

Improved Wireless Secrecy Capacity using Distributed Auction Theory

Zhu Han¹, Ninoslav Marina², Mérouane Debbah³, and Are Hjørungnes²

¹ Electrical and Computer Engineering Department, University of Houston, Houston, USA.

²UNIK - University Graduate Center, University of Oslo, Norway.

³ Alcatel-Lucent Chair on Flexible Radio, SUPÉLEC, Gif-sur-Yvette, France.

Abstract— Physical layer security is an emerging security area that explores possibilities of achieving perfect secrecy data transmission between the intended network nodes, while possible malicious nodes that eavesdrop the communication obtain zero information. The so-called secrecy capacity can be improved using friendly jammers that introduce extra interference to the eavesdroppers. Here, we investigate the interaction between the multiple source-destination links and a friendly jammer who assists by “masking” the eavesdropper. In order to obtain a distributed solution, one possibility is to introduce a distributed auction theoretic approach. The auction is defined such that the source-destination links provide bids for the jammer to interfere the eavesdropper, therefore increasing their secrecy capacities. We propose a distributed auction using the share auction and iteratively updating the bids. To compare with the performances, we construct a centralized solution and a VCG auction, which cannot be implemented in practice. Our analysis and simulation results show the effectiveness of friendly jamming and convergence of the proposed scheme. The distributed game solution is shown to have similar performances to those of the centralized ones.

I. INTRODUCTION

The design of the future wireless networks will have to put a huge effort on the security. The main reason for that is that future networks will be decentralized and ad-hoc in nature, and, hence, allowing various types of network mobile terminals to join and leave. This makes the entire network vulnerable and very sensitive to attacks. Because of the broadcast nature of the wireless transmission, anyone within communication range can intercept the data that was not intended to her. In such a complex environment, the current cryptographic methods with high level security, may not work. This may happen due to difficulty to ex-

This work was supported by US NSF CNS-0910461, and was supported by the Research Council of Norway through the projects entitled “Mobile-to-Mobile Communication Systems (M2M)”, “Optimized Heterogeneous Multiuser MIMO Networks (OptiMO)”, and “Communications under Uncertain Topologies (AURORA)”.

change public keys in such an ad hoc network. To that end it is of big importance to study the possibility of designing a decentralized network with perfect security on physical layer. For that reason, recently, the physical layer security is regaining a new attention. The main goal of this paper is to design a decentralized system that will protect the broadcasted data and make it impossible for the eavesdropper to receive the packets even if it knows the standard encoding and decoding schemes used by the transmitter and receiver, respectively. In systems where physical layer security is studied, the main objective is to maximize the rate of reliable information from the source to the intended destination, while all malicious nodes are kept as ignorant of that information as possible. This maximum reliable rate is known as *secrecy capacity*.

The secrecy capacity work was pioneered by Aaron Wyner, who defined the wiretap channel and established fundamental results that enable creating almost perfect secure communications with no need of private (secret) keys [1] exchange. Wyner showed that when the eavesdropper channel is a degraded (weaker) version of the main channel, the source and the destination can exchange perfectly secure messages at positive rate. With his scheme, a maximal equivocation (i.e., uncertainty) is induced at the eavesdropper, i.e., a maximal level of secrecy is obtained. By ensuring that the equivocation rate is arbitrarily close to the message rate, one can achieve perfect secrecy in the sense that the eavesdropper is now limited to learn *almost nothing* about the source-destination messages from its observations. Follow-up work by Leung-Yan-Cheong and Hellman characterized the secrecy capacity of the additive white Gaussian noise (AWGN) wiretap channel [2]. In their seminal paper, Csiszár and Körner generalized Wyner’s approach by considering the transmission of confidential messages over broadcast channels [3]. Recently, the research in the area of physical layer security exploded. There have been

considerable efforts on generalizing these studies to the wireless channel and multi-user scenarios (see [2, 4–11] and references therein). Jamming [12–14] has been studied for a long time to analyze the hostile behaviors of malicious nodes. Recently, jamming has been employed to physical layer security to reduce the eavesdropper’s ability to decode the source’s information [15]. In other words, the jamming is friendly in this context.

Game theory [16] is a formal framework with a set of mathematical tools to study some complex interactions among interdependent rational players. During the past decade, there has been a surge in research activities that employ game theory to model and analyze modern distributed communication systems. Most of these works [17–20] concentrate on the distributed resource allocation for wireless networks. As far as the authors’ knowledge, the game theory has not yet been used in the physical layer security. In [21], Stackelburg game is employed for multiple jammer one source-destination case. In this paper, we employ auction theory [22] which is an important branch of game theory for one jammer multiple source-destination scenario.

In this paper, we investigate the interaction between the source-destination pairs and its friendly jammer using auction theory. Although the friendly jammer helps the sources by reducing the data rate that is “leaking” from the sources to the malicious node, at the same time it also reduces the useful data rate from the sources to the destinations. Using well chosen amounts of power from the friendly jammer, the secrecy capacity can be maximized. In the auction that we define here, the source-destination pairs provide bids for the jammer to interfere the malicious eavesdropper, and therefore, to increase the secrecy capacity. In modeling the outcome of the above auction, our analysis uses the distributed share auction. Initially, the existence of equilibrium will be studied. The outcome of the distributed algorithm will be compared to the centralized genie aided solution and (Vickrey-Clarke-Grove) VCG auction [22]. From the simulation results, we can see the efficiency of friendly jamming and the convergence of the bids. Moreover, the centralized scheme and the proposed game scheme has similar performances.

The rest of the paper is organized as follows: In Section II, the system model of physical layer security with friendly jamming is described. In Section III, the distributed auction theory model is formulated, and the outcomes as well as properties of the auction are analyzed. In Section IV, two performance bounds are

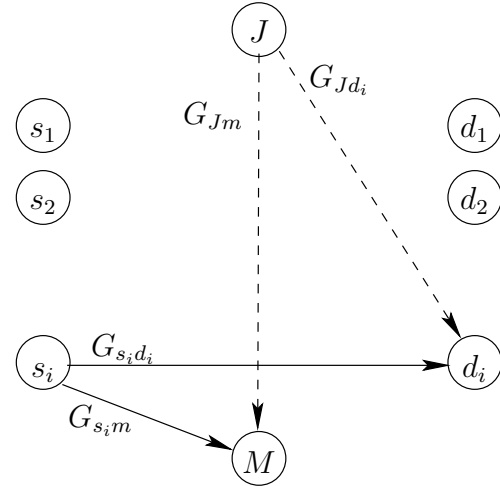


Fig. 1. System Model

developed to compare with the proposed scheme. Simulation results are shown in Section V and conclusions are drawn in Section VI.

II. SYSTEM MODEL

We consider a network with multiple sources s_i , destinations d_i , a malicious eavesdropper node m , and a friendly jammer node J as shown in Figure 1. The malicious node tries to eavesdrop the transmitted data coming from the source nodes. When the eavesdropper channel from the source to the malicious node is a degraded version of the main source-destination channel, the source and destination can exchange perfectly secure messages at a non-zero rate. By transmitting a message at a rate higher than the rate of the malicious node, the malicious node can learn almost nothing about the messages from its observations. The maximum rate of secrecy information from the source to its intended destination is defined by the term secrecy capacity.

Suppose the source s_i transmits with power P_i . The channel gains from the source to the destination and from the source to the malicious node are $G_{s_i d_i}$ and $G_{s_i m}$, respectively. The friendly jammer J , transmits with power P_i^J and the channel gains from J to the destination and the malicious node, are G_{Jd_i} and G_{Jm} , respectively. If the path loss model is used, the channel gain is given by the distance to the negative power of the path loss coefficient. The thermal noise for each channel is σ^2 and the bandwidth is W . The channel

capacity for the source i to the destination i is

$$C_1^i = W \log_2 \left(1 + \frac{P_i G_{s_i d_i}}{\sigma^2 + P_i^J G_{J d_i}} \right). \quad (1)$$

The channel capacity from the source to the malicious node is

$$C_2^i = W \log_2 \left(1 + \frac{P_i G_{s_i m}}{\sigma^2 + P_i^J G_{J m}} \right). \quad (2)$$

Note that here we assume that there is no interference from the other sources, since only one source at a time transmits its own data.

The secrecy capacity is

$$C_{s_i} = \max(C_1^i - C_2^i, 0). \quad (3)$$

We observe that with the increase of the jamming power P_i^J , both C_1 and C_2 are reduced. The questions are whether or not C_{s_i} can be increased, and how to control the jamming power in a distributed manner. We will try to solve the problems in the following section using an auction theoretical approach.

III. PROPOSED AUCTION THEORETIC APPROACH

Here we propose an auction theory approach, in which the source s_i is the bidder, while the jammer J is the auctioneer. The bidder will submit a bid to compete for the P_i^J in order to increase their own utility which is represented by the secrecy capacity. The jammer J has maximal power P_{\max} and distributes P_i^J following the rule of an auction. An auction is a decentralized market mechanism for allocating resources. The essence of an auction is a game, where the players are the bidders, the strategies are the bids, and both allocations and payments are functions of the bids. The type of auction depends the outcome of the system. One well known auction is the Vickrey-Clarke-Grove (VCG) auction, which requires gathering global information from the network and performing centralized computations. To overcome the limitation of VCG auction, we proposed SNR auction which is based on Share-Auction [22–25] as follows:

- Information: Besides the public and local information (i.e., W , P , σ^2 , P_{s_i} , $G_{s_i d_i}$). The jammer J announces a positive reserve bid β . And a price $\pi \geq 0$ to all users before the auction starts.
- Bids: User i submits a scalar $b_i \geq 0$ to the jammer J .
- Allocation: The jammer allocates transmit power according to

$$P_i^J = \frac{b_i P_{\max}}{\beta + \sum_{j \in i} b_j}. \quad (4)$$

- Payment: In the proposed auction, source s_i pays the jammer

$$c_i = \pi P_i^J. \quad (5)$$

A bidder profile is defined as the vector containing the users' bids, $b = (b_1, \dots, b_I)$. We define the others' bid vector as b_{-i} , so that $b = (b_i; b_{-i})$. Source s_i chooses b_i to maximize its payoff

$$U_i(b_i; b_{-i}, \pi) = \Delta C_{s_i}(P_i(b_i; b_{-i})) - c_i(b_i; b_{-i}, \pi), \quad (6)$$

where ΔC_{s_i} is the secrecy capacity change.

The desirable outcome of an auction is called a Nash Equilibrium (NE), which is a bidding profile b^* such that no user wants to deviate unilaterally, i.e.,

$$U_i(b_i^*; b_{-i}^*, \pi) \geq U_i(b_i; b_{-i}^*, \pi), \forall b_i. \quad (7)$$

Define source s_i 's best response as

$$b_i(b_{-i}, \pi) = \{b_i | b_i = \arg \max_{b_i \geq 0} U_i(b_i; b_{-i}, \pi)\}. \quad (8)$$

Here, we omit the dependence on β . If the reserve bid $\beta = 0$, then the bids in (8) only depends on the ratio of the bids. In other words, a bidding profile $k\mathbf{b}$ for any $k > 0$ leads to the same resource allocation, which is not desirable in practice. That is why we need a positive reserve bid. However, the value of β is not important as long as it is positive. For example, if we increase β to $k\beta$, where $k > 0$, then the sources can just scale \mathbf{b} to $k\mathbf{b}$, which results in the same resource allocation. For simplicity, we can simply choose $\beta = 1$ in practice.

If the others' bids b_{-i} are fixed, source i can increase the jammer's power to increase its U_i by increasing b_i . However, the payoff function needs to pay the price for P_i^J . Depending one different price per unit π announced by the relay, there are three different scenarios:

1. If π is too small, the payoff function U_i is still an increasing function. As a result, the source tries to maximize its own benefit by setting price high. Consequently, $b_i \rightarrow \infty$.
2. If π is too large, the payoff function U_i is a decreasing function. As a result, the source would not participate in the bidding by setting $b_i = 0$.
3. If π is set to the right value, the payoff function U_i is a quasi-concave shape function, i.e., it increases first and then decreases within the feasible region. Consequently, there is an optimal b_i for the source to optimize its performance.

IV. PERFORMANCE BOUNDS

In this section, we propose two performance bounds. First, we formulate the problem as a constrained optimization and solve it using a centralized solution. The challenge of collecting all information prohibits this solution from practice. Second, we investigate VCG auction which generates the social optimum. However, the computation complexity is very high. Those two bounds have similar performances. In Section V, we compare the proposed scheme with those two performance bounds.

A. Centralized Problem Formulation

Traditionally, the centralized scheme is employed assuming all channel information is known. Unfortunately, it is extremely difficult to achieve. The objective to optimize the secrecy capacity under the constraints of maximal jamming power.

$$\begin{aligned} \max_{P_i^J} \sum_{i=1}^N C_{s_i}, \quad (9) \\ \text{s.t.} \quad \sum_{i=1}^N P_i^J \leq P_{\max}. \end{aligned}$$

The centralized solution is found by maximizing the secrecy capacity only.

B. VCG Auction

In this subsection, we investigate a performance upper bound similar to the VCG auction proposed in the literature and compared with our proposed approach. In the performance upper bound, the jammer asks all sources to reveal their evaluations of the jammer's power, upon which the jammer calculates the optimal power allocation and allocates accordingly. A source pays the "performance loss" of other sources induced by its own participation of the auction. In the context of wireless secrecy capacity, the performance upper bound can be described as follows:

- *Information*: Public available information includes noise density σ^2 and bandwidth W . Source s_i knows channel gain $G_{s_i d_i}$ and $G_{s_i m}$. The jammer knows channel gains $G_{J d_i}$ for all i , and can estimate the channel gains $G_{J m}$ for all i when it receives bids from the sources.
- *Bids*: Source s_i submits $\Delta C_{s_i}(P_i^J(b_i; b_{-i}))$ to the jammer, which represents the secrecy capacity increase as a function of the jammer parameter P_i^J .

- *Allocation*: The jammer determines the power allocation $\mathbf{P} = [P_1^J \dots P_N^J]$ by solving the following problem

$$\mathbf{P}^* = \arg \max_{\mathbf{P}} \sum_{j \in \mathcal{I}} C_{s_j}(P_j^J). \quad (10)$$

- *Payments*: For each source s_i , the jammer solves the following problem

$$\mathbf{P}^{*/i} = \arg \max_{\mathbf{P}, P_i=0} \sum_j C_{s_j}(P_j^J), \quad (11)$$

i.e., the total distortion decreases without allocating resource to source i . The payment of source i is then

$$c_i = \sum_{j \neq i, j \in \mathcal{I}} C_{s_j}(P_j^{*/i}) - \sum_{j \neq i, j \in \mathcal{I}} C_{s_j}(P_j^*), \quad (12)$$

i.e., the performance loss of all other sources because of including source i in the allocation.

The resource allocation as calculated in (10) achieves the *efficient* allocation as shown in [22]. This is the reason why we select the VCG auction as our performance bound. The auction can achieve the efficient allocation in one shot, by allowing the power to gather a lot of information and perform heavy but local computation.

Although the performance upper bound has the desirable social optimal, it is usually computationally expensive for the relay to solve $I + 1$ nonconvex optimization problems. To solve a nonconvex optimization, the common solution like interior point method needs a complexity of $O(I^2)$. As the result, the overall complexity for the performance upper bound is $O(I^3)$, while the proposed auction algorithm has linear complexity. Furthermore, there is a significant communication overhead to submit $C_{s_i}(P_i^J)$ for each source i . In the proposed scheme, the bids and the corresponding resource allocation are iteratively updated. This is similar to the distributed power control case, where the signal-to-interference-noise ratio and power update are iteratively obtained. As a result, the overall signalling can be reduced.

V. PRELIMINARY SIMULATIONS

To investigate the performances, we conduct the following two simulations. The setup is as follows: There are two source-destination pairs; each source transmits with 10 mW, the noise power is -90 dBm; the maximal power is 100 mW for the jammer; the bandwidth is unit, $W = 1$; the propagation loss factor is 3; $\beta = 1$; the sources are located at (500 m, 0 m) and (500 m, 1000 m), respectively; the destinations are located at (1000

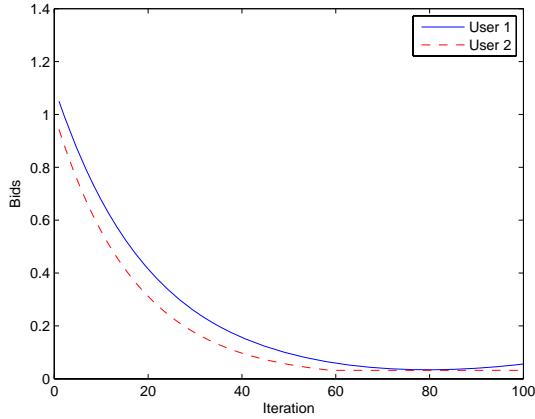


Fig. 2. Bids as a function of iteration

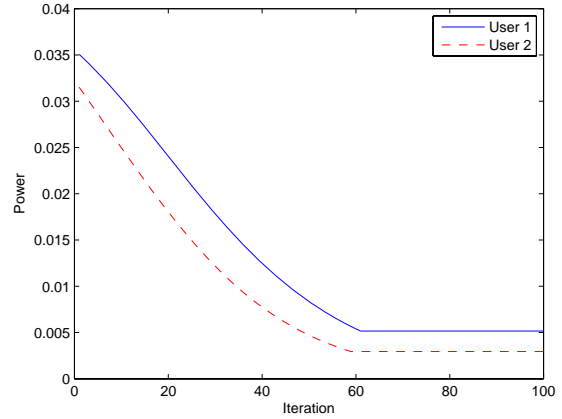


Fig. 4. Jamming Power as a function of iteration

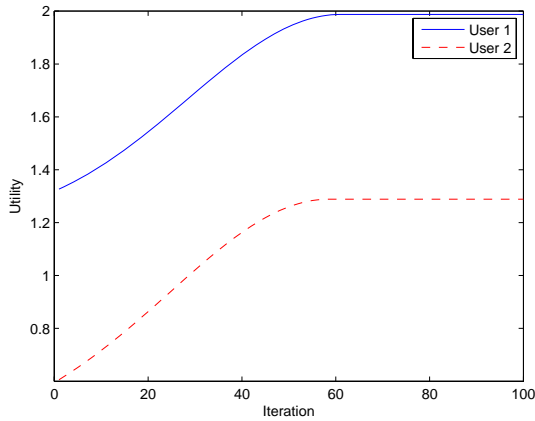


Fig. 3. Utility as a function of iteration

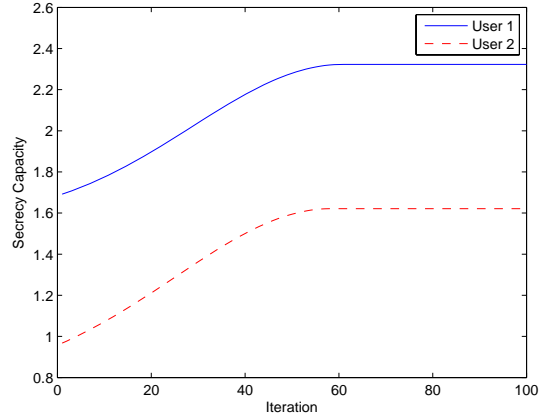


Fig. 5. Secrecy capacity as a function of iteration

m,0 m) and (1000 m,1000 m), respectively, the malicious node is located at (250 m,500 m), and $\pi = 1$.

First we study the convergence of the proposed auction approach. The jammer is located at (0 m,1000 m). In Figures 2, 3, 4, and 5, we show the bids, utilities, allocated jamming power and secrecy capacities as a function of iteration, respectively. Here, we use the simple update function by allowing the bids to be varied by 5% in each iteration. We can see that the proposed scheme converges.

Next, we investigate if the converged solution optimal. We change the location of the jammer from (0 m,0 m) to (0 m,1000 m). In Figures 6 and 7, we show the jamming power and secrecy capacities as a function of the jammer location. We can see that the proposed distributed auction has the similar performance as the performance bounds. Moreover, the secrecy capacity is greatly improved compared with no jammer case.

VI. CONCLUSIONS

Physical layer security is an emerging security technique that is an alternative for traditional cryptographic-based protocols to achieves perfect secrecy capacity as eavesdroppers obtain zero information. Jamming has been shown in the literature to effectively improve secrecy capacity. In this paper, we investigate the interaction between multiple source-destinations and one friendly jammer using the auction theory so as to have a distributed solution. The sources provide bids to the friendly jammer to interfere the malicious eavesdropper so as to increase the secrecy capacity. To analyze the auction outcome, we investigate the Share auction and construct the distributed algorithm. Some properties such as equilibrium and convergence are analyzed. From the simulation results, we can see the convergence and optimality of the proposed scheme.

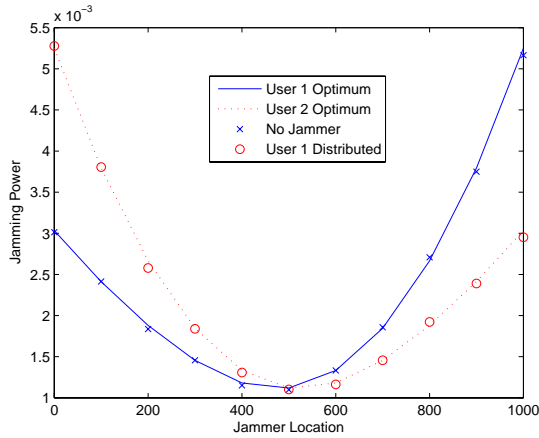


Fig. 6. Jamming power as a function of jammer location

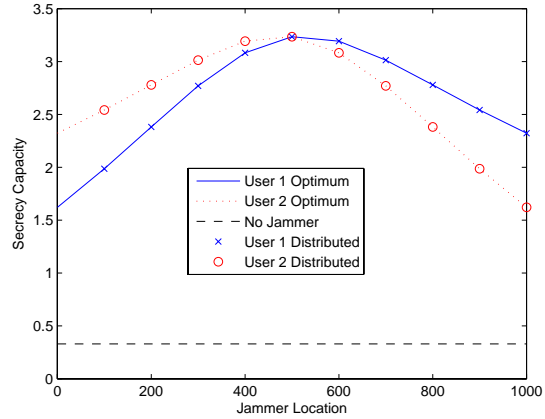


Fig. 7. Secrecy capacity as a function of jammer location

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [4] A. O. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
- [5] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proceedings of 41st Conference on Information Sciences and Systems*, Baltimore, MD, Mar. 2007.
- [6] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proceedings of IEEE Vehicular Technology Conference - Fall*, vol. 3, Dallas, TX, Sep. 2005, pp. 1906–1910.
- [7] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proceedings of IEEE International Symposium on Information Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.
- [8] S. Shafiee and S. Ulukus, "Achievable rates in gaussian miso channels with secrecy constraints," in *Proceedings of IEEE International Symposium on Information Theory*, Nice, France, Jun. 2007, pp. 2466 – 2470.
- [9] Y. Liang, H. V. Poor, and S. S. (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
- [10] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [11] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure collaborative beamforming," in *Proceedings of the Forty-Seventh Annual Allerton Conference on Communication, Control, and Computing*, Allerton, IL, Oct. 2008.
- [12] A. Kashyap, T. Başar, and R. Srikant, "Correlated jamming on mimo gaussian fading channels," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.
- [13] S. Shafiee and S. Ulukus, "Mutual information games in multi-user channels with correlated jamming," in [http : //arxiv.org/abs/cs.IT/0601110](http://arxiv.org/abs/cs.IT/0601110).
- [14] M. H. Brady, M. Mohseni, and J. M. Cioffi, "Spatially-correlated jamming in gaussian multiple access and broadcast channels," in *Proceedings of 40th Annual Conference on Information Sciences and Systems*, Princeton, NJ, Mar. 2006.
- [15] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4005–4019, Oct. 2008.
- [16] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA: MIT Press, 1991.
- [17] C. U. Saraydar, N. B. Mandayam, and D. J. Goodman, "Efficient power control via pricing in wireless data networks," *IEEE Transactions on Communications*, vol. 50, no. 2, pp. 291–303, Feb. 2002.
- [18] G. Scutari, S. Barbarossa, and D. P. Palomar, "Potential games: a framework for vector power control problems with coupled constraints," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, vol. 4, Toulouse, France, May 2006.
- [19] B. Wang, Z. Han, and K. J. R. Liu, "Distributed relay selection and power control for multiuser cooperative communication networks using buyer / seller game," in *Proceedings of Annual IEEE Conference on Computer Communications (INFOCOM 2007)*, Anchorage, AK, May 2009, pp. 2678–2682.
- [20] N. Bonneau, E. A. M. Debbah, and A. Hjørungnes, "Non-atomic games for multi-user systems," *IEEE Journal on Selected Areas in Communications*, issue on.
- [21] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *Proceedings of the IEEE International Conference on Game Theory for Networks (GameNets 2009)*, Istanbul, Turkey, May 2009, pp. 2678–2682.
- [22] V. Krishna, *Auction Theory*. Cambridge, MA: Academic Press, 2002.
- [23] J. Huang, R. Berry, and M. L. Honig, "Auction-based spectrum sharing," *ACM Mobile Networks and Applications Journal*, vol. 11, no. 3, pp. 405 – 418, June 2006.
- [24] J. Huang and Z. Han, "Game theory for spectrum sharing," book chapter in *'Cognitive Radio Networks'*, Auerbach Publications, CRC Press, 2009.
- [25] J. Huang, Z. Han, M. Chiang, and H. V. Poor, "Auction-based resource allocation for cooperative communications," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 7, pp. 1226 – 1237, September 2008.