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 consist 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 Tr$(\cdot)$ stands for trace of a matrix. $A \succeq 0$ indicates that $A$ is a positive
semidefinite matrix. \( \| \cdot \|_2 \) denotes the Euclidean norm of a matrix. \( I \) and \((\cdot)^{-1}\) denote the identity matrix with appropriate size and the inverse of a matrix respectively, whereas \(|A|\) denotes the determinant of \( A \).

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 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, the legitimate receiver and the eavesdropper are equipped with antennas, respectively, whereas the private jammer is equipped with single antenna. The channel coefficients between the legitimate transmitter and the legitimate receiver as well as the eavesdropper are denoted by \( H_t \in \mathbb{C}^{M_T \times N_T} \) and \( H_e \in \mathbb{C}^{M_E \times N_T} \), respectively. On the other hand, \( g \in \mathbb{C}^{M_T \times 1} \) 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:

\[
y_s = H_s x_1 + n_s, \quad y_e = H_e x_1 + g x_2 + n_e,
\]

where \( y_s \) and \( y_e \) denote the received signal at the legitimate receiver and the eavesdropper, respectively. In addition, \( x_1 \in \mathbb{C}^{N_T \times 1} \) is the signal intended for the legitimate user, whereas \( x_2 \) represents the jamming signal to confuse the eavesdropper. The vectors \( n_s \in \mathbb{C}^{M_T \times 1} \) and \( n_e \in \mathbb{C}^{M_E \times 1} \) 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 \( \sigma_s^2 I \) and \( \sigma_e^2 I \), respectively. The transmit covariance matrices of the transmitter is defined as \( Q_1 = E \{ x_1 x_1^H \} \). Thus, the achievable secrecy rate is defined as follows:

\[
R_s = \log |I_1 - \frac{1}{\sigma_s^2} H_s Q_1 H_s^H| + \log |I_1 - \frac{1}{\sigma_e^2} H_e Q_1 H_e^H + p_1 g g^H|,
\]

where \( p_1 \) is the power allocation at the jammer.

3. SECURITY 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:

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

where \( \mu_0 \) 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): \[
\text{max}_{p_1, \mu_0} \ U_j(p_1, \mu_0), \quad \text{s.t.} \ p_1 \geq 0, \mu_0 \geq 0. \tag{2}
\]

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

---

**Fig. 1:** A MIMO secrecy channel in the presence of multi-antenna eavesdropper and with a private cooperative jammer.
of the transmitter can be defined as follows:
\[
U_L(Q_1, p_1) = \lambda_0 R_s - \mu_0 p_1 \|g\|^2 = \lambda_0 \left( \log \left| I + \frac{1}{\sigma_0^2} H, Q_1 H^H \right| \right.
- \log \left| I + \frac{1}{\sigma_0^2} (H, Q_1 H^H + p_1 g g^H) \right| \\
+ \lambda_0 \log \left| I + \frac{1}{\sigma_0^2} p_1 g g^H \right| - \mu_0 p_1 \|g\|^2.
\] (3)

where \( \lambda_0 \) 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):
\[
\max_{Q_1, p_1} U_L(Q_1, p_1), \quad s.t. \quad Q_1 \succeq 0, p_1 \geq 0.
\] (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 \( Q_1^* \) and \( p_1^* \) be the optimal solution for the Problem (B) where \( \mu_0^* \) is the best price for the Problem (A). The solutions \( Q_1^* \), \( p_1^* \) and \( \mu_0^* \) define the Stackelberg equilibrium point if the following conditions are satisfied for any set of \( Q_1, p_1 \) and \( \mu_0 \):
\[
\forall Q_1, p_1 \in (Q_1, p_1, \mu_0) \ni U_L(Q_1, p_1, \mu_0) \\
\forall Q_1, p_1, \mu_0 \ni U_L(Q_1, p_1, \mu_0) \geq U_L(Q_1^*, p_1^*, \mu_0^*).
\] (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, Stackelberg equilibrium can be derived by obtaining first \( Q_1^* \) and \( p_1^* \) from Problem (B), and then by obtaining the best interference price \( \mu_0^* \) 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 \( Q_1 \) and \( p_1 \). Hence, we divide this original problem into two sub-problems where transmit covariance matrix of the legitimate transmitter \( Q_1 \) 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 \( Q_1 \) without the jammer, where \( Q_1 \) will be optimized by using Taylor series expansion [13]. Thus, we first rewrite the secrecy rate maximization problem without the jammer as follows:
\[
\max_{Q_1 \geq 0} \log |I + \frac{1}{\sigma_0^2} H, Q_1 H^H| - \log |I + \frac{1}{\sigma_0^2} H, Q_1 H^H| - \mu_0 p_1 \|g\|^2 = 0.
\] (6)

The objective function of (6) which is not convex in terms of \( Q_1 \), however, it can be approximated as follows:
\[
\max_{Q_1 \geq 0} \tilde{R}_s \approx \log |I + \frac{1}{\sigma_0^2} H, Q_1 H^H| - \log |I + \frac{1}{\sigma_0^2} H, Q_1 H^H| - \mu_0 p_1 \|g\|^2
\] (7)

It can be easily verified that the problem in (7) is convex, and hence \( Q_1 \) can be obtained iteratively by solving the problem (7). Here, we consider two initializations (i.e., \( Q_1 = 0 \)). Based on this initialization, we propose an iterative algorithm to optimize the transmit covariance matrix \( Q_1 \) in the following table:

<table>
<thead>
<tr>
<th>Table 1: Iterative algorithm for secrecy rate maximization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Initialize: ( Q_1 = 0 ).</td>
</tr>
<tr>
<td>2. Repeat</td>
</tr>
<tr>
<td>(a) Solve the problem in (7) to obtain ( Q_1^* ).</td>
</tr>
<tr>
<td>(b) Update ( Q_1 \leftarrow Q_1^* ).</td>
</tr>
<tr>
<td>3. Until the required accuracy.</td>
</tr>
</tbody>
</table>

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 \( Q_1 \). To this end, the following lemma holds for a fixed \( Q_1 \):

**Lemma 1:** The problem in (4) for a fixed \( Q_1 \) 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:
\[
\frac{\partial U_L(Q_1^*, p_1^*)}{\partial p_1} = 0, \quad \lambda_0 \text{Tr}[A_1^{-1} g g^H - A_2^{-1} g g^H] - \mu_0 \|g\|^2 = 0.
\] (8)
where

\[ A_1 = \left( I + \frac{p_1}{\sigma_c^2} g g^H \right), A_2 = I + \frac{1}{\sigma_c^2} (H_e Q_1 H_e^H + p_1 g g^H). \]

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

\[
p_1^* = \frac{-c_1 + c_2}{\sigma_c^2} + \sqrt{\frac{(c_1 - c_2)^2}{\sigma_c^2} + \frac{4\lambda_0 c_1 c_2 (c_1 - c_2)}{\mu_0 ||g||^2}}, \tag{9}
\]

where \( c_1 = g^H g, c_2 = g^H A^{-1} g \) and \( A = I + \frac{1}{\sigma_c^2} H_e Q_1 H_e^H \), 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:

\[
\max_{\mu_0} U_j (p_1^*, \mu_0), \quad \text{s.t.} \quad \mu_0 \geq 0. \tag{10}
\]

Since we have obtained the closed form solution of \( p_1 \) in (9), the optimal closed-form solution of \( \mu_0 \) can be derived.

**Lemma 2:** The problem in (10) for a fixed \( Q_1 \) is a convex problem in terms of \( \mu_0 \), and the optimal solution of \( \mu_0 \) can be expressed as

\[
\mu_0^* = \frac{e}{x ||g||^2}, \tag{11}
\]

where

\[
x = -\frac{d ||g||^2 - \frac{c_1 + c_2}{\sigma_c^2} + \frac{a}{2} ||g||^2 \sqrt{2d^2 - d ||g||^2}}{\frac{2a}{\sigma_c^2} ||g||^2}, \]

\[
= -2(d - b^2 - b\sqrt{b^2 - d})
\]

\[
= 2\sqrt{b^2 - d}(\sqrt{b^2 - d} + b) \tag{12}
\]

where \( a = \frac{c_1 c_2}{\sigma_c^2}, b = \frac{c_1 + c_2}{\sigma_c^2}, d = \frac{(c_1 - c_2)^2}{\sigma_c^2} \) 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 \( \mu_0 \), respectively, for a fixed \( Q_1 \). This confirms that there is a Stackelberg equilibrium \((p_1^*, \mu_0^*)\) for this game. To achieve this Stackelberg equilibrium, first, the jammer announces a relatively low interference price \( \mu_0 \), 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 \((N_T = 4)\) antennas whereas the legitimate receiver and the eavesdropper consist of three \((M_R = M_E = 3)\) antennas. The maximum available transmission power at the legitimate transmitter is considered to be 5. The channel coefficients (i.e., \( H_e, H_l \) and \( g \)) 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 \( \mu_0 \). Figure 4 shows the optimal revenue function of the legitimate transmitter for a given \( \mu_0^* \), and then corresponding optimal value \( p_1^* \) can be obtained, hence, \((p_1^*, \mu_0^*)\) 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.
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


