 2006.

[8] Y. Liang and H. V. Poor, "Multiple-Access Channels with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976-1002, Mar. 2008.

[9] R. Liu, I. Marić, R. D. Yates and P. Spasojević, "The Discrete Memoryless Multiple Access Channel with Condifential Messages," in *Proc. IEEE Int. Symp. Inf. Theory, ISIT*, Seattle, WA, July 2006.

[10] R. Liu, I. Marić, P. Spasojević and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels with Condifential Messages," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 2006.

[11] Y. Liang, A. Somekh Baruch, H. V. Poor, S. Shamai (Shitz) and S. Verdú, "Cognitive Interference Channels with Condifential Messages," in *Proc. Allerton Conf. Commun. Control Comput.*, Monticello, IL, Sep. 2007.

[12] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[13] X. He and A, Yener, "Two-hop Secure Communication Using an Untrusted Relay," *EURASIP Jour. Wireless Commun. Netw., Special Issue on Wireless Physical Layer Security*, vol. 2009, Article ID 305146, 13 pages, 2009. doi:10.1155/2009/305146.

[14] E. Ekrem and S. Ulukus, "Secrecy in Cooperative Relay Broadcast Channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137-155, Jan. 2011.

[15] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian Wiretap Channel With a Helping Interferer," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, Canada, July 2008.

[16] X. He and A. Yener, “Providing Secrecy With Structured Codes: Tools and Applications to Two-User Gaussian Channels,” *IEEE Trans. Inf. Theory*, July 2009, submitted for publication.

[17] I. Stanojev and A. Yener, “Cooperative Jamming via Spectrum Leasing,” in *Proc. IEEE 9th Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, WiOpt*, Princeton, NJ, May 2011.

[18] I. Stanojev, O. Simeone, U. Spagnolini, Y. Bar-Ness and R. Pickholtz, "Cooperative ARQ via Auction-Based Spectrum Leasing," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1843 - 1856, June 2010.

[19] W. Vickrey, “Counterspeculations, Auctions, and Competitive Sealed Tenders,” *Journal of Finance*, vol. 16, pp. 8–37, 1961.

[20] M. J. Osborne and A. Rubenstein, *A Course in Game Theory*, MIT Press, 1994.

[21] P. Klemperer, “Auction Theory: A Guide to the Literature,” *J. Economics Surveys*, vol. 13, no. 3, pp. 227-286, Jul. 1999.

[22] D. Lucking-Reiley, “Vickrey Auctions in Practice: From Nineteenth-Century Philately to Twenty-First-Century E-Commerce,” *Journal of Economic Perspectives,* vol. 14, no. 3, pp. 183–192, Summer 2000.

[23] M. Rothkopf, T. Teisberg, and E. Kahn, “Why Are Vickrey Auctions Rare?” *Journal of Political Economy*, vol. 98, no. 1, pp. 94–109, Feb. 1990.

[24] A. Mukherjee and H. M. Kwon, “Robust Auction-Teoretic Partner Selection in Cooperative Diversity Wireless Networks,” in *Proc. Allerton Conf. Signals, Syst., Computers*, Nov. 2007, pp. 443-447.

[25] C. Demir and C. Comaniciu, “An Auction Based AODV Protocol for Mobile Ad Hoc Networks with Selfish Nodes,” in *Proc. IEEE Int. Conf. Commun.*, June 2007, pp. 3351–3356.

[26] J. Sun, E. Modiano, and L. Zheng, “Wireless Channel Allocation Using an Auction Algorithm,” *IEEE Jour. Select. Areas Commun.*, vol. 24, no. 5, pp. 1085–1096, May 2006.

[27] T. Sandholm, “Issues in Computational Vickrey Auctions,” Int. J. Electronic Commerce, vol. 4, no. 3, pp. 107–129, Mar. 2000.

[28] R. Mochaourab and E. A. Jorswieck, “Optimal Beamforming in Interference Networks with Perfect Local Channel Information,” *IEEE Trans. Signal Proc*., vol. 59, no. 3, pp. 1128-1141, Mar. 2011.

[29] B. Niu, O. Simeone, O. Somekh and A. M. Haimovich, “Ergodic and Outage Performance of Fading Broadcast Channels with 1-Bit Feedback,” *IEEE Trans. Veh. Technol*., vol. 59, no. 3, pp. 1282 - 1293, Mar. 2010.

[30] D. Zhang, R. Shinkuma and N. B. Mandayam, “Bandwidth Exchange: An Energy Conserving Incentive Mechanism for Cooperation,” *IEEE Trans. Wireless Commun*., vol. 9, No. 6, pp. 2055-2065, June 2010.