UNIVERSITY of York

This is a repository copy of *Secrecy rate optimization for secure multicast communications*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/103629/

Version: Accepted Version

Article:
Cumanan, Kanapathippillai orcid.org/0000-0002-9735-7019, Ding, Zhiguo, Xu, Mai et al. (1 more author) (2016) Secrecy rate optimization for secure multicast communications. IEEE Journal of Selected Topics in Signal Processing. 7544593. pp. 1417-1432. ISSN 1932-4553

https://doi.org/10.1109/JSTSP.2016.2600518

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Secrecy Rate Optimization for Secure Multicast Communications

Kanapathippillai Cumanan, *Member, IEEE*, Zhiguo Ding, *Senior Member, IEEE*,
Mai Xu, *Member, IEEE* and H. Vincent Poor *Fellow, IEEE*

***Abstract*—Recently, physical layer security has been recognized as a new design paradigm to provide security in wireless networks. In contrast to the existing conventional cryptographic methods, physical layer security exploits the dynamics of fading channels to enhance security of wireless communications. This paper studies optimization frameworks for a multicasting network in which a transmitter broadcasts the same information to a group of legitimate users in the presence of multiple eavesdroppers. In particular, power minimization and secrecy rate maximization problems are investigated for a multicasting secrecy network. First, the power minimization problem is solved for different numbers of legitimate users and eavesdroppers. Next, the secrecy rate maximization problem is investigated with the help of private jammers to improve the achievable secrecy rates through a game theoretic approach. These jammers charge the transmitter for their jamming services based on the amount of interference caused to the eavesdroppers. For a fixed interference price scenario, a closed-form solution for the optimal interference requirement to maximize the revenue of the transmitter is derived. This rate maximization problem for a non-fixed interference price scenario is formulated as a Stackelberg game in which the jammers and transmitter are the leaders and follower, respectively. For the proposed game, a Stackelberg equilibrium is derived to maximize the revenues of both the transmitter and the private jammers. To support the derived theoretical results, simulation results are provided with different numbers of legitimate users and eavesdroppers. In addition, these results show that physical layer security based jamming schemes could be incorporated in emerging and future wireless networks to enhance the quality of secure communications.**

***Index Terms*—Physical layer security, multicasting network, convex optimization, game theory.**

I. Introduction

In traditional wireless networks, security is achieved in the upper layers based on conventional cryptographic methods. However, some emerging networking paradigms present challenges in terms of key exchange and distribution. Recently, physical layer based secret communication has received considerable attention due to its suitability for dynamic network configurations and distributed processing techniques [1]–[3]. In addition, this approach implements security in the physical layer as a complement to the cryptographic methods by exploiting channel state information (CSI) of legitimate parties as well as eavesdroppers.

The ideas behind physical layer security were first investigated in [4] and [5] based on information theoretic concepts by defining the secrecy capacity of wiretap and related channels. Recently, multiantenna secrecy channels have received considerable attention in the research community since the use of multiple antennas yields spatial diversity and additional secrecy degrees of freedom [6]–[14]. In [6], the secrecy capacity of multiple-antenna wiretap channels was presented under an average power constraint, whereas the same secrecy capacity was established in [7] as the saddle point solution to a min-max problem. A transmit covariance matrix design was considered in [8] to maximize the ergodic secrecy rate with a power constraint for a multiple-input single-output (MISO) wiretap channel model, whereas an optimal transmit design through the semidefinite programming approach is proposed in [9] for the same channel model as in [8]. In [10], full rank solutions have been derived for the multiple-input multiple-output (MIMO) wiretap channel with an average power constraint and an alternative solution based on Taylor series has been proposed for the same problem in [11].

Cooperative jamming is a well known approach to further improve secrecy rates, in which the jamming signals are introduced at the eavesdropper with the help of relays or jamming nodes [15]–[20]. This scheme degrades the eavesdropper's capability of retrieving the information intended for the legitimate users. The achievable rates and an efficient cooperative jamming protocol have been presented for the general Gaussian multiple access and two-way wiretap channels in [15]. In [16], different cooperative jamming strategies have been developed for two-hop relay networks to confuse eavesdroppers with the assumption of global CSI. Opportunistic relaying for secret communications has been presented in [17] through cooperative jamming and relay chatting, whereas full-duplex jamming and optimal cooperative jamming for relays have been proposed in [18] and [19], [20], respectively. On the other hand, jamming signals can be embedded in the transmitted signal from the legitimate transmitter to confuse the eavesdroppers, a strategy known as the artificial noise (AN) technique in the literature [21]–[23]. In [21], a more general framework of AN methods has been presented for multi-antenna nodes. An AN scheme based on spatial selection has been proposed for MISO multi-evesdropper secrecy rate maximization in [22] and a quality of service based beamforming scheme is has been proposed in [23] to employ AN.

Recently, game theoretic techniques have been incorporated

Copyright(c) 2016 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

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 School of Electronic and Information Engineering, Beihang University (email: MaiXu@buaa.edu.cn). H. V. Poor is with Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (mail: poor@princeton.edu).

The work of K. Cumanan and Z. Ding was supported by H2020-MSCARISE-2015 under grant number 690750. The work of Z. Ding was supported in part by the Royal Society International Exchange Scheme and in part by the U.K. EPSRC under grant EP/N005597/1. The work of M. Xu was supported by the NSFC project under Grant 61573037, and the Fok Ying Tung Education Foundation under Grant 151061. The work of H. V. Poor was supported by the U.S National Science Foundation under Grant CMMI-1435778. Corresponding author: Mai Xu.

into the study of secure wireless communications for decision making and resource allocation, e.g., [24]–[30]. In [24], a novel cooperative paradigm has been proposed to improve the secrecy of primary users with the help of the secondary users in cognitive radio networks through a Stackelberg game approach. Secure games have been formulated for a secret communication network with an unfriendly jammer through a non-cooperative zero-sum continuous game in [25]. Physical layer security has been also investigated in a two way untrusted relay system through a Stackelberg game in [26]. In [27], a game theoretic framework has been developed for multi-hop networks in the presence of eavesdroppers. Transmission strategies have been proposed for MIMO secret communication networks in the presence of a multi-antenna eavesdropper through game theoretic approaches in [28], whereas a secrecy game for a Gaussian MISO interference channel has been investigated in [29].

In this paper, we consider a secure multicasting network as shown in Figure 1 where a transmitter broadcasts the same information to multiple legitimate users. To the best of the authors' knowledge, only a few works have investigated multicasting secrecy networks with multiple eavesdroppers. In [31], multicasting secrecy rate maximization was investigated for MISO channels with multiple eavesdroppers equipped with multiple antennas based on convex approximation techniques, whereas performance analysis has been derived for a secure multicasting network consisting of a single-antenna transmitter with multiple multi-antenna receivers as well as multiple multi-antenna eavesdroppers in [32]. In [33], a multicarrier based physical layer security scheme has been investigated for multicasting systems and a waveform design has been proposed for secure single-input single-output multicasting transmission in [34]. Recently, different capacities have been derived for secure multicasting in stochastic MIMO networks, whereas a joint beamforming and user selection scheme has been proposed for MISO wiretap channels with multiple single-antenna eavesdroppers in [35]. However, secure multicasting communications with cooperative jamming has not been considered in these works. In this paper, we propose secrecy rate optimization frameworks with cooperative jamming, in which a game theoretic approach is used to derive the optimal strategies of the legitimate transmitter and the jammers. The contributions of this paper are summarized as follows:

1) *Power minimization*: We consider a beamforming design for a secure communication network consisting of a legitimate user and an eavesdropper, where our goal is to minimize the transmit power with a secrecy rate constraint. This problem can be easily formulated as a second order cone programming (SOCP) problem. Furthermore, we derive a closed-form optimal solution based on the dual problem and Karush-Kuhn-Tucker (KKT) conditions. The derived optimal solution is validated through a comparison with the SOCP results via simulations. Next, the power minimization problem is considered for a scenario with multiple legitimate users and multiple eavesdroppers. This problem is not convex in terms of the beamformer at the transmitter. However, we formulate this problem as a semidefinite programming problem by introducing a new variable and also using semidefinite relaxation.

2) *Game theory based secrecy rate maximization*: In the above power minimization schemes, the legitimate transmitter requires a certain amount of transmit power to satisfy the required secrecy rates. However, it is not always possible to realize the predefined secrecy rates, either because the available transmit power is limited or because it might be expensive to use the required amount of power. To overcome these issues, external jammers can be employed to introduce interference to the eavesdroppers, which will improve the achievable secrecy rate at the legitimate users. Therefore, we consider a multicasting secrecy network with multiple legitimate users and multiple eavesdroppers as shown in Figure 2 in which private jammers introduce interference to the eavesdroppers. Particularly, these private jammers charge the transmitter for their jamming service based on the amount of interference caused at the eavesdroppers. On the other hand, the legitimate users also pay the transmitter according to their achieved secrecy rates, which provides a profit to the transmitter and compensates for the charges of the private jammers. Based on the revenues at both transmitter and the private jammers, we formulate this problem as a Stackelberg game in which the private jammers and the transmitter are the *leaders* and the *follower*, respectively. For the proposed game, we derive a Stackelberg equilibrium solution with different numbers of legitimate users and eavesdroppers, which maximizes the revenues of the transmitter as well as the private jammers.

The remainder of the paper is organized as follows. The system model is described in Section II. Section III presents the power minimization problem with different numbers of legitimate users and eavesdroppers. The Stackelberg game is introduced in Section IV, whereas Stackelberg equilibrium solutions are derived for the proposed game in Section V for different scenarios. Section VI provides simulation results to support the theoretical results. Finally, Section VII concludes the paper.

A. Notation

We use upper case boldface letters for matrices and lower case boldface letters for vectors. $(\cdot)^H$ denotes conjugate transpose. $\mathrm{Tr}(\cdot)$ and $\mathbb{E}\{\cdot\}$ stand for the trace of a matrix and the expectation of a random variable. $\mathbf{A} \succeq \mathbf{0}$ indicates that $\mathbf{A}$ is a positive semidefinite matrix. $\mathbf{I}$ denotes the identity matrix of appropriate size. $\|\cdot\|_2$ represents the Euclidean norm of a matrix. $[x]^+$ denotes $\max\{x, 0\}$.

II. System Model

We consider a multicasting secrecy network with K legitimate users and L eavesdroppers as shown in Figure 1, where a transmitter broadcasts the same information to all the legitimate users in the presence of multiple eavesdroppers. It is assumed that the transmitter is equipped with N_T transmit antennas, whereas each of the legitimate users and the eavesdroppers has a single receive antenna. The channel coefficients

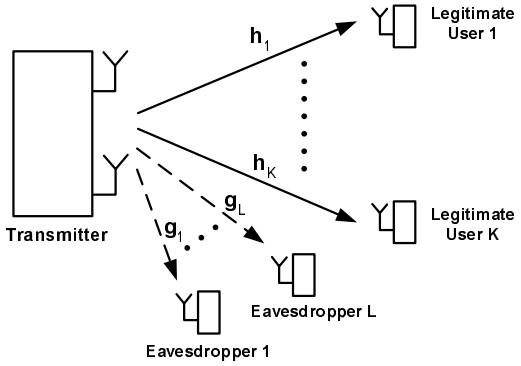

Fig. 1: A multicasting secrecy network in the presence of multiple eavesdroppers.

between the legitimate transmitter and the k^{th} legitimate user and between the legitimate transmitter and 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. Here, it is assumed that the transmitter has perfect CSI of the legitimate users and the eavesdroppers. This assumption is appropriate for the multicasting network being considered here, in which potential eavesdroppers are also legitimate members of the network, but do not have the permission to receive a particular multicast content being protected. This assumption has been widely used in the literature [2], [16], [19], [23], [36]–[41]. The noise powers at the k^{th} legitimate user and the eavesdroppers are assumed to be σ_k^2 and σ_e^2, respectively. The received signals at the k^{th} legitimate user and l^{th} eavesdropper can be written as follows:

$$y_k = \mathbf{h}_k^H \mathbf{w} s + n_k, \quad y_l = \mathbf{g}_l^H \mathbf{w} s + n_l, \tag{1}$$

where s ($\mathbb{E}\{s^2\} = 1$), and $\mathbf{w} \in \mathbb{C}^{N_T \times 1}$ are the signal intended to the legitimate users and the beamformer at the legitimate transmitter, respectively. n_k and n_l denote the noise at the k^{th} legitimate user and l^{th} eavesdropper, respectively. Assuming additive white Gaussian noise, the achievable secrecy rate at the k^{th} legitimate user is given by [7]

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

III. Secrecy Rate Optimizations

In this section, we consider the power minimization problem for a multicasting secrecy network in which the transmitter provides the required secrecy rates for all the legitimate users in the presence of multiple active eavesdroppers. This problem can be formulated as an optimization framework in which the total transmit power is minimized to satisfy the secrecy rate constraints.

A. Power Minimization

First, the power minimization problem is investigated with a single legitimate user and an eavesdropper. For this problem, a closed-form optimal solution can be derived based on the dual problem and KKT conditions. For the scenario of multiple legitimate users in the presence of multiple eavesdroppers, it is formulated into a semidefinite programming framework through semidefinite relaxation.

Single Legitimate User and Single Eavesdropper

With a single legitimate user and a single eavesdropper, the power minimization problem can be formulated with the secrecy rate constraint as follows:

$$\min_{\mathbf{w}} \|\mathbf{w}\|_2^2$$
$$\text{s.t. } \log\left(1+\frac{\mathbf{w}^H \mathbf{h}_1 \mathbf{h}_1^H \mathbf{w}}{\sigma_1^2}\right) - \log\left(1+\frac{\mathbf{w}^H \mathbf{g}_1 \mathbf{g}_1^H \mathbf{w}}{\sigma_e^2}\right) \ge \bar{R}_s, \tag{2}$$

where $\mathbf{h}_1$ and $\mathbf{g}_1$ are the channels between the legitimate transmitter and legitimate user and between the legitimate transmitter and the eavesdropper, respectively. In addition, $\bar{R}_s$ is the required secrecy rate of the legitimate user. The problem in (2) can be formulated into an SOCP problem. However, we derive a closed-form optimal solution based on the dual problem and KKT conditions. In the simulation section, we validate this closed-form solution by comparing it with SOCP results.

Lemma 1: The optimal solution of (2) is given by

$$\mathbf{w}^* = \sqrt{p^*}\tilde{\mathbf{w}}^*, \ \tilde{\mathbf{w}}^* = \frac{\mathbf{w}_1}{\|\mathbf{w}_1\|_2}, \mathbf{w}_1 = v_{max}\left(\hat{\mathbf{h}}_1\hat{\mathbf{h}}_1^H - 2^{\bar{R}_s}\hat{\mathbf{g}}_1\hat{\mathbf{g}}_1^H\right)$$
$$p^* = \lambda_s^*\left(2^{\bar{R}_s}-1\right), \ \lambda_s^* = \frac{1}{\lambda_{\max}\left(\hat{\mathbf{h}}_1\hat{\mathbf{h}}_1^H - 2^{\bar{R}_s}\hat{\mathbf{g}}_1\hat{\mathbf{g}}_1^H\right)}, \tag{3}$$

where $\hat{\mathbf{h}}_1 = \frac{\mathbf{h}_1}{\sigma_1}$, $\hat{\mathbf{g}}_1 = \frac{\mathbf{g}_1}{\sigma_e}$ and $\lambda_{\max}(\cdot)$, $v_{max}(\cdot)$ denote the maximum eigenvalue and the eigenvector corresponding to the maximum eigenvalue, respectively.

Proof: Please refer to Appendix A. ■

Multiple Legitimate Users and Multiple Eavesdroppers

The power minimization problem with multiple legitimate users and multiple eavesdroppers can be formulated as

$$\min_{\mathbf{w}} \|\mathbf{w}\|_2^2$$
$$\text{s.t.} \log\left(1+\frac{\mathbf{w}^H \mathbf{h}_k \mathbf{h}_k^H \mathbf{w}}{\sigma_k^2}\right) - \max_{1\le l\le L} \log\left(1+\frac{\mathbf{w}^H \mathbf{g}_l \mathbf{g}_l^H \mathbf{w}}{\sigma_e^2}\right) \ge \bar{R}_k,$$
$$k = 1, \cdots, K, \quad l = 1, \cdots, L, \tag{4}$$

where $\bar{R}_k$ is the target secrecy rate of the k^{th} legitimate user. This problem is not convex in terms of the transmit beamformer. However, by introducing a new semidefinite matrix $\mathbf{W} = \mathbf{w}\mathbf{w}^H$ and relaxing the rank-one constraint, the above problem can be formulated into a semidefinite programming (semidefinite relaxation problem) as follows:

$$\min_{\mathbf{W}\succeq\mathbf{0}} \quad \text{Tr}\{\mathbf{W}\}$$
$$\text{s.t.} \quad 1 + \text{Tr}\{\tilde{\mathbf{h}}_k \tilde{\mathbf{h}}_k^H \mathbf{W}\} - 2^{\bar{R}_k}\text{Tr}\{\tilde{\mathbf{g}}_l \tilde{\mathbf{g}}_l^H \mathbf{W}\} \ge 2^{\bar{R}_k},$$
$$k = 1, \cdots, K, \quad l = 1, \cdots, L, \tag{5}$$

where $\tilde{\mathbf{h}}_k = \frac{\mathbf{h}_k}{\sigma_k}$ and $\tilde{\mathbf{g}}_l = \frac{\mathbf{g}_l}{\sigma_e}$. If the solution of the above problem is rank-one, then it will be the optimal solution of the original problem in (4). In case of a non-rank-one solution, randomization techniques can be used to construct a rank-one solution from the non-rank-one solution of (5) [42], [43].

IV. Game Theory Based Secrecy Rate Optimization

In order to satisfy the target secrecy rates, the transmitter requires a certain amount of transmit power. However, it

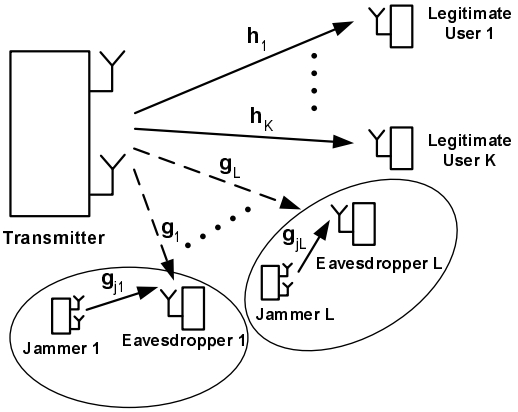

Fig. 2: A multicasting secrecy network with multiple legitimate users, multiple eavesdroppers and private jammers.

is not always possible to provide the target secrecy rates due to limited transmit power or because it might require a significant amount of transmit power which will be infeasible in terms of hardware implementations at the transmitter. On the other hand, in multicasting networks, it is difficult to achieve the target secrecy rates at different legitimate users with a single beamformer. To overcome these issues, cooperative jamming would be a solution, which will enhance the secrecy performance at the legitimate users. Here, we consider a multicasting secrecy network in which a set of private (friendly) jammers are employed to provide jamming services as shown in Figure 2. These private jammers introduce interference to the eavesdroppers who overhear the multicasting transmission from the transmitter. In addition, these jammers ensure that there is no interference leakage to the legitimate users, which 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[1]. These private jammers charge the transmitter for their dedicated jamming service based on the amount of interference caused to each eavesdropper. To compensate for these interference prices, the legitimate transmitter also introduces charges to the legitimate users for its enhanced secured service based on the achieved secrecy rates. For this scenario, we consider secrecy rate maximization with multiple legitimate users, multiple eavesdroppers and multiple corresponding jammers. We formulate this problem as a Stackelberg game and then investigate the Stackelberg equilibrium for the proposed game. A Stackelberg game consists of two set of players, namely, leaders and followers, where both of them try to maximize their revenues or profits. The leaders make a move first and then their followers will move according to the leaders' strategy. The leaders (private jammers) announce a set of unit interference prices for each eavesdropper. Then, the follower (transmitter) decides on the interference requirements at the eavesdroppers according to the interference prices.

[1]Here, it is assumed that the jammers have the perfect CSI of the corresponding eavesdroppers. This is a reasonable assumption, for networks in which the eavesdroppers are also part of the system [16], [19], [23].

A. Stackelberg Game

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

$$I_l = p_l |g_{jl}|^2, \tag{6}$$

where $|g_{jl}|^2$ is the power gain between the corresponding private jammer and the l^{th} eavesdropper and the power allocation at the l^{th} private jammer is represented by p_l. Here, we are only interested in the power allocation policy at the jammer, where the beamformer at the jammer is appropriately designed with no interference leakage to the legitimate users and hence interference is introduced only to the corresponding eavesdropper.

The private jammers' objective is to maximize their revenue by selling interference to the transmitter. The revenue of the l^{th} private jammer can be written as follows:

$$\phi_l(\mu_l, p_l) = \mu_l p_l |g_{jl}|^2, \tag{7}$$

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. The prices for interference at each eavesdropper can be obtained by solving the following optimization problem:

$$\text{Problem (A):} \quad \max_{\boldsymbol{\mu} \succeq \mathbf{0}} \quad \sum_{l=1}^{L} \phi_l(\mu_l, p_l), \tag{8}$$

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

At the same time, the transmitter should maximize its utility by introducing a price for secret communication established between the transmitter and the corresponding legitimate users. The revenue function at the transmitter can be written as

$$\psi_L(\mathbf{p}, \boldsymbol{\mu}) = \sum_{k=1}^{K} \lambda_k R_k - \sum_{l=1}^{L} \mu_l p_l |g_{jl}|^2, \tag{9}$$

where λ_k and R_k are the unit price for the secrecy rate and the achievable secrecy rate at the k^{th} user, respectively. In addition, 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 decide on the interference requirements at different eavesdroppers to maximize its revenue. However, we are only interested in determining the interference requirements at each eavesdroppers for a given beamformer at the transmitter. This problem can be formulated as follows:

$$\text{Problem (B):} \quad \max_{\mathbf{p} \succeq 0} \quad \psi_L(\mathbf{p}, \boldsymbol{\mu}), \tag{10}$$

where $\mathbf{p} = [p_1 \cdots p_L]$ represents the power allocation policy at all jammers.

Problem (A) and *Problem (B)* form a Stackelberg game, in which the jammers (leaders) announce the interference prices at each eavesdropper and then the transmitter (follower) determines the required amount of interference to each eavesdropper. The solution of this game can be obtained by investigating the Stackelberg equilibrium, at which the

transmitter and the jammers come to an agreement on the interference requirements and the interference price at each eavesdropper. The deviation of either the transmitter or the jammers from this equilibrium will introduce loss in their revenues.

B. 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 $\boldsymbol{\mu}$:

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

V. Stackelberg Equilibrium Solution

In this section, we derive Stackelberg equilibrium solutions for the proposed game described in the previous section with different numbers of legitimate users and eavesdroppers. First, the best response of the transmitter is derived in terms of power allocation at the jammers for fixed interference prices. Then, the optimal interference prices are obtained to maximize the revenue of the jammers. In order to obtain the Stackelberg equilibrium points, the best responses of the follower (legitimate transmitter) and the leaders (jammers) should be obtained by solving *Problem (B)* and *Problem (A)*, respectively. Since, the leaders (jammers) derive the optimal interference prices determined by the interference requirements from the legitimate transmitter, the best response function of the follower should be derived first in terms of the interference requirements. For the proposed game, the Stackelberg equilibrium can be derived by obtaining $\mathbf{p}^*$ from *Problem (B)* first and then by obtaining the best interference prices $\boldsymbol{\mu}^*$ from *Problem (A)*. In the following subsections, we solve the proposed Stackelberg game with different numbers of legitimate users and eavesdroppers.

A. Single Legitimate User and Single Eavesdropper

In this subsection, the proposed game is considered with a single legitimate user and an eavesdropper. First, the optimal interference requirement (best response) at the transmitter is obtained to maximize its revenue for the fixed interference price at the jammer. Then, a Stackelberg equilibrium is derived for this game where both the legitimate transmitter and jammer attain an equilibrium by achieving their maximum revenues.

Fixed Interference Price

Here, the optimal interference requirement is obtained for a fixed interference price at the jammer. For a given beamformer at the transmitter, the achievable secrecy rate of the legitimate user in the presence of an eavesdropper is defined as

$$R_{SL-SE} = \log(1+\beta_0) - \log\left(1 + \frac{\beta_1}{\sigma_e^2 + p_1\alpha_1}\right), \qquad (11)$$

where

$$\beta_0 = \frac{\mathbf{w}^H \mathbf{h}_1 \mathbf{h}_1^H \mathbf{w}}{\sigma^2},\ \beta_1 = \mathbf{w}^H \mathbf{g}_1 \mathbf{g}_1^H \mathbf{w},\ \alpha_1 = |g_{j1}|^2. \qquad (12)$$

Hence, the optimal interference requirement at the eavesdropper can be obtained by solving the following optimization problem:

$$\max_{p_1 \geq 0}\ \lambda_1 R_{SL-SE} - \mu_1 p_1 \alpha_1, \qquad (13)$$

where p_1 is the power allocation policy at the corresponding jammer. This problem is convex and the corresponding proof has been provided in the next subsection. Hence, the optimal power allocation can be obtained through standard interior point methods [44]. However, we derive the closed-form solution for the power allocation p_1 to realize the Stackelberg equilibrium in the following subsection.

Stackelberg Game

In this subsection, we derive the Stackelberg equilibrium with a legitimate user and an eavesdropper. To obtain this equilibrium, the best response (i.e., p_1^*) of the follower (transmitter) is derived for a given interference price (μ_1), since the leader (jammer) derives its best response from the interference requirement decided by the follower (transmitter). Note that a closed-form solution for the best response should be obtained to derive the Stackelberg equilibrium of the proposed game. The best response of the follower can be obtained by solving the following problem:

$$\max_{p_1 \geq 0} \qquad \psi_{\text{SL-SE}}(p_1, \mu_1), \qquad (14)$$

where $\psi_{\text{SL-SE}}(p_1, \mu_1)$ is the revenue function for the transmitter and is defined in (15) at the top of the next page. λ_1 and μ_1 are the unit prices for the secrecy rate at the legitimate user and the price for the interference introduced at the eavesdropper. The optimal interference requirement for a given $\mathbf{w}$ and μ_1 can be obtained by solving the following problem:

$$\max_{p_1 \geq 0} \lambda_1 \left[\log(1+\beta_0) - \log\left(1 + \frac{\beta_1}{\sigma_e^2 + p_1\alpha_1}\right)\right] - \mu_1 p_1 \alpha_1, \qquad (16)$$

where

$$\beta_0 = \frac{\mathbf{w}^H \mathbf{h}_1 \mathbf{h}_1^H \mathbf{w}}{\sigma_1^2},\ \beta_1 = \mathbf{w}^H \mathbf{g}_1 \mathbf{g}_1^H \mathbf{w} \text{ and } \alpha_1 = |g_{j1}|^2. \qquad (17)$$

Lemma 2: The optimal interference requirement from the jammer with a given interference price μ_1 is given by

$$p_1^* = \frac{1}{\alpha_1}\left[\sqrt{\frac{\beta_1^2}{4} + \frac{\lambda_1\beta_1}{\mu_1}} - \frac{(2\sigma_e^2 + \beta_1)}{2}\right]^+ \qquad (18)$$

Proof: Please refer to Appendix B. ■

Corollary 1: With a given $\mathbf{w}$ and λ_1, the interference price μ_1 is bounded as follows:

$$\mu_1 \leq \frac{\lambda_1 \beta_1}{\sigma_e^2\,(\sigma_e^2 + \beta_1)}. \qquad (19)$$

Since $p_1 \geq 0$,

$$\sqrt{\frac{\beta_1^2}{4} + \frac{\lambda_1\beta_1}{\mu_1}} \geq \frac{(2\sigma_e^2 + \beta_1)}{2} \Rightarrow \mu_1 \leq \frac{\lambda_1\beta_1}{\sigma_e^2\,(\sigma_e^2 + \beta_1)} \qquad (20)$$

We have thus obtained the optimal interference requirement at the eavesdropper to maximize the revenue of the legitimate transmitter. The jammer should announce the optimal unit

$$\psi_{\text{SL-SE}}(p_1,\mu_1)=\lambda_1\left[\log\left(1+\frac{\mathbf{w}^H\mathbf{h}_1\mathbf{h}_1^H\mathbf{w}}{\sigma_1^2}\right)-\log\left(1+\frac{\mathbf{w}^H\mathbf{g}_1\mathbf{g}_1^H\mathbf{w}}{\sigma_e^2+p_1\alpha_1}\right)\right]-\mu_1p_1\alpha_1 \tag{15}$$

interference price μ_1 to maximize its revenue by selling the interference to the transmitter. The optimal unit interference price can be obtained by solving the following optimization problem:

$$\max_{\mu_1\geq 0}\phi_1(p_1^*,\mu_1)=\mu_1p_1^*\alpha_1 \tag{21}$$

Lemma 3: The optimal unit interference price μ_1 is given as follows:

$$\mu_1^*=\frac{c_2}{2c_1}\left[\frac{c_0}{\sqrt{c_0^2-c_1}}-1\right], \tag{22}$$

where

$$c_0=\frac{\left(2\sigma_e^2+\beta_1\right)}{2\alpha_1},\quad c_1=\frac{\beta_1^2}{4\alpha_1^2}\text{ and }c_2=\frac{\lambda_1\beta_1}{\alpha_1^2}. \tag{23}$$

Proof: Please refer to Appendix C. ■

Hence, a Stackelberg equilibrium for the proposed game with a single legitimate user and an eavesdropper is (p_1^*,μ_1^*). Any deviation from this equilibrium point will cause loss to both the follower (legitimate transmitter) and leader (jammer). Hence, both of them will operate at this Stackelberg equilibrium to maximize their revenues.

Proposition 1: There is a unique Nash equilibrium for the proposed game and the derived Stackelberg equilibrium solution achieves this unique Nash equilibrium.

Proof: As mentioned before, the revenue function of the legitimate transmitter is a concave function of the power allocation policy at the jammer. Hence, the optimal and unique jammer power allocation policy has been derived for a given interference price. Similarly, the revenue function of the jammer is also a concave function in terms of the interference price which results in an optimal and unique interference price. Since, both solutions are unique and optimal, this equilibrium achieves a unique Nash equilibrium for the proposed game. ■

B. Multiple Legitimate Users and Single Eavesdropper

In this subsection, we extend the proposed game to the scenario with multiple legitimate users and a single eavesdropper. As in the previous subsection, first, the optimal interference requirement is obtained for a fixed interference price and then, a Stackelberg equilibrium is derived for the proposed game.

Fixed Interference Price

The achievable secrecy rate of the i^{th} user can be defined as

$$R_{ML-SE}^{(i)}=\log(1+\beta_i)-\log\left(1+\frac{\beta_e}{\sigma_e^2+p_2\alpha_1}\right), \tag{24}$$

where

$$\beta_i=\frac{\mathbf{w}^H\mathbf{h}_i\mathbf{h}_i^H\mathbf{w}}{\sigma^2},\quad \beta_e=\mathbf{w}^H\mathbf{g}_1\mathbf{g}_1^H\mathbf{w}\quad \alpha_1=|g_{j1}|^2. \tag{25}$$

The optimal power allocation policy at the jammer for a fixed interference price can be formulated as

$$\max_{p_1\geq 0}\ \sum_{i=1}^{K}\lambda_iR_{SL-ME}^{(i)}-\mu_1p_2\alpha_1, \tag{26}$$

Lemma 4: The optimal power allocation policy at the jammer to maximize the revenue at the legitimate transmitter is given by

$$p_2^*=\frac{1}{\alpha_1}\left[\sqrt{\frac{\beta_e^2}{4}+\frac{\beta_e\left(\sum_{i=1}^{K}\lambda_i\right)}{\mu_1}}-\frac{(2\sigma_e^2+\beta_e)}{2}\right]^+ \tag{27}$$

Proof: The proof is similar to that of *Lemma 2*. ■

Stackelberg Game

In order to derive the Stackelberg equilibrium with multiple legitimate users and an eavesdropper, the best response of jammer should be obtained by solving the following problem:

$$\max_{\mu_2\geq 0}\phi_1(p_2^*,\mu_2)=\mu_2p_2^*\alpha_1 \tag{28}$$

Lemma 5: The optimal unit interference price μ_2 is given as follows:

$$\mu_2^*=\frac{\bar{c}_2}{2c_1}\left[\frac{c_0}{\sqrt{c_0^2-c_1}}-1\right], \tag{29}$$

where

$$c_0=\frac{\left(2\sigma_e^2+\beta_e\right)}{2\alpha_1},\quad c_1=\frac{\beta_e^2}{4\alpha_1^2}\text{ and }\bar{c}_2=\frac{\beta_e\sum_{i=1}^{K}\lambda_i}{\alpha_1^2}. \tag{30}$$

Proof: The proof is similar to that of *Lemma 3*. ■

Hence, the Stackelberg equilibrium of the proposed game with multiple legitimate users and single eavesdropper is defined as (p_2^*,μ_2^*).

C. Single Legitimate User and Multiple Eavesdroppers

Here, the proposed game is investigated with a single legitimate user and multiple eavesdroppers. This problem is different from the above problems due to the fact that there are the multiple active eavesdroppers. As in the previous subsection, first the fixed-interference scenario is solved, followed by the derivation of the Stackelberg equilibrium of the proposed game.

Fixed Interference Prices

The achievable secrecy rate with multiple eavesdroppers can be defined as

$$R_{SL-ME}=\log(1+\beta_0)-\max_{1\leq i\leq L}\log\left(1+\frac{\beta_i}{\sigma_e^2+p_i\alpha_i}\right), \tag{31}$$

where

$$\beta_0=\frac{\mathbf{w}^H\mathbf{h}_1\mathbf{h}_1^H\mathbf{w}}{\sigma^2},\quad \beta_i=\mathbf{w}^H\mathbf{g}_i\mathbf{g}_i^H\mathbf{w},\ \alpha_i=|g_{ji}|^2. \tag{32}$$

Note that all the eavesdroppers may not necessarily influence the achievable secrecy rate at the legitimate user. The eavesdropper with the highest achieved rate will determine the

achieved secrecy rate of the legitimate user. By introducing jamming to this eavesdropper, the secrecy rate can be improved by reducing the achievable rate at the corresponding eavesdropper. After this jamming, another eavesdropper might now have the highest achievable rate which will deteriorate the achievable secrecy rate of the legitimate user. Hence, it is important to jam this eavesdropper in order to match the achieved rate of the previous eavesdropper. Therefore, only a subset of eavesdroppers require the interference from the jammers and the rest of them do not need any interference from the jammers, since their impact on the secrecy rate is not dominant. Here, we divide these eavesdroppers into two sets, namely, super-active and non-super-active eavesdroppers. The eavesdroppers who receive interference from the jammers and determine the achievable secrecy rate of the legitimate user are called super-active eavesdroppers and the rest of them are defined as non-super active eavesdroppers. In order to improve the revenue of the legitimate transmitter, the optimal interference requirements problem can be formulated as follows:

$$\max_{\mathbf{p}\succeq\mathbf{0}} \ \lambda_1 R_{SL-ME} - \sum_{i\in\mathbb{K}} \mu_i p_i \alpha_i, \tag{33}$$

where the vector $\mathbf{p} = \{p_i \backslash i \in \mathbb{K}\}$ represents the power allocations of private jammers in the set $\mathbb{K}$ consisting of all super-active eavesdroppers. The optimal interference requirements from private jammers corresponding to the super-active eavesdroppers can be obtained by formulating the problem as follows:

$$\begin{aligned} \max_{\mathbf{p}\succeq\mathbf{0},\ t_i,\ t_0} \quad & \lambda_1 \left[\log(1+\beta_0) - t_0\right] - \sum_{i\in\mathbb{K}} \mu_i p_i \alpha_i \\ \text{s.t.} \quad & \log\left(1 + \frac{\beta_i}{\sigma_e^2 + p_i\alpha_i}\right) \leq t_i,\ i \in \mathbb{K} \\ & \max\{t_i \backslash i \in \mathbb{K}\} = t_0, \quad t_i \geq 0,\ i \in \mathbb{K}. \end{aligned} \tag{34}$$

The problem in (34) is convex in $\mathbf{p}$ and can be easily solved by interior point methods. However, one issue that might arise is how to obtain the super-active eavesdroppers' set $\mathbb{K}$ from all available active eavesdroppers. This can be addressed by solving the following optimization problem:

$$\begin{aligned} \max_{\mathbf{p}\succeq\mathbf{0},\ t_i,\ t_0} \quad & \lambda_1 \left[\log(1+\beta_0) - t_0\right] - \sum_{i=1}^{L} \mu_i p_i \alpha_i \\ \text{s.t.} \quad & \log\left(1 + \frac{\beta_i}{\sigma_e^2 + p_i\alpha_i}\right) \leq t_i,\ \forall\ i \\ & \max\{t_1, \cdots, t_L\} = t_0,\ t_i \geq 0,\ \forall\ i, \end{aligned} \tag{35}$$

where the super-active eavesdroppers' set $\mathbb{K}$ is removed and all the available eavesdroppers have been incorporated into the optimization problem.

Proposition 2: At the optimal solution of (35), 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 $t_i,\ i = 1, \cdots, L$, and the corresponding p_i will be higher than that of $t_{min} = t_0$. Hence, the revenue of the transmitter (cost function of (35)) 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 strategy corresponding to the non-super-active eavesdroppers (i.e., $i \notin \mathbb{K}$) will be zeros. ■

Therefore, the optimal interference requirements from the private jammers with fixed interference prices can be obtained by solving the convex problem in (35).

Stackelberg Game

As in the previous subsections, this problem is formulated as a Stackelberg game and the Stackelberg equilibrium is defined for the proposed game. The best response of the transmitter for a given set of interference prices can be determined by solving the following problem:

$$\max_{\mathbf{p}\succeq\mathbf{0}} \ \lambda_1 R_{SL-ME} - \sum_{i\in\mathbb{K}} \mu_i p_i \alpha_i, \tag{36}$$

where $\mathbf{p}$ represents power allocations of the private jammers in the set $\mathbb{K}$ which is the set consisting of all the super-active eavesdroppers. This problem can be formulated into a convex problem as in (35) and the optimal power allocation strategy can be obtained. However, it is necessary to find a closed-form solution to derive a Stackelberg equilibrium for the proposed game.

Lemma 6: The optimal power allocation policy at the i^{th} jammer is given by

$$p_i^* = \frac{1}{\alpha_i}\left[\frac{\beta_i}{\gamma_0^*} - \sigma_e^2\right]^+, \tag{37}$$

where

$$\begin{aligned} \beta_i &= \mathbf{w}^H \mathbf{g}_i \mathbf{g}_i^H \mathbf{w} \\ \gamma_0^* &= \frac{\sum_{i=1}^K \mu_i\beta_i + \sqrt{\sum_{i=1}^K \mu_i\beta_i \left(4\lambda_1 + \sum_{i=1}^K \mu_i\beta_i\right)}}{2\lambda_1} \end{aligned} \tag{38}$$

Proof: Please refer to Appendix D. ■

The optimal interference requirement has been derived to maximize the transmitter's revenue for a given set of interference prices. However, the jammers should announce their optimal interference prices to maximize their revenues. The optimal interference price can be obtained by solving the following problem:

$$\max_{\boldsymbol{\mu}\succeq\mathbf{0}} \sum_{l=1}^{L} \phi_i(p_i^*, \mu_i) = \sum_{l=1}^{L} \mu_i p_i^* \alpha_i. \tag{39}$$

By substituting the optimal power allocations p_i^*s in (37) in terms of the interference prices μ_is, the above optimization problem can be rewritten as

$$\max_{\boldsymbol{\mu}\succeq\mathbf{0}} \left[\frac{2\lambda_1 \sum_{i=1}^K \mu_i\beta_i}{\sum_{i=1}^K \mu_i\beta_i + \sqrt{\sum_{i=1}^K \mu_i\beta_i \left(4\lambda_1 + \sum_{i=1}^K \mu_i\beta_i\right)}} - \sigma_e^2 \sum_{i=1}^K \mu_i\right]^+ \tag{40}$$

It is very difficult to find a closed-form solution for the optimal interference prices μ_is and the problem in (40) generally must be solved using existing numerical methods. However, we can find a closed-form solution if we assume that each private jammer announces the same interference prices (i.e., $\mu_1 = \mu_2 = \cdots = \mu_L = \mu_0$). For this uniform interference price scenario, the optimization problem in (40) can be modified as

$$\max_{\mu_0 \geq 0} \left[\frac{2\lambda_1 \mu_0 \sum_{i=1}^{K} \beta_i}{\mu_0 \sum_{i=1}^{K} \beta_i + \sqrt{\mu_0 \sum_{i=1}^{K} \beta_i \left(4\lambda_1 + \mu_0 \sum_{i=1}^{K} \beta_i\right)}} - K\sigma_e^2 \mu_0 \right]^+ \tag{41}$$

Lemma 7: The optimal interference price μ_0^* in (41) is given by

$$\mu_0^* = \frac{\frac{1}{2}\left[-4\lambda_1 K\sigma^2\eta_1 + 2\lambda_1\sqrt{K\sigma^2\eta_2 + 4K^2\sigma^4\eta_1^2}\right]}{K\sigma^2\eta_2} \tag{42}$$

where

$$\eta_1 = \left(1 + \frac{K\sigma^2}{\bar{c}_2}\right),\ \eta_2 = \left(\bar{c}_2 + K\sigma^2\right),\ \bar{c}_2 = \sum_{i=1}^{K} \beta_i. \tag{43}$$

Proof: Please refer to Appendix E. ■

The Stackelberg equilibrium of the proposed uniform price game with a single legitimate user and multiple eavesdroppers is given by $(p_i^* \ \forall\ i, \mu_0^*)$. By using this equilibrium solution, both the legitimate transmitter and the jammers achieve their maximum revenues.

D. Multiple Legitimate Users and Multiple Eavesdroppers

In this subsection, the proposed game is extended to the scenario with multiple legitimate users and multiple eavesdroppers. As in the previous subsections, the fixed interference price scenario and Stackelberg game are investigated.

Fixed Interference Prices

The achievable secrecy rate of the i^{th} user can be defined as

$$R_{ML-ME}^{(i)} = \log\left(1 + \beta_0^{(i)}\right) - \max_{1 \leq i \leq L} \log\left(1 + \frac{\beta_i}{\sigma_e^2 + p_i\alpha_i}\right), \tag{44}$$

where

$$\beta_0^{(i)} = \frac{\mathbf{w}^H \mathbf{h}_i \mathbf{h}_i^H \mathbf{w}}{\sigma^2}, \quad \beta_i = \mathbf{w}^H \mathbf{g}_i \mathbf{g}_i^H \mathbf{w}. \tag{45}$$

As mentioned in the previous subsection, all the eavesdroppers might not be active due to the different achieved rates. By considering only super-active eavesdroppers, the optimal interference requirements can be obtained by solving the following problem:

$$\max_{\mathbf{p} \succeq \mathbf{0}} \ \sum_{i=1}^{K} \lambda_i R_{SL-ME}^{(i)} - \sum_{i \in \mathbb{K}} \mu_i p_i \alpha_i, \tag{46}$$

where the vector $\mathbf{p}$ represents power allocations of private jammers in the set $\mathbb{K}$ which is the set consisting of all the active eavesdroppers. As in the previous subsection, the optimal interference requirements can be obtained by considering both super-active and non-super-active eavesdroppers through the following problem:

$$\begin{aligned} \max_{\mathbf{p} \succeq \mathbf{0},\ t_i,\ t_0} \quad & \sum_{i=1}^{K} \lambda_i \left[\log\left(1 + \beta_0^{(i)}\right) - t_0\right] - \sum_{i=1}^{L} \mu_i p_i \alpha_i \\ \text{s.t.} \quad & \log\left(1 + \frac{\beta_i}{\sigma_e^2 + p_i\alpha_i}\right) \leq t_i,\ \forall\ i \\ & \max\{t_1, \cdots, t_L\} = t_0,\ \forall\ i,\ t_i \geq 0,\ \forall\ i \end{aligned} \tag{47}$$

At the optimal solution of (47), the achieved rates of the super-active eavesdroppers will be equal and power allocations corresponding to the non-super-active eavesdroppers will be zeros, where the corresponding proof is similar to that of *Proposition 2*.

Stackelberg Game

Here, we solve the Stackelberg game for the scenario with multiple legitimate users and multiple eavesdroppers. The derivation of the Stackelberg equilibrium is similar to that of the scenario with a single legitimate user and multiple eavesdroppers. The best response of the legitimate transmitter can be obtained by solving the following problem:

$$\max_{\mathbf{p} \succeq \mathbf{0}} \ \sum_{i=1}^{K} \lambda_i R_{ML-ME}^{(i)} - \sum_{i \in \mathbb{K}} \mu_i p_i \alpha_i, \tag{48}$$

where the vector $\mathbf{p}$ consists of all the power allocations of the jammers corresponding to the super-active eavesdroppers.

Lemma 8: The optimal power allocation strategy at the i^{th} jammer is given by

$$p_{i_{ML-ME}}^* = \frac{1}{\alpha_i}\left[\frac{\beta_i}{\gamma_1} - \sigma_e^2\right]^+, \tag{49}$$

where

$$\beta_i = \mathbf{w}^H \mathbf{g}_i \mathbf{g}_i^H \mathbf{w}$$

$$\gamma_1 = \frac{\sum_{i=1}^{K} \mu_i\beta_i + \sqrt{\sum_{i=1}^{K} \mu_i\beta_i \left(4\sum_{i=1}^{K} \lambda_i + \sum_{i=1}^{K} \mu_i\beta_i\right)}}{2\sum_{i=1}^{K} \lambda_i}$$

Proof: The proof is similar to that of *Lemma 6*. ■

For this interference requirement, the jammers should determine their optimal interference prices to maximize their revenues which can be obtained by solving the following problem:

$$\max_{\boldsymbol{\mu} \succeq \mathbf{0}} \sum_{i=1}^{K} \phi_i(p_i^*, \mu_i) = \sum_{i=1}^{L} \mu_i p_i^* \alpha_i. \tag{50}$$

However, it is difficult to find a closed-form optimal solution for the problem in (50) with different interference prices μ_is at each jammer. In the case of the uniform interference price (i.e.,$\mu_1 = \mu_2 = \cdots, \mu_L = \mu_0$), the problem in (50) can be modified as follows:

$$\max_{\mu_0 \geq 0} \frac{2\mu_0 \bar{c}_3 \bar{c}_2}{\mu_0 \bar{c}_2 + \sqrt{\mu_0 \bar{c}_2 \left(4\bar{c}_3 + \mu_0 \bar{c}_2\right)}} - K\sigma_e^2 \mu_0 \tag{51}$$

where

$$\bar{c}_2 = \sum_{i=1}^{K} \beta_i,\ \bar{c}_3 = \sum_{i=1}^{K} \lambda_i. \tag{52}$$

Lemma 9: The optimal interference price μ_0^* is given by

$$\mu_{ML-ME}^* = \frac{\frac{1}{2}\left[-4K\sigma^2\bar{c}_3\eta_1 + 2\bar{c}_3\sqrt{K\sigma^2\eta_2 + 4K^2\sigma^4\eta_1^2}\right]}{K\sigma^2\eta_2} \quad (53)$$

where

$$\eta_1 = 1 + \frac{K\sigma^2}{\bar{c}_2},\ \eta_2 = \bar{c}_2 + K\sigma^2. \quad (54)$$

Proof: The proof is similar to that of *Lemma 7*. ■

Hence, a Stackelberg equilibrium of the proposed game with multiple legitimate users and multiple users is defined by $(p_{i_{ML-ME}}^*,\ \forall\ i, \mu_{ML-ME}^*)$ which provides the maximum revenues for both the legitimate transmitter and the private jammers.

VI. Simulation Results

In this section, we provide simulation results to support the theoretical results derived in the previous sections. In order to evaluate the performance of the proposed schemes, we consider a multicasting secrecy network in which 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 in order to improve the secrecy rates at the legitimate users. The legitimate transmitter is equipped with three antennas, whereas the legitimate users and the eavesdroppers have a single-antenna. The unit secrecy rate price has been set to 5 (i.e., $\lambda_1 = 5$). In this secrecy network, all channels have been generated using zero-mean circularly symmetric independent and identically distributed complex Gaussian random variables. The noise power at all the terminals has been assumed to be 0.1.

A. Power Minimization

In this subsection, we provide simulation results to support the closed-form results derived in (3) for the scenario with a single legitimate user and an eavesdropper. As mentioned before, the original power minimization problem can be formulated into a convex optimization (SOCP) framework. However, we derived a closed-form solution in (3). We have obtained the required transmit power and the corresponding beamformer based on the closed-form solution as well as the convex optimization framework for different sets of channels as provided in Table 1 where the target secrecy rate has been set to 3.5. As seen in Table 1, both results are the same which validates the accuracy of the closed-form solution in (3). Due to space limitations, the performance for the corresponding beamformers as well as the simulation results for the case with multiple legitimate users and multiple eavesdroppers are not provided here.

B. Fixed Interference Prices

In this subsection, we evaluate the performance of the proposed schemes with private jammers, where the legitimate transmitter is charged with fixed interference prices. The simulation results are provided with different numbers of legitimate users and eavesdroppers.

Channels	Required Transmit Power	
	Closed Form	Convex Optimization
Channel 1	1.1610	1.1610
Channel 2	1.3431	1.3431
Channel 3	1.2069	1.2069
Channel 4	0.7455	0.7455
Channel 5	0.6082	0.6082

TABLE 1: The required transmit power for the closed-form and convex optimization based solutions.

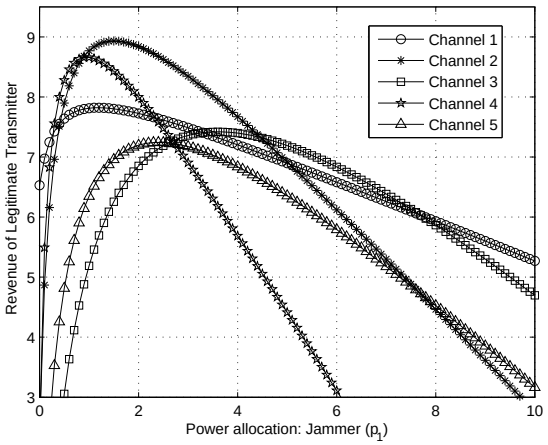

Fig. 3: The revenue of the legitimate transmitter against power allocation at the private jammer for different channels with fixed interference price (i.e., $\mu_1 = 1$).

Single Legitimate User and Single Eavesdropper

A secrecy network with a single legitimate user and an eavesdropper is considered in which a private jammer introduces interference to the eavesdropper by charging the legitimate transmitter with a price of one (i.e., $\mu_1 = 1$) for unit interference. First, we validate the concavity of the revenue function of the legitimate transmitter ($f(p_1)$ in (60)) in terms of the power allocation (p_1) at the private jammer and then simulation results based optimal power allocations are obtained to support the theoretical derivations. Figure 3 shows the revenue function of the legitimate transmitter for different sets of channels for a fixed interference price. As seen in Figure 3, the revenue functions are concave for different sets of channels, which validates the proof of the convexity of $f(p_1)$ provided in Appendix B. On the other hand, Table 2 presents the optimal power allocation policy at the private jammer, the achieved secrecy rate and the corresponding revenue of the legitimate transmitter obtained through theoretical and simulation results. As seen in Table 2, the theoretical and simulation results are identical, which demonstrates the accuracy of the derivations in (18). In addition, the optimal power allocations at the jammer corresponding to the maximum revenue at transmitter in Figure 3 is the same as the theoretical results in Table 2 for the five channels considered in this simulation. Hence, these results confirm the optimality of the derived results for the scenario of the single legitimate user and the single eavesdropper.

Channels	Power Allocation: Jammer		Achieved Secrecy Rate		Revenue: Legitimate Transmitter	
	Derivation	Simulation	Derivation	Simulation	Derivation	Simulation
Channel 1	1.1809	1.2000	1.6445	1.6458	7.8207	7.8206
Channel 2	1.5019	1.5000	2.0534	2.0531	8.9325	8.9325
Channel 3	3.5984	3.6000	2.0505	2.0507	7.4198	7.4198
Channel 4	0.9452	1.0000	1.9921	2.0041	8.6606	8.6583
Channel 5	2.4107	2.4000	1.8168	1.8152	7.2427	7.2427

TABLE 2: The optimal power allocation policy of the private jammers with fixed interference prices $\mu_1 = 1$, achievable secrecy rates and revenues of legitimate transmitter for single legitimate transmitter and single eavesdropper obtained from the closed-form solution and simulation for different sets channels.

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 3: The optimal power allocation policy of the private jammers with fixed interference prices $\mu_1 = 1$ and $\mu_2 = 3$, achievable secrecy rates and revenues of legitimate transmitter. The unit price for the achieved secrecy rate at the legitimate user is 5 ($\lambda_1 = 5$).

Single Legitimate User and Multiple Eavesdroppers

Here, we consider a multicasting secrecy network with a single legitimate user and two eavesdroppers. The price used by the jammers to charge the legitimate transmitter is 1 and 3 (i.e., $\mu_1 = 1,\ \mu_2 = 3$), respectively, for unit interference. Similar to the previous simulations, first, we validate the convexity of the revenue function of the legitimate transmitter in (35) in terms of power allocations (i.e., p_1 and p_2) at the private jammers for different sets of channels. Then, the correctness of the derived theoretical results is supported through numerical results. Figure 4 depicts the revenue functions of the legitimate transmitter for Channel 1 provided in Table 3 which confirms the convexity of the revenue function in terms of power allocation policy at the jammers. In addition, Table 3 provides the theoretical and simulation based optimal power allocations at the private jammers which maximize the revenue of the transmitter for five sets of channels. As seen in Table 3, the theoretical and simulation results are indistinguishable, which validates the derivation of the closed-form power allocations in (37). On the other hand, the maximum revenue from Figure 4 is the same as that of Channel 1 in Table 3 with the same power allocations at the private jammers. This confirms the optimality of the results obtained in Table 3 for different sets of channels. Note that we have only presented the revenue of the transmitter for Channel 1 in Figure 4; however, the rest of the channels in Table 3 provide similar results. We have not presented those results here due to space limitations.

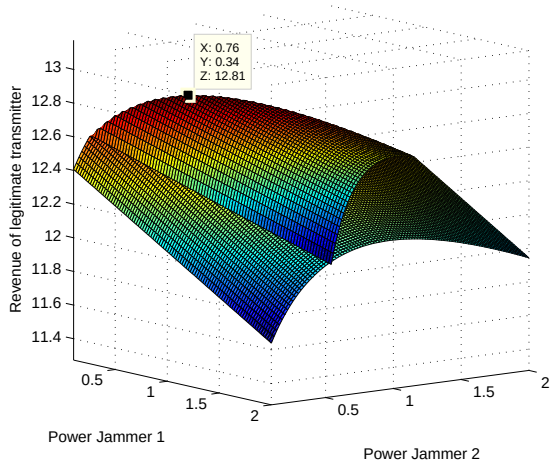

Fig. 4: The revenue of the legitimate transmitter for Channel 1 with different power allocations at both the private jammers for fixed interference prices.

C. Stackelberg Game

In this subsection, we validate the equilibrium of the proposed Stackelberg games for different numbers of legitimate users and eavesdroppers.

Single Legitimate User and Single Eavesdropper

To support the derived Stackelberg equilibrium, a secrecy network with a single legitimate user and an eavesdropper is considered. First, for different sets of channels, the revenue function of the jammer is evaluated with different interference prices as shown in Figure 5. These results confirm that the jammer revenue function is concave with respect to the interference price (i.e., μ_1) and support the proof provided in Appendix C. The choices for the optimal interference prices and the maximum revenues of the jammers are provided in Table 4, which verifies the accuracy of the analytical results. The Stackelberg equilibria (p_1^*, μ_1^*) for the proposed game are also presented in Table 4. These validate the derived unique Stackelberg equilibrium of the game through simulation results, where both the transmitter and the private jammer will come to an agreement to maximize their revenues.

Channels	Interference Price (μ_1):		Revenue of Jammer:		Stackelberg Equilibrium: (p_1^*, μ_1^*)
	Derivation	Simulation	Derivation	Simulation	
Channel 1	4.4313	4.4000	0.5534	0.5530	$(0.3670, 4.4313)$
Channel 2	8.5462	8.5000	2.2242	2.2240	$(0.2929, 8.5462)$
Channel 3	5.6251	5.6000	3.6714	3.6715	$(0.8291, 5.6251)$
Channel 4	8.5640	8.6000	2.1736	2.1735	$(0.1863, 8.5640)$
Channel 5	7.8066	7.8000	2.8496	2.8495	$(0.4779, 7.8066)$

TABLE 4: The optimal interference prices and revenues of the private jammer as well as Stackelberg equilibrium for different sets of channels. The unit price for the achieved secrecy rate at the legitimate user is 5 ($\lambda_1 = 5$).

Channels	Interference Price:		Revenue of Jammers:		Stackelberg Equilibrium: (p_1^*, p_2^*, μ_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 5: 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 ($\lambda_1 = 5$).

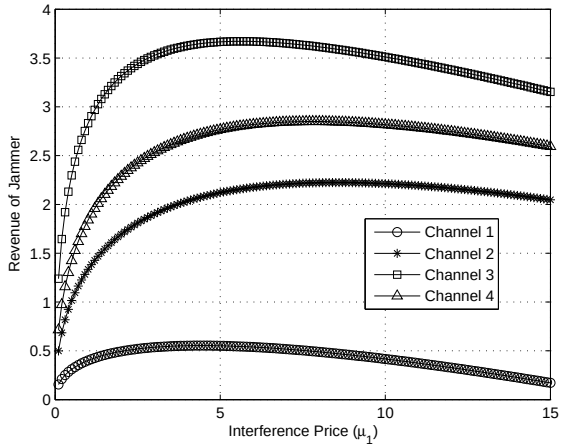

Fig. 5: The revenue of the jammer with a single legitimate user and a single eavesdropper for different sets of channels.

Single Legitimate User and Multiple Eavesdroppers

In order to validate the proposed Stackelberg equilibrium, the same secrecy network as in the fixed interference price case is considered with a single legitimate user and multiple eavesdroppers. First, we evaluate the revenue function of the legitimate transmitter ($f(\gamma_0)$) in (76) in terms of γ_0 for different sets of channels. Figure 6 plots the revenues of the legitimate transmitter versus γ_0 with fixed interference prices (i.e., $\mu_1 = 1,\ \mu_2 = 3$) for different sets of channels. This confirms the derivation of the convexity of $f(\gamma_0)$ (Appendix D) in terms of γ_0. In addition, the achievable maximum revenues are the same as the derived solutions represented in Table 5. Next, we evaluate the achievable revenues of the jammers with different interference prices where it is assumed that the all the jammers introduce the same interference price (i.e., $\mu_1 = \mu_2 = \mu_0$). Figure 7 plots the revenues of the jammers versus the interference price μ_0 for different sets of channels which confirms the convexity of the revenue of the jammers in the interference price μ_0 (Appendix E). Table 5 provides the theoretical and simulation based optimal interference prices (i.e., μ_0^*s) and corresponding revenues of the jammers for the proposed Stackelberg game with different sets of channels, where the theoretical results are the same as the simulated results. In addition, Stackelberg equilibria of the proposed game are also provided in Table 5. The deviation of the legitimate transmitter and jammers from this equilibrium solution will introduce a loss in their corresponding revenues as evidenced by Figures 6 and 7.

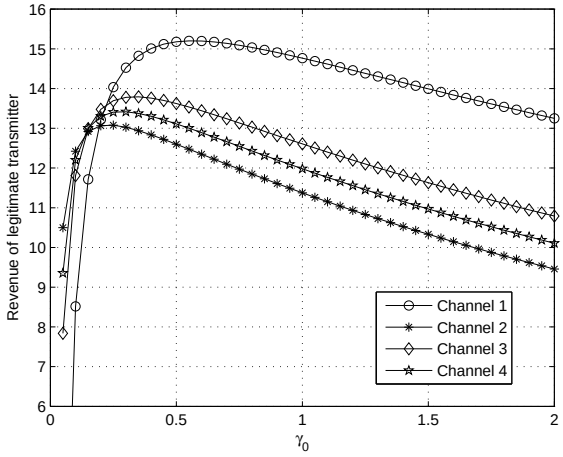

Fig. 6: The revenue of the transmitter in terms of γ_0 with fixed interference prices for different sets of channels.

VII. Conclusions

In this paper, we have proposed optimization techniques for a multicasting secrecy network. For the scenario with a single legitimate user and a single eavesdropper, a closed-form solution has been derived for the power minimization problem based on the corresponding dual problem, whereas it was formulated as a semidefinite programming problem in

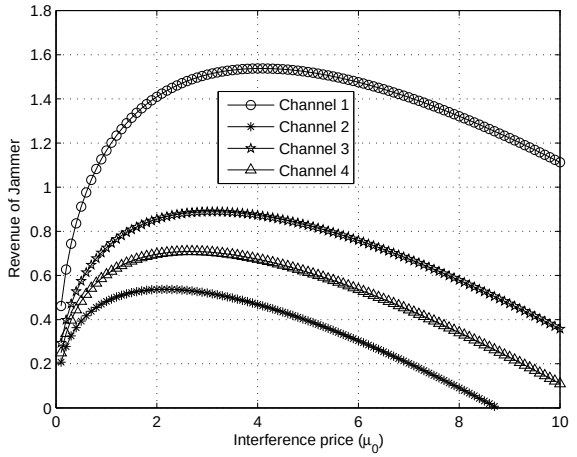

Fig. 7: The revenue of the jammer with different interference prices for different sets of channels.

the case with multiple legitimate users and multiple eavesdroppers. On the other hand, optimization problems have been considered for a multicasting secrecy network with jammers to improve the achievable secrecy rates. These private jammers introduce charges for their jamming service. For fixed interference prices, we have derived the optimal interference requirements for different numbers of legitimate users and eavesdroppers. For non-fixed interference prices, we have formulated the optimization problem into a Stackelberg game in which jammers and the transmitter are the leaders and follower, respectively. A Stackelberg equilibrium has been developed for the proposed game with different numbers of legitimate users and eavesdroppers. To validate the derived theoretical results, simulation results have been provided for a variety of scenarios.

APPENDIX A: PROOF OF LEMMA 1

The original power minimization problem in (2) can be written without of loss of generality as

$$\min_{p,\tilde{\mathbf{w}}} \quad p\tilde{\mathbf{w}}^H\tilde{\mathbf{w}}$$
$$\text{s.t.} \quad \frac{\tilde{\mathbf{w}}^H\left(\mathbf{I}+p\hat{\mathbf{h}}_1\hat{\mathbf{h}}_1^H\right)\tilde{\mathbf{w}}}{\tilde{\mathbf{w}}^H\left(\mathbf{I}+p\hat{\mathbf{g}}_1\hat{\mathbf{g}}_1^H\right)\tilde{\mathbf{w}}}\geq 2^{\bar{R}_s},\ \tilde{\mathbf{w}}^H\tilde{\mathbf{w}}=1,\ p\geq 0, \quad (55)$$

where $\hat{\mathbf{h}}_1=\frac{\mathbf{h}_1}{\sigma_1}$ and $\hat{\mathbf{g}}_1=\frac{\mathbf{g}_1}{\sigma_e}$. In order to obtain the optimal solution of (55) (i.e., $\tilde{\mathbf{w}}^*, p^*$), we derive the corresponding dual problem. The Lagrangian of (2) can be defined as

$$L(\mathbf{w},\lambda_s)=\mathbf{w}^H\mathbf{w}+\lambda_s\left[2^{\bar{R}_s}\left(1+\mathbf{w}^H\hat{\mathbf{g}}_1\hat{\mathbf{g}}_1^H\mathbf{w}\right)-\left(1+\mathbf{w}^H\hat{\mathbf{h}}_1\hat{\mathbf{h}}_1^H\mathbf{w}\right)\right],$$

where λ_s is the Lagrange multiplier associated with the secrecy rate constraint. The corresponding dual problem can be defined as

$$\max_{\lambda_s\geq 0}\lambda_s\left(2^{R_s}-1\right),\ \text{s.t. } \mathbf{Z}\triangleq\mathbf{I}-\lambda_s\left(\hat{\mathbf{h}}\hat{\mathbf{h}}^H-2^{\bar{R}_s}\hat{\mathbf{g}}_1^H\hat{\mathbf{g}}_1\right)\succeq\mathbf{0}. \quad (56)$$

The constraint in (56) means that the matrix $\mathbf{Z}$ should have at least one zero eigenvalue. On the other hand, λ_s can take the maximum to satisfy the positive semidefinite constraint in (56) as

$$\lambda_s^*=\frac{1}{\lambda_{\max}\left(\hat{\mathbf{h}}\hat{\mathbf{h}}^H-2^{\bar{R}_s}\hat{\mathbf{g}}_1^H\hat{\mathbf{g}}_1\right)}, \quad (57)$$

where $\lambda_{\max}(\cdot)$ denotes the maximum eigenvalue of its argument. The original problem in (2) can be formulated as a convex problem. Hence, strong duality holds between the original problem in (2) and the corresponding dual problem in (56). The required minimum power to achieve the secrecy rate constraint is

$$p^*=\lambda_s^*\left(2^{\bar{R}_s}-1\right). \quad (58)$$

On the other hand, the optimal $\mathbf{w}$ should be in the null space of $\mathbf{Z}$:

$$\mathbf{w}_1 \quad = \quad v_{\max}\left(\hat{\mathbf{h}}\hat{\mathbf{h}}^H-2^{R_s}\hat{\mathbf{g}}_1^H\hat{\mathbf{g}}_1\right),\ \tilde{\mathbf{w}}^*=\frac{\mathbf{w}_1}{\|\mathbf{w}_1\|_2}, \quad (59)$$

where $v_{max}(\cdot)$ denotes the the eigenvector corresponding to the maximum eigenvalue. Hence the optimal solution of (2) can be expressed as in (3). This completes the proof for *Lemma 1*. ■

APPENDIX B: PROOF OF LEMMA 2

We first show that the problem in (16) is a convex problem by showing that the following function is concave in p_1:

$$f(p_1)=\lambda_1\left[\log(1+\beta_0)-\log\left(1+\frac{\beta_1}{\sigma_e^2+p_1\alpha_1}\right)\right]-\mu_1 p_1\alpha_1. \quad (60)$$

The concavity of this function can be shown by finding the second derivative respect to p_1 as follows:

$$\frac{\partial f(p_1)}{\partial p_1}=\frac{\lambda_1\alpha_1\beta_1}{(\sigma_e^2+p_1\alpha_1+\beta_1)(\sigma_e^2+p_1\alpha_1)}-\mu_1\alpha_1 \quad (61)$$

$$\frac{\partial^2 f(p_1)}{\partial p_1^2}=-\frac{\lambda_1\alpha_1\beta_1\left(2\alpha_1^2p_1+2\alpha_1\sigma_e^2+\beta_1\alpha_1\right)}{\left[\alpha_1^2p_1^2+\left(2\sigma_e^2+\beta_1\right)\alpha_1p_1+\beta_1\sigma_e^2+\sigma_e^4\right]^2}. \quad (62)$$

Since $\frac{\partial^2 f(p_1)}{\partial p_1^2}<0$, $f(p_1)$ is a concave function in terms of p_1. Hence the optimal solution should satisfy the KKT conditions as follows [44]:

$$\frac{\partial f(p_1)}{\partial p_1}=\frac{\lambda_1\alpha_1\beta_1}{(\sigma_e^2+p_1\alpha_1+\beta_1)(\sigma_e^2+p_1\alpha_1)}-\mu_1\alpha_1=0. \quad (63)$$

By arranging the terms of (63), we obtain the following:

$$\alpha 1^2p_1^2+\left(2\sigma_e^2+\beta_1\right)\alpha_1p_1+\beta_1\sigma_e^2+\sigma_e^4-\frac{\lambda_1\beta_1}{\mu_1}=0. \quad (64)$$

By solving this equation, the optimal power allocation policy p_1 at the jammer is obtained as $p_1\geq 0$,

$$p_1^*=\frac{1}{\alpha_1}\left[\sqrt{\frac{\beta_1^2}{4}+\frac{\lambda_1\beta_1}{\mu_1}}-\frac{(2\sigma_e^2+\beta_1)}{2}\right]^+. \quad (65)$$

This completes the proof of *Lemma 2*. ■

APPENDIX C: PROOF OF LEMMA 3

The problem in (21) can be proven to be a convex problem by showing the following function is concave in the interference price μ_1 for $p_1^*(>0)$ in (18):

$$f(\mu_1)=\mu_1\left(\sqrt{c_1+\frac{c_2}{\mu_1}}-c_0\right), \quad (66)$$

where $c_0,\ c_1$ and c_2 are defined in (23). This function can be shown to be concave by finding its second derivative respect

to μ_1 as follows:

$$\frac{\partial f(\mu_1)}{\partial \mu_1} = \left(c_1 + \frac{c_2}{\mu_1}\right)^{\frac{1}{2}} - \frac{c_2}{2\mu_1}\left(c_1 + \frac{c_2}{\mu_1}\right)^{-\frac{1}{2}} - c_0 \quad (67)$$

$$\frac{\partial^2 f(\mu_1)}{\partial \mu_1^2} = -\frac{c_2^2}{4\mu_1^3}\left(c_1 + \frac{c_2}{\mu_1}\right)^{-\frac{3}{2}}. \quad (68)$$

Hence the second derivative of $f(\mu_1)$ with respect to μ_1 is negative (i.e., $\frac{\partial^2 f(\mu_1)}{\partial \mu_1^2} < 0$), and $f(\mu_1)$ is a concave function in μ_1. In addition, the optimal interference price μ_1^* should satisfy the KKT conditions as follows [44]:

$$\frac{\partial f(\mu_1)}{\partial \mu_1} = \left(c_1 + \frac{c_2}{\mu_1}\right)^{\frac{1}{2}} - \frac{c_2}{2\mu_1}\left(c_1 + \frac{c_2}{\mu_1}\right)^{-\frac{1}{2}} - c_0 = 0. \quad (69)$$

By rearranging the (69), we obtain the following:

$$4c_1\left(c_0^2 - c_1\right)\mu_1^2 + 4c_2\left(c_0^2 - c_1\right)\mu_1 - c_2^2 = 0. \quad (70)$$

By solving the above equation, the optimal interference price μ_1^* to maximize the jammer's revenue is obtained as $\mu_1 > 0$,

$$\mu_1^* = \frac{c_2}{2c_1}\left[\frac{c_0}{\sqrt{c_0^2 - c_1}} - 1\right]. \quad (71)$$

This completes the proof of *Lemma 3*. ■

Appendix D: proof of Lemma 6

With the optimal power allocation in (34), the achieved rates of the super-active eavesdroppers (i.e., $i \in \mathbb{K}$) will be equal as stated in *Proposition 2*. Hence, the power allocation at the i^{th} private jammer can be written as

$$\frac{\beta_i}{\sigma_e^2 + p_i\alpha_i} = \gamma_0, \Longrightarrow p_i = \frac{1}{\alpha i}\left[\frac{\beta_i}{\gamma_0} - \sigma_e^2\right]^+. \quad (75)$$

The original optimization problem in (34) can be formulated in terms of γ_0 as follows:

$$\max_{\gamma_0 \geq 0} \quad \lambda_1\left[\log(1+\beta_0) - \log(1+\gamma_0)\right] - \frac{1}{\gamma_0}\sum_{i=1}^{K}\mu_i\beta_i + \sigma_e^2\sum_{i=1}^{K}\mu_i \triangleq f(\gamma_0) \quad (76)$$

The optimal γ_0^* should satisfy the KKT conditions and therefore we obtain the following:

$$\frac{\partial f(\gamma_0)}{\partial \gamma_0} = -\frac{\lambda_1}{1+\gamma_0} + \frac{\tau}{\gamma_0^2}, \quad \frac{\partial^2 f(\gamma_0)}{\partial \gamma_0^2} = \frac{\lambda_1}{(1+\gamma_0)^2} - \frac{2\tau}{\gamma_0^3}, \quad (77)$$

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

$$\frac{\gamma_0^3}{(1+\gamma_0)^2} \leq \frac{2\tau}{\lambda_1}. \quad (78)$$

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 $\frac{\partial f(\gamma_0)}{\partial \gamma_0} = 0$. The optimal γ_0^* can be obtained by solving the following equation:

$$\lambda_1\gamma_0^2 - \gamma_0\sum_{i=1}^{K}\mu_i\beta i - \sum_{i=1}^{K}\mu_i\beta i = 0, \quad (79)$$

and $\gamma_0 > 0$,

$$\gamma_0^* = \frac{\sum_{i=1}^{K}\mu_i\beta_i + \sqrt{\sum_{i=1}^{K}\mu_i\beta_i\left(4\lambda_0 + \sum_{i=1}^{K}\mu_i\beta_i\right)}}{2\lambda_1}. \quad (80)$$

Hence the optimal power allocation policy of the i^{th} can be written as

$$p_i^* = \frac{1}{\alpha i}\left[\frac{\beta_i}{\gamma_0^*} - \sigma_e^2\right]^+. \quad (81)$$

This completes the proof of *Lemma 6*. ■

Appendix E: proof of Lemma 7

We first show that the revenue function of the jammers in (41) is concave in terms of μ_0 for $p_i > (0)$ in (37) and then we derive the optimal interference price μ_0^*. The revenue function of the jammers is defined as

$$f(\mu_0) = \frac{2\lambda_1\mu_0\bar{c}_1}{\mu_0\bar{c}_1 + \sqrt{\mu_0\bar{c}_1\left(4\lambda_1 + \mu_0\bar{c}_1\right)}} - K\sigma_e^2\mu_0, \quad (82)$$

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 (72), which is at the top of the next page. In order to prove that the function in (82) 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 (73) and (74) which are at the top of the next 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 $\frac{\partial f(\mu_0)}{\partial \mu_0} = 0$ [44]:

$$\frac{2\lambda_1\bar{c}_1}{\mu_0\bar{c}_1 + q} - \frac{2\lambda_1\bar{c}_1\mu_0\left(\bar{c}_1 + \frac{\bar{c}_1^2\mu_0 + 2\lambda_1\bar{c}_1}{\mu_0\bar{c}_1 + q}\right)}{\left(\mu_0\bar{c}_1 + q\right)^2} = 0, \quad (83)$$

$$\mu_0^* = \frac{\frac{1}{2}\left[-4\lambda_1 K\sigma^2\eta_1 + 2\lambda_1\sqrt{K\sigma^2\eta_2 + 4K^2\sigma^4\eta_1^2}\right]}{K\sigma^2\eta_2}.$$

This completes the proof of *Lemma 7*. ■

References

[1] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. Trends Commun. Info. Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[2] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[3] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

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

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[6] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

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

[8] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[9] 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.

[10] S. A. A. Fakoorian and L. A. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, May. 2013.

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

$$\frac{\partial^2 f(\mu_0)}{\partial \mu_0^2} = \frac{-4\lambda_1\bar{c}_1\left(\bar{c}_1+\frac{\bar{c}_1^2\mu_0+2\lambda_1\bar{c}_1}{q}\right)}{\left(\bar{c}_1\mu_0+q\right)^2} + \frac{4\lambda_1\bar{c}_1\mu_0\left(\bar{c}_1+\frac{\bar{c}_1^2\mu_0+2\lambda_1\bar{c}_1}{q}\right)^2}{\left(\bar{c}_1\mu_0+q\right)^3} - \frac{2\lambda_1\bar{c}_1\mu_0\left(\frac{\bar{c}_1^2}{q}-\frac{(\bar{c}_1\mu_0+2\lambda_1\bar{c}_1)^2}{q^3}\right)}{\left(\bar{c}_1\mu_0+q\right)^2} \tag{72}$$

$$\frac{\partial^2 f(\mu_0)}{\partial \mu_0^2} = \frac{-4\lambda_1\bar{c}_1^2 q(q+\bar{c}_1\mu_0+2\lambda_1)[q^2-\bar{c}_1\mu_0(\bar{c}_1\mu_0+\lambda_1)] - 2\lambda_1\bar{c}_1^3\mu_0\left(\bar{c}_1\mu_0+q\right)\left[q^2-(\bar{c}_1\mu_0+2\lambda_1)^2\right]}{q^3\left(\bar{c}_1\mu_0+q\right)^3} \tag{73}$$

$$\text{By substituting } q = \sqrt{\mu_0\bar{c}_1(4\lambda_1+\mu_0\bar{c}_1)}, \Longrightarrow \frac{\partial^2 f(\mu_0)}{\partial \mu_0^2} = \frac{-12\lambda_1^2\bar{c}_1^3 q\mu_0\left(q+\bar{c}_1\mu_0+2\lambda_1\right) - 8\lambda_1^3\bar{c}_1^3\mu_0\left(\bar{c}_1\mu_0+q\right)}{q^3\left(\bar{c}_1\mu_0+q\right)^3} < 0 \tag{74}$$

[11] 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. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May, 2014.

[12] 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.

[13] 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.

[14] 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.

[15] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[16] 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.

[17] 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.

[18] 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.

[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] 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. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May, 2015.

[21] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[22] 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.

[23] 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.

[24] 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.

[25] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818–830, Sep. 2011.

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

[27] 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.

[28] 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.

[29] 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.

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

[31] Q. Li and W. K. Ma, "Multicast secrecy rate maximization for MISO channels with multiple multi-antenna eavesdroppers," in *Proc. 2011 IEEE Int. Conf. Commun*, pp. 1–5, Kyoto, Japan, Jun. 2011.

[32] A. Shrestha, J. Jung, and K. Kwak, "Robust beamforming in cognitive radio," in *Proc. International Symposium on Communications and Information Technologies*, pp. 814–817, Sep. 2013.

[33] T. Lin, K.-Z. Huang, and W.-Y. Luo, "A multicarrier-based physical layer security scheme for the multicast systems," in *Proc. International Conference on Information Science and Technology*, pp. 1584–1587, Mar. 2013.

[34] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1864–1874, Sep. 2013.

[35] X. Liu, F. Gao, G. Wang, and X. Wang, "Joint beamforming and user selection in multicast downlink channel under secrecy-outage constraint," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 82–85, Jan. 2014.

[36] P. K. Gopala, L. Lai, and H. E. Gammal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[37] S. A. A. Fakoorian and L. A. Swindlehurst, "Solution for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[38] M. Dehghan, D. Goeckel, M. Ghaderi, and Z. Ding, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3025–3029, Sept. 2012.

[39] E. A. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," in *Proc. Int. Conf. Telecommun.*, pp. 1–6, 2008.

[40] J. Lin, A. P. Petropulu, and S. Weber, "Secrecy rate optimization under cooperation with perfect channel state information," in *Proc. Asilomar Conf. Sign., Syst. Comp., Pacific Grove, CA*, pp. 824–828, Nov. 2009.

[41] J. Yang, I. M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

[42] N. Sidiropoulos, T. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2239–2251, Jun. 2006.

[43] Z.-Q. Luo, W.-K. Ma, A.-C. So, Y. Ye, and S. Zhang, "Applications of convex optimization in signal processing and digital communication," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May, 2010.

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

Kanapathippillai Cumanan (M'10) received the B.Sc. (Hons.) degree in electrical and electronic engineering from the University of Peradeniya, Sri Lanka, in 2006, and the Ph.D. degree in signal processing for wireless communications from Loughborough University, Loughborough, U.K.,in 2009.

He is currently a Lecturer with the Department of Electronics, University of York, U.K. He was with the School of Electronic, Electrical and System Engineering, Loughborough University, U.K. He was a Teaching Assistant with the Department of Electrical and Electronic Engineering, University of Peradeniya, Sri Lanka, in 2006. In 2011, he was an Academic Visitor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. He was a Research Associate with the School of Electrical and Electronic Engineering, Newcastle University, U.K., from 2012 to 2014. His research interests include physical layer security, cognitive radio networks, relay networks, convex optimization techniques, and resource allocation techniques.

Dr. Cumanan was a recipient of an Overseas Research Student Award Scheme from Cardiff University, Wales, U.K., where he was a Research Student from 2006 to 2007.

Zhiguo Ding (S'03, M'05, SM'15) received the B.Eng. degree in electrical engineering from the Beijing University of Posts and Telecommunications, in 2000, and the Ph.D. degree in electrical engineering from Imperial College London, in 2005. From 2005 to 2014, he was with Queens University Belfast, Imperial College, and Newcastle University. Since 2014, he has been with Lancaster University as a Chair Professor. From 2012 to 2016, he was also with Princeton University as an Academic Visitor. His research interests are 5G networks, game theory, cooperative and energy harvesting networks, and statistical signal processing. He serves as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR NETWORKS, the IEEE WIRELESS COMMUNICATION LETTERS, the IEEE COMMUNICATION LETTERS, and the Journal of Wireless Communications and Mobile Computing. He received the best paper award at the IET Communcation Conference on Wireless, Mobile and Computing, 2009, the IEEE Communication Letter Exemplary Reviewer Award, 2012, and the EU Marie Curie Fellowship 2012-2014.

Mai Xu (M'10) received the B.S. degree from Beihang University in 2003, M.S. degree from Tsinghua University in 2006 and Ph.D degree from Imperial College London in 2010. From 2010-2012, he was working as a research fellow in the Electrical Engineering Department, Tsinghua University. Since Jan. 2013, he has been with Beihang University as an Associate Professor. During 2014 to 2015, he was a visiting researcher of MSRA. His research interests mainly include visual communication and image processing. He has published more than 50 technical papers in international journals and conference proceedings. He is the recipient of best paper awards of two IEEE conferences.

H. Vincent Poor (S'72, M'77, SM'82, F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering. From 2006 till 2016, he served as Dean of Princeton's School of Engineering and Applied Science. Dr. Poor's research interests are in the areas of statistical signal processing, stochastic analysis and information theory, and their applications in wireless networks and related fields. Among his publications in these areas is the recent book *Mechanisms and Games for Dynamic Spectrum Allocation* (Cambridge UniversityPress, 2014).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and a foreign member of the Royal Society. He is also a Fellow of the American Academy of Arts and Sciences and the National Academy of Inventors, and of other national and international academies. He received the Technical Achievement and Society Awards of the IEEE Signal Processing Society in 2007 and 2011, respectively. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, the 2015 EURASIP Athanasios Papoulis Award, the 2016 John Fritz Medal, and honorary doctorates from Aalborg University, Aalto University, HKUST and the University of Edinburgh.