Improving Secrecy Rate via Spectrum Leasing for Friendly Jamming

Igor Stanojev, *Member, IEEE,* and Aylin Yener, *Member, IEEE*

***Abstract*—Cooperative jamming paradigm in secure communications enlists network nodes to transmit noise or structured codewords, in order to impair the eavesdropper's ability to decode messages to be kept confidential from it. Such an approach can significantly help in facilitating secure communication between legitimate parties but, by definition, assumes dedicated and/or altruistic nodes willing to act as cooperative jammers. In this paper, it is demonstrated that cooperative jamming leads to meaningful secrecy rate improvements even when this assumption is removed. A distributed mechanism is developed that motivates jamming participation of otherwise non-cooperative terminals, by compensating them with an opportunity to use the fraction of legitimate parties' spectrum for their own data traffic. With the goal of maximizing their data transmission rate priced by the invested power, cooperative jammers provide the jamming/transmitting power that is generally proportional to the amount of leased bandwidth. The fully decentralized framework is facilitated through a game-theoretic model, with the legitimate parties as the spectrum owners acting as the game leader, and the set of assisting jammers constituting the follower. To facilitate the behavior of non-cooperative and competitive multiple jammers, auctioning and power control mechanisms are applied for a follower sub-game in a two-layer leader-follower game framework.**

***Index Terms*—Information theoretic security, cooperative jamming, game theory, Stackelberg game, auctions.**

I. Introduction

INFORMATION-THEORETIC security provides fundamental limits for communication that is both reliable and confidential from unauthorized parties. Shannon was first to measure information secrecy using mutual information [1]. He reached a somewhat pessimistic conclusion that, in a noiseless setting, in order to reveal no information to the eavesdropper, the legitimate parties need to share a secret key of the same rate as the transmitted message. The wiretap channel was formally defined by Wyner in [2], revealing that the noisy communication medium often enables the possibility of more pragmatic secret communication, without a need for a secret shared key. A coding scheme was constructed that achieves a non-zero secrecy rate, provided that the eavesdropper's channel is degraded respective to the legitimate receiver's. 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 secrecy capacity of the Gaussian wiretap channel was found in [4].

Recently, multi-terminal wireless secure communication scenarios generated significant interest, see for example, [5]-[13]. Of particular interest to this work is the cooperative jamming paradigm introduced in references [5], [7], wherein it was recognized that, while the open nature of the wireless medium makes it susceptible to malicious eavesdropping, it can also be exploited to counter this vulnerability. Cooperative jamming prescribes creating judicious interference by network nodes transmitting noise [5]-[7] or codewords [11], [14], [15], so as to impair the eavesdropper's ability to decode the confidential information, and thus, increase secure communication rates between legitimate parties. The drawback of this approach is the necessity for dedicated and/or altruistic jamming nodes, willing to expend their resources for the communications they are not directly involved with. This may not be practical for scenarios involving mobile nodes with limited batteries.

In this work, we tackle this issue by proposing a game-theoretic framework wherein non-altruistic nodes, i.e., nodes with their own data, can facilitate secure source-destination communication by taking the role of cooperative jammers, if appropriately compensated by spectrum that would enable them to transmit their own data to their destination. The proposed scheme does not require codebook exchanges between any communicating pairs. The scheme is inspired by the *spectrum leasing for cooperation* paradigm [16] [17], where non-altruistic nodes end up performing the role of a relay instead of a cooperative jammer. Reference [18] recently introduced a game-theoretic scheme incorporating a wiretap channel with non-altruistic but friendly jammer. This reference focuses on a single jammer scenario, and proposes the scheme that accommodates simultaneous transmissions of useful data by the legitimate source and the jammer. We will elaborate on the comparison between [18] and our scheme later in the manuscript, in particular in Section VI. Another game-theoretic model for jamming motivation was considered in [19] [20], where the friendly jammers are compensated with a credit-based incentive, rather than with a communication opportunity. Unlike [19] [20], our approach is entirely framed in the communication domain and does not require any policy alteration.

Focusing at first on the scenario with a single potential jammer, the proposed scheme is outlined as follows. Legitimate parties, i.e., a source and its destination, communicate in

Manuscript received November 10, 2011; revised April 24 and August 19, 2012; accepted October 1, 2012. The associate editor coordinating the review of this paper and approving it for publication was J. Wu.

I. Stanojev is with the Department of General Engineering, University of Wisconsin-Platteville, 1 University Plaza, Platteville, WI 53818, USA (e-mail: stanojevi@uwplatt.edu).

A. Yener is with the Department of Electrical Engineering, The Pennsylvania State University, University Park, PA 16802, USA (e-mail: yener@ee.psu.edu).

Digital Object Identifier 10.1109/TWC.2012.120412.112001

the presence of an eavesdropper and a separate non-altruistic node. The source is willing to compensate the non-altruistic node for its participation in cooperative jamming with an access to a fraction of its transmission interval/bandwidth. By doing so, the source aims to maximize its secrecy rate, that is the rate at which information is completely concealed from the eavesdropper. On the other hand, the potential jammer optimizes its power with the goal of maximizing its data transmission rate during the leased interval, discounted by the cost of the overall transmitted power including the jamming power. The ratio of the jamming and data transmission power is determined by the source. This interaction between the source and a potential non-altruistic jammer is conveniently cast in the framework of a *leader-follower* game [21], i.e., a Stackelberg game, with source in the role of the game leader and jammer as the follower, and its outcome is the Stackelberg equilibrium, as elaborated in Section III. This model slightly favors the source-destination pair, and is justified by the fact that the legitimate parties are licensed to operate in the given spectrum.

The scheme is then extended to involve multiple potential jammers, modeling their competition for bandwidth access via distributed resource allocation mechanisms such as *auctioning* [22] [17] in Section IV, and the *power control game* [23] [24] [16] in Section V. Interaction between the source and the set of potential cooperative jammers now becomes a two-layer game, with a Stackelberg game described above as an 'outer' framework, while a set of jammers constitutes the follower entity whose power response is the outcome of the auction or power control sub-game played between jammers. For the former, the follower's response becomes the outcome of the second-price Vickrey auction [25]. In particular, the jammers are modeled as competitive bidders, with invested power as the bidding article and the legitimate pair as the auctioneer. As elaborated in Section IV, the rules of Vickrey auction are modified so as to accommodate non-linearities implied by the communication model. Next, we consider a second multi-jammer scheme where the follower's response is the power allocation given by the *Nash equilibrium* [21] of the power control game played between competitive jammers. Compared to the auctioning scheme, the power control game allows for simultaneous assignment of multiple jammers, while imposing more stringent system information requirements and more extensive signaling, as detailed in Section IV and Section V. The maximization goals, i.e., utilities for both mechanisms are the same as outlined for the simple Stackelberg game.

Results in this paper reveal several insights. Both the secrecy rate and the chosen jammer's utility improve with the proposed mechanisms, despite the nodes' non-cooperative nature. The secrecy rate increases with the number of potential jammers, with the power control scheme outperforming the auction scheme, while the auction outperforms the Stackelberg scheme due to competitiveness. Opposite relations between the three schemes hold for the jammer's utility. Moreover, as the number of potential jammers increases, utility of a chosen jammer for any scheme will start to decrease as the legitimate parties can be more aggressive when leading the game. Interestingly, when the jammers are very close to the eavesdropper, their utility rapidly decreases, as the source requires a relatively small jamming power and can preserve the majority of the bandwidth for itself.

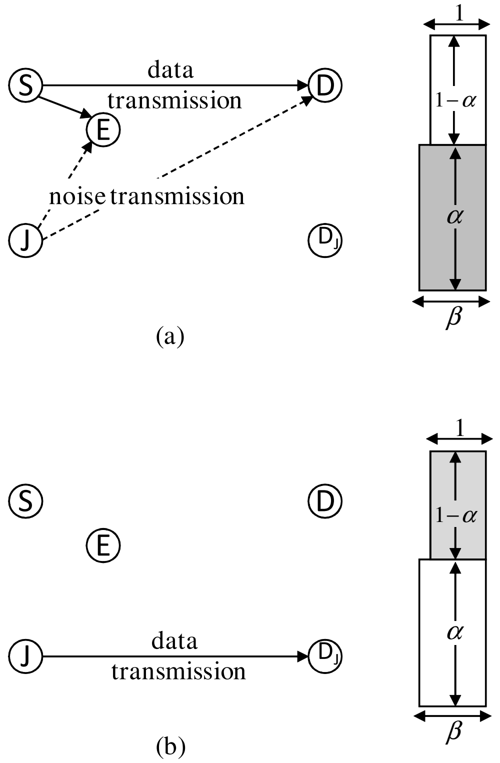


Fig. 1. Example of spectrum leasing for cooperative jamming with $N = 1$ cooperative jammers.

It is noted that, in addition to facilitating a meaningful operating framework for the deployment of cooperative jamming paradigm via spectrum leasing, the proposed solution can be alternatively applied for practical implementation of cognitive radio networks operating according to property-rights model [26]. In such networks, a primary, i.e., a licensed users, may lease portions of a licensed spectrum to a secondary, i.e., an unlicensed users, in exchange for some form of compensation. Here, the role of a primary node is played by the source transmitting a confidential message and that of a secondary by the jamming nodes. Moreover, retribution from secondary to primary nodes is in the form of cooperative jamming to the primary secret transmission. This enables on-the-air decisions and avoids the regulatory issues or money transactions that commonly hinder the implementation of the property-rights spectrum leasing concept.

II. System Parameters and Reference Communication Model

Here, we detail on the system parameters and notation in Section II-A and describe the reference communication model with $N = 1$ potential friendly jammer in Section II-B.

A. System Parameters and Notation

We consider a scenario where source S communicates with destination D using a bandwidth or a time-slot normalized to unity, in a presence of an eavesdropper E from whom the communication must be kept secret. There are N additional nodes J_i, $i = 1, ..., N$ present, each having data to transmit towards its intended receiver $\mathrm{D}_{\mathrm{J},i}$ and possibly acting as a cooperative jammer for the S-D secure communication, as illustrated in Figure 1 for $N = 1$. The channel gains between nodes are modeled as independent complex Gaussian random variables. Instantaneous power channel gains between node S and nodes D and E are denoted as h_{SD} and h_{SE}, respectively, between node J_i and nodes D and E as $h_{\mathrm{J}_i\mathrm{D}}$ and $h_{\mathrm{J}_i\mathrm{E}}$, respectively, and between J_i and $\mathrm{D}_{\mathrm{J},l}$ as $h_{\mathrm{J}_{il}}$, $i, l = 1, .., N$. Average transmit powers for the source S and jammers J_i are P_{S} and P_{J_i}, respectively, with the latter limited by the power budget $P_{\mathrm{J}_i} \leq \bar{P}_{\mathrm{J}_i}$. Independent additive white Gaussian noise variance for each link is σ^2. For the case involving $N = 1$ potential jammer, index is removed from notation for clarity. Throughout the paper, we assume signaling using Gaussian codebooks and cooperative jamming in the form of Gaussian noise.

B. Reference Communication Model

The scenario of interest is illustrated in Figure 1 for $N = 1$ jammer and involves the source S communicating secretly with the destination D in the presence of the eavesdropper E, looking to recruit node J as a cooperative jammer, if this would increase its secrecy rate. In particular, the source is willing to preserve only a bandwidth fraction $\alpha \leq 1$ for its secret communication aided by cooperative jamming, as in Figure 1-(a), and compensate the potential jammer with a remaining bandwidth fraction $1-\alpha$ for jammer's own data transmission, as in Figure 1-(b). The ratio of the average power used by the node J during the cooperative jamming phase, when it transmits Gaussian noise, and data transmission phase, when it transmits its own data, is denoted as β and determined by the legitimate pair.

1) Transmission Powers: Before presenting the expressions describing the nodes' performances, we elaborate on transmission powers during the two intervals illustrated in Figure 1. Denoting the symbols transmitted by the legitimate source during its and jammer's data transmission interval as $X_{\alpha,i}$ and $X_{1-\alpha,j} = 0$, respectively, where $i = 1, .., \alpha K$, $j = \alpha K+1, .., K$ and K is the number of symbols transmitted during the entire normalized interval, the source average power $\mathbb{E}\left[X^2_{\alpha,i}\right]$ during its data transmission is given by:

$$\begin{aligned} P_{\mathrm{S}} &= \frac{1}{K}\sum_{i=1}^{\alpha K}\mathbb{E}\left[X^2_{\alpha,i}\right] + \frac{1}{K}\sum_{j=\alpha K+1}^{K}\mathbb{E}\left[X^2_{1-\alpha,j}\right] \\ &= \frac{1}{K}\sum_{i=1}^{\alpha K}\mathbb{E}\left[X^2_{\alpha,i}\right] \\ &= \alpha\mathbb{E}\left[X^2_{\alpha,i}\right], \end{aligned} \tag{1}$$

and thus reads

$$\mathbb{E}\left[X^2_{\alpha,i}\right] = P_{\mathrm{S}}/\alpha. \tag{2}$$

Similarly, denoting the jammer's transmitted signal during the cooperative jamming phase and its own data transmission phase as $Y_{\alpha,i}$ and $Y_{1-\alpha,j}$, respectively, where $i = 1, .., \alpha K$ and $j = \alpha K + 1, .., K$, we have:

$$P_{\mathrm{J}} = \alpha\mathbb{E}\left[Y^2_{\alpha,i}\right] + (1-\alpha)\mathbb{E}\left[Y^2_{1-\alpha,i}\right]. \tag{3}$$

Applying $\mathbb{E}\left[Y^2_{\alpha,i}\right] = \beta\mathbb{E}\left[Y^2_{1-\alpha,j}\right]$ to (3), we get

$$\mathbb{E}\left[Y^2_{\alpha,i}\right] = \frac{\beta P_J}{\alpha\beta+1-\alpha} \tag{4}$$

$$\mathbb{E}\left[Y^2_{1-\alpha,i}\right] = \frac{P_J}{\alpha\beta+1-\alpha}. \tag{5}$$

2) Performance Measures: The achievable S-D secrecy rate, that is the communication rate at which no information is revealed to the eavesdropper, is considered here in the sense of weak secrecy, see for example [6]. This rate, assisted by cooperative jamming with Gaussian noise, is given by [5] [6]:

$$\begin{aligned} R_{\mathrm{S}}(\alpha,\beta;P_{\mathrm{J}}) = \alpha\Bigg[&\log_2\left(1+\frac{\frac{h_{\mathrm{SD}}P_{\mathrm{S}}}{\alpha}}{\sigma^2+\frac{h_{\mathrm{JD}}\beta P_J}{\alpha\beta+1-\alpha})}\right) - \\ &\log_2\left(1+\frac{\frac{h_{\mathrm{SE}}P_{\mathrm{S}}}{\alpha}}{\sigma^2+\frac{h_{\mathrm{JE}}\beta P_J}{\alpha\beta+1-\alpha}}\right)\Bigg]^+, \end{aligned} \tag{6}$$

where $[x]^+ = \max(0,x)$. In (6), (2) and (4) are used for the source transmission power and the jammer's noise transmission power during the fraction α as in Figure 1-(a), respectively.

The utility of the node acting as cooperative jammer is defined as its achievable reliable communication rate during the fraction $1-\alpha$, as in Figure 1-(b), towards its destination D_{J}, priced by the cost of the overall average transmission power [16]:

$$U_{\mathrm{J}}(\alpha,\beta;P_{\mathrm{J}}) = (1-\alpha)\log_2\left(1+\frac{h_{\mathrm{J}}P_J}{\sigma^2(\alpha\beta+1-\alpha)}\right) - cP_{\mathrm{J}}, \tag{7}$$

where c is the cost per unit transmission power and $P_{\mathrm{J}} \leq \bar{P}_{\mathrm{J}}$. In (7), equation (5) is applied for the jammer's data transmission power. Notice that the first part of the utility (7) reflects the node's satisfaction from accessing the spectrum, in terms of amount of data it can transmit, while the second part stands for its expense, in terms of power required to achieve this satisfaction. We remark that the second part of utility needs not be constrained to a linear function, which is applied here for analytical convenience [17] [23]. Furthermore, notice that jammer's communication is not subject to secrecy requirements.

3) Conditions for Jamming Participation: It was determined in [6] that the following conditions are required for the cooperative jamming to yield improvement on the secrecy rate:

$$\frac{h_{\mathrm{SE}}h_{\mathrm{JD}}}{h_{\mathrm{SD}}h_{\mathrm{JE}}} < 1 \tag{8}$$

$$\frac{h_{\mathrm{SD}}h_{\mathrm{JD}}\left(\sigma^2+h_{\mathrm{SE}}P_{\mathrm{S}}/\alpha\right)}{h_{\mathrm{SE}}h_{\mathrm{JE}}\left(\sigma^2+h_{\mathrm{SD}}P_{\mathrm{S}}/\alpha\right)} < 1. \tag{9}$$

Moreover, the jammer utility (7) is clearly concave with P_{J} and negative when $P_{\mathrm{J}} \to \infty$. For such a function to have a positive value over some range of P_{J}, the condition $\partial U_{\mathrm{J}}/\partial P_{\mathrm{J}}|_{P_{\mathrm{J}}=0} > 0$ must hold:

$$h_{\mathrm{J}} > \sigma^2\left(\frac{\alpha\beta}{1-\alpha}+1\right)c\ln 2. \tag{10}$$

With this condition, utility U_{J} is positive for $P_{\mathrm{J}} \in (0, P_{\mathrm{J}}^{\mathrm{lim}}(\alpha,\beta))$, where $P_{\mathrm{J}}^{\mathrm{lim}}(\alpha,\beta)$ is the positive solution of

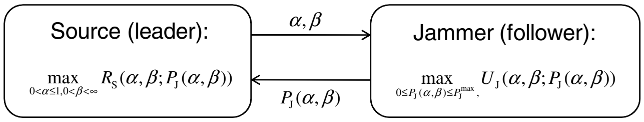

Source (leader):
$\max_{0<\alpha\le 1, 0<\beta<\infty} R_S(\alpha,\beta;P_J(\alpha,\beta))$
α,β
$P_J(\alpha,\beta)$
Jammer (follower):
$\max_{0\le P_J(\alpha,\beta)\le P_J^{\max},} U_J(\alpha,\beta;P_J(\alpha,\beta))$

Fig. 2. Stackelberg interaction between the source and the potential cooperative jamming node.

$U_{\rm J}(\alpha, P_{\rm J}(\alpha,\beta)) = 0$ and reads:

$$P_{\rm J}^{\rm lim}(\alpha,\beta) = \frac{\sigma^2}{h_{\rm J}}\left(-\frac{1}{k(\alpha,\beta)}\mathcal{W}_{-1}\left(-k(\alpha,\beta)e^{k(\alpha,\beta)}\right) - 1\right), \tag{11}$$

where $k(\alpha,\beta) = c\ln 2 \cdot \frac{\sigma^2}{h_{\rm J}} \cdot \left(\frac{\alpha\beta}{1-\alpha} + 1\right)$ and $\mathcal{W}_l\,(x)$ is is the lth branch of the multi-valued Lambert W function [27].

III. Reference Stackelberg Model

This section elaborates on the game theoretic model with $N = 1$ potential friendly jammer, which is the basis for the more sophisticated schemes proposed in Section IV and Section V involving multiple potential jammers. Interaction between the legitimate pair and the jammer, facilitating their self-interested behavior, is described in Section III-A. As will be shown in Section III-A, both parties try to optimize their performance in the leader-follower, i.e., Stackelberg framework, where the legitimate pair will lead the game and the potential jammer will follow. A straightforward extension of the reference Stackelberg scheme to a multi-jammer scenario is given in Section III-B.

A. Game-Theoretic Model

Throughout this work, the nodes are defined as *selfish* and *rational* [21] to mimic a non-altruistic behavior. An appropriate framework for analyzing the interaction between such nodes is game theory [21]. In particular, a convenient setting here is that of the *Stackelberg game* [21], wherein one agent, termed follower, acts subject to the strategy chosen by the other agent, leader, which in turns seeks maximization of its own utility. Here, the game leader and the follower are the source and the cooperative jammer, respectively. This model favors the legitimate pair, which is justified by the fact that any operation here is performed in the legitimate pair's bandwidth. The source's optimal strategy (α^*,β^*) and the corresponding power choice of the jammer $P_{\rm J}^*(\alpha^*,\beta^*)$ are jointly referred to as the *Stackelberg equilibrium.*

Interaction between the source and the potential non-altruistic jammer is shown in Figure 2. The cooperative jammer is aware of parameters (α,β) and optimizes its power towards the goal of maximizing its utility, given by (7). The solution of jammer's problem

$$P_{\rm J}^*(\alpha,\beta) = \arg\max_{P_{\rm J}(\alpha,\beta)} U_{\rm J}(\alpha,\beta;P_{\rm J}(\alpha,\beta)) \tag{12}$$
$$\text{s.t. } 0 \le P_{\rm J} \le \bar{P}_{\rm J},$$

is given by

$$P_{\rm J}^*(\alpha,\beta) = \left[\frac{1-\alpha}{c\ln 2} - \frac{\sigma^2(\alpha\beta+1-\alpha)}{h_{\rm J}}\right]_0^{\bar{P}_{\rm J}}, \tag{13}$$

where $[x]\,_{x_{\min}}^{x_{\max}} = \min(\max(x_{\min},x),x_{\max})$. It is very important to notice from (13) that the power pricing mechanism prevents the source from preserving an unfairly large amount of bandwidth α, as this would in turn typically implicate a small cooperative jamming power $P_{\rm J}^*(\alpha,\beta)$ or even lead to a denial of jamming participation $P_{\rm J}^*(\alpha,\beta) = 0$. Similar conclusions hold for the power ratio parameter β.

On the other hand, the source, acting as the game leader, determines the fraction α and ratio β towards the goal of maximizing its secrecy rate (6), knowing that its decision will affect the strategy selected by the jammer:

$$\alpha^*,\beta^* = \arg\max_{\alpha,\beta} R_{\rm S}(\alpha,\beta;P_{\rm J}^*(\alpha,\beta)) \tag{14}$$
$$\text{s.t. } 0 < \alpha \le 1, 0 < \beta < \infty$$

where $P_{\rm J}^*(\alpha,\beta)$ is given by (13). Equations (13) and (14) constitute the Stackelberg equilibrium for the described model. It is noted that the solution of the one-dimensional optimization (14) requires numerical methods, as presented in Section VII. Furthermore, (14) includes the possibility of refusing the jammer's cooperation, $\alpha = 1$, if the latter is not contributing, in which case the jammer's utility is zero. The source is assumed to have the complete knowledge of all the channel gains in the system, while the knowledge of $h_{\rm J}$ is required at the jammer. Albeit ideal, the assumption of instantaneous Channel State Information (CSI) at transmitters is common in the literature on game-theoretic applications to wireless networks [16] [23] and provides a benchmark for analysis. As a final remark, we consider the scenario where nodes who agree on being cooperative jammers are honest and trusted, i.e., they do not deviate from the expected behavior of jamming with the power ratio prescribed by the source, nor turn malicious.

B. Application to Multi-Jammer Scenario

The framework described above can also be used for the environment involving multiple potential cooperative jammers. In addition to the parameters α and β, the source would also have to indicate the index of the 'winning' jammer, i.e., the one that would mostly contribute to the source's secrecy rate. Although valid, and in fact, used as a reference for numerical analysis in Section VII, this approach fails to fully exploit the selfish and rational features of multiple potential jammers, for which contention for bandwidth access and consequently further improvement for the source are likely. In the following two sections, we elaborate on such two mechanisms that incorporate the competitive jammers' behavior.

IV. Auction Scheme

This section describes the auction scheme involving multiple potential cooperative jammers $\rm J_{\it i}$, $i = 1,..,N$, competing to gain the spectrum access for transmission of their user data towards their single intended receiver $\rm D_{J,\it i}$, by offering cooperative jamming services to the source. It is clear that a competition, in this case, is likely to contribute to the profit of the object seller [21], here the source. The communication model and the interaction between the source and the set of potential jammers follow the lines of Section III, with the notable difference that the follower entity is now a set of N jammers and the follower's response $P^{*}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta)$ is the power outcome of the *auction* game played among jammers, with $w(\alpha,\beta) = 1,..,N$ indicating the winning cooperative jammer, if any, for a source's strategy (α,β), as detailed in the following. Thus, similarly as in Section III, a single node is chosen to participate as the jammer. The competition model is built upon the rules of Vickrey auction, i.e., the sealed-bid second-price auction [25] [22] due to its desirable properties, as detailed in Section IV-A. It is noted that the considered framework is not limited to Vickrey auctions and can be implemented via other auction types, albeit implying extensive signaling and computations at the nodes, as well as an intractable system analysis [17].

A. Vickrey Auction

Auctions are a widely accepted mechanism for distribution of limited amount of resources among competing users [22]. Among various auction types, the sealed bid second-price Vickrey auction, prescribing that the winning bidder is awarded with the bidding item at the price of the second largest bid, is of particular interest, due to its 'truthful bidding' property [25] [22]. Namely, bidders are motivated to bid with the maximum amount they would be willing to pay for the object. Importantly, such a strategic choice corresponds to the game-theoretic concept of *dominant strategy equilibrium* (*DSE*), defined as the state wherein the strategies are required to remain preferable to every player irrespective of the amount of information available on the other players [21]. To provide a brief intuition on the truthful bidding properties 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 an optimal 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 [21] [22] [25] .

Since the price paid by the winning bidder is not larger than its item evaluation, the bidders are guaranteed a non-negative profit. This creates a strong motivation for the users to take part in auction, which in turn increases the profit of the auctioneer. Furthermore, the auctioneer has the option of setting the lowest acceptable price (i.e., the reserve price) which reflects its own evaluation of the bidding item. By declaring a reserve price, the auctioneer is also guaranteed a non-negative payoff. It is noted that the desirable properties of Vickrey auction have already proved useful in wireless communication problems, see for example [17] [28].

B. Modified Vickrey Auction for Communication Model

Here, the auctioneer's utility is defined as the secrecy rate R_{S} as in (6), a bidder J_i's strategy is its power P_{J_i} and a bidder's utility U_{J_i} is defined in (7), given that it is granted the spectrum access, i.e., that it won the auction, and zero otherwise. For a given (α,β), the bids are in the form of the secrecy rate $R_{\mathrm{S}}(\alpha,\beta;P_{\mathrm{J}_i})$, implying that a bidder J_i must be aware of the source's parameters h_{SD} and h_{SE}. The source sets the lowest acceptable rate, i.e., the reserve price, as $R_S(\alpha,\beta;P_{\mathrm{J}}=0)$, accepting only larger bids. Note that the reserve price can be also set as $R_S(\alpha=1,\beta;P_{\mathrm{J}}=0)$, standing for the secrecy rate with no friendly jamming, but would yield no change to the Stackelberg equilibrium, as can be seen in the following. Denoting the bidding strategies in the DSE equilibrium as $P^{\mathrm{bid}}_{\mathrm{J}_i}$, the index of a winning cooperative jammer for a given (α,β) reads

$$w(\alpha,\beta) = \arg\max{}_{i=1,..,N} R_{\mathrm{S}}(\alpha,\beta;P^{\mathrm{bid}}_{\mathrm{J}_i}(\alpha,\beta)), \tag{15}$$

if $R_{\mathrm{S}}(\alpha,\beta;P^{\mathrm{bid}}_{\mathrm{J}_{w(\alpha)}}) > R_S(\alpha,\beta;0)$, otherwise no jammer is chosen. The standard assumption, also adopted here, is that, in the case of multiple equal highest offers, the situation is resolved by random allotment to one of them. Furthermore, the second-best rate $R_{\mathrm{S},2}$ reads:

$$\begin{aligned} R_{\mathrm{S},2}(\alpha,\beta) = \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (16)\\ \max\left(\max{}_{i\neq w(\alpha,\beta)} R_{\mathrm{S}}\left(\alpha,\beta;P^{\mathrm{bid}}_{\mathrm{J}_i}(\alpha,\beta)\right), R_{\mathrm{S}}(\alpha,\beta;0)\right). \end{aligned}$$

Before proceeding to Section IV-C to determine the DSE and the Stackelberg equilibria, we notice that the auctioning analytical tools are developed for relatively simple linear or monotonic utility functions [22], which might not be the case for the model herein. On this line, we borrow the result from [6] that establishes the impact of P_{J_i} on $R_{\mathrm{S}}(\alpha,\beta;P_{\mathrm{J}_i})$ for a given (α,β) and formulate it as the following lemma. As discussed below, the lemma indicates that it is possible to improve the DSE equilibrium for the communication model at hand and also provides a guideline to finding the auction bidding equilibrium $P^{\mathrm{bid}}_{\mathrm{J}_i}(\alpha,\beta)$, $w(\alpha,\beta)$ and the auction outcome $P^{*}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta)$ in Section IV-C.

Lemma 1. *[6] For a given (α,β), the function $R_S(\alpha,\beta;P_{\mathrm{J}_i})$ is quasi-concave in P_{J_i}, for $P_{\mathrm{J}_i} \geq 0$, with the maximum at $P^{S\max}_{\mathrm{J}_i} = \arg\max_{P_{\mathrm{J}_i}} R_{\mathrm{S}}(\alpha,\beta;P_{\mathrm{J}_i}) > 0$ given by*

$$\begin{aligned} P^{S\max}_{\mathrm{J}_i}(\alpha) = \frac{\alpha\beta+1-\alpha}{\beta}\Bigg(\frac{\sigma^2\left(h_{\mathrm{SE}}-h_{\mathrm{SD}}\right)}{h_{\mathrm{SD}}h_{\mathrm{J}_i\mathrm{E}}-h_{\mathrm{SE}}h_{\mathrm{J}_i\mathrm{D}}}+ \\ \sqrt{\frac{\sigma^2 h_{\mathrm{SE}}h_{\mathrm{SD}}\left(h_{\mathrm{J}_i\mathrm{E}}-h_{\mathrm{J}_i\mathrm{D}}\right)}{h_{\mathrm{J}_i\mathrm{D}}h_{\mathrm{J}_i\mathrm{E}}\left(h_{\mathrm{SD}}h_{\mathrm{J}_i\mathrm{E}}-h_{\mathrm{SE}}h_{\mathrm{J}_i\mathrm{D}}\right)}}\cdot \\ \sqrt{\left(\frac{\sigma^2\left(h_{\mathrm{J}_i\mathrm{E}}-h_{\mathrm{J}_i\mathrm{D}}\right)}{h_{\mathrm{SD}}h_{\mathrm{J}_i\mathrm{E}}-h_{\mathrm{SE}}h_{\mathrm{J}_i\mathrm{D}}}+\frac{P_{\mathrm{S}}}{\alpha}\right)}\Bigg). \end{aligned} \tag{17}$$

if the conditions (8)-(9) are met.

Lemma 1 reveals the quasi-concavity of source's utility versus the power P_{J_i} which, together with the fact that a jammer's utility (7) is concave in P_{J_i} (for $P_{\mathrm{J}_i} \geq 0$) brings us to the following observation, illustrated in Figure 3. Unlike the setting in a baseline auction model, wherein the auctioneer and a bidder's utility are monotonically increasing and decreasing in price, respectively, i.e., a profit for one is a negative surplus to another [22], here, due to their (quasi-)concavity, it is possible that the players' utilities for a particular P_{J_i} have slopes of equal signum and, thus, not necessarily incompatible goals, as in the shaded area in Figure 3. This observation

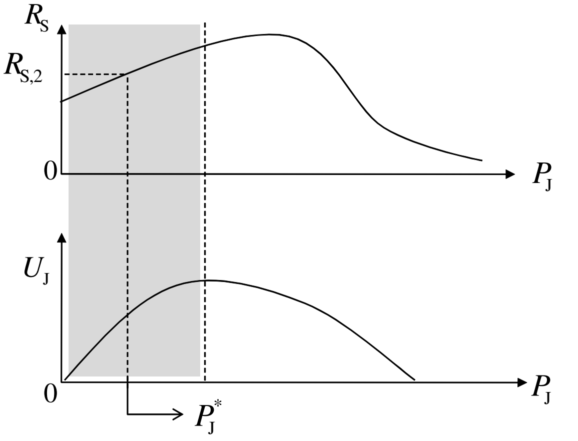


Fig. 3. Auction modification for communication model.

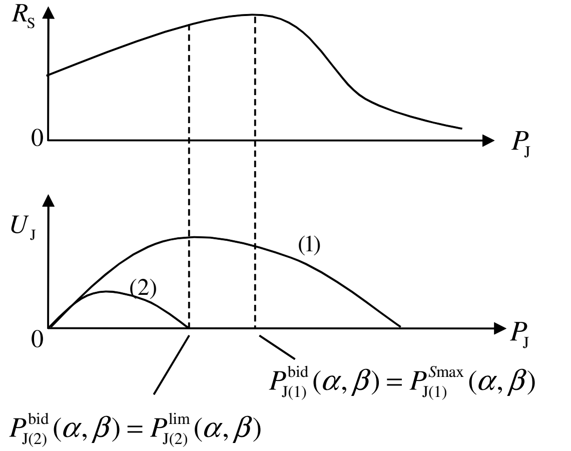


Fig. 4. Illustration of Theorem 1.

leads us to propose the following modification of the Vickrey auction rule that can lead to the performance improvement for all involved nodes in the communication model at hand, except of course the eavesdropper.

Definition 1. In the proposed modification of Vickrey auction, the winning bidder is required to provide the secrecy rate that is *at least* the second largest bid, i.e., $R_{\mathrm{S}}(\alpha,\beta;P^*_{\mathrm{J}_{w(\alpha)}}(\alpha,\beta)) \geq R_{\mathrm{S},2}(\alpha,\beta)$.

The second largest bid $R_{\mathrm{S},2}(\alpha,\beta)$ is given in (16). Unlike the original Vickrey principle, wherein the winning bidder provides the auctioneer with *exactly* the second-best price, this modification enables the winning node to choose a larger value if, as a result, its utility will increase. Notice that neither of the involved nodes, i.e., auctioneer and a bidder, are harmed by this deviation from the Vickrey principles, quite the opposite, as illustrated in Figure 3. The benefits due to this modification will be also clearly visible in the following subsection.

C. Equilibria

The strategy for a bidder in the DSE is given by the following theorem.

Theorem 1. *For a given (α,β), the dominant bidding strategy $P^{\mathrm{bid}}_{\mathrm{J}_i}(\alpha,\beta)$ for a bidder J_i is:*

$$P^{\mathrm{bid}}_{\mathrm{J}_i}(\alpha,\beta) = \min\left(P^{S\max}_{\mathrm{J}_i}(\alpha,\beta), P^{\lim}_{\mathrm{J}_i}(\alpha,\beta), \bar{P}_{\mathrm{J}_i}\right), \quad (18)$$

where $P^{\lim}_{\mathrm{J}_i}(\alpha,\beta)$ and *$P^{S\max}_{\mathrm{J}_i}(\alpha,\beta)$* are given by (11) and (17), respectively.

Proof: The proof is illustrated in Figure 4 for the case $P^{\lim}_{\mathrm{J}_i}(\alpha,\beta) < \bar{P}_{\mathrm{J}_i}$ and given as follows. Since in the case of winning the auction, the bidder has no influence on the second-best bid, the dominant strategy is to maximize the chance of winning, i.e., to bid with $P^{S\max}_{\mathrm{J}_i}(\alpha,\beta)$ if $P^{S\max}_{\mathrm{J}_i}(\alpha,\beta) \leq \min\left(P^{\lim}_{\mathrm{J}_i}(\alpha,\beta), \bar{P}_{\mathrm{J}_i}\right)$ (recall that $P^{S\max}_{\mathrm{J}_i}(\alpha,\beta)$ maximizes R_S). However, in case of $P^{S\max}_{\mathrm{J}_i}(\alpha,\beta) > \min\left(P^{\lim}_{\mathrm{J}_i}(\alpha,\beta), \bar{P}_{\mathrm{J}_i}\right)$, i.e., if $P^{S\max}_{\mathrm{J}_i}(\alpha,\beta)$ yields a negative bidder's utility ($P^{S\max}_{\mathrm{J}_i} > P^{\lim}_{\mathrm{J}_i}$) or is out of permissible power range set by $\bar{P}_{\mathrm{J}_i}$ ($P^{S\max}_{\mathrm{J}_i} > \bar{P}_{\mathrm{J}_i}$), the bidder chooses $\min\left(P^{\lim}_{\mathrm{J}_i}(\alpha,\beta), \bar{P}_{\mathrm{J}_i}\right)$ as bidding with larger P_{J_i} would increase the chance of winning only if incurring a negative bidder's utility or a power that is out of permissible range, while bidding with smaller power would only decrease the chance of winning. ■

The theorem is valid independent of whether Definition 1 is applied or not. Having won the auction, the winning cooperative jammer $\mathrm{J}_{w(\alpha,\beta)}$ has to provide the transmitting/jamming power that produces at least $R_{\mathrm{S},2}(\alpha,\beta)$. The following theorem provides this auction outcome.

Theorem 2. *Under the rule in Definition 1, the power $P^*_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta)$ chosen by the winning cooperative jammer $\mathrm{J}_{w(\alpha,\beta)}$ is given by*

$$P^*_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta) = \begin{cases} P_M, & P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta) > P_M, \\ & R_{\mathrm{S},2}(\alpha,\beta) > 0 \\ P_m, & P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta) < P_m, \\ & R_{\mathrm{S},2}(\alpha,\beta) > 0 \\ P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta), & P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta) \geq P_m, \\ & P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta) \leq P_M, \\ & R_{\mathrm{S},2}(\alpha,\beta) > 0 \\ P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta), & R_{\mathrm{S},2}(\alpha,\beta) = 0, \end{cases} \quad (19)$$

where $P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta)$ is given by (13), while, for $R_{\mathrm{S},2}(\alpha,\beta) > 0$, *$P_m$ and P_M, $P_m \leq P_M$, are the roots of the quadratic equation $R_{\mathrm{S}}\left(\alpha,\beta;P_{\mathrm{J}_{w(\alpha,\beta)}}\right) = R_{\mathrm{S},2}(\alpha,\beta)$.*

Proof: It suffices to show that (19) is the solution of the winning jammer's $\mathrm{J}_{w(\alpha,\beta)}$ utility maximization problem over $P_{\mathrm{J}_{w(\alpha,\beta)}}$under the constraint $R_{\mathrm{S}}\left(\alpha,\beta;P_{\mathrm{J}_{w(\alpha,\beta)}}\right) \geq R_{\mathrm{S},2}(\alpha,\beta)$. This maximization problem is also illustrated in Figure 5. If $R_{\mathrm{S},2}(\alpha,\beta) = 0$, the winner is free to choose any transmission power, as it is not required to improve the secrecy rate. Thus, the winner chooses the power that maximizes its utility $P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta)$, as given in 13. For $R_{\mathrm{S},2}(\alpha,\beta) > 0$, the values P_m and P_M, $P_m \leq P_M$, correspond to the winning bidder's transmission powers that yield exactly the second-best bid, $R_{\mathrm{S},2}(\alpha,\beta)$, as seen in Figure 5. If $P_m \leq P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha)}}(\alpha,\beta)$ or $P_M \geq P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha)}}(\alpha,\beta)$, the jammer $\mathrm{J}_{w(\alpha,\beta)}$ chooses P_m or

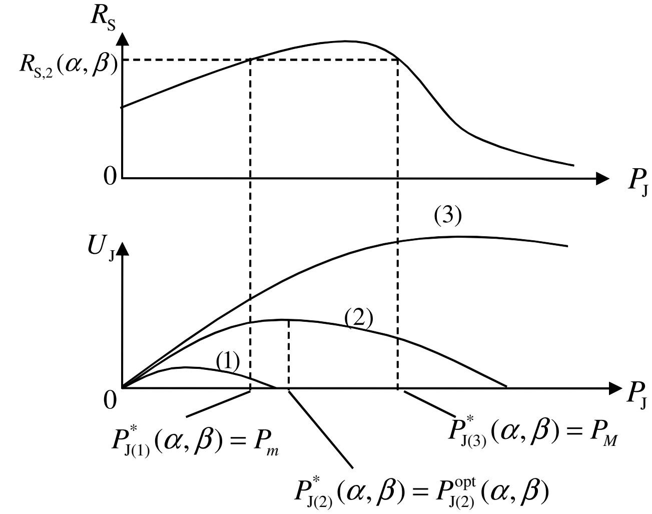

R_S
$R_{S,2}(\alpha,\beta)$
0
P_J
U_J
(3)
(2)
(1)
0
P_J
$P^*_{J(1)}(\alpha,\beta) = P_m$
$P^*_{J(3)}(\alpha,\beta) = P_M$
$P^*_{J(2)}(\alpha,\beta) = P^{\mathrm{opt}}_{J(2)}(\alpha,\beta)$

Fig. 5. Illustration of Theorem 2.

P_M, respectively, to maximize its utility under the constraint of maintaining the second-best bid $R_{\mathrm{S},2}(\alpha,\beta)$. If $P_m \leq P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta) \leq P_M$, the winning bidder can exploit the modification in Definition 1, and thus chooses the transmission power $P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta)$, given by 13, to maximize its utility. ■

Notice in Theorem 2 and Figure 5 that for the case $P_m \leq P^{\mathrm{opt}}_{\mathrm{J}_{w(\alpha,\beta)}}(\alpha,\beta) \leq P_M$, the alteration of Vickrey principle introduced by Definition 1 brings improvement to both the secrecy rate R_{S} and the jammer utility U_{J}.

To conclude this section, the outcome of the auction, as given by (19), constitutes the follower's response in the Stackelberg framework and the Stackelberg equilibrium thus reads

$$(\alpha^*,\beta^*) = \arg\max_{\alpha,\beta} R_{\mathrm{S}}\left(\alpha,\beta; P^*_{\mathrm{J}_{w(\alpha)}}(\alpha,\beta)\right). \qquad (20)$$

Notice that this model essentially requires that the source can anticipate the outcome of the auction game, and thus to be aware of all channel parameters in the system. An alternative to this requirement is for the source to perform a series of auctions with different (α,β) and determine the most contributing one. As for the jamming nodes, a jammer J_i needs the knowledge of the parameters h_{SD} and h_{SE}, in addition to $h_{\mathrm{J}_{ii}}$. On the positive side, a bidder requires no information on number of other bidders, their strategies or channel parameters, which is in line with the basic Vickrey implications[1].

V. Power Control Scheme

In this section, a scheme is proposed that allows the source to employ multiple cooperative jammers simultaneously. Besides setting the fraction α and power ratio β, the source also communicates to the jammers the set $\mathcal{J} \subseteq \{1,..,N\}$ of chosen jammers. During their data transmission phase of duration $1-\alpha$, the participating cooperative jammers, i.e., the jammers from the set $\mathcal{J}$, share the communications resource and their transmission scheme results in an interference channel [30]. Though in general information theoretically suboptimal, we shall assume that interference is treated as noise for our setting [31] [32], which is the standard assumption for a game-theoretic approach to an interference channel [16] [23] [24]. In terms of the Stackelberg framework, the follower's response is the set of powers that is the outcome of a *power control game* the jammers play, in the form of a *Nash equilibrium,* as detailed in Section V-B.

A. Communications Model

Under the setting described above, the source's secrecy rate (6) now becomes:

$$R_{\mathrm{S}}(\alpha,\beta,\mathcal{J};P_{\mathrm{J}_{i\in\mathcal{J}}}) = \alpha\left[\log_2\left(1+\frac{h_{\mathrm{SD}}\frac{P_{\mathrm{S}}}{\alpha}}{\sigma^2+\sum_{i\in\mathcal{J}}\frac{h_{\mathrm{J}_i\mathrm{D}}\beta P_{\mathrm{J}_i}}{\alpha\beta+1-\alpha}}\right)- \log_2\left(1+\frac{h_{\mathrm{SE}}\frac{P_{\mathrm{S}}}{\alpha}}{\sigma^2+\sum_{i\in\mathcal{J}}\frac{h_{\mathrm{J}_i\mathrm{E}}\beta P_{\mathrm{J}_i}}{\alpha\beta+1-\alpha}}\right)\right]^+. \qquad (21)$$

The utility of the chosen jammers $\mathrm{J}_{i\in\mathcal{J}}$, similar to (7), is given by

$$U_{\mathrm{J}_{i\in\mathcal{J}}}(\alpha,\beta,\mathcal{J};P_{\mathrm{J}_i}) = (1-\alpha)\cdot \log\left(1+\frac{h_{\mathrm{J}_{ii}}P_{\mathrm{J}_i}}{\sigma^2(\alpha\beta+1-\alpha)+\sum_{l\in\mathcal{J},l\neq i}h_{\mathrm{J}_{li}}P_{\mathrm{J}_l}}\right)-c_iP_{\mathrm{J}_i}, \qquad (22)$$

with $P_{\mathrm{J}_i} \leq \bar{P}_{\mathrm{J}_i}$.

B. The Power Control Game

According to the Stackelberg framework in Section III-A, the rational and selfish jammers J_i are aware of the parameters α, β and $\mathcal{J}$ set by the source. Competition between chosen jammers is formulated as a non-cooperative power control game [16] [23] [24] in the interference channel during the jammers' data transmission phase of duration $1-\alpha$, with their utilities and power/strategy spaces provided in Section V-A. Each jammer J_i chooses its strategy P_{J_i} in order to maximize its utility (22), aware that this decision will affect the other jammers' strategies. The outcome of the game $P^*_{\mathrm{J}_{i\in\mathcal{J}}}(\alpha,\beta;\mathcal{J})$ can be described by the game-theoretic concept Nash equilibrium (NE), defined as the state whereby any unilateral deviation in player's strategy would not produce any gain [21]. Herein, NE can be conveniently obtained as a fixed point of the best responses [21] of the participating jammers. In particular, the best response of each jammer can be found by setting the derivative of (22) with respect to P_{J_i} to zero:

$$\left.\frac{\partial U_{\mathrm{J}_i}(\alpha,\beta,\mathcal{J};P_{\mathrm{J}_i})}{\partial P_{\mathrm{J}_i}}\right|_{P_{\mathrm{J}_{j\in\mathcal{J},j\neq i}}=P^*_{\mathrm{J}_{j\in\mathcal{J},j\neq i}}} = 0,\ \forall i\in\mathcal{J}, \qquad (23)$$

and the NE is given by the following set of $|\mathcal{J}|$ equations:

$$P^*_{\mathrm{J}_{i\in\mathcal{J}}}(\alpha,\beta;\mathcal{J}) = \left[\frac{1-\alpha}{c_i\ln 2}-\frac{\sigma^2}{h_{\mathrm{J}_{ii}}}(\alpha\beta+1-\alpha)- \sum_{j\in\mathcal{J},j\neq i}\frac{h_{\mathrm{J}_{ji}}}{h_{\mathrm{J}_{ii}}}P^*_{\mathrm{J}_l}(\alpha,\beta;\mathcal{J})\right]_0^{\bar{P}_{\mathrm{J}_i}}. \qquad (24)$$

[1] As noted in Section III-A, the impact of malicious nodes' behavior is out of the scope of this paper. For the protection mechanisms against auction vulnerabilities such as the 'lying auctioneer' or 'bidder collusion', we refer interested readers to [29].

Clearly, the game has a unique NE if the set of equations (24) has a unique solution. This power control game has been considered in [16] and for the more general framework of wideband systems in [23] [24], where it was shown that the NE always exists and that it is unique in the case of weak interference, i.e., if the interference matrix $\mathbf{H}$, defined as $[\mathbf{H}]_{ji} = h_{\mathrm{J}_{ji}}$, is strictly diagonally dominant, i.e., $\sum_{j\in\mathcal{J},j\neq i} h_{\mathrm{J}_{ji}}/h_{\mathrm{J}_{ii}} < 1$. This condition for uniqueness of the NE is intuitive since it simply imposes an upper bound on the interference: in fact, with negligible interference, equations (24) become decoupled and the solution clearly exists and is unique. In the remainder of this work, we assume that this condition is satisfied. It is further noted that the NE can be achieved instantly, i.e., the jammers will adopt the powers in (24), under the assumption of *rationalizability*[2] [21], or using algorithms as in, e.g., [33].

To conclude, the Stackelberg equilibrium is given as

$$(\alpha^*,\beta^*,\mathcal{J}^*) = \arg\max_{(\alpha,\beta,\mathcal{J})} R_{\mathrm{S}}\left(\alpha,\beta,\mathcal{J};P^*_{\mathrm{J}_{i\in\mathcal{J}}}(\alpha,\beta,\mathcal{J})\right) \tag{25}$$

$$\text{s.t. } 0<\alpha\leq 1, 0<\beta<\infty,\ \mathcal{J}\subseteq\{1,..,N\},$$

where $P^*_{\mathrm{J}_{i\in\mathcal{J}}}(\alpha,\beta,\mathcal{J})$ are the $|\mathcal{J}|$ power responses given by (24). Notice that the source needs to be aware of all the instantaneous channel power gains in the system in order to compute the equilibrium (25), i.e., to choose the set of jammers $\mathcal{J}^*$ and parameters α^* and β^*. On the other hand, the cooperative jammers are required to know $h_{\mathrm{J}_{ij}}$, $i,j\in\mathcal{J}$ (recall (24)). Finally, it should be clear that for $N=1$ the power control scheme boils down to the reference Stackelberg scheme described in Section III-A[3].

VI. Discussion on Previous Work

In Section I, we mentioned that another game-theoretic scheme incorporating a wiretap channel with non-altruistic jammer was recently introduced in [18]. Here we provide a brief discussion on comparative relationships between the scheme presented therein and our scheme.

The scheme proposed in [18] allows for a simultaneous transmissions of useful data by the legitimate source and the jammer. Therein, the source allows the jammer to transmit its data if this would in return improve the secrecy rate of the legitimate pair. Notice that the jammer does not transmit any noise, but it is its data transmission that is intended to harm the eavesdropper's decoding of the source's signal. The communication model for this scheme is the same as in Figure 1, except that there is no noise transmission and the simultaneous data transmission from two transmitter spans the whole bandwidth.

To enumerate the differences, we first note that our scheme does not require codebook sharing between any communicating pairs. Thus, we avoid a somewhat dubious assumption that the legitimate pair, concerned with secrecy, would share its codebook with the jamming pairs. Codebook sharing is necessary for [18] to operate. Secondly, unlike our paper, [18] is limited to a single jammer. An attempt to accommodate multiple jammers is made in [18] by simply choosing the jammer that mostly improves the secrecy rate. Such an approach is also considered in this paper, Section III-B, only for comparison with the more sophisticated proposed schemes where *competition* between jamming nodes is considered, Section IV and Section V.

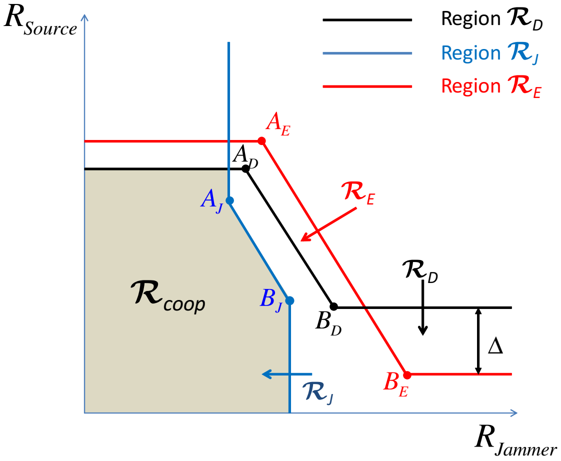


Fig. 6. An illustration of achievable rate regions in a scenario where the presented model outperforms [18].

Next, in order to compare the two schemes in detail, we assume a single jammer. In this case, the scheme in [18] and ours can outperform one another depending on the channel conditions. To illustrate this, we provide an example of rate regions, in the same way as in [18], in Figure 6. Region $\mathcal{R}_D$ denotes the rates R_{Source} achievable at legitimate destination, depending on the rate R_{Jammer}, with no regards to secrecy; region $\mathcal{R}_J$ denotes the rates R_{Jammer} achievable at the jammer's destination, depending on the rate R_{Source}; and region $\mathcal{R}_E$ denotes the rates R_{Source} achievable at the eavesdropper, depending on the rate R_{Jammer}. The achievable rate region for the interference channel including the source, the jammer and their destinations, $\mathcal{R}_{coop}$, with no concern to secrecy, is the intersection of the regions $\mathcal{R}_D$ and $\mathcal{R}_J$, as defined in [18], and for the case in Figure 6 it is the shaded area. Points that define the rate regions are $A_D\left(\gamma\left(h_{JD}P_J/\left(1+h_{SD}P_S\right)\right),\gamma\left(h_{SD}P_S\right)\right)$ and $B_D\left(\gamma\left(h_{JD}P_J\right),\gamma\left(h_{SD}P_S/\left(1+h_{JD}P_J\right)\right)\right)$ for region $\mathcal{R}_D$; $A_J\left(\gamma\left(h_JP_J/\left(1+h_{SJ}P_S\right)\right),\ \gamma\left(h_{SJ}P_S\right)\right)$ and $B_J\left(\gamma\left(h_JP_J\right),\gamma\left(h_{SJ}P_S/\left(1+h_JP_J\right)\right)\right)$ for region $\mathcal{R}_J$; and $A_E\left(\gamma\left(h_{JE}P_J/\ \left(1+h_{SE}P_S\right)\right),\gamma\left(h_{SE}P_S\right)\right)$ and $B_E\left(\gamma\left(h_{JE}P_J\right),\gamma\left(h_{SE}P_S/\ \left(1+h_{JE}P_J\right)\right)\right)$ for region $\mathcal{R}_E$, with $\gamma(x)=\log_2(1+x)$.

Since any point of the region $\mathcal{R}_{coop}$ is inside the region $\mathcal{R}_E$ in Figure 6, the secrecy rate is zero [18], [14]. Following [18], since the jammer can not improve the secrecy rate, it is not allowed to transmit and its rate is zero. It would be required for the transmitters in [18] to change their powers in order to search for some non-zero rate pair. In contrast, for the same scenario in Figure 6, our approach achieves

[2] In game theory, a player is rational if it chooses only the strategies that are the best responses to other players' strategies. Rationalizability prescribes that a player is rational and believes that other players are also rational. If the Nash equilibrium is unique, this concept guarantees that all the players will adopt their Nash equilibrium strategies [21].

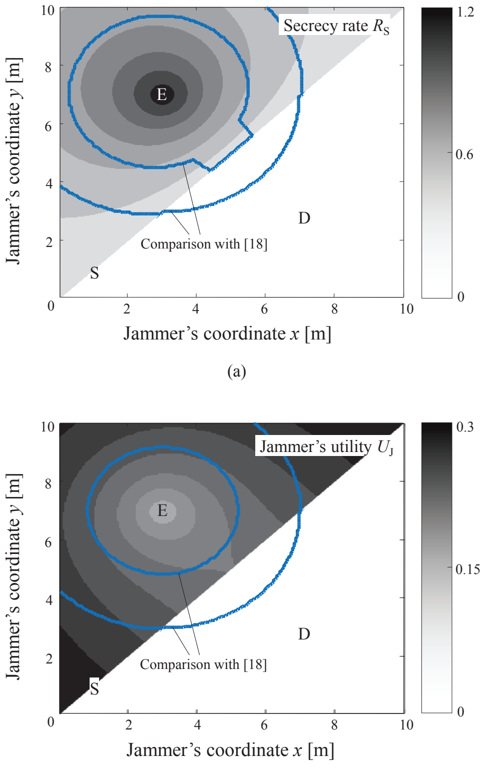
[3] Protection mechanisms against malicious nodes in power control games typically require repeated games framework and can be found in, e.g., [24] [34].

positive rate gains, for both transmitters. Notice on the right of the figure the difference between the achievable rates of source's transmission at the destination and the eavesdropper, $\Delta = \log_2\left(1 + h_{\mathrm{SD}}P_{\mathrm{S}}/\left(1 + h_{\mathrm{JD}}P_J\right)\right) - \log_2(1 + h_{\mathrm{SE}}P_{\mathrm{S}}/(1 + h_{\mathrm{JE}}P_J))$. This difference is a secrecy rate whose fraction (recall (6)) can be achieved *only if the jammer transmits noise (or, equivalently, if the jammer transmits with a large rate, not decodable by neither D or E)*, as in our approach. This conclusion can also be found in Theorem 3 in [14], which is the foundation of the methodology in reference [18].

In general, the smaller values of h_{J} and h_{JD} compared to h_{JE} favor our scheme compared to [18], as in the latter the eavesdropper can decode the jammer's transmission, subtract it from its received signal and decode the source's transmission, producing a small or zero secrecy rate. The opposite scenarios favor the mechanism in [18]. Thus, the two schemes can be used in complementary channel conditions.

VII. Numerical Results

In this section, we provide some insights into the proposed mechanisms via numerical results. All results correspond to the Stackelberg equilibria of the three introduced schemes. The S-D pair secrecy rate R_{S} and the jammer's utility U_{J} are illustrated in Figure 7-(a) and Figure 7-(b), respectively, for the reference Stackelberg model described in Section III, as a function of the jammer's location (x, y). The scheme comparison with [18] is also shown, and explained later in this paragraph. Positions of the nodes S, D and E are indicated in the figure. A simple path-loss model with the propagation factor $\gamma = 2$ is used, with $P_{\mathrm{S}} = \bar{P}_{\mathrm{J}} = 10$ [mWatt], $\sigma^2 = 1$ [mWatt] and $c = 0.25$ [bit/sec/Hz/mWatt]. The channels towards the jammer's intended destination $\mathrm{D_J}$ are as if $\mathrm{D_J}$ is placed $d = 3$ [meter] from the jammer J and $d = d_{SD}$ from the source. Notice that on Figure 7 the dark color indicates higher rates, while the white color indicates zero rates. Since the nodes D and E are equally distanced from the source S, the secrecy rate R_{S} without jamming is zero. Secrecy rate is largest when the jammer is in the eavesdropper's E vicinity, and zero when the jammer is closer to the destination than to the eavesdropper. The latter also holds for the jammer's utility U_{J}. Interestingly, when the jammer is close to the eavesdropper, its utility is very small, as the source needs a relatively small jamming power and can thus preserve the majority of the bandwidth for itself. For the comparison with [18], the area inside thick blue curves encircling the eavesdropper denote the jammer's placement where our scheme performs better, except for the area intersecting with the lower triangle, where both schemes produce a zero secrecy and jammer's rate. Outside of the regions encircled by these curves, [18] produces better results. The smaller and the larger 'radius' correspond to the J-$\mathrm{D_J}$ distance of $d = 3$ [meter] and $d = 5$ [meter], respectively. These results support the discussion in Section VI. In general, the smaller values of h_{J} and h_{JD} compared to h_{JE} favor our scheme compared to [18]. The opposite scenarios favor the mechanism in [18].

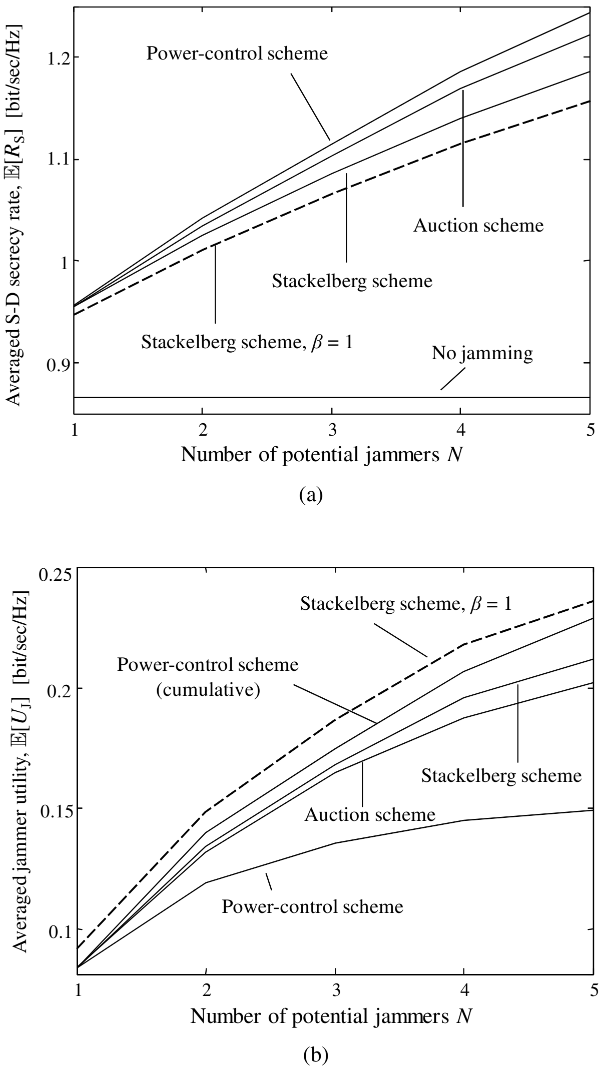


(a)

(b)

Fig. 7. Secrecy rate R_{S} and cooperative jammer's utility U_{J} as functions of the jammer's location, for the reference Stackelberg scheme ($N = 1$). Comparison with [18] is also shown - when the jammer is in the area inside the thick blue lines, the proposed scheme outperforms [18].

The source's secrecy rate and the utility of a chosen cooperative jammer in Stackelberg equilibria, averaged over channel realizations under assumption of independent block-fading, $\mathbb{E}[R_{\mathrm{S}}]$ and $\mathbb{E}[U_{\mathrm{J}}]$, respectively, are shown in Figure 8 as functions of the number of potential jamming nodes N, for the three proposed schemes. Parameters P_{S}, $\bar{P}_{\mathrm{J}}$, σ^2 are chosen as above, with $c_i = c = 0.25$ [bit/sec/Hz/mWatt] same for all jammers J_i, $\mathbb{E}\left[h_{\mathrm{SD}}\right] = \mathbb{E}\left[h_{\mathrm{SE}}\right] = \mathbb{E}\left[h_{\mathrm{J}_i\mathrm{E}}\right] = \mathbb{E}\left[h_{\mathrm{J}_i\mathrm{D}}\right] = \mathbb{E}\left[h_{\mathrm{J}_{ii}}\right] = 0$ dB and $\mathbb{E}\left[h_{\mathrm{J}_{il}}\right] = -10$ dB, $i, l = 1, .., N$, $i \neq l$. These parameters are used in the remainder of this section. Note that the small values for jammers' interference channel gains favor the uniqueness of Nash equilibrium for the power control game, as discussed in Section V. The dashed line represents the performance when the power ratio parameter β is fixed $\beta = 1$, i.e., when the legitimate source cannot use it as an optimization parameter, similarly to [36]. Both the secrecy rate and a chosen jammer's utility benefit with the proposed mechanisms. The secrecy rate increases with N, with the power control scheme, described in Section V, outperforming the auction scheme, in Section IV, due to multiple simultaneous jamming transmissions, while the auction outperforms the multi-jammer Stackelberg scheme, in Section III, due to competitiveness. The opposite relations between the three schemes hold for U_{J}, although the cumulative utility of the chosen jammers for the power control scheme $\sum_{i \in \mathcal{J}} U_{\mathrm{J}_i}$ is the largest as multiple jamming nodes are allowed to transmit data. Moreover, for a small N, the probability of having a contributing jammer is small, as will be clarified in the following, frequently yielding zero jammer's utility and thus



(a)

(b)

Fig. 8. Average secrecy rate $\mathbb{E}[R_\mathrm{S}]$ and winning cooperative jammer's utility $\mathbb{E}[U_\mathrm{J}]$ versus the number of potential cooperative jammers.

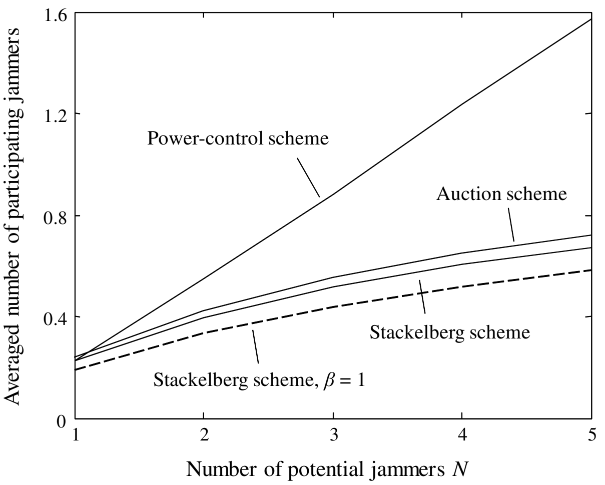


Fig. 9. Averaged number of participating jammers versus the number of potential jammers.

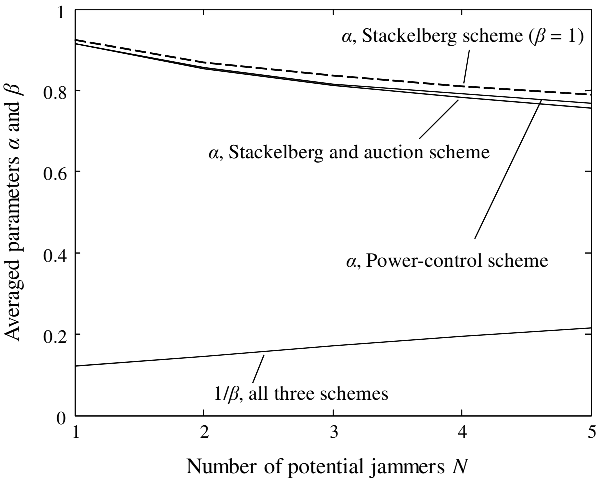


Fig. 10. Average parameters $\mathbb{E}[\alpha]$ and $\mathbb{E}[1/\beta]$ versus the number of potential cooperative jammers.

relatively small average utilities for any of the schemes. It is also noted but not shown here, that as the number of potential jammers N increases, resulting in often more than one jammers that can satisfy the participating conditions (8)-(10), average utility of a chosen jammer for any scheme will start to decrease as the legitimate parties can be more aggressive when deciding on parameters α and β.

Using the parameters defined above, Figure 9 illustrates the average number of chosen jammers for the three schemes. For the Stackelberg and the auctioning scheme, the curves can be interpreted as the probability of having at least one jammer that can satisfy the participating conditions (8)-(10). Notice that the number of chosen jammers for the Stackelberg and auction scheme cannot exceed one, while this is not the case for the power control scheme. We add that for the power control scheme, the number of chosen jammers tends to saturate with a larger number of potential jammers (not shown here). One can appreciate the degree of freedom available to the legitimate parties through parameter β, by observing the dashed curve that shows the average number of contributing jammers for a fixed parameter $\beta = 1$.

Finally, Figure 10 shows the averaged parameters α and β in Stackelberg equilibrium versus the number of potential jammers N, using the same model parameters as above. Again, the dashed line illustrates the performance when $\beta = 1$. For the parameter β, the value $1/\beta$ is more appropriate in order to avoid infinite values for β corresponding to the channel realizations when no jammer is chosen. Both the parameters α and β decrease as number of jammers N increase and there is no significant difference for the parameter β between the three schemes. It should be noted that if only the scenarios resulting in a chosen jammer are considered, these two parameters would increase, as the legitimate pair would benefit from the competition between nodes by playing more aggressively. This is in line with discussion in Section III-A related to (13). Furthermore, notice that the level of legitimate pair aggressiveness, in terms of α, is larger for the power control scheme than for the auction scheme, for which it is in turn larger than for the reference Stackelberg game (this is not visible in the figure due to small differences), as the legitimate pair can exploit competitive nature of jammers.

VIII. Concluding Remarks

In this paper, we have proposed a game-theoretic mechanism for recruiting non-altruistic users as cooperative jammers to enhance secret communications. This mechanism is built upon the spectrum leasing paradigm, wherein a legitimate source-destination pair communicating confidential messages that need to be kept secret from an eavesdropping node, is willing to compensate external potential cooperative jammer(s) with a fraction of its bandwidth. Interaction between the non-cooperative nodes is based on the Stackelberg concept and, for a multi-jammer scenario, also employs auctioning and power control game. Numerical results corroborate the benefits for all involved nodes, despite their selfish nature. It is further shown that the power control outperforms the auction scheme in terms of secrecy rates, while the opposite holds in terms of jammers' individual utilities. The auction scheme is less demanding in terms of the information required at nodes on system parameters.

We remark that game-theoretic mechanisms, such as Vickrey auction, require protection from malicious behavior. For example, the destination may want to measure the received signal-to-noise ratio to ensure that the level of transmitted noise corresponds to the auction outcome. On the other hand, the truthful bidding nature of Vickrey auction assures that there is no cheating while bidding, except if coalitions are formed, as discussed in Section IV.

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Sep. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, 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. 2007 Inf. Theory Appl. Workshop*.

[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. 2006 Allerton Conf. Commun. Control Comput*.

[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. 2006 IEEE Int. Symp. Inf. Theory, ISIT*.

[10] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete memoryless interference and broadcast channels with condifential messages," in *Proc.2006 Allerton Conf. Commun. Control Comput*.

[11] 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.

[12] X. He and A, Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wireless Commun. Netw*., vol. 2009, article ID 305146, 13 pages, 2009. doi:10.1155/2009/305146.

[13] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

[14] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[15] X. He and A. Yener, "Providing secrecy with structured codes: tools and applications to two-user Gaussian channels," *IEEE Trans. Inf. Theory*, 2009, submitted for publication. Available: http://arxiv.org/abs/0907.5388.

[16] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini, and R. Pickholtz, "Spectrum leasing to cooperating secondary ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 203–213, Jan. 2008.

[17] 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.

[18] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security,* vol. 6, no 3, pp. 831–842, Sept. 2011.

[19] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper and friendly jammer," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, June 2009.

[20] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Improved wireless secrecy capacity using distributed auction theory," in *Proc. 2009 International Conf. Mobile Ad-hoc Sensor Netw.*

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

[22] P. Klemperer, "Auction theory: a guide to the literature," *J. Economics Surv.*, vol. 13, no. 3, pp. 227–286, July 1999.

[23] G. Scutari, D. P. Palomar, and S. Barbarossa, "Optimal linear precoding/multiplexing for wideband optimal linear precoding strategies for wideband noncooperative systems based on game theory–part I: Nash equilibria," *IEEE Trans. Signal Process.*, vol. 56, no. 3, pp. 1230–1249, Mar. 2008.

[24] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 517–528, Apr. 2007.

[25] W. Vickrey, "Counterspeculations, auctions, and competitive sealed tenders," *J. Finance*, vol. 16, pp. 8–37, 1961.

[26] J. O. Neel, "Analysis and design of cognitive radio networks and distributed radio resource management algorithms," Ph.D. dissertation, Virginia Polytechnic Institute, Sep. 2006.

[27] R. M. Corless, G. H. Gonnet, D. E. Hare, D. Jeffrey, and D. E. Knuth, "On the Lambert W function," *Adv. Computational Math.*, vol. 5, 1996.

[28] J. Sun, E. Modiano, and L. Zheng, "Wireless channel allocation using an auction algorithm," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 5, pp. 1085–1096, May 2006.

[29] T. Sandholm, "Issues in computational Vickrey auctions," *Int. J. Electron. Commerce*, vol. 4, no. 3, pp. 107–129, Mar. 2000.

[30] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, Jan. 1981.

[31] X. Shang, G. Kramer, and B. Chen, "A new outer bound and the noisy-interference sum-rate capacity for Gaussian interference channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 689–699, Feb. 2009.

[32] V. S. Annapureddy and V. V. Veeravalli, "Gaussian interference networks: sum capacity in the low interference regime and new outer bounds on the capacity region," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3032–3050, July 2009.

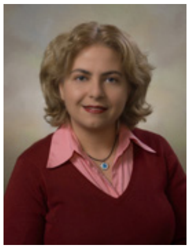
[33] G. Scutari, D. P. Palomar and S. Barbarossa, "Optimal linear precoding/multiplexing for wideband optimal linear precoding strategies for wideband noncooperative systems based on game theory—part II: algorithms," *IEEE Trans. Signal Process.*, vol. 56, no. 3, pp. 1250–1267, Mar. 2008.

[34] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Repeated open spectrum sharing game with cheat-proof strategies," *IEEE Trans. Wireless Commun*., vol. 8, no. 4, Apr. 2009.

[35] I. Stanojev and A. Yener, "Recruiting multi-antenna transmitters as cooperative jammers: an auction-theoretic approach," *2011 Allerton Conf. Commun., Control, Comput.*

[36] I. Stanojev and A. Yener, "Cooperative jamming via spectrum leasing," in *Proc. 2011 IEEE Int. Symp Modeling Optimization Mobile, Ad Hoc, Wireless Networks*.

Igor Stanojev (S'03-M'10) received the Dipl.Ing. degree in Electrical Engineering from the University of Belgrade, Belgrade, Serbia, in 2001, the M.S. degree in Electrical Engineering from the New Jersey Institute of Technology (NJIT), Newark, NJ, USA, in 2006, the Ph.D. degree in Information Engineering from Politecnico di Milano, Milan, Italy, and the Ph.D. degree in Electrical Engineering from NJIT, Newark, NJ, USA. From 2010 to 2012 he was a Postdoctoral Research Associate at Wireless Communications and Networking Laboratory (WCAN) at The Pennsylvania State University, State College, PA, USA. Since 2012, he is a faculty member in the Department of General Engineering at the University of Wisconsin-Platteville, serving as an Assistant Professor. Dr. Stanojev's research contributions are in the cross-layer design of wireless networks, including cooperative communications, hybrid ARQ protocols, cognitive radio and game-theoretic applications to communication networks, as well as the physical layer secrecy.



Aylin Yener (S'91-M'00) received two B.Sc. degrees, with honors, in Electrical and Electronics engineering, and in Physics, from Bo?aziçi University, Istanbul, Turkey, in 1991, and the M.S. and Ph.D. degrees in Electrical and Computer Engineering from Rutgers University, NJ, in 1994 and 2000, respectively. During her Ph.D. studies, she was with Wireless Information Network Laboratory (WINLAB). From September 2000 to December 2001, she was with the Electrical Engineering and Computer Science Department, Lehigh University, PA, where she was a P.C. Rossin Assistant Professor. In January 2002, she joined the faculty of The Pennsylvania State University, University Park, where she was an Assistant Professor, then Associate Professor, and is currently Professor of Electrical Engineering since 2010. During the academic year 2008-2009, she was a Visiting Associate Professor with the Department of Electrical Engineering, Stanford University, Stanford CA. Her research interests are in communication theory, information theory and network science, with emphasis on information theoretic security and green communications.

Dr. Yener received the NSF CAREER award in 2003. She has served as Technical Program chair/co-chair on a number of IEEE Symposia including in ICC, PIMRC and VTC, and as an editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and for the IEEE TRANSACTIONS ON COMMUNICATIONS. Her service to the IEEE Information Theory Society includes chairing the Student Committee between 2007-2011, where she co-founded the Annual School of Information Theory in North America in 2008. She currently serves on the Board of Governors of the IEEE Information Theory Society as its treasurer.