SECRECY RATE OPTIMIZATION FOR A MIMO SECRECY CHANNEL BASED ON *STACKELBERG* GAME

Zheng Chu, Kanapathippillai Cumanan, Zhiguo Ding, Martin Johnston and Stéphane Le Goff

School of Electrical and Electronic Engineering, Newcastle University,
Newcastle Upon Tyne, NE1 7RU, UK.
{z.chu, Kanapathippillai.Cumanan, Zhiguo.Ding, martin.johnston and stephane.le-goff}@ncl.ac.uk

ABSTRACT

In this paper, we consider a multi-input-multi-output (MIMO) wiretap channel with a multi-antenna eavesdropper, where a private cooperative jammer is employed to improve the achievable secrecy rate. The legitimate user pays the legitimate transmitter for its secured communication based on the achieved secrecy rate. We first approximate the legitimate transmitter covariance matrix by employing Taylor series expansion, then this secrecy rate problem can be formulated into a *Stackelberg* game based on a fixed covariance matrix of the transmitter, where the transmitter and the jammer try to maximize their revenues. This secrecy rate maximization problem is formulated into a *Stackelberg* game where the jammer and the transmitter are the leader and follower of the game, respectively. For the proposed game, *Stackelberg* equilibrium is analytically derived. Simulation results are provided to show that the revenue functions of the legitimate user and the jammer are concave functions and the *Stackelberg* equilibrium solution has been validated.

***Index Terms*—** MIMO system, physical-layer secrecy, private jammer, game theory, *Stackelberg* game.

1. INTRODUCTION

The concept of physical-layer security was originally developed for wiretap channels in [1], and has recently been recognized as a promising technology to establish a secured data transmission between a legitimate transmitter and a legitimate receiver in wireless communication [2, 3].
The achievable secrecy rates in multi-antenna wiretap channels are constrained by the information rates achieved by the eavesdroppers. In order to further improve the secrecy rates, relays and jamming nodes have been introduced in the secrecy network, which have the capability of improving the performance at the legitimate receiver or preventing the eavesdroppers from intercepting the messages intended for the legitimate users [4, 5].
Secure communication systems consists of different nodes with different functionalities, and the interaction among these nodes can be naturally captured by applying game theory. Particularly, game theory provides a set of mathematical tools for the design of future wireless and communication networks, where different set of users cooperate to achieve an optimal solution or compete between each other to benefit selfishly [6–9]. *Stackelberg* game is one of the most important games, and has been applied in Femtocell networks [10], where the jammer is considered as the leader and the users follow the jammers decision to maximize their revenues. In addition, game theory has been widely used in security communications [11, 12].
This paper investigates a secrecy optimization problem where a private cooperative jammer is employed to provide a jamming service and improve the secrecy rate of the legitimate user. On the other hand, the legitimate user pays the legitimate transmitter for its secured communication based on the achieved secrecy rate. We formulate this problem into a *Stackelberg* game, where the transmitter and the private cooperative jammer try to maximize their revenues. For this game, we investigate a *Stackelberg* equilibrium solution where both the transmitter and the cooperative jammer come to an agreement on the interference requirement at the eavesdropper and the interference price.
The remainder of the paper is organized as follows. The system model and problem formulation are presented in section II. Section III solves the proposed *Stackelberg* game based secrecy rate maximization problem. Section IV provide the simulation results to support the proposed game, and finally conclusions are drawn in section V.
Notation: We use the upper case boldface letters for matrices and lower case boldface letters for vectors. The $(\cdot)^H$ denotes conjugate transpose, whereas $\mathrm{Tr}(\cdot)$ stands for trace of a matrix. $\mathbf{A} \succeq 0$ indicates that $\mathbf{A}$ is a positive

Zheng Chu, Kanapathippillai Cumanan, Zhiguo Ding, Martin Johnston and Stephane Le Goff are with the School of Electrical and Electronic Engineering, Newcastle University, Newcastle upon tyne, NE1 7RU, U.K. (Emails: z.chu@ncl.ac.uk; Kanapathippillai.Cumanan@ncl.ac.uk; Zhiguo.Ding@ncl.ac.uk; martin.johnston@ncl.ac.uk; stephane.le-goff@ncl.ac.uk).

semidefinite matrix. $\|\cdot\|_2$ denotes the Euclidean norm of a matrix. $\mathbf{I}$ and $(\cdot)^{-1}$ denote the identity matrix with appropriate size and the inverse of a matrix respectively, whereas $|\mathbf{A}|$ denotes the determinant of $\mathbf{A}$.

2. SYSTEM MODEL

We consider a secrecy network with a MIMO wiretap channel in the presence of a multi-antenna eavesdropper as shown in Figure 1, where a jammer is employed to improve the secrecy rate of the MIMO wiretap channel. It is assumed that the the channel between the jammer and the legitimate user is not available. The transmitter employs this private jammer to introduce the interference to the eavesdropper by paying for the jamming services. In addition, it is assumed that the legitimate transmitter,

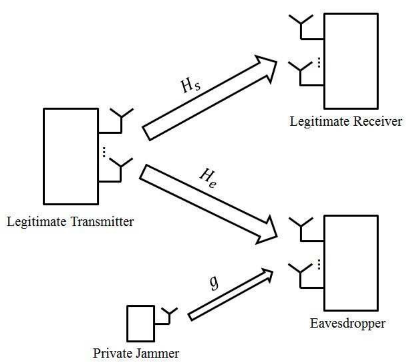

Fig. 1: A MIMO secrecy channel in the presence of multi-antenna eavesdropper and with a private cooperative jammer.

the legitimate receiver and the eavesdropper are equipped with N_T, M_R and M_E antennas, respectively, whereas the private jammer is equipped with only single antenna. The channel coefficients between the legitimate transmitter and the legitimate receiver as well as the eavesdropper are denoted by $\mathbf{H}_s \in \mathbb{C}^{\mathrm{M}_R\times\mathrm{N}_T}$ and $\mathbf{H}_e \in \mathbb{C}^{\mathrm{M}_E\times\mathrm{N}_T}$, respectively. On the other hand, $\mathbf{g} \in \mathbb{C}^{\mathrm{M}_E\times 1}$ represents the channel coefficients between the cooperative jammer and the eavesdropper. The received signals at the legitimate receiver and the eavesdropper can be expressed as follows:

$$\mathbf{y}_r = \mathbf{H}_s\mathbf{x}_1 + \mathbf{n}_r, \;\; \mathbf{y}_e = \mathbf{H}_e\mathbf{x}_1 + \mathbf{g}x_2 + \mathbf{n}_e,$$

where $\mathbf{y}_r$ and $\mathbf{y}_e$ denote the received signal at the legitimate receiver and the eavesdropper, respectively. In addition, $\mathbf{x}_1 \in \mathbb{C}^{N_T\times 1}$ is the signal intended for the legitimate user, whereas x_2 represents the jamming signal to confuse the eavesdropper. The vectors $\mathbf{n}_r \in \mathbb{C}^{M_R\times 1}$ and $\mathbf{n}_e \in \mathbb{C}^{M_E\times 1}$ are the noises at the legitimate receiver and the eavesdropper, and they are assumed to be zero-mean circularly symmetric Gaussian random variables with covariance matrices $\sigma_s^2\mathbf{I}$ and $\sigma_e^2\mathbf{I}$, respectively. The transmit covariance matrices of the transmitter is defined as $\mathbf{Q}_1 = \mathbb{E}\left\{\mathbf{x}_1\mathbf{x}_1^H\right\}$. Thus, the achievable secrecy rate is defined as follows:

$$R_s = \log|\mathbf{I}+\frac{1}{\sigma_s^2}\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H| - \log\frac{\left|\mathbf{I}+\frac{1}{\sigma_e^2}(\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H + p_1\mathbf{g}\mathbf{g}^H)\right|}{|\mathbf{I}+\frac{1}{\sigma_e^2}p_1\mathbf{g}\mathbf{g}^H|},$$

where p_1 is the power allocation at the jammer.

3. SECRECY RATE MAXIMIZATION BASED ON *STACKELBERG* GAME

In this section, we solve the secrecy rate maximization problem based on *Stackelberg* game in the security network as shown in Figure 1. This jammer introduces the interference to the eavesdropper which is listening the communication between the transmitter and the receiver. However, the private cooperative jammer charges for this jamming service based on the amount of interference caused to the eavesdropper. Here, we are only interested in optimizing the power allocation at the private jammer which determines the cost needed to be paid by the legitimate transmitter. Hence, the private jammer is considered with a single antenna. In the case of multiple antennas at the private jammer, the corresponding beamformer will be designed independently. Hence the scenario with multiple antennas with a fixed beamformer can be formulated into the same problem as with a single antenna. We formulate this problem into a *Stackelberg* game and then investigate the *Stackelberg* equilibrium for the proposed *Stackelberg* game [6].

3.1. Stackelberg Game

As shown in Figure 1, the objective of the private jammer is to maximize its revenue by selling the interference to the transmitter. The revenue of the jammer can be defined as follows:

$$U_j(p_1, \mu_0) = \mu_0 p_1 \|\mathbf{g}\|_2^2, \tag{1}$$

where μ_0 is the unit interference price charged by the private jammer to cause the interference to the eavesdropper. According to the interference requirement at the eavesdropper, the interference price should be decided by the jammer to maximize its revenue. The optimal interference price can be obtained by solving the following problem:

Problem (A):

$$\max_{p_1,\mu_0} \; U_j(p_1, \mu_0), \;\; s.t.\; p_1 \geq \mathbf{0}, \mu_0 \geq 0. \tag{2}$$

On the other hand, the legitimate transmitter should maximize its revenue by introducing the price for the achieved secrecy rate at the legitimate user. The revenue function of the transmitter can be defined as follows:

$$U_L(\mathbf{Q}_1,p_1)=\lambda_0 R_s-\mu_0 p_1\|\mathbf{g}\|_2^2=\lambda_0\Bigg(\log\left|\mathbf{I}+\frac{1}{\sigma_s^2}\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H\right| -\log\left|\mathbf{I}+\frac{1}{\sigma_e^2}(\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H+p_1\mathbf{g}\mathbf{g}^H)\right|\Bigg) +\lambda_0\log|\mathbf{I}+\frac{1}{\sigma_e^2}p_1\mathbf{g}\mathbf{g}^H|-\mu_0 p_1\|\mathbf{g}\|_2^2, \quad (3)$$

where λ_0 and R_s are the unit interference price and the achieved secrecy rate, respectively. Hence, the transmitter should design the transmit covariance matrix and decide the interference requirement to maximize its revenue. This problem can be formulated as follows:

Problem (B):

$$\max_{\mathbf{Q}_1,p_1} U_L(\mathbf{Q}_1,p_1),\ \ s.t.\ \mathbf{Q}_1\succeq\mathbf{0},p_1\geq\mathbf{0}. \quad (4)$$

Problem (A) and *Problem (B)* can form a *Stackelberg* game, where the cooperative jammer (leader) announces the interference price and then the legitimate transmitter (follower) decides the amount of the interference required at the eavesdropper. The solution of this game can be obtained by investigating the *Stackelberg* equilibrium points, where the legitimate transmitter and the cooperative jammer come to an agreement on the interference requirement and the interference price. The deviation of either the legitimate transmitter or the cooperative jammer from the equilibrium point will introduce the loss in their revenue functions.

3.2. Stackelberg Equilibrium

The *Stackelberg* equilibrium for the proposed game is defined as follows:

Stackelberg equilibrium: Let $\mathbf{Q}_1^*$ and p_1^* be the optimal solution for the *Problem (B)* where μ_0^* is the best price for the *Problem (A)*. The solutions $\mathbf{Q}_1^*$, p_1^* and μ_0^* define the *Stackelberg* equilibrium point if the following conditions are satisfied for any set of $\mathbf{Q}_1$, p_1 and μ_0:

$$\begin{aligned}&U_L(\mathbf{Q}_1^*,p_1^*,\mu_0^*)\geq U_L(\mathbf{Q}_1,p_1,\mu_0^*)\\&U_j(\mathbf{Q}_1^*,p_1^*,\mu_0^*)\geq U_j(\mathbf{Q}_1^*,p_1^*,\mu_0).\end{aligned} \quad (5)$$

3.3. Stackelberg Equilibrium Solution

In order to obtain the *Stackelberg* equilibrium solution, the best response of the follower (the legitimate transmitter) and the leader (the jammer) should be obtained by solving *Problem (B)* and *Problem (A)*, respectively. Since, the leader (the jammer) derives the optimal interference price for the interference requirement from the legitimate transmitter, the best response of the follower (the legitimate transmitter) should be first derived in terms of the interference price. For the proposed game, *Stackleberg* equilibrium can be derived by obtaining first $\mathbf{Q}_1^*$ and p_1^* from *Problem (B)*, and then by obtaining the best interference price μ_0^* from *Problem (A)*. The best response of the legitimate transmitter can be obtained by solving the problem in (4), which is not jointly convex in terms of $\mathbf{Q}_1$ and p_1. Hence, we divide this original problem into two sub-problems where transmit covariance matrix of the legitimate transmitter $\mathbf{Q}_1$ and the power allocations p_1 at the private cooperative jammer are determined separately for the proposed game.

First, we investigate the design of the covariance matrix of the legitimate transmitter $\mathbf{Q}_1$ without the jammer, where $\mathbf{Q}_1$ will be optimized by using Taylor series expansion [13]. Thus, we first rewrite the secrecy rate maximization problem without the jammer as follows:

$$\begin{aligned}\max_{\mathbf{Q}_1\succeq\mathbf{0}}\ &\log|\mathbf{I}+\frac{1}{\sigma_s^2}\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H|-\log|\mathbf{I}+\frac{1}{\sigma_e^2}\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H|\\ s.t.\ &\mathrm{Tr}(\mathbf{Q}_1)\leq P_1,\mathbf{Q}_1\succeq\mathbf{0}.\end{aligned} \quad (6)$$

The objective function of (6) which is not convex in terms of $\mathbf{Q}_1$, however, it can be approximated as follows:

$$\begin{aligned}\max_{\mathbf{Q}_1\succeq\mathbf{0}}\ \tilde{R}_s\approx\ &\log|\mathbf{I}+\frac{1}{\sigma_s^2}\mathbf{H}_s\mathbf{Q}_1\mathbf{H}_s^H|-\log\left|\mathbf{I}+\frac{1}{\sigma_e^2}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H\right|\\&-\mathrm{Tr}\left[\left(\mathbf{I}+\frac{1}{\sigma_e^2}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H\right)^{-1}\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H\right]\\&+\mathrm{Tr}\left[\left(\mathbf{I}+\frac{1}{\sigma_e^2}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H\right)^{-1}\mathbf{H}_e\tilde{\mathbf{Q}}_1\mathbf{H}_e^H\right],\\ s.t.\ \ &\mathrm{Tr}(\mathbf{Q}_1)\leq P_1,\mathbf{Q}_1\succeq\mathbf{0}.\end{aligned} \quad (7)$$

It can be easily verified that the problem in (7) is convex, and hence $\tilde{\mathbf{Q}}_1$ can be obtained iteratively by solving the problem (7). Here, we consider two initializations (i.e., $\tilde{\mathbf{Q}}_1=\mathbf{0}$). Based on this initialization, we propose an iterative algorithm to optimize the transmit covariance matrix $\mathbf{Q}_1$ in the following table:

Table I: Iterative algorithm for secrecy rate maximization

1. Initialize: $\tilde{\mathbf{Q}}_1=\mathbf{0}$.
2. **Repeat**
   (a) Solve the problem in (7) to obtain $\mathbf{Q}_1^*$.
   (b) Update $\tilde{\mathbf{Q}}_1\leftarrow\mathbf{Q}_1^*$.
3. **Until** the required accuracy.

By exploiting the iterative algorithm, we can obtain the solution of the problem in (7). Then we consider the solution of power allocation p_1 for a given $\mathbf{Q}_1$. To this end, the following lemma holds for a fixed $\mathbf{Q}_1$:

Lemma 1: The problem in (4) for a fixed $\mathbf{Q}_1$ is a convex problem in terms of p_1.

Proof: Please refer to [14]. ■

Since the problem in (4) is convex, the optimal solution p_1^* should satisfy the following KKT condition:

$$\frac{\partial U_L(\mathbf{Q}_1,p_1)}{\partial p_1}=0,\ \lambda_0\mathrm{Tr}[\mathbf{A}_1^{-1}\mathbf{g}\mathbf{g}^H-\mathbf{A}_2^{-1}\mathbf{g}\mathbf{g}^H]-\mu_0\|\mathbf{g}\|_2^2=0, \quad (8)$$

where

$$\mathbf{A}_1 = \left(\mathbf{I} + \frac{p_1}{\sigma_e^2}\mathbf{g}\mathbf{g}^H\right), \mathbf{A}_2 = \mathbf{I} + \frac{1}{\sigma_e^2}(\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H + p_1\mathbf{g}\mathbf{g}^H).$$

From the above KKT conditions in (8), we obtain the closed form solution of p_1 as follows:

$$p_1^* = \frac{-\frac{c_1+c_2}{\sigma_e^2} + \sqrt{\frac{(c_1-c_2)^2}{\sigma_e^4} + \frac{4\lambda_0 c_1 c_2 (c_1-c_2)}{\mu_0\|\mathbf{g}\|^2}}}{2\frac{c_1 c_2}{\sigma_e^4}}, \quad (9)$$

where $c_1 = \mathbf{g}^H\mathbf{g}$, $c_2 = \mathbf{g}^H\mathbf{A}^{-1}\mathbf{g}$ and $\mathbf{A} = \mathbf{I} + \frac{1}{\sigma_e^2}\mathbf{H}_e\mathbf{Q}_1\mathbf{H}_e^H$, and the proof is provided in [14]. Then, the best response of the private cooperative jammer can be obtained for a given interference requirement (i.e., p_1) by solving the following problem:

$$\max_{\mu_0} \; U_j(p_1^*, \mu_0), \quad s.t.\; \mu_0 \geq 0. \quad (10)$$

Since we have obtained the closed form solution of p_1 in (9), the optimal closed-form solution of μ_0 can be derived.

Lemma 2: The problem in (10) for a fixed $\mathbf{Q}_1$ is a convex problem in terms of μ_0, and the optimal solution of μ_0 can be expressed as

$$\mu_0^* = \frac{e}{x\|\mathbf{g}\|^2}, \quad (11)$$

where

$$\begin{aligned} x &= -\frac{\frac{d\|\mathbf{g}\|^2}{2a} - \frac{\frac{b^2\|\mathbf{g}\|^4}{4a^2} + \frac{b\|\mathbf{g}\|^2}{2a}\sqrt{\frac{(b^2-d)\|\mathbf{g}\|^4}{4a^2}}}{\frac{\|\mathbf{g}\|^2}{2a}}}{\frac{\|\mathbf{g}\|^2}{4a}} \\ &= -2(d - b^2 - b\sqrt{b^2-d}) \\ &= 2\sqrt{b^2-d}(\sqrt{b^2-d}+b) \quad (12) \end{aligned}$$

where $a = \frac{c_1 c_2}{\sigma_e^4}$, $b = \frac{c_1+c_2}{\sigma_e^2}$, $d = \frac{(c_1-c_2)^2}{\sigma_e^4}$ and $e = 4\lambda_0 c_1 c_2 (c_1 - c_2)$.

Proof: Please refer to [14]. ■

Hence, both revenue functions of the legitimate transmitter and the private jammer are concave in terms of p_1 and μ_0, respectively, for a fixed $\mathbf{Q}_1$. This confirms that there is a *Stackelberg* equilibrium (p_1^*, μ_0^*) for this game. To achieve this *Stackelberg* equilibrium, first, the jammer announces a relatively low interference price μ_0, for which the legitimate transmitter determines the optimal interference requirement at the eavesdropper. Then, the private jammer increases the interference price by a small amount provided its revenue function increases with the interference price. Otherwise, it will reduce the interference price by a small amount. This procedure will be carried out until the maximum of the jammer's revenue function is achieved which is a *Stackelberg* equilibrium solution. The deviation from this equilibrium point will cause loss to both the legitimate transmitter and the jammer. Hence, both of them will have the same strategy to maximize their revenues.

4. SIMULATION RESULTS

In order to validate our theoretical results and proposed algorithms, we consider a secrecy network in the presence of an eavesdropper as shown in Figure 1. To evaluate the performance of the proposed algorithms, it is assumed that the legitimate transmitter and the cooperative jammer are equipped with four ($\mathrm{N}_T = 4$) antennas whereas the legitimate receiver and the eavesdropper consist of three ($\mathrm{M}_R = \mathrm{M}_E = 3$) antennas. The maximum available transmission power at the legitimate transmitter is considered to be 5. The channel coefficients (i.e., $\mathbf{H}_s$, $\mathbf{H}_e$ and $\mathbf{g}$) are generated using zero-mean circularly symmetric independent and identically distributed Gaussian random variables. The noise covariance matrices at the legitimate receiver and the eavesdropper are assumed to be identity matrices.

We evaluate the *Stackelberg* equilibrium of the proposed game. Figure 2 depicts the revenue function of the legitimate user in terms of interference requirement of p_1. In addition, this result confirms that the revenue function of the legitimate user is concave in terms of p_1 with different channels. On the other hand, Figure 3 represents the revenue function of the private cooperative jammer for different interference prices. As observed in Figure 3, the revenue function of the private cooperative jammer is also concave in terms of μ_0. Figure 4 shows the optimal revenue function of the legitimate transmitter for a given μ_0^*, and then corresponding optimal value p_1^* can be obtained, hence, $(p1^*, \mu_0^*)$ defines the *Stackelberg* equilibrium point as indicated in Figure 4. In addition, the deviation of legitimate user or the private jammer from this equilibrium points will introduce loss in their revenue function.

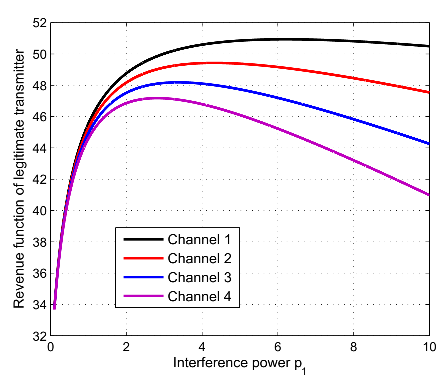

Fig. 2: Revenue function of the legitimate transmitter

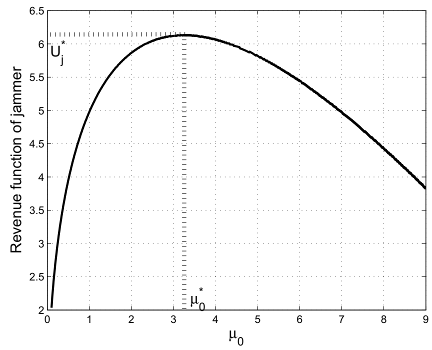

Fig. 3: Revenue function of the cooperative jammer

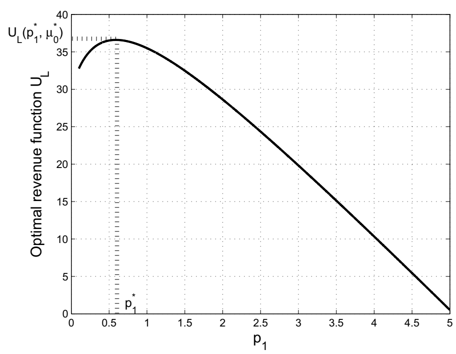

Fig. 4: Optimal revenue function of the legitimate transmitter

5. CONCLUSION

In this paper, a secrecy rate maximization game is proposed where a private cooperative jammer provides jamming service. This problem was formulated into a *Stackelberg* game and *Stackelberg* equilibrium solution is derived for the proposed game. Simulation results have been provided for the proposed *Stackelberg* game and these results confirm that both the revenue functions of the legitimate transmitter and the private cooperative jammer are concave and from which the *Stackelberg* equilibrium solution is obtained for the proposed game.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. Journ.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[3] Y. Liang, H. Vincent Poor, and Shlomo Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4-5, pp. 355–580, Apr. 2009.

[4] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[5] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs relay chatting," *IEEE Trans. Wireless Commun.*, vol. 29, no. 10, pp. 2067–2076, Jun. 2011.

[6] Z. Han, D. Niyato, and W. Saad, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*, Cambridge books online. Cambridge University Press, 2011.

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

[8] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Transa. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[9] A. Mukherjee and A.L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *Signal Processing, IEEE Transactions on*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[10] X. Kang, R. Zhang, and M. Motani, "Price-based resource allocation for spectrum-sharing femtocell networks: A *Stackelberg* game approach," *IEEE J. Sel. Topics in Commun.*, vol. 30, no. 3, pp. 538–549, 2012.

[11] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *Proc. Int. Conf. Game Theory for Networks, Istanbul, Turkey,*, May, 2009, pp. 287–294.

[12] Z. Han, Ninoslav Marina, Mérouane Debbah, and Are Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP J. Wirel. Commun.*, vol. 2009, no. 11, pp. 1–10, May., 2009.

[13] K. Cumanan, Z. Ding, B. Sharif, G.Y. Tian, and K.K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Vehicular Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[14] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *Accepted by IEEE Trans. Vehicular Technol. with minor correction*.