A Cooperative Jamming Game in Wireless Networks under Uncertainty

Zhifan Xu, Melike Baykal-Gürsoy

A Cooperative Jamming Game in Wireless Networks under Uncertainty *

Zhifan Xu[1,3] and Melike Baykal-Gürsoy[2,4]

[1] Department of Industrial and Systems Engineering, Rutgers University, Piscataway, NJ 08854
[2] Department of Industrial and Systems Engineering, Rutgers University, RUTCOR and CAIT.
[3] zhifan.xu@rutgers.edu
[4] gursoy@soe.rutgers.edu

Abstract. Considered is a multi-channel wireless network for secret communication that uses the signal-to-interference-plus-noise ratio (SINR) as the performance measure. An eavesdropper can intercept encoded messages through a degraded channel of each legitimate transmitter-receiver communication pair. A friendly interferer, on the other hand, may send cooperative jamming signals to enhance the secrecy performance of the whole network. Besides, the state information of the eavesdropping channel may not be known completely. The transmitters and the friendly interferer have to cooperatively decide on the optimal jamming power allocation strategy that balances the secrecy performance with the cost of employing intentional interference, while an eavesdropper tries to maximize her eavesdropping capacity. To solve this problem, we propose and analyze a non-zero sum game between the network defenders and an eavesdropper who can only attack a limited number of channels. We show that the Nash equilibrium strategies for the players are of threshold type. We present an algorithm to find the equilibrium strategy pair. Numerical examples demonstrate the equilibrium and contrast it to a baseline strategy.

Keywords: Non-zero sum game · Cooperative jamming · Physical layer security · Incomplete Channel State Information

1 Introduction

Wireless communication networks are vulnerable to eavesdropping attacks due to the wireless signals' multi-cast nature. Considering the fast development of various forms of wireless communication networks, such as wireless sensor networks and vehicle communication networks, information secrecy against eavesdropping attacks has become more and more critical. Traditionally, securing messages transmitted through wireless networks depends on encryption and randomness

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

in coding schemes [24, 29]. It is shown that the difference between the legitimate channel and the eavesdropping channel capacities, which is defined as *Secrecy Capacity*, decides the secrecy level of a transmitter-receiver pair [18].

During the last decade, various efforts have been made to investigate the security of wireless communication networks at the physical layer, which is coined as *Physical Layer Security*. It is shown that intentionally generated interference signals, either mixed by the transmitter or sent by a third party helper, can decrease the channel capacity between the transmitter and the eavesdropper at the physical layer [10, 22, 26, 27]. Thus, the secrecy capacity of the transmitter-receiver channel can be increased by employing intentional interference signals at the transmitter-eavesdropper channel. This approach is usually referred to as *Cooperative Jamming* when the interference signals are sent by helpers or other components (i.e., idle relays) in a wireless network. Researchers have studied the optimal power control strategies and configurations of cooperative jamming signals under various setups [3, 15].

This paper considers the optimal power allocation strategy for cooperative jamming on a multi-channel wireless communication system. Such problems arise, for example, in military operations, where a frequency division multiplexing (FDM) communication system is used to transmit confidential messages in an adversarial environment. Particularly, we focus on the scenario in which the presence of eavesdroppers at each communication channel is uncertain and the state information of the eavesdropper's channels is not completely known. In previous works, the assumption of complete channel state information (CSI) has been widely used to analyze the optimal power allocation strategy for cooperative jamming. However, as argued in [5, 14], CSI may not be easily obtained since eavesdropping channels' state information is closely related to eavesdroppers' private information such as their hidden location and antenna setups. It is unrealistic to assume complete CSI when the existence of an eavesdropper is even unknown.

Traditional power allocation schemes for cooperative jamming on a multi-channel network usually consider passive eavesdroppers listening in all channels. However, considerable portion of cooperative jamming power is wasted under such schemes if some channels are not actually attacked by eavesdroppers. Besides, due to other constraints on the number of antennas or on the available power, an eavesdropper may not be able to attack all channels at the same time. Instead of simply assigning an arbitrary probability to each channel for being under eavesdropping attack, a game theoretic model leaves that decision to the eavesdropper who tries to maximize her eavesdropping capacity. In fact, in such game-theoretic settings, an eavesdropper could be a strategic player or nature. A strategic player tries to maximize his/her own payoff function while nature is always assumed to work against its adversary. As shown in [12] and [19], a natural disaster is considered as an intelligent player who targets the weakest point of the system, while the defender uses limited resources to harden valuable assets. In [32], Yolmeh and Baykal-Gürsoy investigated the optimal patrolling policy against potential terrorist attacks for a railway system. Wei *et al* [28]

studied the protection strategy of a power system against an attacker who has enough knowledge of how power systems operate.

A non-zero sum Nash game is proposed for the multi-channel wireless communication system to describe the confrontation between a friendly interferer and a strategic eavesdropper. In this paper, the eavesdropper is also a decision maker who can select a communication channel to attack. In addition, the game theoretic model incorporates the probability distributions of the eavesdropper's fading channel gains into the players' payoff functions instead of using simple estimators such as the mean. Moreover, we introduce a cost for the usage of cooperative jamming power since the friendly interferer may be a third party service provider. We show that the Nash equilibrium (NE) strategy of each player is of threshold type. We present an algorithm to compute the equilibrium strategy, and apply it to numerical examples to demonstrate its usage and contrast NE to a baseline strategy. If the friendly interferer naively assigns the jamming power without taking into account the presence of a strategic eavesdropper, the system may not reach its ultimate secrecy capacity.

1.1 Related works

Due to limitations on battery and power technologies in their current state, finding optimal power control strategies has been a crucial problem for cooperative jamming. Dong *et al.* [6] studied the case where a wireless wiretap channel with a single source-destination pair and a single eavesdropper is aided by a friendly interferer equipped with multiple antennas. The authors presented the optimal configuration of all jamming antennas to maximize the secrecy capacity under a total power constraint. Yang *et al.* [31] considered a multi-user broadcast network where a single eavesdropper with multiple antennas attacks all data streams simultaneously. They proposed and solved an optimization problem for a friendly interferer to maximize the minimum secrecy rate of all data streams under total power and minimum rate constraints. Cumanan *et al.* [4] investigated a secrecy capacity maximization problem for a single source-receiver pair in the presence of multiple eavesdroppers and multiple friendly interferers. The optimal power levels of each friendly interferer are derived by taking into account the detrimental effect of interference also on the intended receiver. Zhang *et al.* [34] studied wireless cooperative jamming for an orthogonal frequency-division multiplexing (OFDM) communication system, in which the friendly interferer needs to optimally assign the limited harvested jamming power to all subcarriers in order to maximize the total secrecy capacity. In these models, communication networks are controlled by a single decision maker such as a friendly interferer or a transmitter, since the eavesdroppers are assumed to be present at every existing communication channel.

In reality, wireless network secrecy may not only depend on the strategy of one decision maker. A strategic eavesdropper may also be an active decision maker. Game theoretic models arise naturally when conflict of interest exists among different decision makers, as discussed in the survey by Manshaei *et al.* [20]. Altman *et al.* [1] obtained a transmitter's optimal power allocation strategy

against a hostile jammer using game theoretic models. The authors later extended the model to incomplete information CSI case [2]. Han *et al.* [11] studied a pricing game for the negotiation of security service price between transmitters and multiple friendly interferers. Yuan *et al.* [33] obtained the optimal strategy for a two-user Gaussian interference channel in which each user can decide to activate cooperative jamming by themselves. Gradually, researchers started to use game theoretic approaches to explore attack scenarios in which not all communication channels will be eavesdropped. Garnaev and Trappe [9] proposed a type of active eavesdropper who strategically attacks a limited number of wireless channels. In [7], Garnaev *et al.* considered a target selection game between a friendly interferer and an eavesdropper with players working on only one channel at a time. Recently, we have investigated a power control game for cooperative jamming against a strategic eavesdropper who can only attack one of N parallel channels [30]. A threshold type power allocation plan is obtained under the complete CSI assumption.

Most works mentioned above, except [2], which is dealing with a hostile jammer instead of eavesdroppers, assume complete CSI either obtained instantaneously or statistically, ignoring the fact that it is actually difficult to get complete CSI of eavesdropping channels since eavesdroppers are hiding and listening passively. Various efforts have been made to overcome this assumption for the traditional setup when the eavesdroppers are assumed to attack every existing communication channel. Garnaev and Trappe [8] presented a zero sum anti-eavesdropping game for transmission power allocation in a multi-channel communication network under incomplete CSI, where the environment is regarded as a hostile player that makes CSI as worse as possible. Hu *et al.* [13] investigated a cooperative jamming aided multiple-input-single-output (MISO) communication system, where the network defenders work together to maximize secrecy capacity under a constraint of the secrecy outage probability (SOP) when the CSI of the eavesdropping channel is imperfect. Si *et al.* [25] studied the power control problem under SOP constraints for cooperative jamming against another type of active eavesdroppers who will listen and send hostile jamming signals at the same time. In cases that complete CSI is not available, some historical information might be acquired to infer the probability distributions of the eavesdroppers' CSIs.

To the best of our knowledge, this is the first paper studying the cooperative jamming game against a strategic eavesdropper under the incomplete CSI assumption. The NE strategy derived leads to a more intelligent power allocation strategy that can handle complex environments with uncertainty.

1.2 Summary of contributions

The contributions of this paper can be summarized as follows:

1. A non-zero sum cooperative jamming game considering a strategic eavesdropper and jamming costs is proposed.
2. Instead of using estimators directly, the probability distributions of the eavesdropper's CSIs are incorporated into the players' payoff functions.

3. A threshold type power allocation policy is derived. It is also shown that such a policy can be computed via a numerical algorithm.

The structure of the paper is as follows. Section 2 introduces the model setup. Section 3 proposes the two basic optimization problems for the defender and the eavesdropper, respectively. Section 4 presents a non-zero sum game model when the fading channel gains of eavesdropping channels are characterized by discrete distributions. Section 5 demonstrates two numerical examples and compares the game theoretic model in section 4 with the method of approximating fading channel gains using mean values. Section 6 summarizes conclusions and discusses possible future research.

2 System Model and Game Formulation

2.1 System model

Consider a wireless communication network with N parallel channels, such as a frequency division multiplexing communication system as shown in Figure 1. Each channel occupies a different frequency and the interference from adjacent channels is mitigated via techniques like pulse-shaping filters. An eavesdropper, due to budget limitation, or to reduce the risk of Local Oscillator (LO) leakage power emitted from eavesdropping antennas that may reveal her hidden location(see [23, 35]), is using hardware with limited capability and can only listen on n of N different frequencies at the same time. A friendly interferer who can simultaneously send cooperative jamming signals to N communication channels is tasked to enhance the overall secrecy performance against the eavesdropper. Let SINR be the representation of throughput, which is very often used as argued in [16, 17], especially for systems operating under low SINR regime. Thus, the Shannon capacity can be approximated by SINR, and the communication capacity for each channel $i \in \{1, ..., N\}$, is

$$C_{L_i} = \ln\left(1 + \frac{g_i T_i}{\sigma_i}\right) \approx \frac{g_i T_i}{\sigma_i},$$

with T_i as the transmission power to send encrypted signals at channel i, σ_i as the background noise at channel i and g_i as the fading channel gain from the transmitter to the legitimate receiver. We assume that the cooperative jamming signals will not interfere with the legitimate receiver, which might be achieved when the jamming signals are designed to be nullified at the receiver or the friendly interferer is carefully positioned to be away from the receiver [10, 15, 22]. The eavesdropper can intercept encrypted messages on channel i through a degraded eavesdropping channel with capacity

$$C_{E_i}(J_i) = \ln\left(1 + \frac{\alpha_i T_i}{\sigma_i + \beta_i J_i}\right) \approx \frac{\alpha_i T_i}{\sigma_i + \beta_i J_i},$$

with J_i as the cooperative jamming power assigned to channel i, α_i as the fading channel gain from transmitter i to the eavesdropper and β_i as the fading channel gain from the friendly interferer to the eavesdropper at channel i.

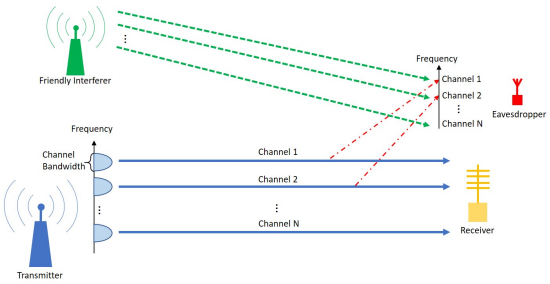


Fig. 1: Frequency division multiplexing communication network with N channels, aided by a friendly interferer.

If channel i is not under an eavesdropping attack, the full communication capacity can be used to transmit secret information. However, if channel i is attacked, information can be transmitted secretly only when the receiver's channel is more capable than the eavesdropper's channel. The difference of these capacities is called channel i's secrecy capacity $C_{S_i}(J_i)$ given as

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

We assume that the friendly interferer does not know the fading channel gains of eavesdropping channels with certainty, but has a belief about the distributions of fading channel gains according to her knowledge of the communication environment and possible locations of the eavesdropper. Let A_i be the random variable representing the fading channel gain to receive transmission signals at eavesdropping channel i such that

$$\Pr(A_i = \alpha_i^m) = q_i^m, \quad \forall m \in \{1, ..., M_i\}.$$

Let B_i be the random variable representing the fading channel gain to receive cooperative jamming signals at eavesdropping channel i such that

$$\Pr(B_i = \beta_i^k) = p_i^k, \quad \forall k \in \{1, ..., K_i\}.$$

Assume A_i and B_i are independent. Thus, with probability $p_i^k q_i^m$, the eavesdropping capacity at channel i is

$$C_{E_i}^{k,m}(J_i) \approx \frac{\alpha_i^m T_i}{\sigma_i + \beta_i^k J_i},$$

and the expected eavesdropping capacity at channel i is

$$\mathbb{E}\left[C_{E_i}(J_i)\right] = \sum_{k=1}^{K_i}\sum_{m=1}^{M_i} p_i^k q_i^m C_{E_i}^{k,m}(J_i) \approx \mathbb{E}\left[A_i\right]\mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right],$$

where

$$\mathbb{E}\left[A_i\right] = \sum_{i=1}^{M_i} q_i^m \alpha_i^m,$$

is the mean of A_i, and

$$\mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right] = \sum_{k=1}^{K_i} p_i^k \frac{T_i}{\sigma_i + \beta_i^k J_i}.$$

The case when A_i's and B_i's are continuous random variables is leaved for discussion in the future. Also, for the sake of simplicity, assume $\mathbb{E}[C_{E_i}(0)]$'s are all distinct.

Note that, every eavesdropping channel should always be a degraded version of the corresponding communication channel, so we assume

$$g_i > \max\{\alpha_i^m, m = 1, ..., M_i\}, \ \ \forall i = 1, ..., N. \tag{1}$$

Under assumption (1), it will be always true that $C_{L_i} > C_{E_i}^{k,m}(J_i)$. Thus, with probability $p_i^k q_i^m$, the secrecy capacity for each channel i is

$$C_{S_i}^{k,m}(J_i) = C_{L_i} - C_{E_i}^{k,m}(J_i) \approx \frac{g_i T_i}{\sigma_i} - \frac{\alpha_i^m T_i}{\sigma_i + \beta_i^k J_i}.$$

Then, the expected secrecy capacity for channel i under cooperative jamming power J_i is

$$\mathbb{E}[C_{S_i}(J_i)] = \sum_{k=1}^{K_i} \sum_{m=1}^{M_i} p_i^k q_i^m C_{S_i}^{k,m}(J_i) \approx \frac{g_i T_i}{\sigma_i} - \mathbb{E}[A_i]\, \mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right],$$

which is a positive concave function w.r.t. $J_i \geq 0$.

We assume that there is a cost, c, associated with employing jamming signal that is proportional to the power usage. Moreover, there is a revenue, r, obtained per unit secrecy capacity. Thus, the payoff to the legitimate users at channel i after applying J_i level of cooperative jamming is

$$\tilde{\mu}_i(J_i) = \begin{cases} r\frac{g_i T_i}{\sigma_i} - cJ_i, & \text{if channel } i \text{ is not attacked,} \\ r(\frac{g_i T_i}{\sigma_i} - \mathbb{E}[A_i]\, \mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right]) - cJ_i, & \text{if channel } i \text{ is attacked.} \end{cases}$$

We will simplify this by substituting $\gamma = c/r$ in the remaining sections as

$$\mu_i(J_i) \equiv \frac{\tilde{\mu}_i(J_i)}{r} = \begin{cases} \frac{g_i T_i}{\sigma_i} - \gamma J_i, & \text{if channel } i \text{ is not attacked,} \\ \frac{g_i T_i}{\sigma_i} - \mathbb{E}[A_i]\, \mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right] - \gamma J_i, & \text{if channel } i \text{ is attacked,} \end{cases}$$

Note that, it is not beneficial to send cooperative jamming signals to channel i if:

1. channel i is not being eavesdropped, or
2. it is too expensive to enhance secrecy capacity by applying cooperative jamming.

The eavesdropper can only attack n out of N channels. Let y_i be the probability that channel i is going to be under an eavesdropping attack, so the expected payoff to the legitimate users at channel i can be written as

$$\mathbb{E}[\mu_i(J_i)] = \frac{g_i T_i}{\sigma_i} - y_i \mathbb{E}[A_i]\, \mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right] - \gamma J_i.$$

Note that $\mathbb{E}[\mu_i(J_i)]$ is a concave function of J_i, since

$$\frac{d}{dJ_i}\mathbb{E}[\mu_i(J_i)] = y_i \sum_{k=1}^{K_i} p_i^k \frac{\mathbb{E}[A_i]\, \beta_i^k T_i}{(\sigma_i + \beta_i^k J_i)^2} - \gamma,$$

is a decreasing function of J_i. It is optimal not to jam channel i unless

$$\frac{d}{dJ_i}\mathbb{E}\left[\mu_i(J_i=0)\right] = y_i\frac{\mathbb{E}\left[A_i\right]\mathbb{E}\left[B_i\right]T_i}{{\sigma_i}^2} - \gamma > 0, \tag{2}$$

where

$$\mathbb{E}\left[B_i\right] = \sum_{i=1}^{K_i} p_i^k \beta_i^k,$$

is the mean of B_i. Inequality (2) presents a lower bound on y_i that makes the friendly interferer jam channel i.

2.2 Formulation of the game

The proposed non-zero sum Nash game solves the friendly interferer's problem of effectively responding to an eavesdropper who strategically picks the channels to attack. The game is played between the friendly interferer as the defender, who decides on the jamming power allocation plan, and a strategic eavesdropper as the attacker. That is, the defender's strategy is $\boldsymbol{J} = (J_1, ..., J_N)$ with $J_i \geq 0,\ \forall i = 1, ..., N$ such that $\sum_{i=1}^{N} J_i \leq J$, where $J > 0$ is the total power available to the friendly interferer. The attacker's strategy is $\boldsymbol{y} = (y_1, ..., y_N)$ with $0 \leq y_i \leq 1,\ \forall i = 1, ..., N$ such that $\sum_{i=1}^{N} y_i = n$, where y_i represents the probability of targeting channel i. Both the friendly interferer and the eavesdropper have complete knowledge about the system parameters.

While the attacker tries to choose n channels to attack in order to maximize her total expected eavesdropping capacity, the defender tries to send cooperative jamming signals to the attacked channels to maximize the overall utility of the whole network. Thus, for a given pair of strategy pair, $(\boldsymbol{J}, \boldsymbol{y})$, the defender's payoff is

$$v_D(\boldsymbol{J}, \boldsymbol{y}) = \sum_{i=1}^{N}\mathbb{E}\left[\mu_i(J_i)\right] = \sum_{i=1}^{N}\frac{g_i T_i}{\sigma_i} - \sum_{i=1}^{N} y_i \mathbb{E}\left[A_i\right]\mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right] - \gamma\sum_{i=1}^{N} J_i, \tag{3}$$

and the eavesdropper's payoff is

$$v_E(\boldsymbol{J}, \boldsymbol{y}) = \sum_{i=1}^{N} y_i \mathbb{E}\left[C_{E_i}(J_i)\right] = \sum_{i=1}^{N} y_i \mathbb{E}\left[A_i\right]\mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right]. \tag{4}$$

Note that increasing the total expected eavesdropping capacity will result in the decrease of the total expected secrecy capacity, so the defender and the eavesdropper are playing a game with conflicting interests. Also note that we are only able to use $\mathbb{E}[A_i]$ but not $\mathbb{E}[B_i]$ in both payoff functions.

To find the best power allocation plan $\boldsymbol{J^*}$, we look for the Nash Equilibrium (NE). That is, we want to find a strategy pair $(\boldsymbol{J}^*, \boldsymbol{y}^*)$ such that

$$v_D(\boldsymbol{J}, \boldsymbol{y}^*) \leq v_D(\boldsymbol{J}^*, \boldsymbol{y}^*), \quad \forall \boldsymbol{J} \in \mathcal{J},$$
$$v_E(\boldsymbol{J}^*, \boldsymbol{y}) \leq v_E(\boldsymbol{J}^*, \boldsymbol{y}^*), \quad \forall \boldsymbol{y} \in \mathcal{Y},$$

where $\mathcal{J}$ is the region containing all possible power allocation strategies $\boldsymbol{J}$ and $\mathcal{Y}$ is the region containing all probabilistic attack strategies $\boldsymbol{y}$ of this game.

3 Best Response Functions

We present two optimization problems each corresponding to the best response for each player when the other player's strategy is fixed.

First consider the case when the defender's cooperative jamming strategy, $\boldsymbol{J} = (J_1, ..., J_N)$, is fixed and is known to the eavesdropper. In this case, the eavesdropper solves the following optimization problem to maximize the total expected eavesdropping capacities,

$$\begin{aligned} \max_{\boldsymbol{y}} \quad & v_E(\boldsymbol{J}, \boldsymbol{y}) = \sum_{i=1}^{N} y_i \mathbb{E}\left[A_i\right] \mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right] \\ \text{s.t.} \quad & \sum_{i=1}^{N} y_i \leq n, \\ & 0 \leq y_i \leq 1, \quad \forall i = 1, ..., N. \end{aligned} \tag{5}$$

Clearly, (5) is a linear optimization problem w.r.t $\boldsymbol{y}$ since $v_E(\boldsymbol{J}, \boldsymbol{y})$ is a linear function of $\boldsymbol{y}$ for fixed $\boldsymbol{J}$, with linear constraints. Thus, the response of the eavesdropper can be found as given in the next theorem.

Theorem 1. *For a fixed cooperative jamming strategy, $\boldsymbol{J}$, the optimal strategy for the active eavesdropper is to eavesdrop on the channels that have the top n largest expected eavesdropping capacities $\mathbb{E}\left[A_i\right] \mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right]$.*

Proof. It is easy to see that

$$\frac{\partial v_E(\boldsymbol{J}, \boldsymbol{y})}{\partial y_i} = \mathbb{E}\left[A_i\right] \mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right], \quad \forall i = 1, ..., N,$$

which are constants for fixed $\boldsymbol{J}$. Thus, to maximize $v_E(\boldsymbol{J}, \boldsymbol{y})$, we should increase y_i's with the largest $\frac{\partial v_E(\boldsymbol{J}, \boldsymbol{y})}{\partial y_i}$ as much as possible. □

Next, consider the case when the defender knows the eavesdropper's attack strategy ahead of time. That is, the probabilistic attacking strategy $\boldsymbol{y} = (y_1, ..., y_N)$ is fixed and is revealed to the defender. In this case, the defender solves the following optimization problem to maximize the total utility of secrecy performance,

$$\begin{aligned} \max_{\boldsymbol{J}} \quad & v_D(\boldsymbol{J}, \boldsymbol{y}) = \sum_{i=1}^{N} \frac{g_i T_i}{\sigma_i} - \sum_{i=1}^{N} y_i \mathbb{E}\left[A_i\right] \mathbb{E}\left[\frac{T_i}{\sigma_i + B_i J_i}\right] - \gamma \sum_{i=1}^{N} J_i \\ \text{s.t.} \quad & \sum_{i=1}^{N} J_i \leq J, \\ & J_i \geq 0, \quad \forall i = 1, ..., N. \end{aligned} \tag{6}$$

Note that $v_D(\boldsymbol{J}, \boldsymbol{y})$ is a convex function w.r.t. $\boldsymbol{J}$. Thus, problem (6) is a convex optimization problem w.r.t. $\boldsymbol{J}$. The best response of the defender can be found as given in the next theorem.

Theorem 2. *The best payoff of the defender against the eavesdropper's strategy,* $\boldsymbol{y} = (y_1, ..., y_N)$ *is*

$$v_D^* = \sum_{i=1}^{N} \frac{g_i T_i}{\sigma_i} - \sum_{i=1}^{N} \Big[\sum_{k=1}^{K_i} p_i^k \frac{y_i \mathbb{E}\left[A_i\right] T_i}{\sigma_i + \beta_i^k J_i^o(w_D)} - \gamma J_i^o(w_D) \Big],$$

where $w_D \geq 0$ *is a threshold value and* $(J_1^o(w_D), ..., J_N^o(w_D))$ *is the optimal power allocation strategy such that*
(a) if

$$y_i T_i \frac{\mathbb{E}\left[A_i\right] \mathbb{E}\left[B_i\right]}{{\sigma_i}^2} - \gamma > w_D$$

then $J_i^o(w_D)$ *is the unique root of the following equation*

$$F_i(x) = w_D,$$

where

$$F_i(x) \coloneqq y_i T_i \sum_{k=1}^{K_i} \frac{\mathbb{E}\left[A_i\right] \beta_i^k p_i^k}{(\sigma_i + \beta_i^k x)^2} - \gamma,$$

(b) if

$$y_i T_i \frac{\mathbb{E}\left[A_i\right] \mathbb{E}\left[B_i\right]}{{\sigma_i}^2} - \gamma \leq w_D$$

then $J_i^o(w_D) = 0$.

Moreover, the threshold value $w_D \geq 0$ *is a real number such that if*

$$\sum_{i=1}^{N} J_i^o(0) > J,$$

then w_D *is the unique root of the equation*

$$\sum_{i=1}^{N} J_i^o(w_D) = J,$$

otherwise $w_D = 0$.

Proof. Note that

$$F_i(J_i) = \frac{\partial v_D(\boldsymbol{J}, \boldsymbol{y})}{\partial J_i},$$

and

$$F_i(0) = y_i T_i \frac{\mathbb{E}\left[A_i\right] \mathbb{E}\left[B_i\right]}{{\sigma_i}^2} - \gamma.$$

By the KKT conditions for problem (6), a vector $\boldsymbol{J} = (J_1, ..., J_N)$ is the optimal solution if there exists a Lagrange multiplier $w_D > 0$ and non-negative coefficients $\lambda_1, ..., \lambda_N$ such that

$$\begin{cases} w_D(J - \sum_{i=1}^{N} J_i) = 0, \\ \lambda_i J_i = 0, \quad \forall i = 1, ..., N, \\ w_D = F_i(J_i) + \lambda_i, \quad \forall i = 1, ..., N. \end{cases}$$

Consider the last equality $w_D = F_i(J_i) + \lambda_i$. Since $\lambda_i \geq 0$ and $F_i(J_i)$ is decreasing in J_i, if $F_i(0) > w_D$, then J_i must be positive. Furthermore, since $\lambda_i J_i = 0$,

$$F_i(J_i) = w_D.$$

On the other hand, if $F_i(0) \leq w_D$, then $J_i = 0$ and $\lambda_i = w_D - F_i(0)$.

Let $\boldsymbol{J^o}(w_D)$ denote the solution to the above KKT conditions as a function of w_D.

If $\sum_{i=1}^{N} J_i^o(0) \leq J$, then $\boldsymbol{J^o}(0)$ is a feasible solution. Thus, $w_D = 0$ and $\boldsymbol{J^o}(0)$ is the optimal solution.

But, if $\sum_{i=1}^{N} J_i^o(0) > J$, then $\boldsymbol{J^o}(0)$ is not a feasible solution. It follows that $w_D > 0$. Thus,

$$\sum_{i=1}^{N} J_i^o(w_D) = J$$

since $w_D(J - \sum_{i=1}^{N} J_i^o(w_D)) = 0$. □

4 Nonzero-sum Game Under Uncertainty

This section considers the general case and looks for the Nash Equilibrium (NE). Since $v_D(\boldsymbol{J}, \boldsymbol{y}^*)$ given $\boldsymbol{y}^*$ is a concave function w.r.t. $\boldsymbol{J} \in \mathcal{J}$ and $v_E(\boldsymbol{J}^*, \boldsymbol{y})$ given $\boldsymbol{J}^*$ is a concave function w.r.t. $\boldsymbol{y} \in \mathcal{Y}$, by the Karush-Kuhn-Tucker Theorem, the NE cooperative jamming strategy $\boldsymbol{J^*}$ should satisfy the KKT conditions

$$\begin{aligned} \left.\frac{\partial v_D(\boldsymbol{J}, \boldsymbol{y^*})}{\partial J_i}\right|_{\boldsymbol{J}=\boldsymbol{J^*}} &= y_i^* \sum_{k=1}^{K_i} p_i^k \frac{\mathbb{E}\left[A_i\right] \beta_i^k T_i}{(\sigma_i + \beta_i^k J_i^*)^2} - \gamma \\ &\begin{cases} = w_D, & if \;\; J_i^* > 0, \quad i = 1, ..., N, \\ \leq w_D, & if \;\; J_i^* = 0, \quad i = 1, ..., N, \end{cases} \end{aligned} \tag{7}$$

and

$$w_D(\sum_{i \in I} J_i^* - J) = 0$$

where $w_D \geq 0$ is a Lagrange multiplier. Similarly, the NE attack strategy $\boldsymbol{y^*}$ should satisfy the KKT conditions

$$\begin{aligned} \left.\frac{\partial v_E(\boldsymbol{J^*}, \boldsymbol{y})}{\partial y_i}\right|_{\boldsymbol{y}=\boldsymbol{y^*}} &= \sum_{k=1}^{K_i} p_i^k \frac{\mathbb{E}\left[A_i\right] T_i}{\sigma_i + \beta_i^k J_i^*} \\ &\begin{cases} \geq w_A, & if \;\; y_i^* = 1, & i = 1, ..., N, \\ = w_A, & if \;\; 0 < y_i^* < 1, & i = 1, ..., N, \\ \leq w_A, & if \;\; y_i^* = 0, & i = 1, ..., N. \end{cases} \end{aligned} \tag{8}$$

where $w_A \geq 0$ is a Lagrange multiplier.

In this paper, we limit the capability of the active eavesdropper to $n = 1$ and leave the case $n > 1$ for future discussion. The next theorem describes the case in which the active eavesdropper adopts a pure strategy in the NE, that is, $y_i^* = 1$ for a single channel $i \in \{1, ..., N\}$.

Theorem 3. *Let m be a positive integer such that*

$$\mathbb{E}\left[C_{E_m}(0)\right] = \max\left\{\mathbb{E}\left[C_{E_i}(0)\right], i = 1, ..., N\right\}.$$

Let $\boldsymbol{y^o}$ be an attack strategy such that

$$y_i^o = \begin{cases} 1, & i = m, \\ 0, & \forall i \neq m, \end{cases}$$

and $\tilde{w}_D$ and $\boldsymbol{J^o}(\tilde{w}_D)$ be the corresponding threshold value and optimal power allocation strategy, respectively, as discussed in Theorem 2. If

$$\mathbb{E}\left[C_{E_m}(\tilde{J}_m^o(\tilde{w}_D))\right] \geq \mathbb{E}\left[C_{E_i}(0)\right], \quad \forall i \neq m,$$

then $(\boldsymbol{J^*}, \boldsymbol{y^*}) = (\boldsymbol{J^o}(\tilde{w}_D), \boldsymbol{y^o})$ is a pair of NE strategies with a pure eavesdropper's strategy.

Proof. We provide a proof in Appendix A. □

When the attacker can not use a pure strategy in the Nash Equilibrium, $\boldsymbol{y^*}$ will be a mixed policy such that $0 \leq y_i^* < 1,\ \forall i = 1, ..., N$. Thus, KKT conditions (8) can be simplified to

$$\begin{aligned} \left.\frac{\partial v_E(\boldsymbol{J^*}, \boldsymbol{y})}{\partial y_i}\right|_{\boldsymbol{y}=\boldsymbol{y^*}} &= \sum_{k=1}^{K_i} p_i^k \frac{\mathbb{E}\left[A_i\right] T_i}{\sigma_i + \beta_i^k J_i^*} \\ &\begin{cases} = w_A, & if\ \ y_i^* > 0, \quad i = 1, ..., N, \\ \leq w_A, & if\ \ y_i^* = 0, \quad i = 1, ..., N. \end{cases} \end{aligned} \tag{9}$$

The next theorem describes the general NE strategy pair.

Theorem 4. *Let w_A be a Lagrangian multiplier with a given value and $\boldsymbol{J}(w_A)$ be a cooperative jamming strategy such that*

$$J_i(w_A) = \begin{cases} \text{the unique root of } R_i(x) = w_A, & if\ \frac{\mathbb{E}[A_i]T_i}{\sigma_i} > w_A, \\ 0, & if\ \frac{\mathbb{E}[A_i]T_i}{\sigma_i} \leq w_A, \end{cases} \tag{10}$$

with

$$R_i(x) \coloneqq \sum_{k=1}^{K_i} p_i^k \frac{\mathbb{E}\left[A_i\right] T_i}{\sigma_i + \beta_i^k x},$$

and the capacity constraint

$$\sum_{i=1}^{N} J_i(w_A) \leq J.$$

Let w_D be another Lagrangian multiplier such that

$$w_D = \begin{cases} \text{the unique root of } \sum\limits_{i \in I(w_A)} y_i(w_A, w_D) = 1, & if\ \sum_{i=1}^N J_i(w_A) = J, \\ 0, & if\ \sum_{i=1}^N J_i(w_A) < J, \end{cases} \tag{11}$$

where

$$I(w_A) = \{i = 1, ..., N : J_i(w_A) > 0\},$$

and $\boldsymbol{y}(w_A, w_D)$ *is an attack strategy such that*

$$y_i(w_A, w_D) = \begin{cases} H_i(w_A, w_D), & \text{if } J_i(w_A) > 0, \\ 0, & \text{if } \frac{\mathbb{E}[A_i]T_i}{\sigma_i} < w_A, \\ \min\left\{ \left[1 - \sum\limits_{j \in I(w_A)} y_i(w_a, w_D) \right]^+, H_i(w_A, w_D) \right\}, & \text{if } \frac{\mathbb{E}[A_i]T_i}{\sigma_i} = w_A, \end{cases} \tag{12}$$

where

$$H_i(w_A, w_D) = \frac{\gamma + w_D}{T_i \sum\limits_{k=1}^{K_i} \frac{p_i^k \mathbb{E}[A_i] \beta_i^k}{(\sigma_i + \beta_i^k J_i(w_A))^2}}.$$

Then, $(\boldsymbol{J^*}, \boldsymbol{y^*}) = (\boldsymbol{J}(w_A), \boldsymbol{y}(w_A, w_D))$ *is a pair of NE strategies if*

1. $w_D \geq 0$, *and*
2. $\sum_{i=1}^{N} y_i(w_A, w_D) = 1$.

Proof. We provide a proof in Appendix B. □

We will now analyze the process to find the value of w_A. Note that $w_A \geq \bar{w}_A$ where $\bar{w}_A$ is the unique root of

$$\sum_{i=1}^{N} J_i(w_A) = J.$$

If $w_A = \bar{w}_A$ and $w_D \geq 0$ as the solution of equations (11) and (12), then a pair of equilibrium strategies has been found.

However, it is possible that $w_D < 0$ when $w_A = \bar{w}_A$. But, this means

$$\sum_{i=1}^{N} y_i(\bar{w}_A, 0) = \sum_{i \in I(\bar{w}_A)} y_i(\bar{w}_A, 0) > 1,$$

suggesting that we should look for $w_A > \bar{w}_A$ that leads to $w_D = 0$ and smaller $y_i(w_A, w_D)$'s.

Clearly, $J_i(w_A)$ is decreasing in w_A. It then follows that $y_i(w_A, w_D)$ is also decreasing w.r.t. $w_A > \bar{w}_A$. Thus, for a given w_A, if $\sum_{i=1}^{N} y_i(w_A, w_D) > 1$, we should look for the NE with $w_A^{'} > w_A$; if $\sum_{i=1}^{N} y_i(w_A, w_D) < 1$, we should look for the NE with $w_A^{'} < w_A$.

Here we present an algorithm to approximate a pair of Nash Equilibrium strategies $(\boldsymbol{J}^*, \boldsymbol{y}^*)$ within a given tolerance factor, ϵ. The algorithm starts searching from $w_A = \bar{w}_A$ and uses a bisection search scheme to converge.

Algorithm 1. Finding NE Strategies $(\boldsymbol{J}^*, \boldsymbol{y}^*)$ under incomplete CSI.
Inputs. State information of the communication network: $T_i, \mathbb{E}[A_i], \beta_i^k, p_i^k$, $\forall k = 1, ..., K_i, \forall i = 1, ..., N$. The background noise σ_i, $\forall i = 1, ..., N$. The total available power J. The explicit tolerance $\epsilon \leq 0.01$.
Step 1. Sort $\mathbb{E}[C_{E_i}(0)]$ in descending order.

Step 2. Let $w_A \leftarrow \bar{w}_A$. Find $(\boldsymbol{J}(w_A), \boldsymbol{y}(w_A, w_D))$ using equations (10), (11) and (12).

Step 2a. If $w_D \geq 0$, then $(\boldsymbol{J}^*, \boldsymbol{y}^*) = (\boldsymbol{J}(w_A), \boldsymbol{y}(w_A, w_D))$ is a pair of NE strategies and the algorithm is terminated. Otherwise, go to step 2b

Step 2b. If $w_D < 0$, let $w_A^{LB} \leftarrow w_A$ and h be the largest integer such that $J_i(w_A) > 0$. Go to step 3.

Step 3. Let $w_A \leftarrow \mathbb{E}\left[C_{E_h}(0)\right]$. Find $(\boldsymbol{J}(w_A), \boldsymbol{y}(w_A, w_D))$ using equations (10), (11) and (12).

Step 3a. If $|\sum_{i=1}^{N} y_i(w_A, w_D) - 1| \leq \epsilon$, then $(\boldsymbol{J}^*, \boldsymbol{y}^*) = (\boldsymbol{J}(w_A), \boldsymbol{y}(w_A, w_D))$ is a pair of NE strategies and the algorithm is terminated. Otherwise, go to step 3b

Step 3b. If $\sum_{i=1}^{N} y_i(w_A, w_D) > 1 + \epsilon$, then let $w_A^{LB} \leftarrow w_A$ and $h \leftarrow h - 1$. Go to step 3. Otherwise, go to step 3c.

Step 3c. If $\sum_{i=1}^{N} y_i(w_A, w_D) < 1 - \epsilon$, then let $w_A^{UB} \leftarrow w_A$. Go to step 4.

Step 4. Let $w_A \leftarrow \frac{1}{2}(w_A^{UB} + w_A^{LB})$. Find $(\boldsymbol{J}(w_A), \boldsymbol{y}(w_A, w_D))$ using equations (10), (11) and (12).

Step 4a. If $|\sum_{i=1}^{N} y_i(w_A, w_D) - 1| \leq \epsilon$, then $(\boldsymbol{J}^*, \boldsymbol{y}^*) = (\boldsymbol{J}(w_A), \boldsymbol{y}(w_A, w_D))$ is a pair of NE strategies and the algorithm is terminated. Otherwise, go to step 4b

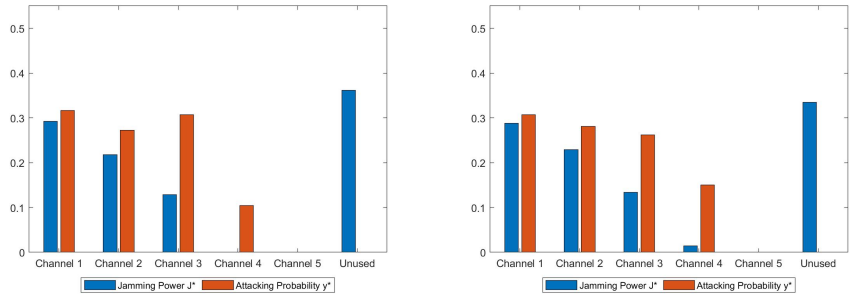
Step 4b. If $\sum_{i=1}^{N} y_i(w_A, w_D) > 1 + \epsilon$, then let $w_A^{LB} \leftarrow w_A$. Go to step 4. Otherwise, go to step 4c.

Step 4c. If $\sum_{i=1}^{N} y_i(w_A, w_D) < 1 - \epsilon$, then let $w_A^{UB} \leftarrow w_A$. Go to step 4.

5 Numerical Illustrations

This section compares the following four different power allocation strategies for the friendly interferer:

1. Strategy 1: the game theoretic power allocation strategy derived by Theorem 4, which takes into account the uncertainty of the eavesdropper's fading channel gains.
2. Strategy 2: the game theoretic power allocation strategy that uses mean values of the eavesdropper's fading channel gains as estimators. It can be calculated following Theorem 4 with $R_i(x) = \frac{\mathbb{E}[A_i]T_i}{\sigma_i + \mathbb{E}[B_i]x}$ and $H_i(w_A, w_D) = \frac{(\gamma + w_D)(\sigma_i + \mathbb{E}[B_i]J_i(w_A))^2}{T_i \mathbb{E}[A_i]\mathbb{E}[B_i]}$.
3. Strategy 3: the power allocation strategy of a friendly interferer who expects eavesdropping attacks at every channel with equal probability but still takes into account the uncertainty of the eavesdropper's fading channel gains. This strategy can be derived following Theorem 2.
4. Strategy 4: the power allocation strategy of a friendly interferer who expects eavesdropping attacks at every channel with equal probability, but this time the friendly interferer uses mean values of the eavesdropper's fading channel gains as estimators. This strategy can be calculated following Theorem 2 with $F_i(x) \coloneqq y_i T_i \frac{\mathbb{E}[A_i]\mathbb{E}[B_i]}{(\sigma_i + \mathbb{E}[B_i]x)^2} - \gamma$.



(a) Strategy 1. (b) Strategy 2.

Fig. 2: plots of $\boldsymbol{J}^*$ and $\boldsymbol{y}^*$ for strategies 1 and 2.

Consider a wireless communication network with 5 parallel channels. Let A_i's be the random eavesdropping channel gains of transmission signals whose mean values are $\{\mathbb{E}[A_i], i = 1, ..., 5\} = (0.75,\ 0.6,\ 0.4,\ 0.275,\ 0.25)$. Let B_i's be the random eavesdropping channel gains of jamming signals such that

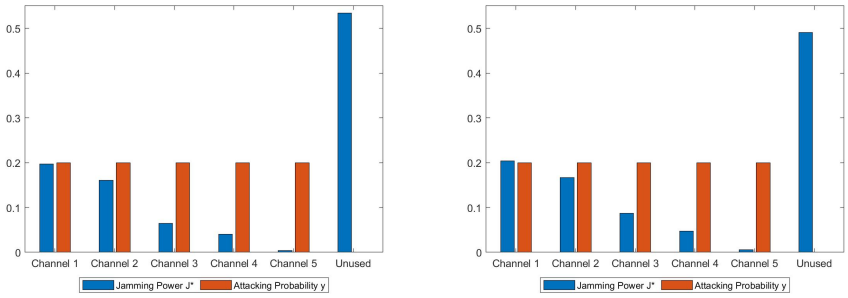
$$\left[\beta_i^k\right] = \begin{bmatrix} 0.4 & 0.8 & 1.2 \\ 0.4 & 0.7 & 1.0 \\ 0.1 & 0.5 & 0.9 \\ 0.25 & 0.6 & 0.95 \\ 0.15 & 0.45 & 0.75 \end{bmatrix}, \left[p_i^k\right] = \begin{bmatrix} 0.33 & 0.34 & 0.33 \\ 0.33 & 0.34 & 0.33 \\ 0.33 & 0.34 & 0.33 \\ 0.33 & 0.34 & 0.33 \\ 0.33 & 0.34 & 0.33 \end{bmatrix},$$

where the ith row stands for channel i and the kth column stands for scenario k. Note that the mean values of B_i's are $\{\mathbb{E}[B_i], i = 1, ..., 5\} = (0.8,\ 0.7,\ 0.5,\ 0.6,\ 0.45)$. Also, let $\{g_i, i = 1, ..., 5\} = (1.2,\ 1.0,\ 0.9,\ 0.75,\ 0.7)$, $\gamma = 1.5$, $J = 1$, $T_i = 1$ and $\sigma_i = 0.12,\ \ \forall i = 1, ..., N$.

For strategy 1, the optimal power allocation plan is $\boldsymbol{J}_{\mathrm{I}}^* = (0.292,\ 0.218,\ 0.129,\ 0,\ 0)$ with payoff $v_D(\boldsymbol{J}_{\mathrm{I}}^*, \boldsymbol{y}_{\mathrm{I}}^*) = 34.668$, as shown in Figure 2a. The eavesdropper's best response is $\boldsymbol{y}_{\mathrm{I}}^* = (0.317,\ 0.272,\ 0.307,\ 0.104,\ 0)$. Due to the cost coefficient γ, channel 4 is not protected by cooperative jamming even when there is unused power.

For strategy 2, the optimal power allocation plan is $\boldsymbol{J}_{\mathrm{II}}^* = (0.288,\ 0.229,\ 0.134,\ 0.014,\ 0)$ as shown in Figure 2a. Compared to strategy 1, the friendly interferer adjusts the jamming powers to cover channel 4. If the friendly interferer uses $\boldsymbol{J}_{\mathrm{II}}^*$ to face the eavesdropper who is still using the NE strategy $\boldsymbol{y}_{\mathrm{I}}^*$ given by Theorem 4, then the payoff given by equation (3) is $v_D(\boldsymbol{J}_{\mathrm{II}}^*, \boldsymbol{y}_{\mathrm{I}}^*) = 34.661$, which is 0.02% worse than the payoff brought by strategy 1.

For strategy 3, let $\boldsymbol{y} = (0.2,\ 0.2,\ 0.2,\ 0.2,\ 0.2)$. The optimal power allocation plan is $\boldsymbol{J}_{\mathrm{III}}^* = (0.197,\ 0.160,\ 0.065,\ 0.040,\ 0.004)$, as shown in Figure 3a. Compared to strategies 1, the friendly interferer covers every channel instead of using a threshold policy. To use this power allocation plan $\boldsymbol{J}_{\mathrm{III}}^*$ against a strategic eavesdropper who commits to $\boldsymbol{y}_{\mathrm{I}}^*$, the friendly interferer will waste cooperative jamming power on channel 5, and the expected payoff given by equation (3) is 34.566, which is 0.29% worse than strategy 1.



(a) Strategy 3. (b) Strategy 4.

Fig. 3: plots of $\boldsymbol{J}^*$ and $\boldsymbol{y}$ for strategy 3 and 4.

For strategy 4, still let $\boldsymbol{y} = (0.2, 0.2, 0.2, 0.2, 0.2)$. The optimal power allocation plan is again covering all channels with $\boldsymbol{J}^*_{\text{IV}} = (0.204, 0.167, 0.087, 0.047, 0.006)$, as shown in Figure 3b. To use this power allocation plan $\boldsymbol{J}^*_{\text{IV}}$ against a strategic eavesdropper who commits to $\boldsymbol{y}^*_{\text{I}}$, the expected payoff given by equation (3) is 34.581, which is 0.25% worse than strategy 1 and 0.23% worse than strategy 2.

These examples demonstrate that the friendly interferer in choosing the best resource allocation plan should not assume a simplistic attack behavior for a strategic eavesdropper. Additionally, even though strategies 1 and 2 (also 3 and 4) have quite similar performance in the given examples, in more realistic FDM systems involving more than 100 channels (see [21]), these differences are expected to be much more significant.

6 Conclusions and Future Research

In this paper, we consider a cooperative jamming game for a multi-channel wireless communication network against an active eavesdropper when the eavesdropping channel gains are uncertain. We present a non-zero sum game to help the defender find the optimal cooperative jamming power allocation strategy under the assumption that the eavesdropper will strategically pick her targets. It turns out that the optimal power allocation strategy follows the classic water-filling scheme. An algorithm to approximate the optimal strategy to within a given tolerance is also presented. We show that the uncertain eavesdropping gains, especially the channel gain of cooperative jamming signals, should not be simply approximated using the mean values if the defender wants to use the optimal power allocation strategy.

Of interest for future research is an extension of this model to the case in which the strategic eavesdropper can attack more than a single channel. Another possible extension is to include the transmission power control problem as part of the defender's decision.

References

1. Altman, E., Avrachenkov, K., Garnaev, A.: A jamming game in wireless networks with transmission cost. In: International Conference on Network Control and Optimization. pp. 1–12. Springer (2007)
2. Altman, E., Avrachenkov, K., Garnaev, A.: Jamming in wireless networks under uncertainty. Mobile Networks and Applications **16**(2), 246–254 (2011)
3. Atallah, M., Kaddoum, G., Kong, L.: A survey on cooperative jamming applied to physical layer security. In: 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB). pp. 1–5. IEEE (2015)
4. Cumanan, K., Alexandropoulos, G.C., Ding, Z., Karagiannidis, G.K.: Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis. IEEE Transactions on Vehicular Technology **66**(8), 7495–7505 (2017)
5. Ding, Z., Leung, K.K., Goeckel, D.L., Towsley, D.: Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting. IEEE Transactions on Wireless Communications **10**(6), 1725–1729 (2011)
6. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Cooperative jamming for wireless physical layer security. In: 2009 IEEE/SP 15th Workshop on Statistical Signal Processing. pp. 417–420. IEEE (2009)
7. Garnaev, A., Baykal-Gürsoy, M., Poor, H.V.: Incorporating attack-type uncertainty into network protection. IEEE Transactions on Information Forensics and Security **9**(8), 1278–1287 (2014)
8. Garnaev, A., Trappe, W.: An eavesdropping game with SINR as an objective function. In: International Conference on Security and Privacy in Communication Systems. pp. 142–162. Springer (2009)
9. Garnaev, A., Trappe, W.: Secret communication when the eavesdropper might be an active adversary. In: International Workshop on Multiple Access Communications. pp. 121–136. Springer (2014)
10. Goel, S., Negi, R.: Guaranteeing secrecy using artificial noise. IEEE Transactions on Wireless Communications **7**(6) (2008)
11. Han, Z., Marina, N., Debbah, M., Hjørungnes, A.: Physical layer security game: interaction between source, eavesdropper, and friendly jammer. EURASIP Journal on Wireless Communications and Networking **2009**, 1–10 (2010)
12. Haphuriwat, N., Bier, V.M.: Trade-offs between target hardening and overarching protection. European Journal of Operational Research **213**(1), 320–328 (2011)
13. Hu, L., Wen, H., Wu, B., Tang, J., Pan, F., Liao, R.F.: Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers. IEEE Transactions on Vehicular Technology **67**(3), 2108–2117 (2017)
14. Hyadi, A., Rezki, Z., Alouini, M.S.: An overview of physical layer security in wireless communication systems with CSIT uncertainty. IEEE Access **4**, 6121–6132 (2016)
15. Jameel, F., Wyne, S., Kaddoum, G., Duong, T.Q.: A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Communications Surveys & Tutorials **21**(3), 2734–2771 (2018)
16. Kim, S.L., Rosberg, Z., Zander, J.: Combined power control and transmission rate selection in cellular networks. In: Gateway to 21st Century Communications Village. VTC 1999-Fall. IEEE VTS 50th Vehicular Technology Conference (Cat. No. 99CH36324). vol. 3, pp. 1653–1657. IEEE (1999)
17. Koo, I., Ahn, J., Lee, J.A., Kim, K.: Analysis of erlang capacity for the multimedia DS-CDMA systems. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences **82**(5), 849–855 (1999)

18. Leung-Yan-Cheong, S., Hellman, M.: The Gaussian wire-tap channel. IEEE Transactions on Information Theory **24**(4), 451–456 (1978)
19. Majumder, R., Warier, R.R., Ghose, D.: Game theory-based allocation of critical resources during natural disasters. In: 2019 Sixth Indian Control Conference (ICC). pp. 514–519 (2019)
20. Manshaei, M.H., Zhu, Q., Alpcan, T., Başar, T., Hubaux, J.P.: Game theory meets network security and privacy. ACM Computing Surveys (CSUR) **45**(3), 1–39 (2013)
21. National Instruments Measurement Fundamentals: OFDM and Multi-Channel Communication Systems (2015), https://www.ni.com/en-us/innovations/white-papers/06/ofdm-and-multi-channel-communication-systems.html
22. Rabbachin, A., Conti, A., Win, M.Z.: Intentional network interference for denial of wireless eavesdropping. In: 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011. pp. 1–6 (Dec 2011)
23. Salem, A., Liao, X., Shen, Y., Jiang, X.: Provoking the adversary by detecting eavesdropping and jamming attacks: A game-theoretical framework. Wireless Communications and Mobile Computing **2018** (2018)
24. Shannon, C.E.: Communication theory of secrecy systems. Bell System Technical Journal **28**(4), 656–715 (1949)
25. Si, J., Cheng, Z., Li, Z., Cheng, J., Wang, H.M., Al-Dhahir, N.: Cooperative jamming for secure transmission with both active and passive eavesdroppers. arXiv preprint arXiv:2002.06324 (2020)
26. Tang, X., Liu, R., Spasojevic, P., Poor, H.V.: Interference assisted secret communication. IEEE Transactions on Information Theory **57**(5), 3153–3167 (May 2011)
27. Tang, X., Liu, R., Spasojevic, P., Poor, H.V.: The Gaussian wiretap channel with a helping interferer. In: 2008 IEEE International Symposium on Information Theory. pp. 389–393. IEEE (2008)
28. Wei, L., Moghadasi, A.H., Sundararajan, A., Sarwat, A.I.: Defending mechanisms for protecting power systems against intelligent attacks. In: 2015 10th System of Systems Engineering Conference (SoSE). pp. 12–17. IEEE (2015)
29. Wyner, A.D.: The wire-tap channel. Bell System Technical Journal **54**(8), 1355–1387 (1975)
30. Xu, Z., Baykal-Gürsoy, M.: A Friendly Interference Game in Wireless Secret Communication Networks. In: Forthcoming in the Proceedings of the 10th International Conference on NETwork Games, COntrol and OPtimization (NETGCOOP). Cargèse, France (Sep 2021), https://hal.archives-ouvertes.fr/hal-02870629
31. Yang, J., Kim, I.M., Kim, D.I.: Joint design of optimal cooperative jamming and power allocation for linear precoding. IEEE Transactions on Communications **62**(9), 3285–3298 (2014)
32. Yolmeh, A., Baykal-Gürsoy, M.: Urban rail patrolling: A game theoretic approach. Journal of transportation security **11**(1-2), 23–40 (2018)
33. Yuan, Z., Wang, S., Xiong, K., Xing, J.: Game theoretic jamming control for the gaussian interference wiretap channel. In: 2014 12th International Conference on Signal Processing (ICSP). pp. 1749–1754. IEEE (2014)
34. Zhang, G., Xu, J., Wu, Q., Cui, M., Li, X., Lin, F.: Wireless powered cooperative jamming for secure OFDM system. IEEE transactions on vehicular technology **67**(2), 1331–1346 (2017)
35. Zhao, G., Shi, W., Li, L., Li, S.: Passive primary receiver detection for underlay spectrum sharing in cognitive radio. IEEE Signal Processing Letters **21**(5), 564–568 (2014)

Appendix A: Proof of Theorem 3

Note that

$$\mathbb{E}\left[C_{E_i}(J_i)\right] = \frac{\partial v_E(\boldsymbol{J}, \boldsymbol{y})}{\partial y_i}.$$

Given $y_m^o = 1$ and $y_i^o = 0,\ \forall i \neq m$, by Theorem 2, we have

$$y_i^o T_i \sum_{k=1}^{K_i} \frac{\mathbb{E}\left[A_i\right] \beta_i^k p_i^k}{{\sigma_i}^2} - \gamma = -\gamma < w_D,\ \forall i \neq m,$$

which leads to $\tilde{J}_m^o(\tilde{w}_D, \boldsymbol{y^o}) = 0,\ \forall i \neq m$.

Assume $(\tilde{\boldsymbol{J}}^{\boldsymbol{o}}(\tilde{w}_D), \boldsymbol{y})$ is a pair of NE strategies. It is required that

$$w_A \geq \mathbb{E}\left[C_{E_i}(0)\right],\ \forall i \neq m$$

by KKT conditions (8). Also, since $y_m^o > 0$, then

$$w_A = \mathbb{E}\left[C_{E_m}(J_m^o(\tilde{w}_D))\right] \leq \mathbb{E}\left[C_{E_m}(0)\right]$$

by KKT conditions (8). Thus, it must be true that

$$\mathbb{E}\left[C_{E_m}(0)\right] \geq \mathbb{E}\left[C_{E_i}(0)\right],\ \forall i \neq m,$$
$$\mathbb{E}\left[C_{E_m}(J_m^o(\tilde{w}_D))\right] \geq \mathbb{E}\left[C_{E_i}(0)\right],\ \forall i \neq m$$

for the assumption to be true. □

Appendix B: Proof of Theorem 4

Let w_A be the Lagrange multiplier for the eavesdropper's optimization problem (6). Note that

$$R_i(J_i) = \frac{\partial v_E(\boldsymbol{J}, \boldsymbol{y})}{\partial y_i},$$
$$R_i(0) = \frac{\mathbb{E}\left[A_i\right] T_i}{\sigma_i},$$

and $R_i(J_i)$ is decreasing w.r.t. $J_i \geq 0$. Let $\boldsymbol{J^*}$ be the cooperative jamming strategy in the NE. Note that

$$R_i(J_i^*) \leq w_A,\ \forall i = 1, ..., N,$$

as required by KKT condition (9). Thus, if $R_i(0) > w_A$, then $J_i^* > 0$. Let w_D be the Lagrange multiplier for the defender's optimization problem (5) and $\boldsymbol{y^*}$ be the attacking strategy in the NE. By KKT condition (7), if $J_i^* > 0$, then

$$y_i^* T_i \sum_{k=1}^{K_i} \frac{\mathbb{E}\left[A_i\right] \beta_i^k p_i^k}{(\sigma_i + \beta_i^k J_i^*)^2} - \gamma = w_D \geq 0,$$

so $y_i^* > 0$. And if $y_i^* > 0$, then

$$R_i(J_i^*) = w_A,$$

by KKT condition (9). In summary, if $R_i(0) > w_A$, then J_i^* is the unique root of the equation

$$R_i(x) = w_A.$$

If $R_i(0) \leq w_A$, then

$$w_A \geq R_i(0) > R_i(J_i), \ \forall J_i > 0.$$

which leads to $J_i^* = 0$ since $R_i(J_i^*) < w_A$ if $J_i^* > 0$. Thus, we can define $\boldsymbol{J}(w_A) \coloneqq \boldsymbol{J^*}$ to show that the NE cooperative jamming strategy is dependent on w_A.

Note that $H_i(w_A, w_D)$ is the unique root of the equation

$$\left.\frac{\partial v_D(\boldsymbol{J}, \boldsymbol{y^*})}{\partial J_i}\right|_{\boldsymbol{J}=\boldsymbol{J^*}} = w_D$$

w.r.t. y_i^*.

If $R_i(0) > w_A$, then $J_i^* > 0$, which leads to $y_i^* = H_i(w_A, w_D)$ by KKT condition (7).

If $R_i(0) < w_A$, then $R_i(J_i^*) = R_i(0) < w_A$ since $J_i^* = 0$. It follows that $y_i^* = 0$ by KKT condition (9).

If $R_i(0) = w_A$, then $J_i^* = 0$, but it is possible to have $y_i^* > 0$ in a NE as long as

$$\begin{cases} \left.\frac{\partial v_D(\boldsymbol{J}, \boldsymbol{y^*})}{\partial J_i}\right|_{\boldsymbol{J}=\boldsymbol{J^*}} \leq w_D, \text{by KKT condition (7)}, \\ y_i^* \geq 0, \\ y_i^* + \sum\limits_{j \in I(w_A)} y_j^* \leq 1. \end{cases}$$

Thus, $\boldsymbol{y}(w_A, w_D)$ in (12) is correctly defined to satisfy KKT conditions (7) and (9). Note that it is possible to have

- $y_i(w_A, w_D) = H_i(w_A, w_D) < 1 - \sum\limits_{j \in I(w_A)} y_j(w_A, w_D)$, or
- $\sum\limits_{j \in I(w_A)} y_j(w_A, w_D) > 1$.

So the constraint $\sum_{i=1}^N y_i(w_A, w_D) = 1$ is not guaranteed by (12).

Finally, it is required that

$$w_D(J - \sum_{i=1}^N J_i(w_A)) = 0.$$

Thus, if $\sum_{i \in I(w_A)} J_i(w_A) < J$, then $w_D = 0$. In this case, the only requirement missing for $(\boldsymbol{J}(w_A), \boldsymbol{y}(w_A, w_D))$ to be a pair of NE strategies is to satisfy

$$\sum_{i=1}^N y_i(w_A, w_D) = 1.$$

Now look at the case when $\sum_{i \in I(w_A)} J_i(w_A) = J$. Following (11) and (12) when $\sum_{i \in I(w_A)} J_i(w_A) = J$, it is guaranteed that $\sum_{i=1}^N y_i(w_A, w_D) = 1$. However, it is possible that $w_D < 0$, so the only requirement for $(\boldsymbol{J}(w_A), \boldsymbol{y}(w_A, w_D))$ to be a pair of NE strategies is to satisfy $w_D \geq 0$.

In summary, following (10), (11) and (12), if

1. $w_D \geq 0$, and
2. $\sum_{i=1}^N y_i(w_A, w_D) = 1$,

then (w_D, w_A) is a proper pair of Lagrange multipliers for the Nash equilibrium problem. □