Power Allocation for Cooperative Jamming Against a Strategic Eavesdropper over Parallel Channels

Zhifan Xu, *Student Member, IEEE*, Melike Baykal-Gürsoy

***Abstract*—This paper considers a friendly interferer allocating jamming power to eavesdropping channels to increase the level of secrecy of a wireless network. The friendly interferer has access to limited power, while the eavesdropper may not have the ability to attack all channels simultaneously. When all channels used for secret communication are under the threat of eavesdropping attacks, the optimal power allocation policy results from solving a convex optimization problem. In this case, the optimal policy is unique and can be obtained via a water-filling scheme. When the eavesdropper can not attack all channels, the eavesdropper should behave strategically and may select the targets probabilistically. We propose a non-zero-sum game that helps the friendly interferer predict and concentrate on the targets selected by the eavesdropper. Under certain conditions, we prove that there exists a unique Nash equilibrium (NE) strategy pair, which has a threshold type structure. We provide conditions under which the eavesdropper's equilibrium strategy is deterministic. We devise a strategy iteration algorithm to compute an equilibrium power allocation strategy. We present examples showing that the game-theoretic power allocation strategy performs better than the conservative power allocation strategy that assumes every channel to be under attack.**

***Index Terms*—Physical layer security, cooperative jamming, non-zero sum game, power control.**

I. Introduction

EAVESDROPPING attacks are major threats to wireless communication networks due to their multi-cast nature. The pioneering work of Shannon [1], Wyner [2], Csiszar and Korner [3], Leung-Yan-Cheong and Hellman [4] show that secrecy of wireless communication can be guaranteed through proper coding techniques if the legitimate communication channel's capacity is greater than the eavesdropper channel's capacity. The difference between the communication and eavesdropping channel capacities is then defined as the *Secrecy Capacity*, which is the primary metric to evaluate a wireless channel's secrecy level.

Instead of relying only on encryption and randomness in coding schemes, *Physical Layer Security* [5]–[7] has emerged as a viable, information theoretic approach to counter eavesdropping attacks by finding the optimal transmission signal configurations at the physical layer. A major physical layer security approach for a network of parallel channels is optimizing transmission power allocation to increase the network's secrecy capacity. This technology can achieve security even without the need for encryption/decryption [8].

Realizing that intentional interference or jamming may decrease the eavesdroppers' capabilities [9]–[12], the use of friendly jammers has been introduced as a promising approach for improving the secrecy capacity in physical layer security [13]–[16]. Tekin and Yener [15], [16] coin the term *cooperative jamming* for the proposed approach.

In this paper, we consider the problem of allocating friendly jamming power to a network of parallel channels in order to increase the total secrecy capacity of the network. Existing literature usually adopts the conservative assumption that all channels are attacked simultaneously by the eavesdropper [17]. However, the eavesdropper may have limited capability to attack a number of channels that must be chosen strategically, thus necessitating the inclusion of the eavesdropper as a strategic participant in a game-theoretic setting. We present conditions under which the best cooperative jamming power allocation strategy is unique and develop algorithms that converge to the best strategy.

A. Related Research

The effect of interference on eavesdroppers has inspired investigations into using intentionally generated interference signals to decrease the capacity of eavesdropping channels (see [13], [14]). Tekin and Yener [15], [16] study a Gaussian wireless wire-tap network consisting of multiple sender-receiver links and an eavesdropper. The authors show that the network's secrecy capacity could be increased if some senders choose to interfere the eavesdropper. Tang et al. [18], [19] analyze the maximum achievable secrecy rate when an independent friendly interferer is employed to jam passive eavesdroppers. Zhang et al. [20] consider the joint problem of subcarrier pairing and power allocation also with cooperative jamming. The authors assume the proportion of power used for cooperative jamming is fixed, moreover the eavesdropper is not strategic. A more comprehensive survey of the development of cooperative jamming can be found in [21].

Physical layer security, including cooperative jamming, relies on efficient power control allocation due to battery and power technology limitations in their current state, especially for networks of parallel channels. Wang *et al.* [8] investigate transmission power control and sub-carrier assignment under a power constraint over an OFDMA network between a single base station and two types of receivers maintaining the long term secret transmission rate for secure users, while maximizing the expected overall achievable information rate

This material is based upon work supported by the National Science Foundation under Grant No.1901721

Zhifan Xu is with the Department of Industrial and Systems Engineering, Rutgers University, Piscataway, NJ, 08854, USA. E-mail: zhifan.xu@rutgers.edu.

Melike Baykal-Gürsoy is with the Department of Industrial and Systems Engineering of Rutgers University, RUTCOR and CAIT. E-mail: gursoy@soe.rutgers.edu.

for normal users. Karachontzitis *et al.* [22] study the secrecy performance of such an OFDMA network under the attack of a passive eavesdropper, while focusing on max-min fairness criteria over users secrecy rate as the objective. They formulate a mixed integer nonlinear program to find the base station's best action. A brief review of resource allocation over parallel channels can be found in chapter 8 of [6].

Resource allocation, especially power allocation under constraints, is also a key problem for operations of cooperative jamming over complex wireless networks. Dong *et al.* [23] investigate the power allocation problem between a transmitter and a friendly interferer, who has multiple antennas. Rabbachin *et al.* [24] consider a wireless network assisted by multiple friendly interferers. Hu *et al.* [25] discuss a situation in which a transmitter embeds artificial noise in the transmission signal while aided by a friendly interferer at the same time. The authors solve for the transmitter's optimal power level to generate artificial noise in order to maximize the secrecy rate under a bounded secrecy outage probability. Zhang *et al.* [17] consider an orthogonal frequency-division multiplexing (OFDM) network with N mutually independent sub-carriers, where a friendly interferer first harvests wireless charging power from the transmitter and then jams a passive eavesdropper. Instead of assuming that a central controller manages transmitters and friendly interferers, game-theoretic models have been adopted to study the interaction between transmitters and friendly interferers. Han *et al* [26] investigate a Stackelberg pricing game in which multiple friendly interferers bargain with the users of a single wireless communication network. Wang *et al.* [27] propose another Stackelberg pricing game for a multi-user OFDM network in which the users bid for cooperative jamming power for their own sub-channels.

Game theory has been widely adopted for solving power control problems against intelligent adversaries over wireless networks. Altman *et al.* [28] obtain a base station's optimal power allocation strategy against an intelligent jammer. Yang *et al.* [29] construct an optimal transmission power allocation plan for a multi-channel wireless network using a Stackelberg game, in which a smart jammer can adjust the jamming strategy based on observed transmission configuration. Game-theoretic power control and resource allocation algorithms are also crucial for anti-eavesdropping physical layer security methods to maximize the secrecy capacity of wireless networks. Gabalou and Maham [30] propose a zero-sum game for a secure OFDMA system under the attack of a hostile jammer, in which the base station needs to guarantee no user can overhear transmissions on sub-carriers used by other users. Yüksel *et al.* [31] investigate a rate allocation game between a sender and a hostile jammer who cooperates with a passive eavesdropper. Recently, Garnaev and Trappe [32] study a power control game with a transmitter facing a strategic jammer and a passive eavesdropper simultaneously. Game theoretic approaches have been used to find optimal transmission power against other type of adversaries. Garnaev and Trappe [33] introduce a zero-sum power allocation game for a transmitter working against nature. The authors present another power control game against a strategic eavesdropper that can eavesdrop only on one of multiple parallel channels in [34]. It is shown that Nash Equilibria of such games exhibit the water-filling principle [35], [36].

Few researchers have considered the eavesdropper as a strategic participant in the literature of cooperative jamming until recently. Garnaev *et al.* [37] describe the interaction between a friendly interferer and an eavesdropper on a multi-channel wireless network using a zero-sum game, in which both players can only select one channel as target. Xu and Baykal-Gürsoy [38] is the first to study the power control problem for a friendly interferer on a multi-channel network against a strategic eavesdropper who can only attack a single channel. This paper completes the discussion in [38] by including the full representation of the Nash equilibrium against a more capable eavesdropper who can attack multiple channels simultaneously. We also relax our previous assumptions on the value of channel state information, and still take into consideration the detrimental effect of cooperative jamming on legitimate communication.

B. Contributions

The contributions of this paper can be summarized as follows:

1) We present a game-theoretic model for a friendly interferer to decide on allocating cooperative jamming power over a network of parallel channels. In contrast to the most prior work, the strategic behavior of eavesdroppers is taken into consideration.
2) As opposed to the prior research that assumes a strategic eavesdropper who can attack only one channel, we extend the analysis to multi-channel attack situations.
3) We show that there always exists a unique Nash Equilibrium, and the friendly interferer can find the equilibrium strategy pair through a numerical search algorithm.
4) We demonstrate that the detrimental effect of cooperative jamming plays an important role in the problem formulation.

The organization of the paper is as follows: Section II sets up the background of the problem. Section III is the main part of the paper, which reveals the Nash Equilibrium's water-filling structure in a cooperative jamming game with an eavesdropper that can attack n of N channels. Different methods to find the Nash Equilibrium are presented depending on the value of n. Section IV demonstrates numerical examples. Section V summarizes our results and discusses future research.

II. System Model and Problem Formulation

A. System Model

Consider a wireless communication network consisting of N parallel legitimate source-receiver channels. This paper adopts a block-based quasi-static channel model [8], [17] by assuming the channel state information (CSI) remain constant over a transmission block of length B, and may change from one block to another. A friendly interferer (Ian) can assign J_i out of J amount of power to interfere a potential eavesdropper who tries to attack channel i. An eavesdropper (Eve) can

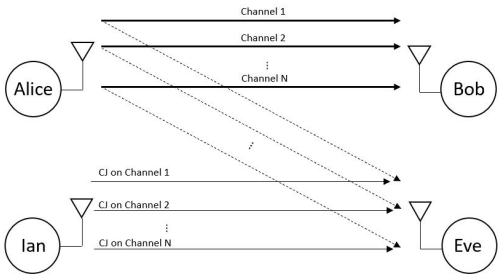


Fig. 1: Cooperative jamming (CJ) over parallel channels

attack n out of N channels simultaneously. Such a network of parallel channels can be an OFDM system of N orthogonal sub-carriers, where each sub-carrier is a Gaussian fading channel under potential attack of a wireless eavesdropping channel [17].

For each legitimate source-receiver channel $i \in \{1, ..., N\}$, the communication capacity that can be used to transmit confidential messages under cooperative jamming is

$$C_{L_i}(J_i) = \ln\big(1 + \frac{g_i^L T_i}{\sigma^2 + h_i^L J_i}\big),$$

where T_i is a fixed transmission power applied to channel i. Note that perfect interference cancellation at the legitimate channel i, i.e., $h_i^L = 0$, is a special case. Ideally, every channel i should have $h_i^L = 0$, which might be achieved if Ian can share the jamming signals generators and random seed chosen at the beginning of each transmission block with Bob [39]. In general, cooperative jamming signals may not be canceled out at evert channel [17], [18]. This paper studies the general case where $h_i^L \geq 0$, so legitimate source-receiver channels may be degraded by cooperative jamming. It will be shown that the value of h_i^Ls significantly affect the friendly interferer's decisions.

Following the Gaussian wire-tap model [4], the eavesdropper can intercept the information transmitted over channel i through an eavesdropping channel with capacity

$$C_{E_i}(J_i) = \ln\big(1 + \frac{g_i^E T_i}{\sigma^2 + h_i^E J_i}\big).$$

Without the threat of an eavesdropping attack, Alice and Bob can utilize channel i's full communication capacity $C_{L_i}(J_i)$ to transmit messages securely. Meanwhile, under an eavesdropping attack, channel i's capacity that can be used to transmit secret messages is defined as its secrecy capacity $C_{S_i}(J_i)$ (see [2], [4], [24], [26]), which is

$$C_{S_i}(J_i) = \left[C_{L_i}(J_i) - C_{E_i}(J_i)\right]^+,$$

where $[x]^+ \coloneqq \max\{x, 0\}$.

Each quasi-static transmission block consists of the following 4 stages.

1. **CSI estimation and exchanging.** Alice, Bob and Ian will first observe the instantaneous CSI g_i^Ls and h_i^Ls. This paper considers the scenario in which the instantaneous CSI of intended receiver, g_i^Ls and h_i^Ls, are perfectly known (see, e.g., [17], [23], [40], [41]). Because the eavesdropper is typically in passive listening mode, only statistical CSIs of the eavesdropping channels are available [42]–[45]. Deep-learning based methods are currently being developed for various scenarios to achieve more accuracy in CSI estimation [46]–[48]. Here g_i^Es and h_i^Es may denote gain estimates or may correspond to worst case values. For the sake of simplicity, we assume $g_i^L \neq g_i^E$ and $h_i^L \neq h_i^E$.
2. **Start of communication.** Alice decides on transmission power T_i for every channel i. In this paper, Alice adopt an on-off transmission scheme [49] such that channel i with $g_i^L < g_i^E$ will not be used to exchange secret messages in this block since the default secrecy capacity $C_{S_i}(0) = 0$. Transmission power T_is will then be observed by Ian and Eve.
3. **Anti-eavesdropping cooperative jamming.** Ian and the Eve will make their decisions simultaneously. Ian needs to decide the level of J_i for cooperative jamming to enhance the secret communication over channel i. Hence, a power allocation policy for the friendly interferer is a vector $\boldsymbol{J} = (J_1, ..., J_N)$ such that $\sum_{i=1}^N J_i \leq J$. Meanwhile, Eve decides on which channels to attack.
4. **End of communication.** Alice, Ian and Eve stop their actions at the end of the transmission block.

The whole transmission block involves two-level decision-making. In the first level, Alice acts as a leader, deciding on T_is while anticipating the actions of Ian and Eve. In the second level, Ian and Eve need to decide on power allocation and attack actions, respectively. This paper focuses on the second level problem, that is, to find the optimal cooperative jamming power allocation strategies for the friendly interferer at stage 3, which lays the foundation for the source to decide how to cooperate with the friendly interferer back in the first level problem.

Remark. For channel i with $g_i^L < g_i^E$, although $C_{S_i}(0) = 0$, it may still be possible to achieve positive secrecy capacity under friendly jamming if also $h_i^L < h_i^E$ and $\frac{g_i^L}{g_i^E} > \frac{h_i^L}{h_i^E}$. However, positive secrecy capacity is possible only if $J_i > \hat{J}_i$ for some lower bound $\hat{J}_i$. Besides, the friendly interferer may not have enough power to satisfy these lower bound constraints. Deciding which channels to jam among such channels against an eavesdropper who can simultaneously attack every channel leads to mixed integer non-linear programming (MINLP) problems that are nonconvex. Solving such MINLP is beyond the scope of this paper. Thus, we impose the above on-off transmission scheme for senders.

B. Problem Formulation

Our objective is to help the friendly interferer find a power allocation strategy $\boldsymbol{J}$ at stage 3 to maximize the expected transmission rate that can be used for secret communication over the whole network, assuming the eavesdropper will attack strategically. Let $\mathcal{I} = \{i | g_i^L > g_i^E, T_i > 0, i = 1, ..., N\}$ be the set of channels used for sending secret messages in a transmission block. Clearly, $J_i = 0, \ \forall i \notin \mathcal{I}$.

If the number of channels in $\mathcal{I}$, that is the cardinality of $\mathcal{I}$, denoted as $|\mathcal{I}|$, satisfies $|\mathcal{I}| \leq n$, then the eavesdropper can simply listen on all ongoing secret communications simultaneously. Thus, the friendly interferer needs to solve the following optimization problem,

$$\begin{aligned} \max_{\boldsymbol{J}} \quad & u_S(\boldsymbol{J}) = \sum_{i\in\mathcal{I}} C_{S_i}(J_i) = \sum_{i\in\mathcal{I}} [C_{L_i}(J_i) - C_{E_i}(J_i)]^+ \\ \text{s.t.} \quad & \sum_{i\in\mathcal{I}} J_i \leq J, \\ & J_i \geq 0, \quad \forall i \in \mathcal{I}, \\ & J_i = 0, \quad \forall i \notin \mathcal{I}, \end{aligned} \tag{1}$$

where $u_S(\boldsymbol{J})$ is the total secrecy capacity of the network. Note that $C_{S_i}(J_i)$ may not be a concave function even though both $C_{L_i}(J_i)$ and $C_{E_i}(J_i)$ are decreasing and concave, especially if cooperative jamming decreases $C_{L_i}(J_i)$ faster than $C_{E_i}(J_i)$.

On the other hand, if $|\mathcal{I}| > n$, then the eavesdropper needs to pick the targets to attack intelligently. This paper considers a scenario in which the eavesdropper probabilistically selects targets in order to maximize the expected total achievable rate for eavesdropping over all channels being used for secret communication. Let p_i represent the probability that channel i is targeted by the eavesdropper. Note that, the eavesdropper will only target channel i if it is being used for secret communication in the current block, i.e., $i \in \mathcal{I}$. Hence, an attack policy for the eavesdropper is a vector $\boldsymbol{p} = (p_1, ..., p_N)$ such that: 1) $p_i = 0, \ \forall i \notin \mathcal{I}$; 2) $0 \leq p_i \leq 1, \ \forall i \in \mathcal{I}$; and 3) $\sum_{i\in\mathcal{I}} p_i = n$. Let R_{E_i} be the random variable representing the achievable rate for eavesdropping over channel i such that

$$R_{E_i} = \begin{cases} C_{E_i}(J_i), & \text{with probability } p_i, \\ 0, & \text{with probability } 1 - p_i. \end{cases}$$

Let R_{S_i} be the random variable representing the achievable rate for secret transmissions over channel i such that

$$R_{S_i} = \begin{cases} C_{S_i}(J_i), & \text{with probability } p_i, \\ C_{L_i}(J_i), & \text{with probability } 1 - p_i. \end{cases}$$

Therefore, given a pair of power allocation policy $\boldsymbol{J}$ and attack policy $\boldsymbol{p}$, the eavesdropper's payoff is,

$$u_E(\boldsymbol{J}, \boldsymbol{p}) = \mathbb{E}\left[\sum_{i\in\mathcal{I}} R_{E_i}\right] = \sum_{i\in\mathcal{I}} p_i C_{E_i}(J_i), \tag{2}$$

and the friendly interferer's payoff is the expected total achievable rate for secret communication, that is,

$$\begin{aligned} u_S(\boldsymbol{J}, \boldsymbol{p}) &= \mathbb{E}\left[\sum_{i\in\mathcal{I}} R_{S_i}\right] \\ &= \sum_{i\in\mathcal{I}} \left[(1-p_i) C_{L_i}(J_i) + p_i C_{S_i}(J_i)\right]. \end{aligned} \tag{3}$$

From another point of view, $u_S(\boldsymbol{J}, \boldsymbol{p})$ quantifies the average portion of transmission rate that is secured if Alice simply uses $C_{L_i}(J_i)$ as the default transmission rate for channel $i \in \mathcal{I}$.

Since it is difficult for the friendly interferer and the eavesdropper to know each other's decision ahead of time, this paper considers that the friendly interferer and the eavesdropper are playing a Nash game. That is, they aim to find the best power allocation policy $\boldsymbol{J}^*$ and best attack policy $\boldsymbol{p}^*$ such that

$$u_S(\boldsymbol{J}^*, \boldsymbol{p}^*) \geq u_S(\boldsymbol{J}, \boldsymbol{p}^*), \quad \forall \boldsymbol{J} \in \mathcal{J}, \tag{4}$$

$$u_E(\boldsymbol{J}^*, \boldsymbol{p}^*) \geq u_E(\boldsymbol{J}^*, \boldsymbol{p}), \quad \forall \boldsymbol{p} \in \mathcal{P}, \tag{5}$$

where $\mathcal{J}$ and $\mathcal{P}$ are the space of all possible policies of the friendly interferer and the eavesdropper, respectively.

III. Solutions of the Power Allocation Policy

This section discusses the optimal power allocation policy $\boldsymbol{J}^*$ for cooperative jamming at stage 3 of a transmission block. The friendly interferer first comes up with the set of channels $\mathcal{I}$ to be enhanced, and then solves one of the following problems depending on the value of $|\mathcal{I}|$.

A. When $|\mathcal{I}| \leq n$

In this case, $\boldsymbol{J}^*$ is the solution to optimization problem (1). Whether it is beneficial to enhance channel $i \in \mathcal{I}$ is related to how serious the communication signals sent to Bob over channel i will suffer from cooperative jamming, that is, the instantaneous value of h_i^L.

If $h_i^L > h_i^E$, Bob suffers more from the cooperative jamming signal than Eve over channel i. The following lemma provides a formal proof for the intuitive conclusion that not interfering channel i is the best defense policy in this situation.

Lemma 1. *For $i \in \mathcal{I}$, if $h_i^L > h_i^E$, then $C_{S_i}(0) > 0$ and $C_{S_i}(0) > C_{S_i}(J_i), \forall J_i > 0$.*

Proof. Notice $g_i^L > g_i^E$ for $i \in \mathcal{I}$, it follows that $C_{S_i}(0) = C_{L_i}(0) - C_{E_i}(0) > 0$ by definition.

Given $h_i^L > h_i^E$, assume there exists $J_i > 0$ such that $C_{S_i}(0) \leq C_{S_i}(J_i)$. It follows that $C_{S_i}(J_i) > 0$. Therefore,

$$\begin{aligned} & \exp\left(C_{S_i}(J_i)\right) \geq \exp\left(C_{S_i}(0)\right), \\ \Rightarrow & \left(1+\tfrac{g_i^L T_i}{\sigma^2+h_i^L J_i}\right) / \left(1+\tfrac{g_i^E T_i}{\sigma^2+h_i^E J_i}\right) \geq \left(1+\tfrac{g_i^L T_i}{\sigma^2}\right) / \left(1+\tfrac{g_i^E T_i}{\sigma^2}\right), \\ \Rightarrow & \left(1+\tfrac{g_i^E T_i}{\sigma^2}\right) / \left(1+\tfrac{g_i^E T_i}{\sigma^2+h_i^E J_i}\right) \geq \left(1+\tfrac{g_i^L T_i}{\sigma^2}\right) / \left(1+\tfrac{g_i^L T_i}{\sigma^2+h_i^L J_i}\right), \\ \Rightarrow & \frac{1+\frac{g_i^E T_i}{\sigma^2}}{1+\frac{g_i^E T_i}{\sigma^2+h_i^L J_i}} > \frac{1+\frac{g_i^L T_i}{\sigma^2}}{1+\frac{g_i^L T_i}{\sigma^2+h_i^L J_i}}, \text{given } h_i^L > h_i^E, \\ \Rightarrow & \frac{\sigma^2 + g_i^E T_i}{\sigma^2 + h_i^L J_i + g_i^E T_i} > \frac{\sigma^2 + g_i^L T_i}{\sigma^2 + h_i^L J_i + g_i^L T_i}, \end{aligned}$$

which is impossible when $g_i^L > g_i^E$. So the assumption can not be true. □

Hence, $J_i^* = 0$ if $h_i^L > h_i^E, \forall i \in \mathcal{I}$. The friendly interferer should then consider only enhancing channels with $h_i^L < h_i^E$. The next lemma shows that the objective function of optimization problem (1) can now be simplified by dropping $[]^+$ in $C_{S_i}(J_i)$, that is $C_{S_i}(J_i) = C_{L_i}(J_i) - C_{E_i}(J_i)$ if $h_i^L < h_i^E, \forall i \in \mathcal{I}$.

Lemma 2. *For $i \in \mathcal{I}$, if $h_i^L < h_i^E$, then $C_{S_i}(J_i) > 0, \forall J_i > 0$.*

Proof. It must be true that $\frac{g_i^L T_i}{\sigma^2+h_i^L J_i} > \frac{g_i^E T_i}{\sigma^2+h_i^E J_i}, \forall J_i > 0$, given $g_i^L > g_i^E$ and $h_i^L < h_i^E$. It follows that $C_{L_i}(J_i) > C_{E_i}(J_i), \forall J_i > 0$. □

Let $\mathcal{I}^+ = \{i | h_i^L < h_i^E, i \in \mathcal{I}\}$ be the subset of channels to be protected by friendly interferer, and let $\mathcal{I}^- = \mathcal{I} \setminus \mathcal{I}^+$. Then the objective function of optimization problem (1) can be reduced to

$$\begin{aligned} u_S(\boldsymbol{J}) &= \sum_{i\in\mathcal{I}^+} C_{S_i}(J_i) + \sum_{i\in\mathcal{I}^-} C_{S_i}(0) \\ &= \sum_{i\in\mathcal{I}^+} [C_{L_i}(J_i) - C_{E_i}(J_i)] + \sum_{i\in\mathcal{I}^-} C_{S_i}(0). \end{aligned}$$

Let

$$c_i(J_i) \coloneqq \frac{d}{dJ_i} C_{S_i}(J_i) = \frac{d}{dJ_i} C_{L_i}(J_i) - \frac{d}{dJ_i} C_{E_i}(J_i),$$

where

$$\frac{d}{dJ_i} C_{L_i}(J_i) = \frac{-g_i^L h_i^L T_i}{(g_i^L T_i + \sigma^2 + h_i^L J_i)(\sigma^2 + h_i^L J_i)},$$

$$\frac{d}{dJ_i} C_{E_i}(J_i) = \frac{-g_i^E h_i^E T_i}{(g_i^E T_i + \sigma^2 + h_i^E J_i)(\sigma^2 + h_i^E J_i)}.$$

Clearly, if $h_i^L = 0$, then $i \in \mathcal{I}^+$, moreover $c_i(J_i) > 0$ and decreasing w.r.t. $J_i \geq 0$. Thus $C_{S_i}(J_i)$ is increasing and concave w.r.t. $J_i \geq 0$.

If $0 < h_i^L < h_i^E$, then $C_{S_i}(J_i)$ has the following properties [38]:

- $C_{S_i}(J_i)$ is unimodal w.r.t. $J_i \in [0, +\infty)$, and there exists a unique $\bar{J}_i \geq 0$ such that $c_i(\bar{J}_i) = 0$,
- $C_{S_i}(J_i)$ is increasing and concave w.r.t. $J_i \in [0, \bar{J}_i]$,

Define

$$\bar{J}_i = \begin{cases} +\infty, & \text{if } h_i^L = 0, \\ \arg\max\limits_{J_i \geq 0} C_{S_i}(J_i), & \text{if } 0 < h_i^L < h_i^E, \end{cases} \tag{6}$$

then $C_{S_i}(J_i) = C_{L_i}(J_i) - C_{E_i}(J_i)$ is a positive, increasing and concave function w.r.t. $0 \leq J_i \leq \bar{J}_i$ for every channel $i \in \mathcal{I}^+$.

Remark. If $h_i^L \neq 0$, it is possible to have $\bar{J}_i = 0$ for $i \in \mathcal{I}^+$. Note that, if $c_i(0) \leq 0$ for $i \in \mathcal{I}^+$, that is,

$$\frac{g_i^L h_i^L}{g_i^E h_i^E} \cdot \frac{g_i^E T_i + \sigma^2}{g_i^L T_i + \sigma^2} \geq 1,$$

then $C_{S_i}(J_i)$ is non-increasing w.r.t. $J_i \geq 0$ and $\bar{J}_i = 0$ follows.

Therefore, optimization problem (1) can be reduced to

$$\begin{aligned} \max_{\boldsymbol{J}} \quad & u_S(\boldsymbol{J}) = \sum_{i\in\mathcal{I}^+} [C_{L_i}(J_i) - C_{E_i}(J_i)] + \sum_{i\in\mathcal{I}^-} C_{S_i}(0) \\ \text{s.t.} \quad & \sum_{i\in\mathcal{I}^+} J_i \leq J, \\ & 0 \leq J_i \leq \bar{J}_i, \quad \forall i \in \mathcal{I}^+, \\ & J_i = 0, \quad \forall i \notin \mathcal{I}^+, \end{aligned} \tag{7}$$

which is a convex optimization problem that can be solved using existing convex optimization software [50]–[52]. Moreover, $\boldsymbol{J}^*$ is subject to a water-filling structure. For the sake of simplicity, we adopt a common assumption that all wireless channels are sorted (see, e.g., [37], [53]). For the case $|\mathcal{I}| \leq n$, we assume the channels are sorted in the following way.

Algorithm 1 Finding $\boldsymbol{J}^*$ when $|\mathcal{I}| \leq n$

Input: $C_{S_i}(J_i)$ and $c_i(J_i)$ functions for all $i \in \mathcal{I}^+$; total power: J; and tolerance: $\epsilon \leq 0.01$.
Output: Optimal power allocation strategy $\boldsymbol{J}^*$.

```
Initialization: Find M̄. Define c_{M̄+1}(0) = 0.
Compute J̄_i as the solution of c_i(J_i) = 0, ∀i = 1, ..., M̄.
if (Σ_{i=1}^{M̄} J̄_i < J) then
    Let J_i^* ← J̄_i, ∀i = 1, ..., M̄.
else
    for (m = 1 to M̄) do
        w ← c_{m+1}(0).
        Compute J* as solution of (8).
        if (Σ_{i=1}^{m} J_i^* ≥ J − ε) then
            break.
        end if
    end for
    w_A^{UB} ← c_m(0) and w_A^{LB} ← w.
    while (|Σ_{i=1}^{m} J_i^* − J| > ε) do
        w ← ½(w_A^{UB} + w_A^{LB}).
        Compute J* as solution of (8).
        if (Σ_{i=1}^{m} J_i^* − J < −ε) then
            w_A^{UB} ← w.
        else if (Σ_{i=1}^{m} J_i^* − J > ε) then
            w_A^{LB} ← w.
        end if
    end while
end if
return J*.
```

Assumption 1. *Assume $\mathcal{I}^+ = \{1, ..., M\}$ where $M \leq N$, and $c_1(0) > ... > c_M(0)$.*

This assumption can be satisfied by re-labeling all channels in $\mathcal{I}^+$. Then, as shown in Theorem 1 of [38], there exists an index $m \geq 0$ and a real value $w \geq 0$ such that

$$\begin{cases} c_1(J_1^*) = ... = c_m(J_m^*) = w, \\ J_i^* = 0, \ \forall i > m. \end{cases} \tag{8}$$

Let $\bar{M}$ be the largest positive integer such that $\bar{M} \leq M$ and $c_{\bar{M}}(0) > 0$. Clearly, $m \leq \bar{M}$. Hence, we propose Algorithm 1 to find $\boldsymbol{J}^*$ by performing bisection search on the value of w.

B. When $|\mathcal{I}| > n$

In this case, $\boldsymbol{J}^*$ is a part of the Nash equilibrium (NE) strategy pair $(\boldsymbol{J}^*, \boldsymbol{p}^*)$ that satisfies NE conditions (4) and (5), which are equivalent to optimization problems given the adversary's decision for the friendly interferer and the eavesdropper, respectively.

Firstly, consider the NE condition (5) that describes the eavesdropper's strategic behaviors. Given a power allocation

policy $\boldsymbol{J}^*$, the eavesdropper's best response $\boldsymbol{p}^*$ is the solution to the following optimization problem

$$\begin{aligned} \max_{\boldsymbol{p}} \quad & u_E(\boldsymbol{J}^*, \boldsymbol{p}) = \sum_{i\in\mathcal{I}} p_i C_{E_i}(J_i^*) \\ \text{s.t.} \quad & \sum_{i\in\mathcal{I}} p_i = n, \\ & 0 \le p_i \le 1, \quad \forall i \in \mathcal{I}, \\ & p_i = 0, \quad \forall i \notin \mathcal{I}, \end{aligned} \tag{9}$$

which is a linear optimization problem, since $u_E(\boldsymbol{J}^*, \boldsymbol{p})$ is linear in $\boldsymbol{p} \in \mathcal{P}$ and feasible region $\mathcal{P}$ is convex and compact.

Secondly, consider the NE condition (4) that describes the optimal power allocation policy. Given an attack policy $\boldsymbol{p}^*$, the friendly interferer's best response $\boldsymbol{J}^*$ is the solution to the following optimization problem

$$\begin{aligned} \max_{\boldsymbol{J}} \quad & u_S(\boldsymbol{J}, \boldsymbol{p}^*) = \sum_{i\in\mathcal{I}} [(1-p_i^*)C_{L_i}(J_i) + p_i^* C_{S_i}(J_i)] \\ \text{s.t.} \quad & \sum_{i\in\mathcal{I}} J_i \le J, \\ & J_i \ge 0, \quad \forall i \in \mathcal{I}, \\ & J_i = 0, \quad \forall i \notin \mathcal{I}. \end{aligned} \tag{10}$$

Still, we may have either $h_i^L > h_i^E$ or $h_i^L < h_i^E$ for $i \in \mathcal{I}$. Now define $G_i(J_i|p_i^*) \coloneqq (1-p_i^*)C_{L_i}(J_i) + p_i^* C_{S_i}(J_i)$ as a function of J_i. The next lemma shows that, if $h_i^L > h_i^E$ for a channel $i \in \mathcal{I}$, then any power allocation strategy $\boldsymbol{J}$ with $J_i > 0$ is dominated.

Lemma 3. *$\forall i \in \mathcal{I}$, if $h_i^L > h_i^E$, then $G_i(0|p_i^*) > 0$ and $G_i(0|p_i^*) > G_i(J_i|p_i^*), \forall J_i > 0$.*

Proof. Note that $g_i^L > g_i^E, \forall i \in \mathcal{I}$, then $C_{S_i}(0) > 0$ follows. Since $C_{L_i}(0) > 0$ by definition, so $G_i(0|p_i^*) > 0$.

Given $g_i^L > g_i^E$ and $h_i^L > h_i^E$, $C_{S_i}(0) > C_{S_i}(J_i), \forall J_i > 0$ by lemma 1. Also, $C_{L_i}(J_i)$ is strictly decreasing w.r.t. $J_i \ge 0$, so $G_i(0|p_i^*) > G_i(J_i|p_i^*), \forall J_i > 0$ follows. □

Hence, the friendly defender should only consider to allocate cooperative jamming power to channel i with $h_i^L < h_i^E$. Still let $\mathcal{I}^+ = \{i | h_i^L < h_i^E, i \in \mathcal{I}\}$, then $C_{S_i}(J_i) > 0, \forall i \in \mathcal{I}^+$, by lemma 2. It follows that,

$$G_i(J_i|p_i^*) = C_{L_i}(J_i) - p_i^* C_{E_i}(J_i), \forall i \in \mathcal{I}^+.$$

Intuitively, when $p_i^* = 0$, then $G_i(J_i|p_i^*)$ is non-increasing w.r.t. $J_i \ge 0$, so the friendly interferer should not work on that channel $i \in \mathcal{I}^+$. When $p_i^* > 0$ and $h_i^L = 0$, similar to $C_{S_i}(J_i)$, $G_i(J_i|p_i^*)$ has the following properties for a channel $i \in \mathcal{I}^+$:

- $G_i(J_i|p_i^*) > 0$ w.r.t. $J_i \in [0, +\infty)$,
- $G_i(J_i|p_i^*)$ is concave and increasing w.r.t. $J_i \in [0, +\infty)$.

When $p_i^* > 0$ and $0 < h_i^L < h_i^E$, $G_i(J_i|p_i^*)$ has the following properties $\forall i \in \mathcal{I}^+$:

- $G_i(J_i|p_i^*) > 0$ w.r.t. $J_i \in [0, +\infty)$,
- $G_i(J_i|p_i^*)$ is a unimodal function w.r.t. $J_i > 0$, and there exists a unique $\bar{J}_{i|p_i^*} \ge 0$ such that $G_i(J_i|p_i^*)$ reaches its maximum at $J_i = \bar{J}_{i|p_i^*}$.
- $G_i(J_i|p_i^*)$ is concave and increasing w.r.t. $J_i \in [0, \bar{J}_{i|p_i^*}]$.

In summary, define

$$\bar{J}_{i|p_i^*} = \begin{cases} 0, & \text{if } p_i^* = 0, \\ +\infty, & \text{if } p_i^* > 0 \text{ and } h_i^L = 0, \\ \arg\max\limits_{J_i \ge 0} G_i(J_i|p_i^*), & \text{if } p_i^* > 0 \text{ and } 0 < h_i^L < h_i^E, \end{cases} \tag{11}$$

then $G_i(J_i|p_i^*)$ is a positive, increasing and concave function w.r.t. $0 \le J_i \le \bar{J}_i$ for every channel $i \in \mathcal{I}^+$.

Remark. When $h_i^L > 0$, it is possible that $\bar{J}_{i|p_i^*} = 0$ for $i \in \mathcal{I}^+$ even though $p_i^* > 0$, as long as p_i^* is small enough. To see this, let

$$c_i(J_i|p_i^*) \coloneqq \frac{\partial G_i(J_i|p_i^*)}{\partial J_i} = \frac{d}{dJ_i} C_{L_i}(J_i) - p_i^* \frac{d}{dJ_i} C_{E_i}(J_i).$$

If $c_i(J_i|p_i^*) \le 0$, that is,

$$p_i^* \le \frac{g_i^L h_i^L}{g_i^E h_i^E} \cdot \frac{g_i^E T_i + \sigma^2}{g_i^L T_i + \sigma^2},$$

then $c_i(J_i|p_i^*) \le 0, \ \forall J_i \ge 0$. It follows that $G_i(J_i|p_i^*)$ is non-increasing w.r.t. $J_i \ge 0$ and reaches its maximal at $\bar{J}_{i|p_i^*} = 0$.

Clearly, $J_i^* = 0, \forall i \in \mathcal{I}^-$, and $C_{S_i}(0) > 0, \forall i \in \mathcal{I}^-$, since $g_i^L > g_i^E$. It follows that

$$G_i(0|p_i^*) = C_{L_i}(0) - p_i^* C_{E_i}(0), \forall i \in \mathcal{I}^-.$$

Therefore, optimization problem (10) can be reduced to

$$\begin{aligned} \max_{\boldsymbol{J}} \quad & u_S(\boldsymbol{J}, \boldsymbol{p}^*) = \sum_{i\in\mathcal{I}^+} G_i(J_i|p_i^*) + \sum_{i\in\mathcal{I}^-} G_i(0|p_i^*) \\ & \qquad = \sum_{i\in\mathcal{I}^+} [C_{L_i}(J_i) - p_i^* C_{E_i}(J_i)] \\ & \qquad + \sum_{i\in\mathcal{I}^-} [C_{L_i}(0) - p_i^* C_{E_i}(0)] \\ \text{s.t.} \quad & \sum_{i\in\mathcal{I}^+} J_i \le J, \\ & 0 \le J_i \le \bar{J}_{i|p_i^*}, \quad \forall i \in \mathcal{I}^+, \\ & J_i = 0, \quad \forall i \notin \mathcal{I}^+, \end{aligned} \tag{12}$$

which has a concave objective function as well as a convex and compact feasible region. And optimization problem (9) can be reduced to

$$\begin{aligned} \max_{\boldsymbol{p}} \quad & u_E(\boldsymbol{J}^*, \boldsymbol{p}) = \sum_{i\in\mathcal{I}^+} p_i C_{E_i}(J_i^*) + \sum_{i\in\mathcal{I}^-} p_i C_{E_i}(0) \\ \text{s.t.} \quad & \sum_{i\in\mathcal{I}} p_i = n, \\ & 0 \le p_i \le 1, \quad \forall i \in \mathcal{I}, \\ & p_i = 0, \quad \forall i \notin \mathcal{I}, \end{aligned} \tag{13}$$

which is still a linear optimization problem.

The NE strategy pair $(\boldsymbol{J}^*, \boldsymbol{p}^*)$ are solutions to optimization problems (12) and (13), respectively. Since $u_S(\boldsymbol{J}, \boldsymbol{p}^*)$ is concave in $\boldsymbol{J}$, while $u_E(\boldsymbol{J}^*, \boldsymbol{p})$ is linear in $\boldsymbol{p}$ in their respective compact and convex feasible regions, the existence a unique NE strategy pair $(\boldsymbol{J}^*, \boldsymbol{p}^*)$ is guaranteed [54]. However, this strategy pair cannot be obtained in closed form. Thus, in the next subsections, we will state some properties of the NE in order to design an algorithm that converges to the equilibrium.

1) Structure of the NE: For a pair of NE strategies $(\boldsymbol{J}^*, \boldsymbol{p}^*)$, the KKT optimality conditions should hold. From the defender's perspective, optimal power allocation strategy $\boldsymbol{J}^*$ should subject to KKT conditions for optimization problem (12), i.e., there exists a Lagrange multiplier $w_D \geq 0$ such that, for all $i \in \mathcal{I}^+$,

$$\frac{\partial u_S(\boldsymbol{J}^*, \boldsymbol{p}^*)}{\partial J_i} \coloneqq \frac{d}{dJ_i} C_{L_i}(J_i^*) - p_i^* \frac{d}{dJ_i} C_{E_i}(J_i^*) \begin{cases} = w_D, \text{ if } \ J_i^* > 0, \\ \leq w_D, \text{ if } \ J_i^* = 0, \end{cases} \tag{14}$$

and also $w_D(\sum_{i\in\mathcal{I}^+} J_i^* - J) = 0$. Notice that, for all $i \in \mathcal{I}^+$, $\frac{d}{dJ_i} C_{L_i}(J_i) < 0$ and $\frac{d}{dJ_i} C_{E_i}(J_i) < 0, \ \forall J_i \geq 0$.

Similarly, the eavesdropper's optimal attack strategy $\boldsymbol{p}^*$ should subject to KKT conditions for optimization problem (13), i.e., there exists a Lagrange multiplier $w_A \geq 0$ such that, for all $i \in \mathcal{I}$,

$$\frac{\partial u_E(\boldsymbol{J^*}, \boldsymbol{p}^*)}{\partial p_i} = C_{E_i}(J_i^*) \begin{cases} \geq w_A, \text{ if } p_i^* = 1, \\ = w_A, \text{ if } 0 < p_i^* < 1, \\ \leq w_A, \text{ if } p_i^* = 0, \end{cases} \tag{15}$$

where $C_{E_i}(J_i^*) = C_{E_i}(0), \ \forall i \in \mathcal{I}^-$. Equations (15) shows that the Lagrange multiplier w_A works as a threshold value such that the eavesdropper will only attack channels whose eavesdropping capacity is greater than w_A in an NE. For the sake of simplicity, we adopt the following assumption for the case $|\mathcal{I}| > n$.

Assumption 2. *Assume $\mathcal{I} = \{1, ..., H\}$ where $H \leq N$ and $C_{E_1}(0) > ... > C_{E_H}(0)$.*

This assumption can be satisfied by re-labeling all channels in $\mathcal{I}$. Then, the eavesdropper will attack the first few channels within set $\mathcal{I}$ in a NE, as shown by the next two lemmas. We will refer to such a NE as threshold type strategy.

Lemma 4. *For NE strategies $(\boldsymbol{J^*}, \boldsymbol{p^*})$, if there exists an index $j \in \mathcal{I}$ such that $p_j^* = 0$, then $p_i^* = 0, \ \forall i > j, i \in \mathcal{I}$.*

Proof. Let $j \in \mathcal{I}$ such that $p_j^* = 0$. If $j \in \mathcal{I}^-$, then $J_j^* = 0$. If $j \in \mathcal{I}^+$, then $\frac{\partial u_S(\boldsymbol{J}^*, \boldsymbol{p}^*)}{\partial J_i} = \frac{d}{dJ_i} C_{L_i}(J_i^*) < 0 \leq w_D$, so $J_j^* = 0$ still hold by KKT condition (14). Therefore, $C_{E_j}(J_j^*) = C_{E_j}(0)$ always hold for such $j \in \mathcal{I}$.

Since $p_j^* = 0$, then $C_{E_j}(J_j^*) \leq w_A$ by KKT condition (15). It follows that $w_A \geq C_{E_j}(J_j^*) = C_{E_j}(0) > C_{E_i}(0) > C_{E_i}(J_i^*), \ \forall i > j, i \in \mathcal{I}$, since $C_{E_i}(J_i^*)$ is decreasing w.r.t. $J_i \geq 0$. Hence, $p_i^* = 0, \ \forall i \geq j, i \in \mathcal{I}$ by equations (15). □

Lemma 5. *For NE strategies $(\boldsymbol{J^*}, \boldsymbol{p^*})$, if there exists an index $j \in \mathcal{I}$ such that $p_j^* > 0$, then $p_i^* > 0, \ \forall i < j, i \in \mathcal{I}$.*

Proof. Let $j \in \mathcal{I}$ such that $p_j^* > 0$. Assume there exists another index $i \in \mathcal{I}$ such that $i < j$ and $p_i^* = 0$. Then by lemma 4, it must be true that $p_j^* = 0$, which is impossible. □

Also notice that $J_i^* = 0$ if $p_i^* = 0$ since it is not necessary to interfere a channel that is not attacked. Thus, by lemmas 4 and 5, there exists an index h such that $n \leq h \leq H$ and

$$\begin{cases} p_i^* > 0, & \forall i = 1, ..., h, \\ p_i^* = 0, \ \ J_i^* = 0, & \forall i > h, \end{cases} \tag{16}$$

which reveals the threshold structure of NE strategies $(\boldsymbol{J}^*, \boldsymbol{p}^*)$.

2) Optimality gap: Note that, even though a threshold type strategy pair satisfies equations (16), it may not satisfy KKT conditions (14) and (15). This section proposes the criteria, called the optimality gap, to measure how far a given threshold type strategy pair is away from the NE. Hence, the friendly interferer can verify the eavesdropper's action in the NE and find the best response. Furthermore, we proposed an optimization model to find NE using the optimality gap.

As a starting point, a simple threshold type attack policy for the eavesdropper is to attack channels 1 to n deterministically. That is, let $\boldsymbol{p}^o = \{p_1^o, ..., p_H^o\}$ where $p_i^o = 1, \ \forall i \leq n$ and $p_i^o = 0, \ \forall i > n$. We call $\boldsymbol{p}^o$ a pure threshold type attack policy. Let $\boldsymbol{J}^o = \{J_1^o, ..., J_H^o\}$ be the best response of the defender given $\boldsymbol{p}^* = \boldsymbol{p}^o$ by solving optimization problem (12). The following theorem presents the condition under which the pure threshold type attack policy $\boldsymbol{p}^o$ is an NE strategy.

Theorem 1. *Given $(\boldsymbol{J}^o, \boldsymbol{p}^o)$, let $w_A^o = \min\{C_{E_i}(J_i^o), i = 1, ..., n\}$, then $(\boldsymbol{J}^o, \boldsymbol{p}^o)$ is the unique NE strategy pair if $w_A^o \geq C_{E_{n+1}}(0)$.*

Proof. Firstly, $\boldsymbol{J}^o$ satisfies defender's KKT condition (14) since it is the optimal solution to (12). Secondly, $C_{E_i}(J_i^o) \geq w_A^o, \ \forall p_i^o = 1, i \in \mathcal{I}$ by definition. If $w_A^o \geq C_{E_{n+1}}(0)$, then $w_A^o \geq C_{E_i}(0) = C_{E_i}(J_i^o), \ \forall p_i^o = 0, i \in \mathcal{I}$ under Assumption 2. Thus, the attacker's KKT condition (15) is also satisfied. □

When the pure threshold type attack policy can not be a NE strategy, then $h > n$, giving a mixed NE attack strategy $\boldsymbol{p}^*$. That is, $\exists\, i \leq h$ such that $p_i^* < 1$. Let $\boldsymbol{p}^{\mathbf{I}} = (p_1^{\mathrm{I}}, ..., p_N^{\mathrm{I}})$ be a mixed attack policy with threshold index $h > n$ where $0 < p_i^{\mathrm{I}} \leq 1, \ \forall i \leq h$ and $p_i^{\mathrm{I}} = 0, \ \forall i > h$. Let $\boldsymbol{J}^{\mathrm{I}} = \{J_1^{\mathrm{I}}, ..., J_N^{\mathrm{I}}\}$ be the best response of the defender given $\boldsymbol{p}^* = \boldsymbol{p}^{\mathrm{I}}$ by solving optimization problem (12). The following theorem presents the conditions for $(\boldsymbol{J}^{\mathbf{I}}, \boldsymbol{p}^{\mathbf{I}})$ to be a NE strategy pair.

Theorem 2. *Given $(\boldsymbol{J}^{\mathbf{I}}, \boldsymbol{p}^{\mathbf{I}})$, let $w_A^{\mathrm{I}} = \min\{C_{E_i}(J_i^{\mathrm{I}}), i = 1, ..., h\}$, then $(\boldsymbol{J}^{\mathbf{I}}, \boldsymbol{p}^{\mathbf{I}})$ is the unique NE strategy pair if*

A) $C_{E_i}(J_i^{\mathrm{I}}) = w_A^{\mathrm{I}}$ when $p_i^{\mathrm{I}} < 1$, or $C_{E_i}(J_i^{\mathrm{I}}) \geq w_A^{\mathrm{I}}$ when $p_i^{\mathrm{I}} = 1, \ \forall i = 1, ..., h$; and

B) $w_A^{\mathrm{I}} \geq C_{E_{h+1}}(0)$ if $h < H$.

Proof. Firstly, $\boldsymbol{J}^{\mathrm{I}}$ satisfies defender's KKT condition (14) since it is the optimal solution to (12).

When Theorem 2's condition (A) is satisfied by $\boldsymbol{p}^{\mathbf{I}}$, then the first two inequalities of attacker's KKT condition (15) are satisfied. For the last inequality of (15), if $h = H$, then $\nexists i \in \mathcal{I}$ such that $p_i^{\mathrm{I}} = 0$; if $h < H$ and $w_A^{\mathrm{I}} \geq C_{E_{h+1}}(0)$, then $w_A^{\mathrm{I}} \geq C_{E_i}(0) = C_{E_i}(J_i^{\mathrm{I}}), \ \forall p_i^{\mathrm{I}} = 0, i \in \mathcal{I}$ under Assumption 2, hence the last inequality of (15) is also satisfied. □

When an attack policy $\boldsymbol{p}^{\mathbf{I}}$ with threshold index $h \geq n$ does not satisfy conditions (A) and (B) listed in Theorem 2, then it is not a NE strategy, and there are two possible reasons:

R_1) $\exists\, k \leq h$ such that $p_k^{\mathrm{I}} < 1$ but $C_{E_k}(J_k^{\mathrm{I}}) > w_A^{\mathrm{I}}$, or

R_2) $h < H$, but $C_{E_{h+1}}(0) > w_A^{\mathrm{I}}$.

Note that (R_1) and (R_2) happen because the value of w_A^{I} is too small and some channels' eavesdropping capacities under $\boldsymbol{J}^{\mathbf{I}}$ are still too large, such as channel k in (R_1), or channel

$h+1$ in (R_2). It implies that, those channels are actually better targets for the eavesdropper under $\boldsymbol{J}^{\mathbf{I}}$. Define

$$v_A^{\mathrm{I}} \coloneqq \max\{C_{E_i}(J_i^{\mathrm{I}}), i = 1, ..., H | p_i^{\mathrm{I}} < 1\}$$

which is the largest marginal increase on the attacker's payoff if she has more attack resources. Let ϵ be a small positive real number standing for computational tolerance, then $(\boldsymbol{J}^{\mathbf{I}}, \boldsymbol{p}^{\mathbf{I}})$ are NE strategies when $v_A^{\mathrm{I}} - w_A^{\mathrm{I}} \leq \epsilon$ since the eavesdropper has no motivation to deviate from attack policy $\boldsymbol{p}^{\mathbf{I}}$ anymore. We define $\Delta^{\mathrm{I}} = v_A^{\mathrm{I}} - w_A^{\mathrm{I}}$ as $\boldsymbol{p}^{\mathbf{I}}$'s optimality gap to the NE.

Therefore, we can find a pair of NE strategies by solving the following optimization problem,

$$\begin{aligned} \min_{\boldsymbol{p}^{\mathbf{I}}} \quad & \Delta^{\mathrm{I}} = v_A^{\mathrm{I}} - w_A^{\mathrm{I}} \\ \text{s.t.} \quad & \boldsymbol{p}^{\mathbf{I}} \text{ is a threshold type attack policy,} \\ & \boldsymbol{J}^{\mathbf{I}} \text{ is the solution to (12) given } \boldsymbol{p}^{\mathbf{I}}, \end{aligned} \tag{17}$$

where v_A^{I} and w_A^{I} are decided by $\boldsymbol{p}^{\mathbf{I}}$ and $\boldsymbol{J}^{\mathbf{I}}$ as defined before. By Theorem 2, $\Delta^{\mathrm{I}} = 0$ is the optimal solution of problem (17) when the NE is found. Notice that problem (17) is a bi-level optimization problem since it contains an inner level optimization problem (12) to solve for $\boldsymbol{J}^{\mathbf{I}}$. Also, we do not have an analytical form for the objective function w.r.t. decision variable $\boldsymbol{p}^{\mathbf{I}}$. Such a problem may be solved using black-box optimization methods such as Genetic Algorithms or Bayesian Optimization.

3) Strategy iteration algorithm to find NE: Unfortunately, most black-box optimization methods do not guarantee convergence to the global optimal solution, while it is critical for the friendly interferer to have $\Delta^{\mathrm{I}} = 0$ to make sure the power allocation strategy $\boldsymbol{J}^{\mathbf{I}}$ founded is in NE. Remainder of this section discusses the algorithm we propose to iterate on the value of threshold type attack policies to reach NE, using $(\boldsymbol{J}^o, \boldsymbol{p}^o)$ as the initial solution.

Given $\boldsymbol{p}^{\mathbf{I}}$, w_A^{I}, v_A^{I} and $v_A^{\mathrm{I}} > w_A^{\mathrm{I}}$, a rational eavesdropper should attack the channel with eavesdropping capacity v_A^{I} more frequently, while paying less attention to channels with eavesdropping capacity w_A^{I}. The next theorem shows that, it is possible to decrease the gap when a threshold type attack policy changes by moving some attack resource from channel j with $C_{E_j}(J_j^{\mathrm{I}}) = w_A^{\mathrm{I}}$ to a more vulnerable channel k with $C_{E_k}(J_k^{\mathrm{I}}) = v_A^{\mathrm{I}}$.

Theorem 3. *Given $(\boldsymbol{J}^{\mathbf{I}}, \boldsymbol{p}^{\mathbf{I}})$, w_A^{I}, and v_A^{I} where $v_A^{\mathrm{I}} > w_A^{\mathrm{I}}$, then $(\boldsymbol{J}^{\mathbf{I}}, \boldsymbol{y}^{\mathbf{I}})$ is not a NE strategy pair consequently. Let $j \leq h$ be an integer such that $C_{E_j}(J_j^{\mathrm{I}}) = w_A^{\mathrm{I}}$, and $k \leq h+1$ be another integer such that $C_{E_k}(J_k^{\mathrm{I}}) = v_A^{\mathrm{I}}$ and $p_k^{\mathrm{I}} < 1$.*

Let $\delta > 0$ be a small real number, $\boldsymbol{p}^{\mathbf{II}} = (p_1^{\mathrm{II}}, ..., p_N^{\mathrm{II}})$ be a new attack policy such that

$$\begin{cases} p_j^{\mathrm{II}} = p_j^{\mathrm{I}} - \delta, \\ p_k^{\mathrm{II}} = p_k^{\mathrm{I}} + \delta, \\ p_i^{\mathrm{II}} = p_i^{\mathrm{I}}, \ \ \forall i \neq j, i \neq k, \end{cases}$$

and $\boldsymbol{J}^{\mathbf{II}}$ be a solution to optimization problem (7) given $\boldsymbol{p}^* = \boldsymbol{p}^{\mathbf{II}}$, then:
A) if $J_j^{\mathrm{I}} > 0$ and $J_k^{\mathrm{I}} > 0$,

$$\Delta^{\mathrm{II}} = C_{E_k}(J_k^{\mathrm{II}}) - C_{E_j}(J_j^{\mathrm{II}}) < C_{E_k}(J_k^{\mathrm{I}}) - C_{E_j}(J_j^{\mathrm{I}}) = \Delta^{\mathrm{I}};$$

B) if $J_j^{\mathrm{I}} = 0$ or $J_k^{\mathrm{I}} = 0$,

$$\Delta^{\mathrm{II}} = C_{E_k}(J_k^{\mathrm{II}}) - C_{E_j}(J_j^{\mathrm{II}}) \leq C_{E_k}(J_k^{\mathrm{I}}) - C_{E_j}(J_j^{\mathrm{I}}) = \Delta^{\mathrm{I}}$$

Proof. We provide a proof in the appendix. □

Based on theorem 1 to 3, the basic idea of the proposed strategy iteration algorithm is shown below:

- **Step 1**: Initialize attack strategy $\boldsymbol{p}^{\mathbf{I}}$ as $\boldsymbol{p}^{\boldsymbol{o}}$, and check $\boldsymbol{p}^{\boldsymbol{o}}$ via Theorem 1.
- **Step 2**: If $\boldsymbol{p}^{\mathbf{I}}$ is not in the NE, find updated attack policy $\boldsymbol{p}^{\mathbf{II}}$ via Theorem 3. Let $\boldsymbol{p}^{\mathbf{I}} \leftarrow \boldsymbol{p}^{\mathbf{II}}$.
- **Step 3**: Check updated $\boldsymbol{p}^{\mathbf{I}}$ via Theorem 2. If it is not on the NE, that is, $v_A^{\mathrm{I}} - w_A^{\mathrm{I}} > \epsilon$, go to step 2.

Notice that δ works as the search step size in Theorem 3. When δ is too large, the algorithm may run into cycling, such as $C_{E_k}(J_k^{\mathrm{II}})$ becoming too small while $C_{E_j}(J_j^{\mathrm{II}})$ becoming too large after the update. On the other hand, if δ is too small, the algorithm may take a long time to terminate. To speed up the search process, we design an adaptive search step size mechanism working in the following way:

- **Step 1**: Start with a given value of δ. Initialize an empty set S to track every channel whose attack probability has been increased by δ.
- **Step 2**: Run the algorithm. At each iteration, identify channel indices j and k defined in Theorem 3. Check if the selected channel j is in set S.
- **Step 3**: If $j \notin S$, let $S \leftarrow S \cup \{k\}$; if $j \in S$, let $\delta \leftarrow \frac{\delta}{2}$ and reset $S \leftarrow \emptyset$. Continue.

Once channel $j \in S$ is selected for decreasing p_j^{I}, it implies that p_j^{I} had been increased too much in the previous steps. Thus, reducing δ by 50% will avoid cycling. Since the number of channels is finite, it is expected that δ will gradually decrease.

The detailed description of the strategy iteration algorithm with adaptive search step size is summarized in Algorithm 2.

Remark. Algorithm 1 can be used to solve the optimization problem given in eq. (12) with $c_i(J_i|p_i^*)$ replacing $c_i(J_i)$.

IV. Numerical illustrations

This section compares the following cooperative jamming power control strategies for a network of parallel channels:

- **Without CJ**: Not sending cooperative jamming signals to any channel.
- **EP Algorithm**: Assign cooperative jamming power equally to every channel $i \in \mathcal{I}$.
- **OP Algorithm**: Always assume $n \geq |\mathcal{I}|$ and assign cooperative jamming power by solving an optimization problem with Algorithm 1.
- **GT Algorithm**: Follow the game-theoretic model and assign cooperative jamming power with Algorithm 2.

Consider an OFDM wireless communication network consisting of 25 sub-channels, that is, $N = 25$, with $g_i^L = r_L \cdot p^{i-1}$ for $i \in [1, 25]$ where $r_L \in (0, 1)$ and $p \in (0, 1)$ correspond to Rayleigh fading. Similarly, for the eavesdropper, let $g_i^E = r_E \cdot q^{i-1}$ for $i \in [1, 25]$ where $r_E \in (0, 1)$ and $q \in (0, 1)$. Let $n = 10$, i.e., the eavesdropper can attack 10 sub-channels at the same time. Furthermore, set $J = 1$, $\sigma^2 = 0.1$ and $T_i = 1, h_i^E = 0.5, \ \forall i = 1, ..., 25$.

Algorithm 2 Strategy iteration algorithm to find NE

Input: $C_{L_i}(J_i)$ and $C_{E_i}(J_i)$ functions for all $i \in \mathcal{I}$; total power: J; attack capability: n; initial search step size: δ; and tolerance: $\epsilon \leq 0.01$.

Output: NE power allocation strategy $\boldsymbol{J}^*$.

Initialization: Define $C_{E_{H+1}}(0) = 0$. Get $\boldsymbol{p^o}$. Let $S \leftarrow \emptyset$.

Find $\boldsymbol{J}^o$ by solving problem (12) with $\boldsymbol{p^*} = \boldsymbol{p^o}$.
$w_A^o \leftarrow \min\{C_{E_i}(J_i^o), i = 1, ..., n\}$.
if $(w_A^o \geq C_{E_{n+1}}(0))$ **then**
  $\boldsymbol{J}^* \leftarrow \boldsymbol{J}^o$.
else
  Let $w_A^{\mathrm{I}} \leftarrow w_A^o$, $\boldsymbol{p^{\mathrm{I}}} \leftarrow \boldsymbol{p^o}$, $\boldsymbol{J^{\mathrm{I}}} \leftarrow \boldsymbol{J}^o$.
  Let $h \leftarrow n + 1$.
  $v_A^{\mathrm{I}} \leftarrow \max\{C_{E_i}(J_i^{\mathrm{I}}), i = 1, ..., h | p_i^{\mathrm{I}} < 1\}$.
  while $(v_A^{\mathrm{I}} - w_A^{\mathrm{I}} > \epsilon)$ **do**
    Let $j \leftarrow \min\{i = 1, ..., h | C_{E_i}(J_i^{\mathrm{I}}) = w_A^{\mathrm{I}}, p_i^{\mathrm{I}} > 0\}$.
    Let $k \leftarrow \min\{i = 1, ..., h | C_{E_i}(J_i^{\mathrm{I}}) = v_A^{\mathrm{I}}, p_i^{\mathrm{I}} < 1\}$.
    if $j \in S$ **then**
      $\delta \leftarrow \frac{\delta}{2}$ and $S \leftarrow \emptyset$.
    end if
    $S \leftarrow S \cup \{k\}$.
    Let $\boldsymbol{p^{\mathrm{II}}} \leftarrow \boldsymbol{p^{\mathrm{I}}}$.
    $p_k^{\mathrm{II}} \leftarrow \min\{p_k^{\mathrm{II}} + \delta, 1\}$.
    $p_j^{\mathrm{II}} \leftarrow p_j^{\mathrm{I}} - (p_k^{\mathrm{II}} - p_k^{\mathrm{I}})$.
    Let $\boldsymbol{J^{\mathrm{II}}}$ be solution of problem (12) with $\boldsymbol{p^*} = \boldsymbol{p^{\mathrm{II}}}$.
    $w_A^{\mathrm{II}} \leftarrow \min\{C_{E_i}(J_i^{\mathrm{II}}), i = 1, ..., h\}$.
    $v_A^{\mathrm{II}} \leftarrow \max\{C_{E_i}(J_i^{\mathrm{II}}), i = 1, ..., h | p_i^{\mathrm{II}} < 1\}$.
    if $v_A^{\mathrm{II}} < C_{E_{h+1}}(0)$ **then**
      Let $v_A^{\mathrm{I}} \leftarrow C_{E_{h+1}}(0)$, $w_A^{\mathrm{I}} \leftarrow w_A^{\mathrm{II}}$.
      Let $\boldsymbol{J^{\mathrm{I}}} \leftarrow \boldsymbol{J^{\mathrm{II}}}$, $\boldsymbol{p^{\mathrm{I}}} \leftarrow \boldsymbol{p^{\mathrm{II}}}$.
      Let $h \leftarrow h + 1$.
    else
      Let $v_A^{\mathrm{I}} \leftarrow v_A^{\mathrm{II}}$, $w_A^{\mathrm{I}} \leftarrow w_A^{\mathrm{II}}$.
      Let $\boldsymbol{J^{\mathrm{I}}} \leftarrow \boldsymbol{J^{\mathrm{II}}}$, $\boldsymbol{p^{\mathrm{I}}} \leftarrow \boldsymbol{p^{\mathrm{II}}}$.
    end if
  end while
  $\boldsymbol{J}^* \leftarrow \boldsymbol{J}^{\mathrm{I}}$.
end if
return $\boldsymbol{J}^*$.

Next two subsections present numerical examples for both scenarios when $|\mathcal{I}| \leq n$ and when $|\mathcal{I}| > n$. In both scenarios, it is shown that the value of h_i^L's, which represent the detrimental effect of cooperative jamming, plays a key role in deciding the optimal cooperative jamming power allocation strategy. To help us observe this effect, let $h_i^L = h^L, \ \forall i = 1, ..., 25$ where h^L is a single real number that increases from 0.2.

A. When $|\mathcal{I}| \leq n$

For the case with $r_L = 0.45$, $p = 0.95$, $r_E = 0.97$ and $q = 0.9$, $g_i^L < g_i^E, \ \forall i = 1, ..., 15$, while $g_i^L > g_i^E, \ \forall i = 16, ..., 25$, It follows that $\mathcal{I} = \{16, ..., 25\}$ and $|\mathcal{I}| = n = 10$.

Fig. 2(a) presents the optimal power allocation strategy following Algorithm 1 (OP Algorithm), as h^L increases from 0.2 to 0.495. As shown in Fig. 2(a), $h^L = 0.422$ is the boundary where it is not beneficial for the friendly interferer to protect all channels anymore. When $h^L \leq 0.422$, the sum of the ideal cooperative jamming power level for each channel exceeds the available power, i.e., $\sum_{i \in \mathcal{I}} \bar{J}_i > J$. Algorithm 1 provides the optimal power $J_i^* < \bar{J}_i, \ \forall i \in \mathcal{I}$. Note that all jamming power is allocated to counter eavesdropping attacks and $J_i^* > 0, \ \forall i \in \mathcal{I}$. In this situation, additional jamming power can be utilized to further increase the wireless network's secrecy capacity. On the other hand, for $h_i^L > 0.422$, the power constraint is not binding, i.e., $\sum_{i \in \mathcal{I}} \bar{J}_i < J$, then $J_i^* = \bar{J}_i, \ \forall i \in \mathcal{I}$ using the bisection algorithm. The total power used for cooperative jamming keeps decreasing as h^L's increase. This situation confirms the intuition that the cooperative jamming signal should be tuned carefully to avoid interference with communication signals sent to the intended receiver.

Fig. 2(b) illustrates the average total secrecy capacity when the friendly interferer optimizes his power allocation plan with the OP Algorithm, uses the EP Algorithm, and do nothing (Without CJ), respectively. As h^L increases, the OP Algorithm always outperform the others. Moreover, EP Algorithm is even worth than Without CJ starting from $h^L = 0.422$ since the detrimental effect of cooperative jamming on some sub-channels starts to be larger than the benefit of cooperative jamming.

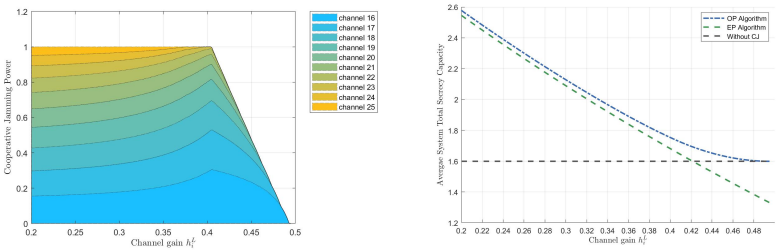
B. When $|\mathcal{I}| > n$

For the case with $r_L = 0.86$, $p = 0.99$, $r_E = 0.95$ and $q = 0.98$, $g_i^L < g_i^E, \ \forall i = 1, ..., 10$, while $g_i^L > g_i^E, \ \forall i = 11, ..., 25$. Thus, $\mathcal{I} = \{11, ..., 25\}$ and $|\mathcal{I}| = 15 > n$, that is the eavesdropper cannot attack all active channels simultaneously.

Fig. 3(a) and Fig. 3(b) present the NE power allocation strategy and the NE attack strategy following the game theoretic model, as h^L increases from 0.2 to 0.4. As shown in Fig. 3(a), when $h^L \leq 0.292$, all cooperative jamming power is utilized for defense. When $h^L > 0.292$, it is not beneficial to use up all jamming power anymore. The jamming power allocated to each channel starts decreasing and the number of channels under protection decreases as well. Fig. 3(b) depicts the eavesdropper's policy as she concentrates on a fewer channels as h_L increases beyond 0.336.

It is assumed that the eavesdropper will always take the best response facing different cooperative power control strategies. When facing GT Algorithm based strategy, the eavesdropper will also adopt a NE attack strategy coming from the game theoretic model. When facing other cooperative jamming power control strategies, the eavesdropper will pick the $n = 10$ channels with the largest eavesdropping capacity to attack.

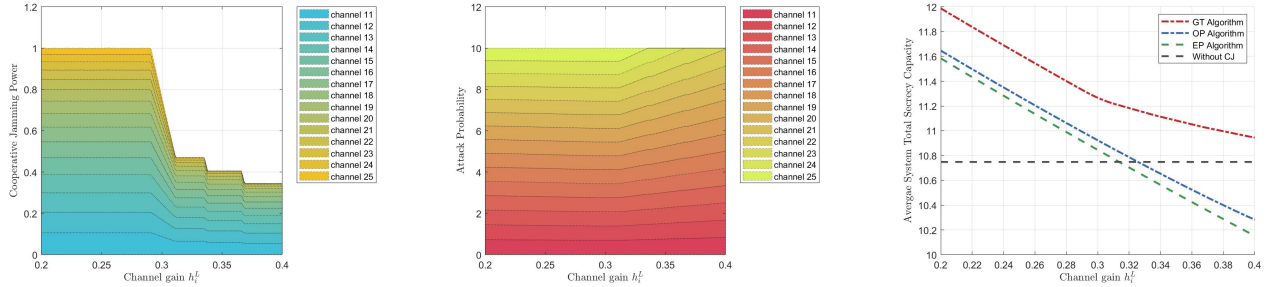
Fig. 3(c) depicts the average total secrecy capacity when the friendly interferer uses the game theoretic model backed GT Algorithm, uses the OP Algorithm that assumes all channels are under attack, uses the EP Algorithm, and adopts Without CJ, respectively. As h_i^L increases, the GT Algorithm still outperform the others. More importantly, the performance of both the OP Algorithm and EP Algorithm drops towards the baseline of Without CJ as h_i^L increases, and are even worse than not sending cooperative jamming signals at all when h_i^L is large, since some channels that will not be attacked



(a) Optimal power allocation plan $\boldsymbol{J}^*$ (OP Algorithm)

(b) Average total secrecy capacity

Fig. 2: When all channels in $\mathcal{I}$ can be attacked simultaneously ($n = 10, |\mathcal{I}| = 10$).



(a) Optimal power allocation plan $\boldsymbol{J}^*$ (GT Algorithm)

(b) Eavesdropper's best response $\boldsymbol{p}^*$ (GT Algorithm)

(c) Average system total secrecy capacity

Fig. 3: When the eavesdropper can not attack all channels in $\mathcal{I}$ simultaneously ($n = 10, |\mathcal{I}| = 15$).

by the eavesdropper are affected by the detrimental effect of cooperative jamming.

V. Conclusions

This paper studies the optimal power allocation strategy for cooperative jamming on a network of parallel channels against an eavesdropper who can strategically select the channels to attack. The eavesdropper can attack multiple channels simultaneously but may not cover the whole network. A convex optimization model is proposed when the eavesdropper can cover all channels being used for secret communication. A game-theoretic model represents the case when the number of channels that transmit secret messages is more than the number of channels the attacker can attack simultaneously. For the later case, we prove the existence of the optimal power allocation strategy of the friendly interferer as part of a pair of Nash Equilibrium strategies in a nonzero-sum game. It turns out that the optimal power allocation strategy will be subject to a water-filling scheme such that both the friendly interferer and the eavesdropper will focus on the top few channels that have the highest eavesdropping capacities. We present a bisection search algorithm to solve the convex optimization problem, and a strategy iteration algorithm to approximate the NE power allocation strategy of the game-theoretic model to within a given tolerance.

Also taking into account the effect of interference on communication signals sent to the intended receiver, we show that the fading gains of interference signals at the legitimate receivers' side are key parameters that affect the performance of cooperative jamming. Large fading gains of interference signals at the legitimate receivers' side will prevent the friendly interferer from utilizing all cooperative jamming power. Thus, the interference signals should be carefully tuned such that no cooperative jamming power will be wasted.

Future research interests include the extensions to the current model that were discussed in section II-A. We plan to explore how the transmitter could cooperate with the friendly interferer to improve the total secrecy capacity by setting proper T_is, possibly under a total power constraint. This situation may be modeled as a leader-follower game in which the transmitter source optimizes T_is in stage 2 based on the anticipated followers' actions in stage 3. Another extension focuses on the case with $g_i^L < g_i^E$. As was discussed in the remark at the end of section II-A, such a model requires solving mixed integer programs for the friendly interferer. We plan to explore developing heuristic algorithms to obtain Stackelberg and Nash equilibrium power allocation and attack strategies for the extended models.

A model in which the capability of the eavesdropper is not known with certainty is also of interest. As shown in section IV, the GT Algorithm outperforms the OP algorithm (that is, when $n = N$) since it utilizes the accurate knowledge of the eavesdropper's attack capability. However, such knowledge may not be completely available to the helper. Various approaches may be used to tackle this challenge. For instance, one can consider a Bayesian game in which eavesdroppers

with different attack capabilities appear according to a probability distribution.

APPENDIX

PROOF of THEOREM 3

Let w_D^{I} be the friendly interferer's Lagrange multiplier associated with $\boldsymbol{J}^{\mathbf{I}}$ and w_D^{II} be the Lagrange multiplier associated with $\boldsymbol{J}^{\mathbf{II}}$. Define

$$\begin{aligned} c_i(J_i|\boldsymbol{p}) \coloneqq c_i(J_i|p_i) &= \frac{\partial G_i(J_i|p_i)}{\partial J_i} \\ &= \frac{d}{dJ_i}C_{L_i}(J_i) - p_i\frac{d}{dJ_i}C_{E_i}(J_i) \\ &= p_i\frac{g_i^E h_i^E T_i}{(g_i^E T_i + \sigma^2 + h_i^E J_i)(\sigma^2 + h_i^E J_i)} \\ &- \frac{g_i^L h_i^L T_i}{(g_i^L T_i + \sigma^2 + h_i^L J_i)(\sigma^2 + h_i^L J_i)} \end{aligned}$$

is the slope of the interferer's payoff as a function w.r.t. $J_i \geq 0$ given $\boldsymbol{p} = (p_1, ..., p_N)$. Let $\bar{J}_i(\boldsymbol{p}) \geq 0$ be such that $G_i(J_i|p_i)$ reaches its maximum at $J_i = \bar{J}_i(\boldsymbol{p})$. Notice that, if $\bar{J}_i(\boldsymbol{p}) > 0$, then $c_i(J_i|\boldsymbol{p})$ is strictly decrease w.r.t. $0 \leq J_i \leq \bar{J}_i(\boldsymbol{p})$ for all $i \in \mathcal{I}^+$ and $c_i(\bar{J}_i(\boldsymbol{p})|\boldsymbol{p}) = 0$.

A) If $J_j^{\mathrm{I}} > 0$ and $J_k^{\mathrm{I}} > 0$, we will show that $J_j^{\mathrm{II}} < J_j^{\mathrm{I}}$ and $J_k^{\mathrm{II}} > J_k^{\mathrm{I}}$.

Since $J_j^{\mathrm{I}} > 0$, then $j \in \mathcal{I}^+$ and $w_D^{\mathrm{I}} = c_j(J_j^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{I}})$ holds. In addition, $J_k^{\mathrm{I}} > 0$ implies that $k \in \mathcal{I}^+$, $w_D^{\mathrm{I}} = c_k(J_k^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{I}})$ and $p_k^{\mathrm{I}} > 0$, so $k \leq h$.

Assume $J_j^{\mathrm{II}} \geq J_j^{\mathrm{I}}$, then $J_j^{\mathrm{II}} > 0$ and $w_D^{\mathrm{II}} = c_j(J_j^{\mathrm{II}}|\boldsymbol{p}^{\mathbf{II}})$ follow. Given $p_j^{\mathrm{II}} < p_j^{\mathrm{I}}$ and $j \in \mathcal{I}^+$, then

$$w_D^{\mathrm{II}} = c_j(J_j^{\mathrm{II}}|\boldsymbol{p}^{\mathbf{II}}) \leq c_j(J_j^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{II}}) < c_j(J_j^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{I}}) = w_D^{\mathrm{I}}$$

must hold, which requires $w_D^{\mathrm{I}} > 0$ and $\sum_{i\in\mathcal{I}^+} J_i^{\mathrm{I}} = J$. Now consider the relationship between J_i^{II} and J_i^{I}, $\forall i = 1, ..., h,\ i \neq j$. Since $p_k^{\mathrm{II}} > p_k^{\mathrm{I}}$, then

$$c_k(J_k^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{II}}) > c_k(J_k^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{I}}) = w_D^{\mathrm{I}} > w_D^{\mathrm{II}},$$

which implies that $J_k^{\mathrm{II}} > J_k^{\mathrm{I}}$ must hold. For any $i = 1, ..., h$ but $i \neq j$ and $i \neq k$, if $J_i^{\mathrm{I}} = 0$, then $J_i^{\mathrm{II}} \geq J_i^{\mathrm{I}}$ by definition; if $J_i^{\mathrm{I}} > 0$, then $i \in \mathcal{I}^+$, and it follows that

$$c_i(J_i^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{II}}) = c_i(J_i^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{I}}) = w_D^{\mathrm{I}} > w_D^{\mathrm{II}},$$

since $p_i^{\mathrm{II}} = p_i^{\mathrm{I}},\ \forall i \neq j, i \neq k$, which leads to $J_i^{\mathrm{II}} > J_i^{\mathrm{I}}$. Hence,

$$\sum_{i=1}^{h} J_i^{\mathrm{II}} > \sum_{i=1}^{h} J_i^{\mathrm{I}} = \sum_{i\in\mathcal{I}^+} J_i^{\mathrm{I}} = J,$$

which is infeasible. So the assumption $J_j^{\mathrm{II}} \geq J_j^{\mathrm{I}}$ can not be true. Therefore, $J_j^{\mathrm{II}} < J_j^{\mathrm{I}}$ must hold and $C_{E_j}(J_j^{\mathrm{II}}) > C_{E_j}(J_j^{\mathrm{I}})$ follows.

Now assume $J_k^{\mathrm{II}} \leq J_k^{\mathrm{I}}$. Since $k \in \mathcal{I}^+$ and $p_k^{\mathrm{II}} > p_k^{\mathrm{I}}$, then

$$w_D^{\mathrm{II}} \geq c_k(J_k^{\mathrm{II}}|\boldsymbol{p}^{\mathbf{II}}) > c_k(J_k^{\mathrm{II}}|\boldsymbol{p}^{\mathbf{I}}) > c_k(J_k^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{I}}) = w_D^{\mathrm{I}},$$

must hold. Now consider the relationship between J_i^{II} and J_i^{I}, $\forall i = 1, ..., h,\ i \neq k$. Since $p_j^{\mathrm{II}} < p_j^{\mathrm{I}}$, then

$$c_j(J_j^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{II}}) < c_j(J_j^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{I}}) = w_D^{\mathrm{I}} < w_D^{\mathrm{II}},$$

which implies $J_j^{\mathrm{II}} < J_j^{\mathrm{I}}$ given $j \in \mathcal{I}^+$. For any $i = 1, ..., h$, but $i \neq k$ and $i \neq j$, if $i \in \mathcal{I}^-$, then $J_i^{\mathrm{II}} = J_i^{\mathrm{I}} = 0$; if $i \in \mathcal{I}^+$, since $p_i^{\mathrm{II}} = p_i^{\mathrm{I}}$, then

$$c_i(J_i^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{II}}) = c_i(J_i^{\mathrm{I}}|\boldsymbol{p}^{\mathbf{I}}) \leq w_D^{\mathrm{I}} < w_D^{\mathrm{II}},$$

always hold, which leads to $J_i^{\mathrm{II}} < J_i^{\mathrm{I}}$ if $J_i^{\mathrm{I}} > 0$ and $J_i^{\mathrm{II}} = J_i^{\mathrm{I}}$ if $J_i^{\mathrm{I}} = 0$. Hence,

$$\sum_{i\in\mathcal{I}^+} J_i^{\mathrm{II}} = \sum_{i=1}^{h} J_i^{\mathrm{II}} < \sum_{i=1}^{h} J_i^{\mathrm{I}} = \sum_{i\in\mathcal{I}^+} J_i^{\mathrm{I}} \leq J,$$

and $w_D^{\mathrm{II}} = 0$ follows, which contradicts with $w_D^{\mathrm{II}} > w_D^{\mathrm{I}} \geq 0$. So the assumption $J_k^{\mathrm{II}} \leq J_k^{\mathrm{I}}$ can not be true. Therefore, $J_k^{\mathrm{II}} > J_k^{\mathrm{I}}$ must hold, which implies $C_{E_k}(J_k^{\mathrm{II}}) < C_{E_k}(J_k^{\mathrm{I}})$.

The proof for situation (A) of Theorem (3) is complete.

B) If $J_j^{\mathrm{I}} = 0$ or $J_k^{\mathrm{I}} = 0$, we will show that $J_j^{\mathrm{II}} \leq J_j^{\mathrm{I}}$ and $J_k^{\mathrm{II}} \geq J_k^{\mathrm{I}}$.

First, we prove that, if $J_j^{\mathrm{I}} = 0$, then $J_j^{\mathrm{II}} = 0$. When $J_j^{\mathrm{I}} = 0$, one of the following three situations must be true: a) $j \in \mathcal{I}^-$; b) $j \in \mathcal{I}^+$ and $c_j(0|\boldsymbol{p}^{\mathbf{I}}) \leq 0$; c) $j \in \mathcal{I}^+$ and $c_j(0|\boldsymbol{p}^{\mathbf{I}}) > 0$. If case (a) is true, then $J_j^{\mathrm{II}} = 0$. If case (b) is true, since $p_j^{\mathrm{II}} \leq p_j^{\mathrm{I}}$, then $c_j(0|\boldsymbol{p}^{\mathbf{II}}) < 0$ and $J_j^{\mathrm{II}} = 0$ follows. If case (c) is true, then $w_D^{\mathrm{I}} \geq c_j(0|\boldsymbol{p}^{\mathbf{I}}) > 0$, thus $\sum_{i\in\mathcal{I}^+} J_i^{\mathrm{I}} = J$ follows. Now assume $J_j^{\mathrm{II}} > 0$ in case (c), then

$$w_D^{\mathrm{II}} = c_j(J_j^{\mathrm{II}}|\boldsymbol{p}^{\mathbf{II}}) < c_j(0|\boldsymbol{y}^{\mathbf{II}}) < c_j(0|\boldsymbol{y}^{\mathbf{I}}) \leq w_D^{\mathrm{I}},$$

must hold, which leads to $J_i^{\mathrm{II}} \geq J_i^{\mathrm{I}}$, $\forall i = 1, ..., h$, $i \neq j$, following similar steps discussed in situation (A). It follows that

$$\sum_{i=1}^{h} J_i^{\mathrm{II}} > \sum_{i=1}^{h} J_i^{\mathrm{I}} = \sum_{i\in\mathcal{I}^+} J_i^{\mathrm{I}} = J,$$

which is infeasible. So the assumption can not be true in case (c). In summary, $J_j^{\mathrm{II}} = 0$ always hold if $J_j^{\mathrm{I}} = 0$.

Next, we consider three different possibilities of situation (B) separately. That is,

B_1) $J_j^{\mathrm{I}} = 0$ and $J_k^{\mathrm{I}} = 0$;
B_2) $J_j^{\mathrm{I}} = 0$ and $J_k^{\mathrm{I}} > 0$;
B_3) $J_j^{\mathrm{I}} > 0$ and $J_k^{\mathrm{I}} = 0$.

For situation B_1, $J_j^{\mathrm{II}} = J_j^{\mathrm{I}} = 0$ holds as it is just proved, and $J_k^{\mathrm{II}} \geq J_k^{\mathrm{I}}$ by definition.

For situation B_2, $J_j^{\mathrm{II}} = J_j^{\mathrm{I}} = 0$ holds. Also, $k \in \mathcal{I}^+$. Assume $J_k^{\mathrm{II}} < J_k^{\mathrm{I}}$, then

$$w_D^{\mathrm{II}} > w_D^{\mathrm{I}} \geq 0, \quad \text{and} \quad \sum_{i\in\mathcal{I}^+} J_i^{\mathrm{II}} < J,$$

following similar steps shown in situation (A), which contradict each other. Thus, $J_k^{\mathrm{II}} \geq J_k^{\mathrm{I}}$ must be true. Note that it is possible to have $J_k^{\mathrm{II}} = J_k^{\mathrm{I}}$ in this situation as opposed to situation (A). Since, under the assumption that $J_k^{\mathrm{II}} \leq J_k^{\mathrm{I}}$, $\sum_{i\in\mathcal{I}} J_i^{\mathrm{II}} = \sum_{i\in\mathcal{I}} J_i^{\mathrm{I}} = J$ may hold without requiring $J_j^{\mathrm{I}} > 0$, and thus, there will not be any contradiction.

For situation B_3, $J_k^{\mathrm{II}} \geq J_k^{\mathrm{I}}$ holds by definition. Assume $J_j^{\mathrm{II}} > J_j^{\mathrm{I}}$, then

$$w_D^{\mathrm{II}} < w_D^{\mathrm{I}}, \quad \text{and} \quad \sum_{i=1}^{h} J_i^{\mathrm{II}} > J,$$

following similar steps shown in situation (A), which is infeasible. Thus, $J_j^{\mathrm{II}} \leq J_j^{\mathrm{I}}$ must be true. Again notice that it is possible to have $J_j^{\mathrm{II}} = J_j^{\mathrm{I}}$ in this situation as opposed to situation (A). Since, if we assume $J_j^{\mathrm{II}} \geq J_j^{\mathrm{I}}$, we may have $\sum_{i=1}^{h} J_i^{\mathrm{II}} = \sum_{i=1}^{h} J_i^{\mathrm{I}} = J$ without $J_k^{\mathrm{I}} > 0$, which is feasible.

In summary, it is always true that $J_j^{\mathrm{II}} \leq J_j^{\mathrm{I}}$ and $J_k^{\mathrm{II}} \geq J_k^{\mathrm{I}}$, which implies $C_{E_j}(J_j^{\mathrm{II}}) \geq C_{E_j}(J_j^{\mathrm{I}})$ and $C_{E_k}(J_k^{\mathrm{II}}) \leq C_{E_k}(J_k^{\mathrm{I}})$. The proof for situation (B) is complete.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[5] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[6] X. Zhou, L. Song, and Y. Zhang, *Physical layer security in wireless communications*. CRC Press, 2013.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[8] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 693–702, 2011.

[9] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.

[10] R. D. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," in *2008 IEEE International Symposium on Information Theory*, July 2008, pp. 374–378.

[11] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," in *2008 IEEE International Symposium on Information Theory*, July 2008, pp. 379–383.

[12] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Transactions on Information Theory*, vol. 55, no. 2, pp. 604–619, 2009.

[13] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 62, no. 3. Citeseer, 2005, p. 1906.

[14] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, 2008.

[15] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming," in *2007 Information Theory and Applications Workshop*, 2007, pp. 404–413.

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

[17] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative jamming for secure ofdm system," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1331–1346, 2017.

[18] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," in *2008 IEEE International Symposium on Information Theory*. IEEE, 2008, pp. 389–393.

[19] ——, "Interference assisted secret communication," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[20] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Transactions on industrial informatics*, vol. 12, no. 5, pp. 1714–1725, 2015.

[21] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2734–2771, 2018.

[22] S. Karachontzitis, S. Timotheou, I. Krikidis, and K. Berberidis, "Security-aware max–min resource allocation in multiuser OFDMA downlink," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 529–542, 2014.

[23] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*. IEEE, 2009, pp. 417–420.

[24] A. Rabbachin, A. Conti, and M. Z. Win, "Intentional network interference for denial of wireless eavesdropping," in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, Dec 2011, pp. 1–6.

[25] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R.-F. Liao, "Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2108–2117, 2017.

[26] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–10, 2010.

[27] A. Wang, Y. Cai, W. Yang, and Z. Hou, "A Stackelberg security game with cooperative jamming over a multiuser OFDMA network," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2013, pp. 4169–4174.

[28] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," in *International Conference on Network Control and Optimization*. Springer, 2007, pp. 1–12.

[29] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: A Stackelberg game approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 8, pp. 4038–4047, 2013.

[30] V. F. Gabalou and B. Maham, "Jamming game for secure OFDMA systems," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018, pp. 1–6.

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

[32] A. Garnaev and W. Trappe, "A power control game involving jamming and eavesdropping defense," in *2019 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2019, pp. 1–6.

[33] ——, "An eavesdropping game with SINR as an objective function," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2009, pp. 142–162.

[34] ——, "Secret communication when the eavesdropper might be an active adversary," in *International Workshop on Multiple Access Communications*. Springer, 2014, pp. 121–136.

[35] L. Lai and H. El Gamal, "The water-filling game in fading multiple-access channels," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2110–2122, 2008.

[36] E. Altman, K. Avrachenkov, and A. Garnaev, "Closed form solutions for water-filling problems in optimization and game frameworks," *Telecommunication Systems*, vol. 47, no. 1-2, pp. 153–164, 2011.

[37] A. Garnaev, M. Baykal-Gürsoy, and H. V. Poor, "Incorporating attack-type uncertainty into network protection," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1278–1287, 2014.

[38] Z. Xu and M. Baykal-Gürsoy, "A friendly interference game in wireless secret communication networks," in *Network Games, Control and Optimization, NETGCOOP 2021*. Springer, Cham, 2021, pp. 25–37.

[39] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 180–190, 2016.

[40] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.

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

[42] Z. Yuan, S. Wang, K. Xiong, and J. Xing, "Game theoretic jamming control for the Gaussian interference wiretap channel," in *2014 12th International Conference on Signal Processing (ICSP)*. IEEE, 2014, pp. 1749–1754.

[43] L. Wang, H. Wu, and G. L. Stber, "Cooperative jamming-aided secrecy enhancement in P2P communications with social interaction

constraints," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1144–1158, 2017.

[44] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R. Liao, "Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2108–2117, 2018.

[45] L. You, J. Wang, W. Wang, and X. Gao, "Secure multicast transmission for massive MIMO with statistical channel state information," *IEEE Signal Processing Letters*, vol. 26, no. 6, pp. 803–807, 2019.

[46] M. Boloursaz Mashhadi and D. Gündüz, "Deep learning for massive MIMO channel state acquisition and feedback," *Journal of the Indian Institute of Science*, vol. 100, no. 2, pp. 369–382, 2020.

[47] C. Luo, J. Ji, Q. Wang, X. Chen, and P. Li, "Channel state information prediction for 5G wireless communications: A deep learning approach," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 227–236, 2018.

[48] C.-K. Wen, W.-T. Shih, and S. Jin, "Deep learning for massive MIMO CSI feedback," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 748–751, 2018.

[49] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1923–1936, 2013.

[50] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7495–7505, 2017.

[51] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[52] Y. Ye, *Interior point algorithms: theory and analysis*. John Wiley & Sons, 2011, vol. 44.

[53] K. Firouzbakht, G. Noubir, and M. Salehi, "Linearly constrained bimatrix games in wireless communications," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 429–440, 2015.

[54] K. J. Arrow and G. Debreu, "Existence of an equilibrium for a competitive economy," *Econometrica: Journal of the Econometric Society*, pp. 265–290, 1954.