Secure Multicast Communications with Private Jammers

K. Cumanan, Z. Ding, M. Xu, and H. Vincent Poor

***Abstract*— This paper investigates secrecy rate optimization for a multicasting network, where legitimate 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 cause interference to the eavesdroppers. However, these private jammers introduce the charges for their jamming services based on the amount of interference received at the eavesdroppers. This secrecy rate maximization problem is formulated into a *Stackelberg* game, where the private jammers and the legitimate transmitter are the leaders and the follower of the game, respectively. First, we consider the fixed interference price scenario, where a closed-form solution is derived for the optimal interference requirements at the eavesdroppers to maximize the revenue of the legitimate transmitter. Based on this solution, we then derive the *Stackelberg* equilibrium of the proposed game, at which both legitimate transmitter and the private jammers achieve their maximum revenues. To validate these theoretical derivations, simulation results are provided for fixed interference prices and *Stackelberg* game scenarios.**

I. Introduction

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

Multi-antenna terminals have the potential to enhance the performance of secrecy communications by exploiting their spatial diversity and additional degrees of freedom. However, the achievable secrecy rates with multi-antenna terminals are limited and mainly depend on the quality of the associated channels between legitimate transmitter and the legitimate receivers as well as the eavesdroppers [2], [3]. On the other hand, the performance of the secrecy communications can be further improved through cooperative jamming and artificial noise techniques, where jamming signals are transmitted from the external jammers or embedded with the intended signals for the legitimate users [3], [4]. These approaches degrade the capability of retrieving the legitimate users' signals at the eavesdroppers, which enhance the achievable secrecy rates of the legitimate users.

Recently, game theoretic approaches have significantly influenced in the resource allocations problems associated with secrecy communications [5]–[12]. In [5], a zero-sum game is solved for a secrecy network by considering the SINR difference between the legitimate user and the eavesdropper as the utility function of the game. An information secrecy game is investigated for cognitive radio networks through *Stackelberg* game in [6]. Cooperative game theory has been exploited to improve the secrecy capacity of ad-hoc network in [8], whereas a distributed tree formation game is proposed for multihop wireless networks in [7]. Physical layer security has been explored through a *Stackelberg* game for a two way relay networks with unfriendly jammers in [9] and a distributed auction theory is exploited to enhance the secrecy capacity in [10]. Jamming games have been proposed for a MIMO wiretap channels with an active eavesdropper in [11] whereas a secrecy game for a Gaussian MISO interference channel is investigated in [12].

In this paper, a multicating network is considered as shown in Fig. 1, where the same information is transmitted to all the legitimate users in the presence of multiple eavesdroppers. In order to improve the achievable secrecy rates of the legitimate users, the private jammers are employed to provide the dedicated jamming to the eavesdroppers. However, these private jammers introduces the charges for their jamming services based on the amount of interference caused to the eavesdroppers. To compensate these jamming charges, the legitimate users also pay the transmitter for its enhanced secured communications. Based on these interactions between the legitimate transmitter and the legitimate users as well as the private jammers, we formulate the original secrecy rate maximization problem into a *Stackelberg* game. First, a fixed interference price scenario is considered and then a closed-form solution is derived for the interference requirements at each eavesdropper. Based on this solution, we then investigate the corresponding *Stackelberg* equilibrium for the proposed game. In addition, simulation results are provided to validate the theoretical derivations of the proposed game.

II. System Model

A secrecy network with K legitimate users, L eavesdroppers and private jammers is considered as shown in Fig.1, where the transmitter broadcasts the same information to all the legitimate users in the presence of multiple eavesdroppers. In this secrecy network, the transmitter consists of N_T transmit antennas, whereas the legitimate users and the eavesdroppers are equipped with a single receive antenna. The channel coefficients between the legitimate transmitter and the k^{th} legitimate user as well as the l^{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 introduce interference to the eavesdroppers and they ensure that there is no interference leakage to the legitimate users. This could be 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 interference only from the corresponding private jammer. However, these private jammers charge for their dedicated jamming service based on the amount of interference caused to each eavesdropper. To compensate these interference prices, the legitimate transmitter also introduces charges for legitimate users for its enhanced secured communication based on the achieved secrecy rates. The power gain between the l^{th} eavesdropper and the corresponding jammer is represented 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 widely used in the literature [13]–[15]. Assuming white Gaussian

K. Cumanan is with the Department of Electronics, University of York, YO10 5DD, UK. Email: kanapathippillai.cumanan@york.ac.uk. Z. Ding is with the School of Computing and Communications, Lancaster University Lancaster, LA1 4WA, UK. Email: z.ding@lancaster.ac.uk. M. Xu is with Department of Electrical Engineering, Beihang University. Email: MaiXu@buaa.edu.cn. H. V. Poor is with Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA. Email: poor@princeton.edu.

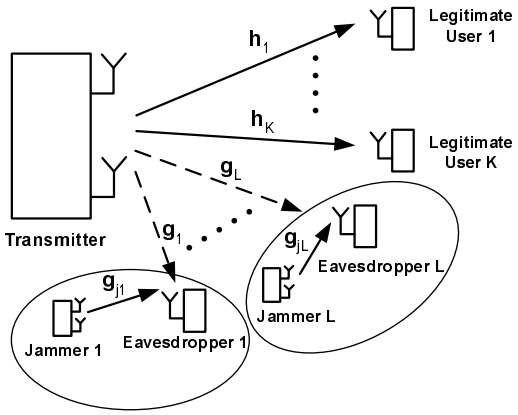

Fig. 1: A multicasting secrecy network with multiple legitimate users, multiple eavesdroppers and private jammers.

noise at the legitimate users and the eavesdroppers, achievable secrecy rate at the k^{th} legitimate user can be written as [16]

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

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

III. Game Theory Based Secrecy Rate Optimization

In this section, we formulate the secrecy rate maximization into a *Stackelberg* game and then investigate the *Stackelberg* equilibrium for the proposed game. This game consists two set of players: a) leader and b) followers. Both of these players try to maximize their revenues, where the leaders first make a move and the followers will move according to the leaders' strategy. In the multicasting network considered in this paper, the private jammers (leaders) announce their interference prices for each eavesdropper and then the legitimate transmitter (follower) determines the interference requirements according to the interference prices.

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

$$I_l=p_l|g_{jl}|^2. \quad (2)$$

Here, we are only interested in the power allocation at the jammer, where the beamformer at the jammer is appropriately designed with no interference leakage to the legitimate users and introducing interference only to the corresponding eavesdropper. The private jammers aim to maximize their revenues by selling interference to the transmitter. The revenue of the l^{th} private jammer can be written as follows:

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

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

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

where $\boldsymbol{\mu}=[\mu_1\cdots\mu_L]$ represents the interference prices for all eavesdroppers.

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

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

where λ_k and R_k are the unit price for the secrecy rate and the achieved secrecy rate at the k^{th} user, respectively. It is assumed that the unit price for the secrecy rate for each user is fixed to a certain value. Hence, the transmitter should determine the beamforming vector and determine the interference requirements at different eavesdroppers to maximize its revenue. However, we here only focus on the interference requirements at each eavesdroppers for a given beamformer at the transmitter, which can be formulated into an optimization framework as

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

where $\mathbf{p}=[p_1\cdots p_L]$ represents the power allocation at all jammers. *Problem (A)* and *Problem (B)* form a *Stackelberg* game, for which we investigate the *Stackelberg* equilibrium. The solution obtained through this equilibrium will be the best solution in terms of both revenues of the transmitter and the jammers.

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 $\boldsymbol{\mu}$:

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

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, 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)*. First, we solve the problem for a fixed interference price scenario. Based on this solution, we then derive *Stackelberg* equilibrium for the proposed game. Here, we only consider the secrecy 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 investigate the solution for fixed interference price scenario with a single legitimate user and multiple eavesdroppers. However, note that all the eavesdroppers in the network might not necessarily influence the achievable secrecy rate of the legitimate user and the eavesdropper with the highest achieved rate will only determine the secrecy rate of the legitimate user. Therefore, introducing jamming to this particular eavesdropper will improve the achievable secrecy rate of the legitimate user. At the same time, another eavesdropper might have the highest achieved rate, which will now determine the achievable secrecy rate of the legitimate user.

Therefore, a set of eavesdroppers will only influence the achievable secrecy rate of the legitimate user and they 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

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

where

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

The optimal interference requirements at each eavesdropper can be formulated as

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

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

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

This problem is convex in terms of the power allocation at the private jammers and can be efficiently solved through interior point methods [17].

Proposition 1: At the optimal solution of (10), the achieved rates of the super-active eavesdroppers (i.e., $t_i, \;\; i \in \mathbb{K}$) will be equal and power allocations p_is of 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. Let consider 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 the $t_{min} = t_0$. 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 achieved rates of the super-active eavesdroppers (i.e., $t_i, \;\; i \in \mathbb{K}$) will be equal at the optimal solution and the power allocations corresponding to the non-super-active eavesdroppers (i.e., $i \notin \mathbb{K}$) will be zeros. ■

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 the both leaders and the follower should be obtained. The best response of the legitimate transmitter can be obtained by solving the following problem:

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

where the vector $\mathbf{p} = [p_1 \cdots p_K]$ consists of the power allocations of private jammers in the super-active eavesdroppers' set $\mathbb{K}$. As we discussed in the previous subsection in (10), this problem is convex and the optimal power allocation can be obtained. However, the closed-form solution of this power allocation should be determined to derive the *Stackelberg* equilibrium of the proposed game.

Lemma 1: The optimal power allocation at the i^{th} jammer is given by

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

where

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

Proof: Please refer to Appendix A. ■

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

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

Based on the closed-form solution of the optimal power allocations p_i^*s in (12) in terms of the interference prices μ_is, the optimal interference prices problem can be reformulated as

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

The optimal interference prices μ_is might 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 consider the same interference price (uniform interference price) with 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:

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

Lemma 2: The optimal interference price μ_0^* in (16) is given by

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

where

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

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 through simulation results. Here, we consider a multicasting network with 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 legitimate transmitter is equipped with three

antennas whereas the legitimate user and each eavesdropper consist of single antenna. The channel coefficients between all terminals are generated through zero-mean circularly symmetric independent and identically distributed complex Gaussian random variables and the noise variance at all terminals is assumed to be 0.1. In the following subsections, we provide simulation results for fixed interference price and *Stackelberg* game scenarios, 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 allocations and corresponding revenues of the legitimate transmitter for different set 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 and the simulation based *Stackelberg* equilibriums as well as the corresponding jammer revenues with the uniform interference price scenario (i.e., $\mu_1 = \mu_2 = \mu_0$) for different set of channels. The theoretical results are the same as the simulation results and they support the theoretical results and validate the *Stackelberg* equilibrium of the proposed game for different set of channels. The deviations of the legitimate transmitter and the jammers from these equilibria will introduce loss in their revenues.

VI. Conclusions

In this paper, we studied secrecy rate optimization problem for a multicasting network, where the same information is transmitted for multiple users in the presence of multiple eavesdroppers. To improve the secrecy rate performance, private jammers were employed to cause interference to the eavesdroppers. In addition, these jammers charge for their jamming services. This original problem was formulated into a *Stackelberg* game, where the private jammers and the legitimate transmitter are the players of the game. First, we investigated the fixed interference price scenario and a closed-form solution was derived for optimal interference requirements at the eavesdroppers. 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 for fixed interference price and the *Stackelberg* game scenarios.

Appendix A: proof of Lemma 1

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

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

The original optimization problem in (10) can be formulated in terms of γ_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 γ_0^* should satisfy the KKT conditions and therefore we obtain the following:

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

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 γ_0^* can be obtained if λ_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 by introducing interference to the eavesdroppers with the help of the private jammers. However, the optimal γ_0^* should satisfy the KKT conditions.

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

The optimal γ_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 of the i^{th} can be written as

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

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 a concave in terms of μ_0 for $p_i > (0)$ in (12) and then we derive the optimal interference price μ_0^*. The revenue function of the jammers is defined as

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

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 μ_0 as in (19), which is in the previous page. 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 μ_0 and the optimal μ_0^* should satisfy the KKT conditions $\frac{\partial f(\mu_0)}{\partial \mu_0} = 0$ [17]:

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

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

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.

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 $\mu_2 = 3$, achieved secrecy rates and revenues of legitimate transmitter obtained from closed-form solution and simulation for different sets of channels. The unit price for the achieved secrecy rate at the legitimate user is 5 ($\lambda_1 = 5$).

Channels	Interference Price:		Revenue of Jammers:		*Stackelberg* Equilibrium: $\left(p_1^*, p_2^*, \mu_0^*\right)$
	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 achieved secrecy rate at the legitimate user is 5 ($\lambda_1 = 5$).

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

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

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

[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] 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.

[5] A. Garnaev and W. Trappe, "An eavesdropping game with SINR as an objective function," in *Proc. SECURECOMM,*, pp. 142–162, 2009.

[6] 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.

[7] 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.

[8] W. Saad, Z. Han, M. Debbah, A. Hjørungenes, and T. Basar, "Physical layer security: Coalitional games for distributed cooperation," in *Proc. 7th WiOpt*, 2009.

[9] 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.

[10] Z.Han, N. Marina, M. Debbah, and A. Hjørugnes, "Improved wireless secrecy capacit using distributed auction game theory," in *Proc. 5th ICMAS*, China 2009.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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