

Physical Layer Security Game: Interaction between Source, Eavesdropper and Friendly Jammer

Han Zhu, Marina Ninoslav, Merouane Debbah, Are Hjorungnes

▶ **To cite this version:**

Han Zhu, Marina Ninoslav, Merouane Debbah, Are Hjorungnes. Physical Layer Security Game: Interaction between Source, Eavesdropper and Friendly Jammer. EURASIP Journal on Wireless Communications and Networking, 2009, 21 p. hal-00446934

HAL Id: hal-00446934

https://centralesupelec.hal.science/hal-00446934

Submitted on 13 Jan 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Physical Layer Security Game: Interaction between Source, Eavesdropper and Friendly Jammer

Zhu Han[1], Ninoslav Marina[2], Mérouane Debbah[3], and Are Hjørungnes[2]
[1] Electrical and Computer Engineering Department, University of Houston, USA.
[2]UniK - 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 source that transmits the useful data and friendly jammers who assist the source by "masking" the eavesdropper. In order to obtain a distributed solution, one possibility is to introduce a game theoretic approach. The game is defined such that the source pays the jammers to interfere the eavesdropper, therefore increasing the secrecy capacity. The friendly jammers charge the source with a certain price for the jamming and there is a tradeoff for the price. If the price is too low, the profit of the jammers is low and if the price is too high, the source would not buy the "service" (jamming power) or would buy it from other jammers. To analyze the game outcome, we define and investigate a Stackelburg type of game and construct a distributed algorithm. Our analysis and simulation results show the effectiveness of friendly jamming and the tradeoff for setting the price. The distributed game solution is shown to have similar performances to those of the centralized one.

This work was supported by NSF CNS-0831371, and was supported by the Research Council of Norway through the project entitled "Mobile-to-Mobile Communication Systems (M2M)".

I. Introduction

The future communication systems will be decentralized and ad-hoc, therefore allowing various types of network mobile terminals to join and leave. This aspect makes the whole system vulnerable and susceptible to attacks. Anyone within communication range can listen and possibly extract information. While these days we have numerous cryptographic methods with high level security, there is no system with perfect security on physical layer. Therefore, the physical (PHY) 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 encoding/decoding schemes used by the transmitter/receiver. In approaches where PHY layer security is applied, 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*.

This line of work was pioneered by Aaron Wyner, who defined the wiretap channel and established the possibility to create almost perfect secure communication links without relying on private (secret) keys [1]. Wyner showed that when the eavesdropper channel is a degraded version of the main channel, the source and the destination can exchange perfectly secure messages at a non-zero rate. The main idea proposed by him is to exploit the additive noise impairing the eavesdropper by using a stochastic encoder that maps each message to many codewords according to an appropriate probability distribution. With this scheme, a maximal equivocation (i.e., uncertainty) is induced at the eavesdropper. In other words, 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 landmark paper, Csiszár and Körner generalized Wyner's approach by considering the transmission of confidential messages over broadcast channels [3]. Recently, there have been considerable efforts on generalizing these studies to the wireless channel and multi-user scenarios (see [4–12] and references therein). Jamming [13–15] 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 [16]. In other words, the jamming is friendly in this context. Moreover, the friendly helper can assist the secrecy by sending codewords, bring further gains relative to unstructured Gaussian noise [16–18].

Game theory [19] 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 [20–23] 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 this paper, we investigate the interaction between the source and its friendly jammers using game theory. Although the friendly jammers help the source by reducing the data rate that is "leaking" from the source to the malicious node, at the same time they also reduce the useful data rate from the source to the destination. Using well chosen amounts of power from the friendly jammers, the secrecy capacity can be maximized. In the game that we define here, the source pays the jammers to interfere the malicious eavesdropper, and therefore, to increase the secrecy capacity. The friendly jammers charge the source with a certain price for the jamming the eavesdropper. One could notice that there is a tradeoff for the proposed price: If the price of a certain jammer is too low, its profit is also low; if its price is too high, the source will buy from the other jammers. In modeling the outcome of the above games our analysis uses the Stackelberg type of game. Initially, the existence of equilibrium will be studied. Then, a distributed algorithm will be proposed and its convergence will be investigated. The outcome of the distributed algorithm will be compared to the centralized genie aided solution. Some implementation concerns are also discussed. From the simulation results, we can see the efficiency of friendly jamming and tradeoff for setting the price, the source prefers buying service from only one jammer, and the centralized scheme and the proposed game scheme has similar performance.

The rest of the paper is organized as follows: In Section II, the system model of physical layer security with friendly jamming users is described. In Section III, the game models are formulated, and the outcomes as well as properties of the game are analyzed. Simulation results are shown in Section IV and conclusions are drawn in Section V.

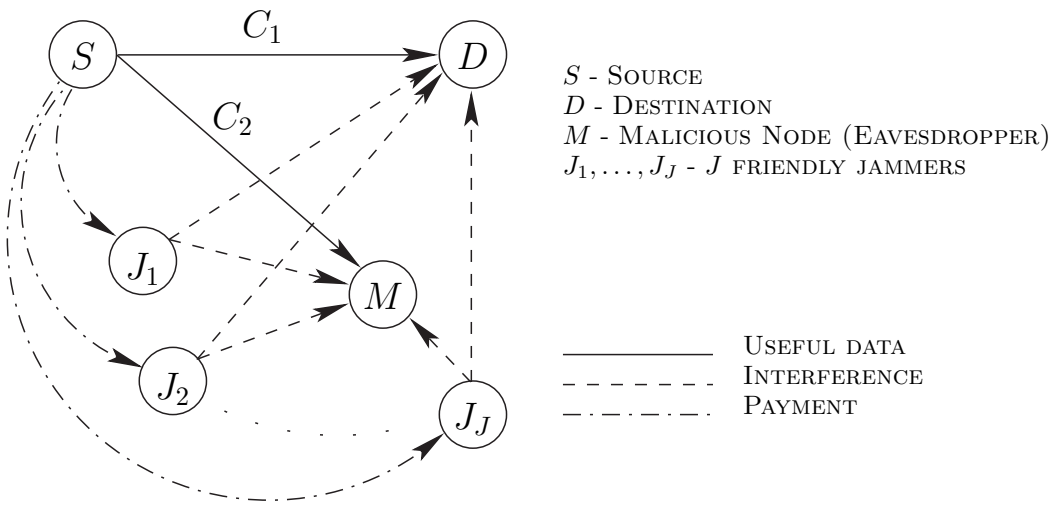


Fig. 1. System Model for Physical Layer Security Game

II. System Model

We consider a network with a source, a destination, a malicious eavesdropper node, and J friendly jammer nodes as shown in Figure I. The malicious node tries to eavesdrop the transmitted data coming from the source node. 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 transmits with power P_0. The channel gains from the source to the destination and from the source to the malicious node are G_{sd} and G_{sm}, respectively. Each friendly jammer i, $i = 1, \ldots, J$ transmits with power P_i and the channel gains from it to the destination and the malicious node, are G_{id} and G_{im}, respectively. For convenience, we denote by $\mathcal{J}$ the set of indices $\{1, 2, \ldots, J\}$. 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 to the destination is

$$C_1 = W \log_2 \left(1 + \frac{P_0 G_{sd}}{\sigma^2 + \sum_{i \in \mathcal{J}} P_i G_{id}} \right). \tag{1}$$

The channel capacity from the source to the malicious node is

$$C_2 = W \log_2 \left(1 + \frac{P_0 G_{sm}}{\sigma^2 + \sum_{i \in \mathcal{J}} P_i G_{im}}\right). \tag{2}$$

The secrecy capacity is

$$C_s = (C_1 - C_2)^+ \tag{3}$$

where $(\cdot)^+ = max(\cdot, 0)$. Both C_1 and C_2 are decreasing and convex functions of jamming power P_i. However, $C_s = C_1 - C_2$ is not a monotonous and convex function. This is because the jamming power might decrease C_1 faster than C_2. As a result, C_s might increase in some region of value P_i. So, the questions are whether or not C_s 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 a game theoretical approach.

III. Game for Physical Layer Security

In this section, we study how to use game theory to analyze the physical layer security. First, we define the game between the source and friendly jammers. Next, we optimize the source and jammer sides, respectively. Then, we prove some properties of the proposed game. Furthermore, a comparison with the centralized scheme is constructed. Finally, we discuss some implementation concerns.

A. Game Definition

The source can be modeled as a buyer who wants to optimize its secrecy capacity minus cost by modifying the "service" (jamming power P_i) from the friendly jammers, i.e.,

$$\text{Source's Game: } \max\ U_s = \ (a \max(C_1 - C_2, 0) - M), \tag{4}$$

$$\text{s.t. } P_i \leq P_{max},$$

where a is the gain per unit capacity, P_{max} is the maximal power that a jammer can provide, and M is the cost to pay for the other friendly jamming nodes. Here

$$M = \sum_{i \in \mathcal{J}} p_i P_i, \tag{5}$$

where p_i is the price per unit power for the friendly jammer, P_i is the friendly jammer's power, and $\mathcal{J}$ is the set of friendly jammers. From (4) we note that the source will not participate in the game if $C_1 < C_2$, or in other words, the secrecy capacity is zero. For each jammer, $U_i(p_i, P_i(p_i))$, is the utility function of the price and power bought by the source. For the jammer's (seller's) utility, in this paper we define the following utility

$$U_i = p_i P_i^{c_i}, \tag{6}$$

where $c_i \geq 1$ is a constant to balance from the payment $p_i P_i$ from the source and the transmission cost P_i. Notice that P_i is also a function of the vector of prices $(p_1, \dots p_N)$ since the power that the source will buy also depends on the price that the friendly jammers ask. Hence, for each friendly jammer, the optimization problem is

$$\text{Friendly Jammer's Game: } \max_{p_i} U_i. \tag{7}$$

In the next two subsections, we analyze the optimal strategies for the source and friendly jammers to maximize their own utilities.

B. Source (Buyer) Side Analysis

Introducing $A = P_0 G_{sd}/\sigma^2$, $B = P_0 G_{sm}/\sigma^2$, $u_i = G_{id}/\sigma^2$, and $v_i = G_{im}/\sigma^2$, $i \in \mathcal{J}$, we have

$$U_s = aW \left(\log\left(1 + \frac{A}{1 + \sum_{j\in\mathcal{J}} u_j P_j}\right) - \log\left(1 + \frac{B}{1 + \sum_{j\in\mathcal{J}} v_j P_j}\right)\right)^+ - \sum_{j\in\mathcal{J}} p_j P_j, \tag{8}$$

For the source (buyer) size, we first analyze the case where $C_1 > C_2$. By differentiating (4), we have

$$\frac{\partial U_s}{\partial P_i} = -\frac{aWAu_i/\ln 2}{(1 + A + \sum_{j\in\mathcal{J}} u_j P_j)(1 + \sum_{j\in\mathcal{J}} u_j P_j)} + \frac{aWBv_i/\ln 2}{(1 + B + \sum_{j\in\mathcal{J}} v_j P_j)(1 + \sum_{j\in\mathcal{J}} v_j P_j)} - p_i = 0. \tag{9}$$

Rearranging the above equation, we have

$$P_i^4 + F_{i,3} P_i^3 + F_{i,2}(p_i) P_i^2 + F_{i,1}(p_i) P_i + F_{i,0}(p_i) = 0, \tag{10}$$

where

$$F_{i,3} = (2 + 2\alpha_i + A)^2 + (2 + 2\beta_i + B)^2, \tag{11}$$

$$F_{i,2}(p_i) = \frac{(2 + 2\alpha_i + A)(2 + 2\beta_i + B)}{u_i v_i} + \frac{L_i}{v_i^2} + \frac{K_i}{u_i^2} - \frac{aW}{p_i u_i v_i}\left(\frac{B}{v_i} - \frac{A}{u_i}\right), \tag{12}$$

$$F_{i,1}(p_i) = \frac{L_i C_i + K_i D_i}{u_i^2 v_i^2} + \frac{aW(AD_i - BC_i)}{p_i u_i^2 v_i^2}, \tag{13}$$

$$F_{i,0}(p_i) = \frac{K_i L_i}{u_i^2 v_i^2} + \frac{aW(Au_i L_i - Bv_i K_i)}{p_i u_i^2 v_i^2}, \tag{14}$$

and

$$\alpha_i = \sum_{j \neq i} G_{jd} P_j, \tag{15}$$

$$\beta_i = \sum_{j \neq i} G_{jm} P_j, \tag{16}$$

$$K_i = (1 + \alpha_i)(1 + \alpha_i + A), \tag{17}$$

$$L_i = (1 + \beta_i)(1 + \beta_i + B), \tag{18}$$

$$C_i = u_i(2 + 2\alpha_i + A), \tag{19}$$

$$D_i = v_i(2 + 2\beta_i + B). \tag{20}$$

The solutions of the quartic can be expressed in closed form but this is not the primary goal here. It is important that the solution we are interested in is given by the following function

$$P_i^* = P_i^*(p_i, A, B, \{u_j\}, \{v_j\}, \{P_j\}_{j \neq i}) \tag{21}$$

Note that $0 \leq P_i \leq P_{max}$. Since P_i satisfies the polynomial function, we can have the optimal strategy as

$$P_i^* = \min[\max(P_i, 0), P_{max}]. \tag{22}$$

Because of the complexity of the closed form solution of a quartic equation in (22), we also consider two special cases: lower interference case and high interference case.

B.1 Interference at the Destination is much Smaller than the Noise

Remember the definitions: $A = P_0 G_{sd}/\sigma^2$, $B = P_0 G_{sm}/\sigma^2$, $u_i = G_{id}/\sigma^2$ and $v_i = G_{im}/\sigma^2$. Imagine a situation in which all jammers are close to the malicious node and far from the destination node. In that case the interference from the jammers to the destination is very small in comparison to the additive noise and therefore we have

$$U_s \approx aW \left(\log(1 + A) - \log\left(1 + \frac{B}{1 + \sum_{j \in \mathcal{J}} v_j P_j}\right)\right)^+ - \sum_{j \in \mathcal{J}} p_j P_j. \tag{23}$$

Then

$$\frac{\partial U_s}{\partial P_i} = \frac{aWBv_i/\ln 2}{(1+B+\sum_{j\in\mathcal{J}} v_j P_j)(1+\sum_{j\in\mathcal{J}} v_j P_j)} - p_i = 0. \tag{24}$$

Rearranging we get

$$P_i^2 + \frac{2+2\beta_i+B}{v_i} P_i + \frac{(1+\beta_i)(1+B+\beta_i)}{v_i^2} - \frac{aWB}{p_i v_i \ln 2} = 0. \tag{25}$$

Solving the above equation we obtain a closed-form solution

$$\begin{aligned} P_i^* &= -\frac{2+2\beta_i+B}{2v_i} + \sqrt{\frac{(2+2\beta_i+B)^2}{4v_i^2} - \frac{(1+\beta_i)(1+B+\beta_i)}{v_i^2} + \frac{aWB}{p_i v_i \ln 2}} \\ &= q_i + \sqrt{w_i + \frac{z_i}{p_i}}. \end{aligned} \tag{26}$$

Finally, by comparing P_i^* with the power under the boundary conditions ($P_i = 0$, $P_i = P_{max}$ and $C_s = 0$), the optimal P_i^* in the low SNR region can be obtained.

B.2 One Jammer with Interference that is much Higher than the Noise but much Smaller than the Received Power at the Destination and the Malicious Node

In this case the interference from the jammer is much higher than the additive noise but much smaller than the power of the received signal at the destination and the malicious node. In other words, that means $1 << u_1 P_1 << A$ and $1 << v_1 P_1 << B$. Therefore the utility function of the source is given by

$$U_s \approx aW\left(\log\left(1+\frac{A}{u_1 P_1}\right) - \log\left(1+\frac{B}{v_1 P_1}\right)\right) - p_1 P_1 \approx \frac{aWA}{u_1 P_1} - \frac{aWB}{v_1 P_1} - p_1 P_1. \tag{27}$$

If $\frac{B}{v_1} - \frac{A}{u_1} \leq 0$, U_s is a decreasing function of P_1. As a result, P_s is optimized when $P_1 = 0$, i.e. the jammer would not participate the game. On the other hand, if $\frac{B}{v_1} - \frac{A}{u_1} > 0$, in order to find the maximizing powers we have to calculate

$$\frac{\partial U_s}{\partial P_i} = -\frac{aWA}{u_1 P_1^2} + \frac{aWB}{v_1 P_1^2} - p_1 = 0. \tag{28}$$

Hence

$$P_1^* = \sqrt{\frac{aW}{p_1}\left(\frac{B}{v_1} - \frac{A}{u_1}\right)} = \sqrt{\frac{D_1}{p_1}}. \tag{29}$$

From this equation we get the optimal closed-form solution P_i^*, and similarly by comparing P_1^* with the power under the boundary conditions ($P_1 = 0$, $P_1 = P_{max}$ and $C_s = 0$), we can obtain the optimal solution for the this special case.

C. Friendly Jammer (Seller) Side Analysis

In this subsection, we study how the friendly jammers can set the optimal price to maximize its utility. By differentiating the utility in (6) and setting it to zero, we have

$$\frac{\partial U_i}{\partial p_i} = (P_i^*)^{c_i} + p_i c_i (P_i^*)^{c_i - 1} \frac{\partial P_i^*}{\partial p_i} = 0. \tag{30}$$

This is equivalent to

$$(P_i^*)^{c_i - 1} \left(P_i^* + p_i c_i \cdot \frac{\partial P_i^*}{\partial p_i} \right) = 0. \tag{31}$$

This happens either if $P_i^* = 0$ or if

$$P_i^* + p_i c_i \cdot \frac{\partial P_i^*}{\partial p_i} = 0. \tag{32}$$

From the closed form solution of P_i^* the solution of p_i^* will be a function given as

$$p_i^* = p_i^*(\sigma^2, G_{sd}, G_{sm}, \{G_{id}\}, \{G_{im}\}). \tag{33}$$

Notice that p_i^* should be positive. Otherwise, the friendly jammer would not play.

D. Properties

In this subsection, we prove some properties of the proposed game. First, we prove that the power is monotonous function of the price under the two extreme cases. The properties can help for the proof of equilibrium existence in the later part of this subsection.

Property 1: Under the two special cases, the optimal power consumption P_i^* for friendly jammer i is monotonous with its price p_i, when the other friendly jammers prices are fixed. The proof is straightforward from (26) and (29).

We investigate the following analysis of the relation between the price and power. We find out that the friendly jammer power P_i bought from the source is convex in its own price p_i under some conditions. To prove this we need to check whether the second derivative $\partial^2 P_i / \partial p_i^2 < 0$.

In the first special case in which the interference is small

$$\frac{\partial P_i^*}{\partial p_i} = -\frac{z_i}{2p_i^2\sqrt{w_i + \frac{z_i}{p_i}}} \tag{34}$$

and

$$\frac{\partial^2 P_i^*}{\partial p_i^2} = \frac{z_i}{p_i^3\left(w_i + \frac{z_i}{p_i}\right)^{1/2}}\left(1 - \frac{1}{4\left(\frac{p_i w_i}{z_i} + 1\right)}\right). \tag{35}$$

The above equation is greater than zero when p_i is small. This means when the interference is small and the price is small, the power is convex as a function of the price.

In the second special case in which the interference is severe

$$\frac{\partial P_i^*}{\partial p_i} = -\frac{1}{2}\sqrt{D_1}p_1^{-3/2} \tag{36}$$

and

$$\frac{\partial^2 P_i^*}{\partial p_i^2} = \frac{3}{4}\sqrt{D_1}p_1^{-5/2} > 0. \tag{37}$$

This means when the interference is severe, the power is a convex function of the price.

Next, we investigate the equilibrium of the proposed game. In other word, no user can improve the its utility by changing its own strategy only. We first define the Stackelberg equilibrium as follow:

Definition 1: P_i^{SE} and p_i^{SE} are the Stackelberg equilibrium of the proposed game, if when p_i is fixed,

$$U_s(\{P_i^{SE}\}) = \sup_{P_{max} \geq \{P_i^{SE}\} \geq 0, \forall i} U_s(\{P_i\}),\ \forall i \in \mathcal{J} \tag{38}$$

and when P_i is fixed,

$$U_i(p_i^{SE}) = \sup_{p_i} U_i(p_i),\ \forall i \in \mathcal{J}. \tag{39}$$

Finally, from the analysis in the previous two subsections, we can shown the following property for the proposed game.

Property 2: The pair of $\{P_i^*\}_{i=1}^N$ in (22) and $\{p_i^*\}_{i=1}^N$ in (33) is the Stackelberg equilibrium for the proposed game.

Notice that there might be multiple roots in 10, as a result, there might be multiple Stackelberg equilibriums. In the simulation results shown in later section, we will show that the proposed scheme can still achieve the equilibriums with better performances than those of the no-jammer case.

E. Distributed Algorithm and Convergence

In this subsection, we study how the distributed game can converge to the Stackelberg equilibrium defined in the above subsection. After rearranging (30), we have

$$p_i = I_i(\mathbf{p}) = -\frac{(P_i^*)}{c_i \frac{\partial P_i^*}{\partial p_i}}, \tag{40}$$

where $\mathbf{p} = [p_1, \ldots, p_N]^T$ and $I_i(\mathbf{p})$ is the price update function. Notice that P_i^* is a function of $\mathbf{p}$. The information for the update can be obtained from the source node. This is similar to the distributed power control [26]. The update of the friendly jammers' prices can be written in a vector form as

$$\text{Distributed Algorithm: } \mathbf{p}(t+1) = \mathbf{I}(\mathbf{p}(t)), \tag{41}$$

where $\mathbf{I} = [I_1, \ldots, I_N]^T$, and the iteration is from time t to time $t+1$. Next we show that the convergence of the proposed scheme by proving that the price update function in (41) is a standard function [24] defined as

Definition 2: A function $\mathbf{I}(\mathbf{p})$ is standard, if for all $\mathbf{p} \geq \mathbf{0}$, the following properties are satisfied

1. Positivity: $\mathbf{p} > \mathbf{0}$,
2. Monotonicity: if $\mathbf{p} \geq \mathbf{p}'$, then $\mathbf{I}(\mathbf{p}) \geq \mathbf{I}(\mathbf{p}')$, or $\mathbf{I}(\mathbf{p}) \leq \mathbf{I}(\mathbf{p}')$,
3. Scalability: For all $\eta > 1$, $\eta\mathbf{I}(\mathbf{p}) \geq \mathbf{I}(\eta\mathbf{p})$.

In [24], it has been proved that the price will converge to the fixed point (i.e. the Stackelberg equilibrium in our case) from any feasible initial price vector. The positivity is very easy to prove. If the price p_i goes up, the source would buy less from the i^{th} friendly jammer. As a result, $\frac{\partial P_i^*}{\partial p_i}$ in (30) is negative, and we prove positivity $p_i = I_i(\mathbf{p}) > 0$.

For monotonicity and scalability, we can only show the two special cases. For the low interference case, from (26) it is obvious that

$$I_i(\mathbf{p}) = -\frac{(P_i^*)}{c_i \frac{\partial P_i^*}{\partial p_i}} = \frac{2\sqrt{w_i p_i^2 + z_i p_i}(q_i p_i + \sqrt{w_i p_i^2 + z_i p_i})}{c_i z_i} \tag{42}$$

which is monotonically increasing in p_i. For scalability, we have

$$\frac{I_i(\eta\mathbf{p})}{\eta I_i(\mathbf{p})} = \frac{\sqrt{w_i p_i^2 + z_i p_i/\eta}(q_i p_i + \sqrt{w_i p_i^2 + z_i p_i/\eta})}{\sqrt{w_i p_i^2 + z_i p_i}(q_i p_i + \sqrt{w_i p_i^2 + z_i p_i})} < 1, \tag{43}$$

since $\eta > 1$.

For the large interference case, from (29) we have

$$I_i(\mathbf{p}) = -\frac{(P_i^*)}{c_i \frac{\partial P_i^*}{\partial p_i}} = \frac{2p_i}{c_i} \tag{44}$$

which is monotonically increasing in p_i and scalable.

For more general cases, the analysis cannot be tractable. In the simulation section later, we employ the general simulation setups. The simulation results show that the proposed scheme can converge and outperform the no-jammer case.

F. Centralized Scheme

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

$$\max_{P_i} \; C_s = \max \left[W \log_2 \left(\frac{1 + \frac{P_0 G_{sd}}{\sigma^2 + \sum_{i \in \mathcal{J}} P_i G_{id}}}{1 + \frac{P_0 G_{sm}}{\sigma^2 + \sum_{i \in \mathcal{J}} P_i G_{im}}} \right), 0 \right]. \tag{45}$$

$$\text{s.t. } 0 \leq P_i \leq P_{max}, \forall i.$$

The centralized solution is found by maximizing the secrecy capacity only. If we do not consider the constraint, we have

$$\frac{\partial C_s}{\partial P_i} = -\frac{AWu_i}{(1 + \alpha_i + u_i P_i)(1 + A + \alpha_i + u_i P_i)} + \frac{BWv_i}{(1 + \beta_i + u_i P_i)(1 + B + \beta_i + u_i P_i)} = 0. \tag{46}$$

Rearranging we get

$$P_i^2 + \frac{Au_i^2(2 + B + 2\beta_i) - Bv_i^2(2 + A + 2\alpha_i)}{Au_i^3 - Bv_i^3} P_i + \frac{Au_i(1 + \beta_i)(1 + B + \beta_i) - Bv_i(1 + \alpha_i)(1 + A + \alpha_i)}{Au_i^3 - Bv_i^3} = 0. \tag{47}$$

Using the KKT condition theorem [25], the final solution would be obtained by comparing the boundary conditions (i.e. $P_i = 0$, $P_i = P_{max}$, and $C_s = 0$).

Notice that our proposed algorithm is distributive, in the sense that only the pricing information needs to be exchanged. In the simulation results, we compare the proposed game theoretical approach with this centralized scheme.

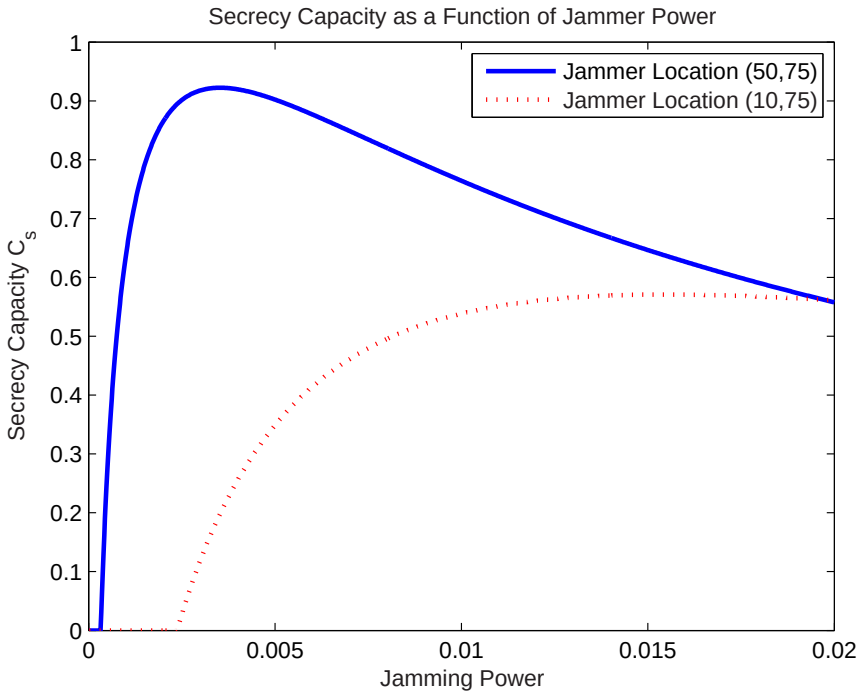


Fig. 2. Secrecy Capacity vs. Jamming Power

Finally, from the simulation results in the next section, we show that the distributed solution and the centralized solution is asymptotically the same if a is sufficiently large (the source cares the secrecy capacity more than the payment, i.e., the source is sufficiently rich).

G. Implementation Discussion

There are several implementation concerns for the proposed scheme. First, the channel information from the source to the malicious eavesdropper might not be known or accurately known. Under this condition, the secrecy capacity formula should be rewritten considering the uncertainty. If the direction of arrival is known, multiple antenna techniques can be employed such as in [12]. Second, the proposed scheme need iteratively updating the price and power information. A natural question arises that if the distributed scheme has less signalling than the centralize scheme. The comparison is similar to distributed and centralized power control in the literature [24, 26]. Since the channel condition is continuously changing, the distributed solution only needs to update the difference of the parameters such as power and price to be adaptive, while the centralized scheme requires all channel information in each time period. As a result, the distributed solution has a clear advantage and dominates the current and future wireless network design. For example, the power control for cellular networks, the

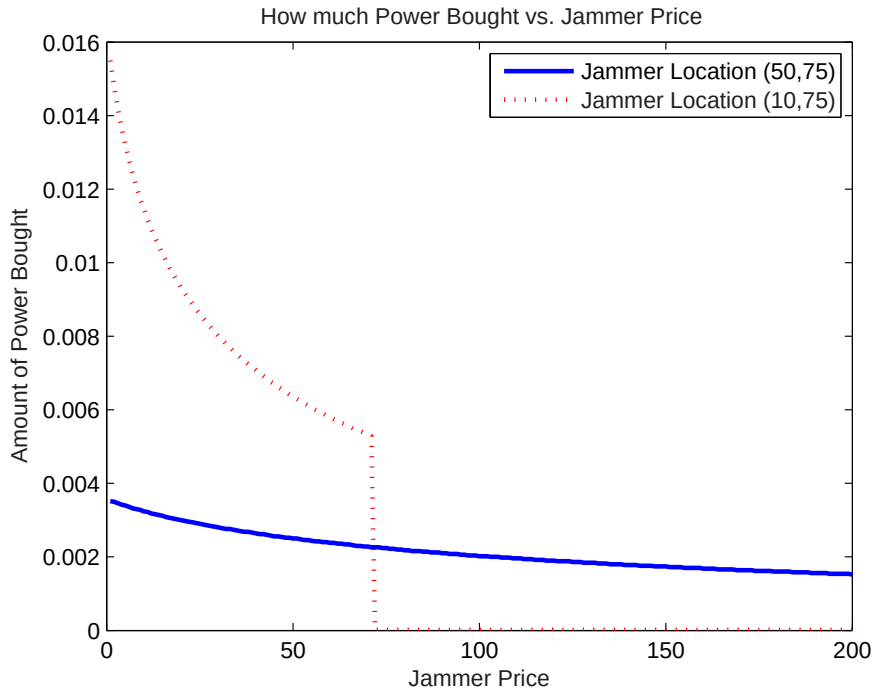


Fig. 3. How much Power the Source Would Buy vs. Price

open loop power control is done only once during the link initialization, while the close loop power control (distributed power allocation such as [24]) is performed 1500 times for UMTS and 800 times for CDMA2000. Finally, for the multi-source multi-destination case, there are two possible choices to solve the problem. First, we can use clustering method to divide the network into sub-networks, and then employ the single-source-destination pair and multiple-friendly-jammer solution proposed in this paper. Or if we consider the jamming power can be useful for multiple eavesdroppers, some techniques such as double auction can be investigated. The detailed discussion is beyond the scope of this paper and would be considered in our future research.

IV. Simulation Results

The simulation is set up as follows: The source and friendly jammer have power of 0.02, the bandwidth is 1, the noise level is 10^{-8}, the propagation loss factor is 3, AWGN channel is assumed. the source, destination, and eavesdropper are located at the coordinate (0,0), (100,0), and (50,50), respectively. Here we select $a = 2$ for the friendly jammer utility in (6).

For single friendly jammer case, we show the simulation with the friendly jammer at the location of (50,75) and (10,75). In Figure 2, we show the secrecy capacity as a function of jamming power.

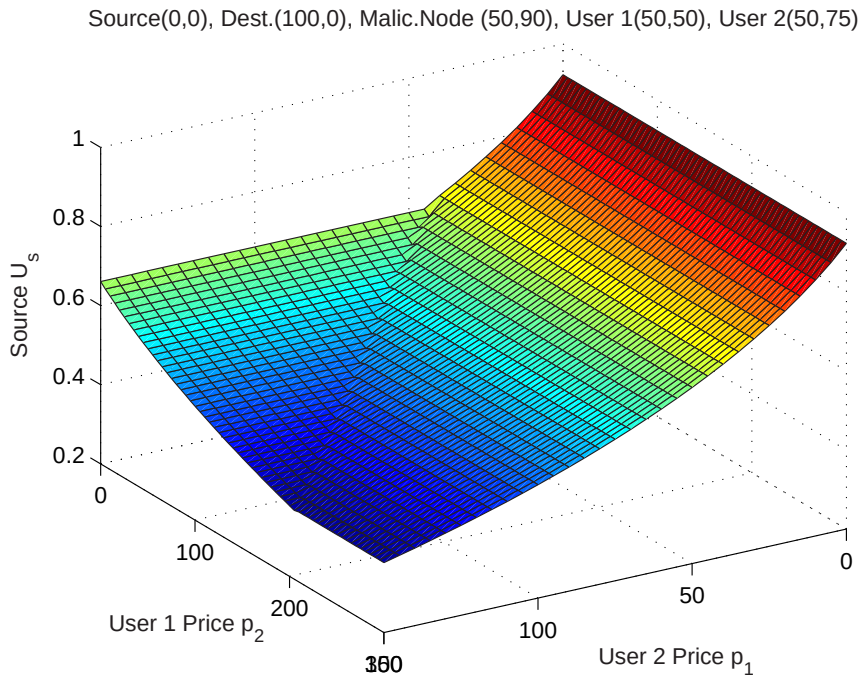


Fig. 4. U_s vs. Prices of Two Users

We can see that with the increase of the jamming power, the secrecy capacity first increases and then decreases. This is because the jamming power has different effects on C_1 and C_2. So there is an optimal point for the jamming power. Also the optimal point depends on the location of the friendly jammer, and the friendly jammer close to the eavesdropper is more effective to improve the secrecy capacity. Moreover, notice that the curve is not convex and not concave. In Figure 3, we show the how much power the source buys from the jammer as a function of the requested price. We can see that the power is reduced if the price goes high. At some point, the source would stop buying the power. So there is a tradeoff for setting the price, i.e., if the price too high, the source would buy less power or even would buy nothing.

For the two-user case, we set up the following simulations. Malicious node is located at (50,90), friendly jammer one is located at (50,50), and friendly jammer two is located at (50,75). In Figure 4, Figure 5, and Figure 6, we show the source's utility U_s, jammer one's utility U_1, and jammer two's utility U_2 as function of both users' price, respectively. We can see that the source would buy service from only one of the friendly jammers. If the friendly jammer asks too low price, the jammer's utility is very low. On the other hand, if the jammer asks too high price, it risks the situation in

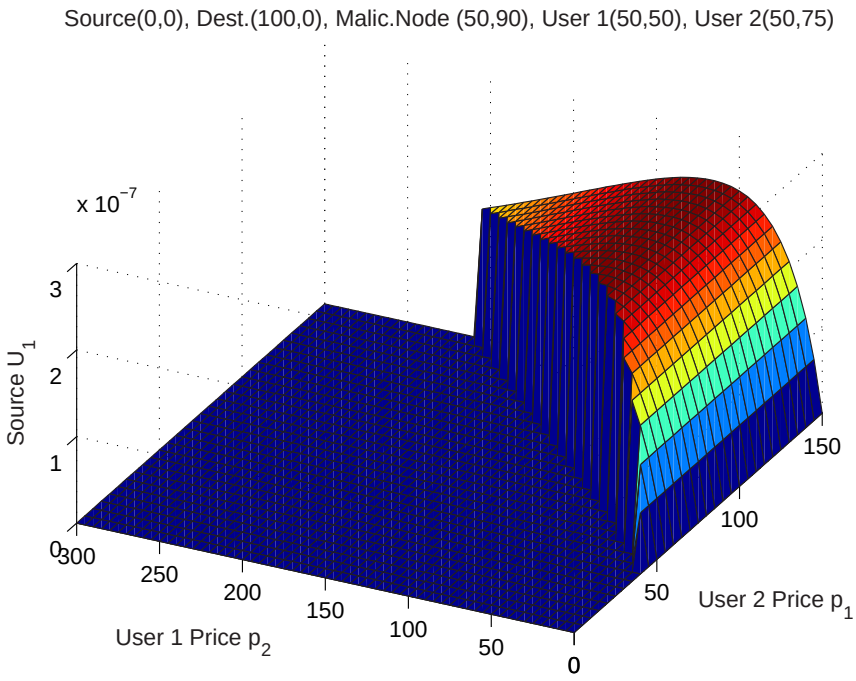


Fig. 5. U_1 vs. Prices of Two Users

which the source would buy the service from the other friendly jammer. There is an optimal price for each friendly jammer to ask, and the source would always select the one that can provide the best performance improvement.

Next, we set up a simulation of mobility. The first friendly jammer is fixed at (50,50), while the second friendly jammer moves from (-50,75) to (100,75). In Figure 7, we show the source utilities of the centralized scheme and the proposed game. We can see that the centralized scheme serves as a performance upper bound. The game result is not far away from the upper bound, while the game solution can be implemented in a distributed manner. The performance game is trivial when the friendly jammer 2 is close to the malicious eavesdropper from (20,75) to (70,75). In Figure 8, we show the jammers' power as a function of jammer 2's location. We can see that depending on the jammers' location, the source switches between two jammers for the best performance. Moreover, the source also buys the optimal amount of jamming power: when the jammer is close to the malicious eavesdropper, the source would buy less power since the jammer is more effective to improve the secrecy capacity. In Figure 9, we show the corresponding friendly jammers' utilities of the proposed game.

Finally, we show the effect of parameter a for the friendly jammer utility in (6). When a is large, the

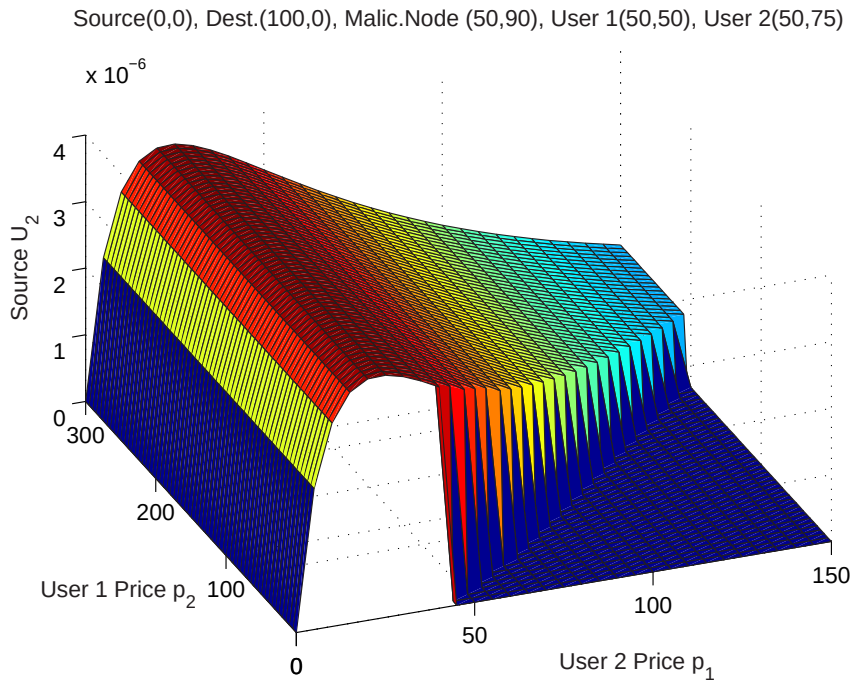


Fig. 6. U_2 vs. Prices of Two Users

friendly jammer's utility reduces quick if the source does not buy the service. As a result, the friendly jammer would not ask arbitrary price, and performance gap to the optima solution is small. In Figure 10, we show the secrecy capacity as a function of a when the jammer two is located at (0,75). We can see that the performance gap is shrinking when a is increasing. Notice that for the condition in which the game almost converges to the optimal solution, most value of $a > 1$ will achieve good solution, e.g. the friendly jammer two located at (50,75).

V. 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 the source and friendly jammers using the game theory so as to have a distributed solution. The source pays the friendly jammers to interfere the malicious eavesdropper so as to increase the secrecy capacity. The friendly jammers charge the source with a price for the jamming. To analyze the game outcome, we investigate the Stackelburg game and construct the distributed algorithm. Some properties such as equilibrium and convergence are analyzed.

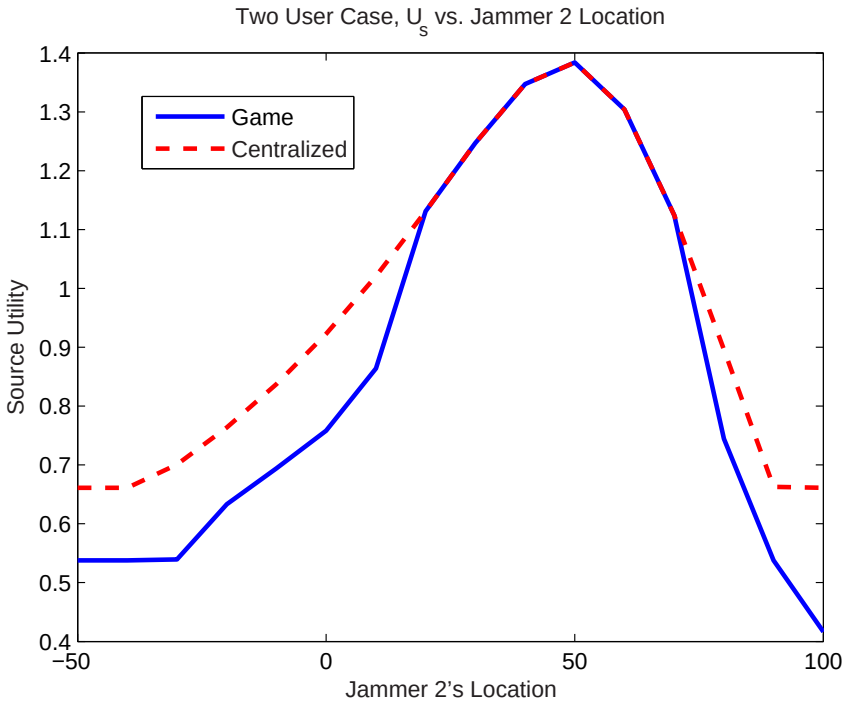


Fig. 7. U_s vs. Jammer 2 Location

From the simulation results, we can see the following points. First, there is a tradeoff for the price: if the price is too low, the profit is low; if the price is too high, the source would not buy or buy from the other jammers. Second, for the multiple jammer case, the source would buy service from only one jammer. Third, the centralized scheme and distributed scheme has a similar performance, especially when α is sufficiently large. Overall, the proposed game theoretical scheme can achieve a comparable performance with distributed implementation.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, pp. 451 - 456, July 1978.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, 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, December 2003.

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, pp. 451 - 456, July 1978.

[6] Z. Li, W. Trappe and R. Yates, "Secret communication via multi-antenna transmission," in Proc. of *41st Conference on*

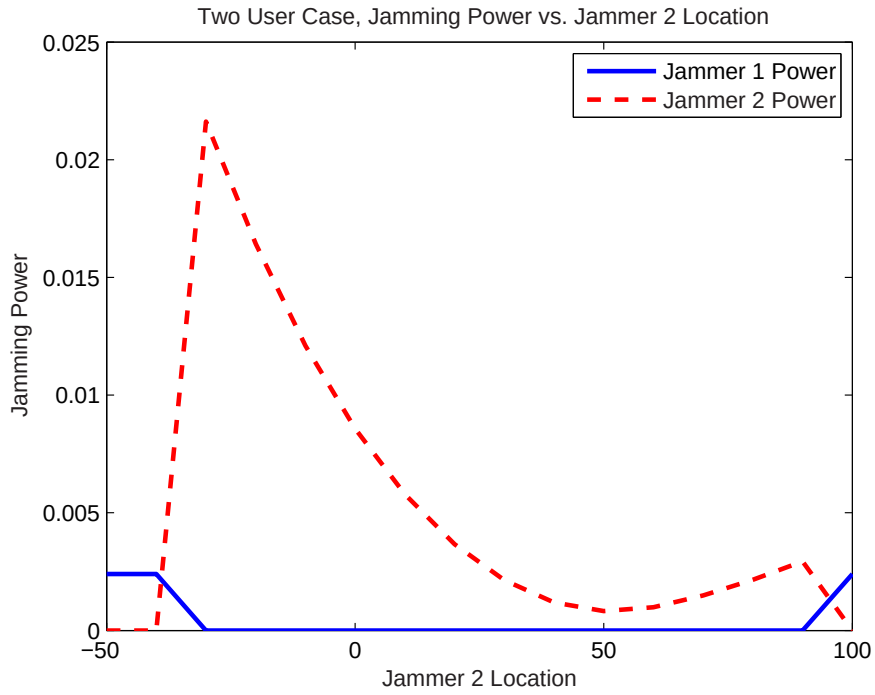


Fig. 8. Power vs. Jammer 2 Location

Information Sciences and Systems, Baltimore, MD, March 2007.

[7] R. Negi and S. Goelm "Secret communication using artificial noise," in Proc. of *IEEE Vehicular Technology Conference*, vol. 3, pp. 1906-1910, September 2005.

[8] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels." in Proc. of *IEEE International Symposium on Information Theory*, pp. 2152 - 2155, September 2005.

[9] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in Proc. of *IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[10] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels", *IEEE Transactions on Information Theory*, vol. 54, no. 6, p.p. 2470-2492, June 2008.

[11] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, to appear.

[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure collaborative beamforming", in Proc. of Allerton Conference on Communication, Control, and Computing, Allerton, IL, October 2008.

[13] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels", *IEEE Transactions on Information Theory*, Vol. 50, Issue: 9, Page: 2119- 2123, Sept. 2004.

[14] S. Shafiee and S. Ulukus, "Mutual information games in multi-user channels with correlated jamming", *http : //arxiv.org/abs/cs.IT/*0601110

[15] M. H. Brady, M. Mohseni, and J. M. Cioffi, "Spatially-correlated jamming in gaussian multiple access and broadcast channels", in Proc. of *40th Annual Conference on Information Sciences and Systems*, Princeton, NJ, March 2006.

[16] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information*

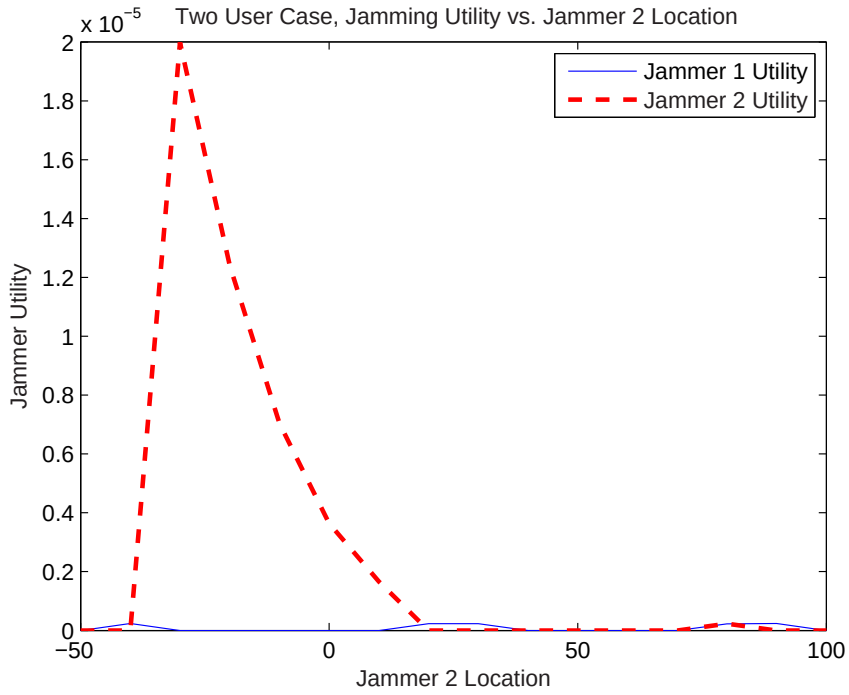


Fig. 9. Utility vs. Jammer 2 Location

Theory, to appear,

[17] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian Wiretap Channel With a Helping Interferer", in Proc. of *IEEE ISIT 2008*, Toronto, Ontario, Canada, Jul. 2008.

[18] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-Assisted Secret Communication", in Proc. of *IEEE ITW 2008*, Porto, Portugal, May 2008.

[19] D. Fudenberg and J. Tirole, *Game theory*, MIT Press, Cambridge, MA, 1991.

[20] C. U. Saraydar, N. B. Mandayam, and D. J. Goodman, "Efficient power control via pricing in wireless data networks", *IEEE Transations on Communications*, vol.50, no.2, p.p.291-303, Feburary 2002.

[21] G. Scutari, S. Barbarossa, and D. P. Palomar, "Potential games: a framework for vector power control problems with coupled constraints", in Proc. of *IEEE International Conference on Acoustics, Speech and Signal Processing, (ICASSP)*, Volume 4, Issue , 14-19 May 2006.

[22] 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 Proc. of *Annual IEEE Conference on Computer Communications, INFOCOM*, Anchorage, AK, May 2007.

[23] N. Bonneau, M. Debbah, E. Altman, and A. Hjørungnes, "Non-atomic games for multi-user systems" *IEEE Journal on Selected Areas in Communications*, issue on "Game Theory in Communication Systems", vol.26, no.7, p.p.1047-1058, September 2008.

[24] R. Yates, "A framework for uplink power control in cellular radio systems", *IEEE Journals on Selected Areas on Commununications*, vol.13, no.7, pp.1341-1348, September 1995.

[25] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge University Press, 2006. (http://www.stanford.edu/ ˜

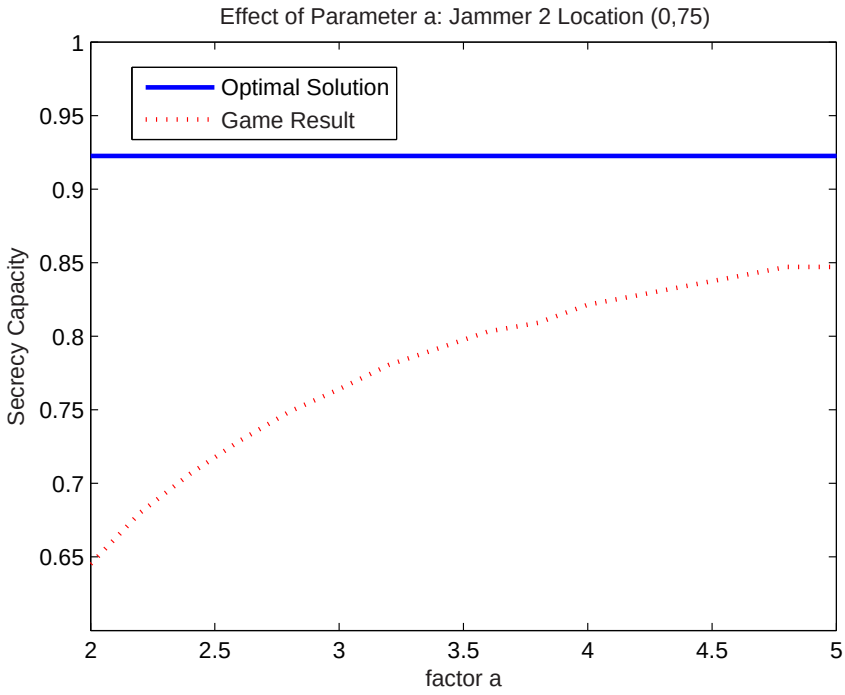


Fig. 10. Effect of Parameter a on the Game

boyd/cvxbook.html)

[26] Z. Han and K. J. R. Liu, *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications*, Cambridge University Press, UK, April, 2008.