# Secure Multicast Communications with Private Jammers

Kanapathippillai Cumanan[†], Zhiguo Ding[‡], Mai Xu[⋆], and H. Vincent Poor[§]
[†] Department of Electronics, University of York, York, YO10 5DD, UK.
[‡] School of Computing and Communications, Lancaster University, Lancaster, UK.
[⋆] Department of Electrical Engineering, Beihang University, China.
[§] Department of Electrical Engineering, Princeton University, Princeton, NJ, USA.



***Abstract*—This paper investigates secrecy rate optimization for a multicasting network, in which a transmitter broadcasts the same information to multiple legitimate users in the presence of multiple eavesdroppers. In order to improve the achievable secrecy rates, private jammers are employed to generate interference to confuse the eavesdroppers. These private jammers charge the legitimate transmitter for their jamming services based on the amount of interference received at the eavesdroppers. Therefore, this secrecy rate maximization problem is formulated as a Stackelberg game, in which the private jammers and the transmitter are the leaders and the follower of the game, respectively. A fixed interference price scenario is considered first, in which a closed-form solution is derived for the optimal amount of interference generated by the jammers to maximize the revenue of the legitimate transmitter. Based on this solution, the Stackelberg equilibrium of the proposed game, at which both legitimate transmitter and the private jammers achieve their maximum revenues, is then derived. Simulation results are also provided to validate these theoretical derivations.**

## I. Introduction

The concept of information theoretic security was first investigated in [1] for wiretap channels by defining the concept of the secrecy capacity. Since then, information theoretic security has received considerable attention due to its low complexity implementation and suitability for the dynamic configurations of wireless networks, in which the physical layer characteristics of wireless channels are exploited to establish secure communication between legitimate terminals. This novel paradigm complements the conventional cryptographic methods implemented in the upper networking layers by providing additional security at the physical layer.

Multi-antenna terminals have the potential to enhance the performance of secret communications by exploiting spatial degrees of freedom. However, the secrecy rates which are achievable by using multi-antenna terminals are still limited by the quality of the wireless channels between the legitimate transmitter and the receivers, including the legitimate receivers and the eavesdroppers [2]–[7]. The existing works in [3], [8], [9] demonstrate that the performance of secret communications can be further improved by using cooperative jamming and artificial noise techniques, in which jamming signals are transmitted from external jammers or integrated with the information bearing signals sent by the legitimate transmitter. These approaches effectively degrade the capability of the eavesdroppers for retrieving the legitimate users' signals, and hence enhance the achievable secrecy rates.

Recently, game theoretic approaches have been applied to the resource allocation problems in wireless secret communication networks [10]–[18]. In [10], a zero-sum game was formulated for a secret communication network by considering the signal-to-interference-plus-noise rate (SINR) difference between the legitimate receiver and the eavesdropper as the utility function. The interaction among the nodes in cognitive radio networks has been investigated by using the Stackelberg game [11]. Cooperative game theory has been used to improve the secrecy capacity of ad-hoc networks in [13], and a distributed tree formation game was proposed for multihop wireless networks in [12]. Physical layer security has been investigated through a Stackelberg game for a two-way relaying network with unfriendly jammers in [14], and a distributed auction based approach has been used to enhance the secrecy capacity in [15]. Jamming games have been formulated for multiple-input multiple-output (MIMO) wiretap channels with an active eavesdropper in [16], and a secrecy game for a Gaussian multiple-input single-output (MISO) interference channel has been investigated in [17].

In this paper, a multicating network is considered as shown in Fig. 1, where all the legitimate users are to receive the same information in the presence of multiple eavesdroppers. In order to improve the achievable secrecy rates of the legitimate users, the private jammers are employed to generate artificial noise and confuse the eavesdroppers. These private jammers introduce the costs for their jamming services based on the amount of interference generated to the eavesdroppers. To compensate these jamming costs, the legitimate users pay the transmitter for their enhanced secret communications. Based on these interactions between the legitimate transceivers and the private jammers, we formulate the secrecy rate maximization problem as a Stackelberg game. A fixed interference price scenario is considered first and then a closed-form solution for the optimal amount of interference generated to each eavesdropper is obtained. Based on this solution, we then investigate the corresponding Stackelberg equilibrium for the formulated game. In addition, simulation results are provided to validate the theoretical derivations of the proposed game theoretic approach.

## II. System Model

A secret communication network with $K$ legitimate users, $L$ eavesdroppers and $L$ private jammers is considered in this paper, as shown in Fig.1, where the transmitter broadcasts a common message to be received by all the legitimate users in the presence of multiple eavesdroppers. In this secure network, the transmitter is equipped with $N_T$ transmit antennas, whereas the legitimate users and the eavesdroppers are equipped with a single receive antenna, respectively. The channel coefficients between the legitimate transmitter and the $k^{\text{th}}$ legitimate user as well as the $l^{\text{th}}$ eavesdropper are denoted by $\mathbf{h}_k \in \mathbb{C}^{N_T \times 1}$ and $\mathbf{g}_l \in \mathbb{C}^{N_T \times 1}$, respectively.

In addition, a set of private (friendly) jammers are employed to provide jamming services as shown in Fig.1. These private jammers generate artificial interference to confuse the eavesdroppers and they ensure that there is no interference leakage to the legitimate users. This is achieved by appropriately designing the beamformers at the jammers and employing a dedicated jammer near to each eavesdropper. Since, a dedicated jammer is closely located to the corresponding eavesdropper, each eavesdropper receives strong co-channel interference from its corresponding private jammer.

Note that these private jammers charge the legitimate transceivers for their dedicated jamming services based on the amount of interference generated to each eavesdropper. To compensate these interference costs, the legitimate transmitter introduces the charges to the legitimate users for their enhanced secure communications, by using the achievable secrecy rates as the criteria. The channel gain between the $l^{\text{th}}$ eavesdropper and the corresponding jammer is denoted by $|g_{jl}|^2$. Furthermore, it is assumed that the legitimate transmitter and the jammers have the perfect channel state information of the eavesdroppers. This assumption is appropriate in a multicasting network, where potential eavesdroppers are also legitimate users of the network. This assumption has been commonly used in the literature [19]–[21]. The achievable secrecy rate at the $k^{\text{th}}$ user can be written as follows: [22]

$$R_k = \left[\log\left(1+\frac{\mathbf{w}^H\mathbf{h}_k\mathbf{h}_k^H\mathbf{w}}{\sigma_k^2}\right) - \max_{1\le l\le L}\log\left(1+\frac{\mathbf{w}^H\mathbf{g}_l\mathbf{g}_l^H\mathbf{w}}{\sigma_e^2+p_k|g_{jk}|^2}\right)\right]^+, \tag{1}$$

where $\mathbf{w} \in \mathbb{C}^{N_T \times 1}$ and $p_k$ are the beamformer at the legitimate transmitter and the power allocation coefficient for the $k^{\text{th}}$ private jammer, respectively. The $\sigma_k^2$ as well as $\sigma_e^2$ denote the noise variances at the $k^{\text{th}}$ legitimate user and the eavesdropper, respectively, and $[x]^+$ represents $\max\{x, 0\}$.

## III. Game Theoretic Approach for Secrecy Rate Optimization

In this section, we formulate the secrecy rate maximization problem into a Stackelberg game and then investigate the Stackelberg equilibrium for the proposed game. This game consists of two sets of players: a) leader and b) followers. All these players try to maximize their revenues, where the leaders first make a move and the followers will choose their strategies according to the leaders' decisions. In the multicasting

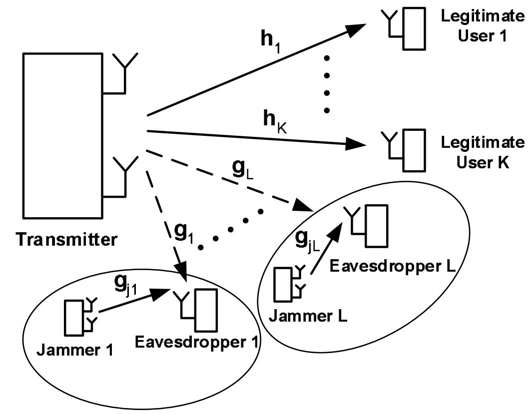


Fig. 1: A multicasting secure network with $K$ legitimate users, $L$ eavesdroppers and $L$ private jammers.

network considered in this paper, the private jammers (leaders) announce their interference prices and then the legitimate transmitter (follower) determines the interference requirements according to the interference prices.

The interference received at the $l^{\text{th}}$ eavesdropper from the corresponding private jammer can be written as follows:

$$I_l = p_l|g_{jl}|^2. \tag{2}$$

Here, we are only interested in the transmit power used by the jammer, where the beamformer at the jammer is appropriately designed to ensure that there is no interference leakage to the legitimate users. The private jammers aim to maximize their revenues by selling interference to the transmitter. The revenue of the $l^{\text{th}}$ private jammer can be written as follows:

$$\phi_l(\mu_l) = \mu_l p_l |g_{jl}|^2, \tag{3}$$

where $\mu_l$ is the unit interference price charged by the corresponding jammer to cause interference at the $l^{\text{th}}$ eavesdropper. Depending on the interference requirement at the $l^{\text{th}}$ eavesdropper, the interference price should be determined by the corresponding jammer to maximize its revenue. These interference prices can be determined by solving the following optimization problem:

$$\text{Problem (A):} \quad \max_{\boldsymbol{\mu}\succeq\mathbf{0}} \sum_{l=1}^{L}\phi_l(\mu_l, p_l), \tag{4}$$

where $\boldsymbol{\mu} = [\mu_1 \cdots \mu_L]$ includes the interference prices.

On the other hand, the transmitter aims to maximize its revenue by charging the legitimate users based on their achievable secrecy rates, where the revenue function at the transmitter can be written as follows:

$$\psi_L(\mathbf{p}, \boldsymbol{\mu}) = \sum_{k=1}^{K}\lambda_k R_k - \sum_{l=1}^{L}\mu_l p_l |g_{jl}|^2, \tag{5}$$

where $\lambda_k$ and $R_k$ are the unit price for the secrecy rate and the achievable secrecy rate at the $k^{\text{th}}$ user, respectively. It is assumed that the unit price for each user is fixed at a predetermined value. Hence, the transmitter should determine the beamforming vector as well as the interference requirements at different eavesdroppers in order to maximize its revenue. We first focus on the interference requirements at each eavesdropper with a fixed beamformer at the transmitter, which can be formulated into an optimization problem as follows:

$$\text{Problem (B):} \quad \max_{\mathbf{p}\succeq 0} \quad \psi_L(\mathbf{p}, \boldsymbol{\mu}), \tag{6}$$

where $\mathbf{p} = [p_1 \cdots p_L]$ represents the power allocation coefficients at all jammers. *Problem (A)* and *Problem (B)* form a Stackelberg game, and it is important to investigate the corresponding Stackelberg equilibrium.

### A. Stackelberg Equilibrium

The Stackelberg equilibrium for the proposed game is defined as follows:
Stackelberg equilibrium: Let $\mathbf{p}^*$ be the optimal solution for *Problem (B)* whereas $\boldsymbol{\mu}^*$ contains the best prices for *Problem (A)*. The solutions $\mathbf{p}^*$ and $\boldsymbol{\mu}^*$ define the Stackelberg equilibrium point if the following conditions are satisfied for any set of $\mathbf{p}$ and $\boldsymbol{\mu}$:

$$\psi_L(\mathbf{p}^*, \boldsymbol{\mu}^*) \geq \psi_L(\mathbf{p}, \boldsymbol{\mu}^*), \ \ \phi_l(p_l^*, \mu_l^*) \geq \phi_l(p_l^*, \mu_l), \forall \ l.$$

## IV. Stackelberg Equilibrium Solution

In this section, we derive the Stackelberg equilibrium solution for the proposed game. In order to analyze this equilibrium, the best response of the transmitter is first derived in terms of the interference requirement at each eavesdropper for fixed interference prices. Then, the optimal interference prices for the private jammers are obtained to maximize their revenues. These best responses can be derived by solving *Problem (A)* and *Problem (B)*. Particularly, we first solve the problem for a scenario with fixed interference prices. Based on this solution, we then derive the Stackelberg equilibrium for the proposed game. Note that we only consider the secure communication network with a single legitimate user and multiple eavesdroppers. However, this can be easily extended for a scenario with multiple legitimate users and multiple eavesdroppers.

### A. Fixed Interference Prices

In this subsection, we focus on the fixed interference price scenario with a single legitimate user and multiple eavesdroppers. Note that for a particular user, eavesdroppers with large achievable rates are more damaging since they significantly reduce the secrecy rate of this legitimate user. Therefore, introducing jamming to these eavesdroppers will effectively improve the achievable secrecy rate of the legitimate user. Therefore, a set of eavesdroppers which have strong connections to the source are defined as super-active eavesdroppers. The rest of the eavesdroppers are referred as non-super-active eavesdroppers. The achievable secrecy rate of the legitimate user is defined as follows:

$$R_1 = \log(1+\beta_0) - \max_{1\leq i\leq L} \log\left(1 + \frac{\beta_i}{\sigma_e^2 + p_i\alpha_i}\right), \tag{7}$$

where

$$\beta_0 = \frac{\mathbf{w}^H\mathbf{h}_1\mathbf{h}_1^H\mathbf{w}}{\sigma^2}, \quad \beta_i = \mathbf{w}^H\mathbf{g}_i\mathbf{g}_i^H\mathbf{w}, \ \alpha_i = |g_{ji}|^2. \tag{8}$$

The optimal interference requirements at each eavesdropper can be formulated as follows:

$$\max_{\mathbf{p}\succeq\mathbf{0}} \ \lambda_1 R_1 - \sum_{i\in\mathbb{K}} \mu_i p_i \alpha_i, \tag{9}$$

where vector $\mathbf{p} = [p_1 \cdots p_K]$ includes the power allocation coefficients of the private jammers in the set $\mathbb{K}$ consisting of all super-active eavesdroppers. Without loss of generality, this problem can be reformulated as follows:

$$\begin{aligned} \max_{\mathbf{p}\succeq\mathbf{0}, \ t_i, \ t_0} \ & \lambda_1 \left[\log(1+\beta_0) - t_0\right] - \sum_{i=1}^{K} \mu_i p_i \alpha_i \\ \text{s.t.} \ & \log\left(1 + \frac{\beta_i}{\sigma_e^2 + p_i\alpha_i}\right) \leq t_i, \ \forall \ k \\ & \max\{t_1, \cdots, t_K\} = t_0, \ \forall \ k, \ t_i \geq 0, \ \forall \ k. \end{aligned} \tag{10}$$

This problem is convex with respect to the power allocation coefficients at the private jammers and can be efficiently solved through interior point methods [23].

*Proposition 1*: By using the optimal solution of (10), the achievable rates of the super-active eavesdroppers (i.e., $t_i, \ i \in \mathbb{K}$) will be equal and the power allocation coefficients of the non-super-active eavesdroppers (i.e., $i \notin \mathbb{K}$) will be all zeros.

*Proof*: Assume that $t_i, \ i \in \mathbb{K}$ are not equal. Assume that the minimum $t_i = t_{min} < t_0$ from all $t_i, \ i = 1, \cdots, K$, and the corresponding $p_i$ will be higher than that of $t_{min} = t_0$. Hence, the revenue of the transmitter (cost function of (10)) with $t_i = t_{min}$ will be less than that with $t_i = t_0$. Thus, the achievable rates of the super-active eavesdroppers (i.e., $t_i, \ i \in \mathbb{K}$) will be equal when the optimal solution is used and the power allocation coefficients for the non-super-active eavesdroppers (i.e., $i \notin \mathbb{K}$) will be zero.■

Hence, the optimal interference requirements can be obtained by solving the convex problem in (10).

### B. Stackelberg Game

In this subsection, we formulate the problem into a Stackelberg game and investigate the Stackelberg equilibrium for the proposed game. In order to derive the equilibrium of the game, the best responses of both the leaders and the follower should be obtained. The best response of the legitimate transmitter can be obtained by solving the following problem:

$$\max_{\mathbf{p}\succeq\mathbf{0}} \ \lambda_1 R_{SL-ME} - \sum_{i\in\mathbb{K}} \mu_i p_i \alpha_i, \tag{11}$$

where the vector $\mathbf{p} = [p_1 \cdots p_K]$ consists of the power allocation coefficients of the private jammers in the super-active eavesdropper set $\mathbb{K}$. As we discussed in the previous subsection in (10), this problem is convex and the optimal power allocation can be obtained. Furthermore, the closed-form solution of this power allocation problem should be determined by deriving the Stackelberg equilibrium of the proposed game, as shown in the following lemma.

*Lemma 1:* The optimal power allocation coefficient at the $i^{\text{th}}$ jammer is given by

$$p_i^* = \frac{1}{\alpha_i}\left[\frac{\beta_i}{\gamma_0} - \sigma_e^2\right]^+, \tag{12}$$

where

$$\begin{aligned}\beta_i &= \mathbf{w}^H \mathbf{g}_i \mathbf{g}_i^H \mathbf{w} \\ \gamma_0^* &= \frac{\sum_{i=1}^K \mu_i\beta_i + \sqrt{\sum_{i=1}^K \mu_i\beta_i \left(4\lambda_1 + \sum_{i=1}^K \mu_i\beta_i\right)}}{2\lambda_1}\end{aligned} \tag{13}$$

*Proof:* Please refer to Appendix A. ■

The private jammers need to announce their interference prices to maximize their revenues. These optimal interference prices can be obtained by solving the following problem:

$$\max_{\boldsymbol{\mu}\succeq\mathbf{0}} \sum_{l=1}^{L} \phi_i(p_i^*, \mu_i) = \sum_{l=1}^{L} \mu_i p_i^* \alpha_i. \tag{14}$$

Based on the closed-form solution of the optimal power allocation coefficients $p_i^*$s in (12) in terms of the interference prices $\mu_i$s, the optimal interference prices problem can be reformulated as

$$\max_{\boldsymbol{\mu}\succeq\mathbf{0}} \frac{2\lambda_1 \sum_{i=1}^K \mu_i\beta_i}{\sum_{i=1}^K \mu_i\beta_i + \sqrt{\sum_{i=1}^K \mu_i\beta_i \left(4\lambda_1 + \sum_{i=1}^K \mu_i\beta_i\right)}} - \sigma_e^2 \sum_{i=1}^{K} \mu_i. \tag{15}$$

The optimal interference prices $\mu_i$s can be obtained by solving the above problem through existing numerical methods. However, the closed-form solutions of these interference prices are not easy to derive. Therefore, we assume the use of the same interference price (uniform interference price) for all private jammers (i.e., $\mu_1 = \mu_2 = \cdots = \mu_K = \mu_0$). The problem in (15) can be formulated with the uniform interference price as follows:

$$\max_{\mu_0\geq 0} \frac{2\lambda_1\mu_0 \sum_{i=1}^K \beta_i}{\mu_0\sum_{i=1}^K \beta_i + \sqrt{\mu_0\sum_{i=1}^K \beta_i \left(4\lambda_1 + \mu_0\sum_{i=1}^K \beta_i\right)}} - K\sigma_e^2\mu_0. \tag{16}$$

*Lemma 2:* The optimal interference price $\mu_0^*$ in (16) is given by

$$\mu_0^* = \frac{0.5\left[-4\lambda_1 K\sigma^2\eta_1 + 2\lambda_1\sqrt{K\sigma^2\eta_2 + 4K^2\sigma^4\eta_1^2}\right]}{K\sigma^2\eta_2} \tag{17}$$

where

$$\eta_1 = \left(1 + \frac{K\sigma^2}{\bar{c}_2}\right),\ \eta_2 = \left(\bar{c}_2 + K\sigma^2\right),\ \bar{c}_2 = \sum_{i=1}^{K} \beta_i. \tag{18}$$

*Proof:* Please refer to Appendix B. ■

Hence, the Stackelberg equilibrium of the proposed game with uniform interference price can be defined by ($p_i^*\ \forall\ i, \mu_0^*$), at which both the transmitter and the private jammers maximize their revenues.

## V. Simulation Results

In this section, we validate the derived theoretical results by using computer simulations. Here, we consider a multicasting network with a single legitimate user and two eavesdroppers, where the transmitter broadcasts the same information to all the legitimate users in the presence of multiple eavesdroppers. In addition, private jammers are employed to confuse the eavesdroppers by introducing interference, which will improve the achievable secrecy rates of the legitimate users. It is assumed that the legitimate transmitter is equipped with three antennas whereas the legitimate user and the eavesdroppers have a single antenna. The channel coefficients between all the terminals are generated through zero-mean circularly symmetric independent and identically distributed complex Gaussian random variables and the noise variance at all the terminals is assumed to be 0.1. In the following subsections, we provide simulation results for the scenario with the fixed interference prices and the Stackelberg game scenario, respectively.

### A. Fixed Interference Prices

In this subsection, we evaluate the performance of the proposed schemes with fixed interference prices at the private jammers. The fixed unit interference prices at the jammers are assumed to be 1 and 3 (i.e., $\mu_1 = 1,\ \mu_2 = 3$), respectively. Table 1 provides the theoretical and simulation based optimal power allocation coefficients and the corresponding revenues of the legitimate transmitter for different sets of channels. These results validate the derivation of the theoretical results which are indistinguishable with the simulation based results.

### B. Stackelberg Game

In this subsection, we validate the derived Stackelberg equilibrium of the proposed game. Table 2 provides the derived theoretical Stackelberg equilibrium and the simulation based one, as well as the corresponding jammer revenues with the uniform interference price assumption (i.e., $\mu_1 = \mu_2 = \mu_0$) for different sets of channels. The simulation results are consistent to the theoretical ones and validate the Stackelberg equilibrium of the proposed game for different sets of channels. It is worth pointing out that any deviations from these equilibria caused by different strategies of the legitimate transmitter and the jammers will introduce loss in their revenues.

## VI. Conclusions

In this paper, we studied the secrecy rate optimization problem for a multicasting network, where multiple users are to receive the same information in the presence of multiple eavesdroppers. To improve the secrecy rate performance, private jammers were employed to generate interference to the eavesdroppers. In addition, these jammers charge the legitimate transceivers for their jamming services. This optimization

| Channels | Power Allocation: Jammer 1 | | Power Allocation: Jammer 2 | | Achieved Secrecy Rate | | Revenue: Legitimate Transmitter | |
|---|---|---|---|---|---|---|---|---|
| | Derivation | Simulation | Derivation | Simulation | Derivation | Simulation | Derivation | Simulation |
| Channel 1 | 0.3324 | 0.3324 | 0.7457 | 0.7458 | 2.7083 | 2.7241 | 13.0855 | 12.8145 |
| Channel 2 | 0.1264 | 0.1264 | 0.5729 | 0.5430 | 3.3334 | 3.3223 | 15.2002 | 15.2016 |
| Channel 3 | 3.3886 | 3.3889 | 1.0284 | 1.0284 | 2.8085 | 2.8234 | 13.4161 | 13.4203 |
| Channel 4 | 1.1613 | 1.1614 | 1.0441 | 1.0442 | 2.9185 | 2.9296 | 13.7907 | 13.7928 |
| Channel 5 | 0.2778 | 0.2778 | 2.0209 | 2.0211 | 3.2938 | 3.2949 | 15.1031 | 15.1031 |

TABLE 1: The optimal power allocation of the private jammers with fixed interference prices $\mu_1 = 1$ and $\mu_2 = 3$, achievable secrecy rates and revenues of legitimate transmitter obtained from closed-form solution and simulation for different sets of channels. The unit price for the achievable secrecy rate at the legitimate user is 5 ($\lambda_1 = 5$).

| Channels | Interference Price: | | Revenue of Jammers: | | Stackelberg Equilibrium: $(p_1^*, p_2^*, \mu_0^*)$ |
|---|---|---|---|---|---|
| | Derivation | Simulation | Derivation | Simulation | |
| Channel 1 | 4.0721 | 4.1000 | 1.5381 | 1.5378 | $(0.0677, 0.3070, 4.0721)$ |
| Channel 2 | 2.1647 | 2.2000 | 0.5372 | 0.5378 | $(0.3076, 0.6900, 2.1647)$ |
| Channel 3 | 2.6639 | 2.7000 | 0.7088 | 0.7084 | $(0.1501, 1.0917, 2.6639)$ |
| Channel 4 | 3.1023 | 3.1000 | 0.8887 | 0.8892 | $(0.1501, 0.6996, 3.1023)$ |
| Channel 5 | 4.0322 | 4.0000 | 1.4932 | 1.4935 | $(2.5895, 0.7858, 4.0322)$ |

TABLE 2: The optimal interference prices and revenues of the private jammers as well as Stackelberg equilibrium for different sets of channels. The unit price for the achievable secrecy rate at the legitimate user is 5 ($\lambda_1 = 5$).

$$\begin{aligned}\frac{\partial f(\mu_0)}{\partial \mu_0} &= \frac{2\lambda_1\bar{c}_1}{\mu_0\bar{c}_1+q} - \frac{2\lambda_1\bar{c}_1\mu_0\left(\bar{c}_1+\frac{\bar{c}_1^2\mu_0+2\lambda_1\bar{c}_1}{\mu_0\bar{c}_1+q}\right)}{(\mu_0\bar{c}_1+q)^2}, \text{ where } q=\sqrt{\mu_0\bar{c}_1(4\lambda_1+\mu_0\bar{c}_1)},\quad \bar{c}_1=\sum_{i=1}^{K}\beta_i \\ \frac{\partial^2 f(\mu_0)}{\partial \mu_0^2} &= \frac{-4\lambda_1\bar{c}_1\left(\bar{c}_1+\frac{\bar{c}_1^2\mu_0+2\lambda_1\bar{c}_1}{q}\right)}{(\bar{c}_1\mu_0+q)^2} + \frac{4\lambda_1\bar{c}_1\mu_0\left(\bar{c}_1+\frac{\bar{c}_1^2\mu_0+2\lambda_1\bar{c}_1}{q}\right)^2}{(\bar{c}_1\mu_0+q)^3} - \frac{2\lambda_1\bar{c}_1\mu_0\left(\frac{\bar{c}_1^2}{q}-\frac{(\bar{c}_1\mu_0+2\lambda_1\bar{c}_1)^2}{q^3}\right)}{(\bar{c}_1\mu_0+q)^2} \end{aligned} \tag{19}$$

$$\frac{\partial^2 f(\mu_0)}{\partial \mu_0^2} = \frac{-4\lambda_1\bar{c}_1^2 q(q+\bar{c}_1\mu_0+2\lambda_1)[q^2-\bar{c}_1\mu_0(\bar{c}_1\mu_0+\lambda_1)] - 2\lambda_1\bar{c}_1^3\mu_0\left(\bar{c}_1\mu_0+q\right)\left[q^2-(\bar{c}_1\mu_0+2\lambda_1)^2\right]}{q^3\left(\bar{c}_1\mu_0+q\right)^3} \tag{20}$$

$$\text{By substituting } q = \sqrt{\mu_0\bar{c}_1(4\lambda_1+\mu_0\bar{c}_1)}, \Longrightarrow \frac{\partial^2 f(\mu_0)}{\partial \mu_0^2} = \frac{-12\lambda_1^2\bar{c}_1^3 q\mu_0\left(q+\bar{c}_1\mu_0+2\lambda_1\right) - 8\lambda_1^3\bar{c}_1^3\mu_0\left(\bar{c}_1\mu_0+q\right)}{q^3\left(\bar{c}_1\mu_0+q\right)^3} < 0 \tag{21}$$

problem was formulated into a Stackelberg game, where the private jammers and the legitimate transmitter are the players of the game. We first focused on the fixed interference price scenario and a closed-form solution was derived for the optimal interference requirements. Based on this solution, a Stackelberg equilibrium was derived to maximize the revenues of both the legitimate transmitter and the private jammers. Simulation results were provided to support the derived theoretical results.

## APPENDIX A: PROOF OF LEMMA 1

With the optimal power allocation coefficients in (10), the achievable rates of the super-active eavesdroppers (i.e., $i \in \mathbb{K}$) will be equal as stated in *Proposition 1*. Hence, the power allocation coefficient at the $i^{\text{th}}$ private jammer can be written as follows:

$$\frac{\beta_i}{\sigma_e^2+p_i\alpha_i} = \gamma_0, \Longrightarrow p_i = \frac{1}{\alpha i}\left[\frac{\beta_i}{\gamma_0}-\sigma_e^2\right]^+. \tag{22}$$

The original optimization problem in (10) can be formulated in terms of $\gamma_0$ as follows:

$$\max_{\gamma_0\geq 0} \quad \lambda_1\left[\log(1+\beta_0)-\log(1+\gamma_0)\right]-\frac{1}{\gamma_0}\sum_{i=1}^{K}\mu_i\beta_i+\sigma_e^2\sum_{i=1}^{K}\mu_i \triangleq f(\gamma_0) \tag{23}$$

The optimal $\gamma_0^*$ should satisfy the KKT conditions and therefore we obtain the following:

$$\frac{\partial f(\gamma_0)}{\partial \gamma_0} = -\frac{\lambda_1}{1+\gamma_0}+\frac{\tau}{\gamma_0^2},\quad \frac{\partial^2 f(\gamma_0)}{\partial \gamma_0^2} = \frac{\lambda_1}{(1+\gamma_0)^2}-\frac{2\tau}{\gamma_0^3}, \tag{24}$$

where $\tau = \sum_{i=1}^{K}\mu_i\beta_i$. The function $f(\gamma_0)$ is concave if the following condition is satisfied:

$$\frac{\gamma_0^3}{(1+\gamma_0)^2} \leq \frac{2\tau}{\lambda_1}. \tag{25}$$

Hence, the optimal $\gamma_0^*$ can be obtained if $\lambda_1$ is large enough to satisfy the above condition. This means that the legitimate transmitter should charge the legitimate user a reasonable price to make a profit. Note that the optimal $\gamma_0^*$ should satisfy the KKT conditions.

$$\frac{\partial f(\gamma_0)}{\partial \gamma_0} = 0. \tag{26}$$

The optimal $\gamma_0^*$ can be obtained by solving the following equation:

$$\lambda_1 \gamma_0^2 - \gamma_0 \sum_{i=1}^{K} \mu_i \beta i - \sum_{i=1}^{K} \mu_i \beta i = 0. \tag{27}$$

and $\gamma_0 > 0$,

$$\gamma_0^* = \frac{\sum_{i=1}^{K} \mu_i \beta_i + \sqrt{\sum_{i=1}^{K} \mu_i \beta_i \left(4\lambda_0 + \sum_{i=1}^{K} \mu_i \beta_i\right)}}{2\lambda_1}. \tag{28}$$

Hence the optimal power allocation coefficient of the $i^{\mathrm{th}}$ can be written as follows:

$$p_i^* = \frac{1}{\alpha i}\left[\frac{\beta_i}{\gamma_0^*} - \sigma_e^2\right]^+. \tag{29}$$

This completes the proof of *Lemma 1*. ■

## APPENDIX B: PROOF OF LEMMA 2

We first show that the revenue function of the jammers in (16) is concave in terms of $\mu_0$ for $p_i > (0)$ in (12), and then we derive the optimal interference price $\mu_0^*$. The revenue function of the jammers is defined as follows:

$$f(\mu_0) = \frac{2\lambda_1 \mu_0 \bar{c}_1}{\mu_0 \bar{c}_1 + \sqrt{\mu_0 \bar{c}_1 \left(4\lambda_1 + \mu_0 \bar{c}_1\right)}} - K\sigma_e^2 \mu_0, \tag{30}$$

where $\bar{c}_1 = \sum_{i=1}^{K} \beta_i$. The concavity of $f(\mu_0)$ can be proven by finding the second derivative with respect to $\mu_0$ as in (19). In order to prove that the function in (30) is concave, we need to show that the second derivative (i.e.,$\frac{\partial^2 f(\mu_0)}{\partial \mu_0^2}$) is negative. This has been proved in (20) and (21) which are in the previous page. This confirms that the revenue function of the jammers is concave in $\mu_0$ and the optimal $\mu_0^*$ should satisfy the KKT conditions $\frac{\partial f(\mu_0)}{\partial \mu_0} = 0$ [23]:

$$\frac{2\lambda_1 \bar{c}_1}{\mu_0 \bar{c}_1 + q} - \frac{2\lambda_1 \bar{c}_1 \mu_0 \left(\bar{c}_1 + \frac{\bar{c}_1^2 \mu_0 + 2\lambda_1 \bar{c}_1}{\mu_0 \bar{c}_1 + q}\right)}{\left(\mu_0 \bar{c}_1 + q\right)^2} = 0, \tag{31}$$

$$\mu_0^* = \frac{0.5\left[-4\lambda_1 K\sigma^2 \eta_1 + 2\lambda_1 \sqrt{K\sigma^2 \eta_2 + 4K^2 \sigma^4 \eta_1^2}\right]}{K\sigma^2 \eta_2}.$$

This completes the proof of *Lemma 2*. ■

## REFERENCES


[1] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. Journ.*, vol. 54, pp. 1355–1387, Jan. 1975.

[2] Q. Li and W.-K. Ma, “Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming,” *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[3] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, “Improving physical layer secrecy using full-duplex jamming receivers,” *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[4] K. Cumanan, Z. Ding, B. Sharif, T. G. Y., 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.

[5] W. Xiang, S. L. Goff, M. Johnston, and K. Cumanan, “Signal mapping for bit-interleaved coded modulation schemes to achieve secure communications,” *IEEE Wireless Commun. Lett.*, vol. 4, no. 3, pp. 249–252, Jun. 2015.

[6] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, “Robust outage secrecy rate optimizations for a MIMO secrecy channel,” *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 86–89, Feb. 2015.

[7] Z. Chu, K. Cumanan, M. Xu, and Z. Ding, “Robust secrecy rate optimisations for multiuser multiple-input-single-output channel with device-to-device communications,” *IET Commun.*, vol. 9, no. 3, pp. 396–403, 2015.

[8] Q. Li and W.-K. Ma, “Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization,” *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[9] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, “Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer,” *IEEE Trans. Vehicular Technol.*, vol. 64, no. 5, pp. 1833–1847, May, 2015.

[10] A. Garnaev and W. Trappe, “An eavesdropping game with SINR as an objective function,” in *Proc. SecureComm, Athens, Greece*, pp. 142–162, Sep. 2009.

[11] Y. Wu and K. Liu, “An information secrecy game in cognitive radio networks,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[12] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, “Tree formation with physical layer security considerations in wireless multi-hop networks,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, Nov. 2012.

[13] W. Saad, Z. Han, M. Debbah, A. Hjørungenes, and T. Basar, “Physical layer security: Coalitional games for distributed cooperation,” in *Proc. 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, pp. 1–8, Seoul, Korea, Jun. 2009.

[14] R. Zhang, L. Song, Z. Han, and B. Jiao, “Physical layer security for two-way untrusted relaying with friendly jammers,” *IEEE Trans. Vehicular Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct., 2012.

[15] Z. Han, N. Marina, M. Debbah, and A. Hjørugnes, “Improved wireless secrecy capacity using distributed auction game theory,” in *Proc. IEEE International Conference on Mobile Ad-hoc and Sensor Networks*, Wu Yi Mountain, China, Dec. 2009.

[16] A. Mukherjee and A. Swindlehurst, “Jamming games in the MIMO wiretap channel with an active eavesdropper,” *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[17] S. A. A. Fakoorian and A. L. Swindlehurst, “Competing for secrecy in the MISO interference channel,” *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 170–181, Jan. 2013.

[18] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, “Secrecy rate optimization for a MIMO secrecy channel based on Stackelberg game,” in *Proc. European Signal Processing Conference (EUSIPCO)*, pp. 126–130, Lisbon, Portugal, Sep. 2014.

[19] 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.

[20] J. Huang and L. A. Swindlehurst, “Cooperative jamming for secure communication in MIMO relay networks,” *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[21] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, “QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach,” *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[22] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas II: The MIMOME wiretap channel,” *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[23] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.