



A Friendly Interference Game in Wireless Secret Communication Networks

Zhifan Xu, Melike Baykal-Gürsoy

► To cite this version:

Zhifan Xu, Melike Baykal-Gürsoy. A Friendly Interference Game in Wireless Secret Communication Networks. 10th International Conference on NETwork Games, COntrol and OPTimization (NETG-COOP 2021), Sep 2021, Carpi, France. ff10.1007/978-3-030-87473-5_4f f.fhal-02870629ff

HAL Id: hal-02870629

<https://hal.archives-ouvertes.fr/hal-02870629>

Submitted on 16 Jun 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Friendly Interference Game in Wireless Secret Communication Networks [★]

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. This paper considers a parallel wireless network in which multiple individuals exchange confidential information through independent sender-receiver links. An eavesdropper can intercept encrypted information through a degraded channel of each sender-receiver link. A friendly jammer, by applying interference to the eavesdropping channels, can increase the level of secrecy of the network. The optimal power allocation strategy of the friendly jammer under a power constraint is derived. A convex optimization model is used when all channels are under the threat of an eavesdropping attack and a non-zero sum game model is analyzed when the eavesdropper can only attack a limited quantity of channels.

Keywords: Friendly jammer · Eavesdropping · Non-zero sum game

1 Introduction and Problem Formulation

Eavesdropping attacks are major threats for wireless communication networks due to their multi-cast nature. Instead of depending only on encryption and randomness in coding schemes [8, 10, 13], various efforts have been made to investigate possibilities to facilitate the security of wireless communication networks. Recent investigations reveal that intentionally generated interference signals can decrease the eavesdropping capacity of communication channels [6], which leads to the practice of employing a friendly jammer to counter eavesdropping attacks [9, 11, 12].

Due to the limitations of battery and power technology in current state, algorithms for efficient power control are crucial in wireless networks, and game theory has been widely adopted when an intelligent adversary exists. Altman *et al.* [1] obtained the base station's optimal power allocation strategy in jamming games. Garnaev and Trappe [4, 5] investigated the optimal transmission power

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

allocation problem against an eavesdropper using zero-sum games. Garnaev *et al.* [3] described the interaction between a friendly jammer and an eavesdropper using a zero-sum game. It is shown that Nash Equilibria of such games exhibits a water-filling scheme [2, 7].

This paper considers a wireless communication network consisting of n parallel legitimate sender-receiver links where a friendly jammer can assign J_i amount of power to interfere a potential eavesdropper at channel i . The total amount of power that can be utilized by the friendly jammer is bounded by J . Moreover, the fact that it is almost inevitable for the interference signals to degrade legitimate sender-receiver channels is taken into consideration.

For each legitimate sender-receiver link $i \in \{1, \dots, n\}$, the communication capacity that can be used to transmit messages under friendly jamming is

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

where T_i is pre-decided transmission power applied to channel i , σ is the Gaussian noises, g_i^L is the channel gain of transmission signals on channel i , and h_i^L is the channel gain of interference signals on channel i . At the same time, the eavesdropper can intercept information transmitted through channel i using an eavesdropping channel with capacity

$$C_{E_i}(J_i) = \ln \left(1 + \frac{g_i^E T_i}{\sigma + h_i^E J_i} \right),$$

where g_i^E is the channel gain of transmission signals and h_i^E is the channel gain of interference signals on eavesdropping channel i . We assume that $g_i^L > g_i^E$, $\forall i = 1, \dots, n$ to represent the fact that every eavesdropping channel is a degraded version of the corresponding communication channel. We also assume that $h_i^L < h_i^E$, $\forall i = 1, \dots, n$ to represent the fact that interference signals are more effective on eavesdropping channels than communication channels. So a power allocation policy for the friendly jammer is a vector $\mathbf{J} = (J_1, \dots, J_n)$ such that $\sum_{i=1}^n J_i \leq J$.

Without the threat of an eavesdropping attack, legitimate users can utilize channel i 's full communication capacity $C_{L_i}(J_i)$ to transmit messages securely. Meanwhile, channel i 's capacity that can be used to transmit secret messages under an eavesdropping attack is defined as its secrecy capacity $C_{S_i}(J_i)$ (see [8, 9, 13]), which is

$$C_{S_i}(J_i) = (C_{L_i}(J_i) - C_{E_i}(J_i))^+ = \left(\ln \left(1 + \frac{g_i^L T_i}{\sigma + h_i^L J_i} \right) - \ln \left(1 + \frac{g_i^E T_i}{\sigma + h_i^E J_i} \right) \right)^+.$$

Note that $C_{L_i}(0) > C_{E_i}(0)$, $\forall i = 1, \dots, n$, under the assumption $g_i^L > g_i^E$, $\forall i = 1, \dots, n$. Thus, $C_{S_i}(0) > 0$, $\forall i = 1, \dots, n$, which means all channels have positive secrecy capacity without friendly interference. Also note that it is always true that $\ln \left(1 + \frac{g_i^L T_i}{\sigma + h_i^L J_i} \right) > \ln \left(1 + \frac{g_i^E T_i}{\sigma + h_i^E J_i} \right)$, $\forall J_i \geq 0, i = 1, \dots, n$, since $g_i^L > g_i^E$ and $h_i^L < h_i^E$, $\forall i = 1, \dots, n$. Hence, the expression of a secrecy capacity $C_{L_i}(J_i)$

w.r.t. $J_i \geq 0$ can be simplified as

$$C_{S_i}(J_i) = \ln \left(1 + \frac{g_i^L T_i}{\sigma + h_i^L J_i} \right) - \ln \left(1 + \frac{g_i^E T_i}{\sigma + h_i^E J_i} \right).$$

In addition, assume $\frac{d}{dJ_i} C_{S_i}(J_i = 0) > 0$, so that the friendly jammer has an incentive to increase channel i 's secrecy capacity under an eavesdropping attack.

The structure of the paper is as follows: Section 2 discusses the key properties of the secrecy capacity functions $C_{S_i}(J_i)$'s and considers a single player power allocation problem where all communication channels are under the threat of an eavesdropping attack. Section 3 is the main part of the paper, which reveals the water-filling structure of the Nash Equilibrium in a friendly interference game where the eavesdropper can only attack a limited number of channels. Based on these theoretical results, section 3.2 presents a computational algorithm to determine the optimal power allocation strategy. Section 4 demonstrates numerical examples. Section 5 summarizes the conclusions and discusses possible future research.

2 Basic Optimization Model

This section considers the scenario in which communication channels are under the threat of eavesdropping attacks all at the same time, so the friendly jammer is the only decision maker. The friendly jammer aims to maximize the overall secrecy capacity of this network.

2.1 Properties of $C_{S_i}(J_i)$'s

The following lemmas present the key properties of the secrecy capacity functions $C_{S_i}(J_i)$, $\forall i = 1, \dots, n$.

Lemma 1. $C_{S_i}(J_i)$ is unimodal w.r.t. $J_i \geq 0$ and has a unique maximum at $J_i = \bar{J}_i$ such that $\frac{d}{dJ_i} C_{S_i}(\bar{J}_i) = 0$.

Proof. Let $c_i(J_i) := \frac{d}{dJ_i} C_{S_i}(J_i)$, then,

$$c_i(J_i) = \frac{g_i^E h_i^E T_i}{(g_i^E T_i + \sigma + h_i^E J_i)(\sigma + h_i^E J_i)} - \frac{g_i^L h_i^L T_i}{(g_i^L T_i + \sigma + h_i^L J_i)(\sigma + h_i^L J_i)} = \frac{A_i(J_i)}{B_i(J_i)},$$

$$\text{where } \begin{cases} A_i(J_i) = (g_i^E h_i^L - g_i^L h_i^E) h_i^E h_i^L T_i J_i^2 + (g_i^E - g_i^L) \cdot 2\sigma h_i^E h_i^L T_i J_i + C_i, \\ B_i(J_i) = (g_i^E T_i + \sigma + h_i^E J_i)(\sigma + h_i^E J_i)(g_i^L T_i + \sigma + h_i^L J_i)(\sigma + h_i^L J_i), \\ C_i = [g_i^E h_i^E (g_i^L T_i + \sigma) - g_i^L h_i^L (g_i^E T_i + \sigma)] \sigma T_i. \end{cases}$$

Note that $A_i(0) > 0$ since $c_i(0) > 0$ and $A_i(J_i)$ is a concave quadratic function since $g_i^E h_i^L - g_i^L h_i^E < 0$, then there exists a unique value $\bar{J}_i > 0$ such that $A_i(\bar{J}_i) = 0$. Also note that $B_i(J_i) > 0$, $\forall J_i \geq 0$. Thus, $J_i = \bar{J}_i$ is the unique solution to $c_i(J_i) = 0$ w.r.t. $J_i \geq 0$.

Moreover, note that $A_i(J_i) > 0$, $\forall 0 \leq J_i < \bar{J}_i$ and $A_i(J_i) < 0$, $\forall J_i > \bar{J}_i$, so $c_i(J_i) > 0$, $\forall 0 \leq J_i < \bar{J}_i$ and $c_i(J_i) < 0$, $\forall J_i > \bar{J}_i$, since $c_i(J_i) = \frac{A_i(J_i)}{B_i(J_i)}$ and

$B_i(J_i) > 0$, $\forall J_i \geq 0$. Furthermore, $c_i(J_i)$ is also continuous w.r.t. $J_i \geq 0$, so $c_i(J_i)$ crosses the horizontal axis exactly once in $[0, \infty)$ at $J_i = \bar{J}_i$. Thus, $C_{S_i}(J_i)$ is unimodal w.r.t. $J_i \geq 0$ and it has a unique maximum at $J_i = \bar{J}_i$. $\square$

Since $C_{S_i}(J_i)$ is unimodal w.r.t. $J_i \geq 0$ and it has a unique maximum at $J_i = \bar{J}_i$, then $C_{S_i}(J_i) < C_{S_i}(\bar{J}_i)$, $\forall J_i > \bar{J}_i$. Hence, the friendly jammer will put at most $\bar{J}_i$ power to channel i if she aims to maximize channel i 's secrecy capacity. To solve the friendly jammer's power allocation problem, it is enough to consider $C_{S_i}(J_i)$'s properties w.r.t. the refined feasible region $J_i \in [0, \bar{J}_i]$, $\forall i = 1, \dots, n$.

Lemma 2. $C_{S_i}(J_i)$ is concave and strictly increasing w.r.t. $J_i \in [0, \bar{J}_i]$ for all $i = 1, \dots, n$.

Proof. Let $c_i(J_i)$, $A_i(J_i)$ and $B_i(J_i)$ be defined as in lemma 1. Note that:

- (a) $A_i(J_i)$ is a concave quadratic function and is strictly decreasing w.r.t. $J_i \geq 0$ since $g_i^E h_i^L - g_i^L h_i^E < 0$ and $g_i^E - g_i^L < 0$,
- (b) $B_i(J_i)$ is strictly increasing w.r.t. $J_i \geq 0$,
- (c) $A_i(J_i) \geq 0$ and $B_i(J_i) > 0$ for all $J_i \in [0, \bar{J}_i]$.

Thus, $c_i(J_i) = \frac{A_i(J_i)}{B_i(J_i)}$ is strictly decreasing w.r.t. $J_i \in [0, \bar{J}_i]$, which implies $C_{S_i}(J_i)$ is a concave function on $J_i \in [0, \bar{J}_i]$.

Also, $C_{S_i}(J_i)$ is strictly increasing w.r.t. $J_i \in [0, \bar{J}_i]$, since $c_i(J_i) > 0$, $\forall J_i \in [0, \bar{J}_i]$ as proved in lemma 1. $\square$

Although it is impossible for the friendly jammer's optimal power allocation policy $\mathbf{J}^*$ to have $J_i^* \geq \bar{J}_i$, we would like to present a full description of the shape of $C_{S_i}(J_i)$ w.r.t. $J_i \in [0, +\infty)$ without going into tedious proofs of all details.

First, consider $c_i(J_i)$ w.r.t. $J_i \in [\bar{J}_i, +\infty)$. Note that: (a) $A_i(J_i)$ is concave, quadratic, strictly decreasing and negative w.r.t. $J_i > \bar{J}_i$, (b) $B_i(J_i)$ is quartic, strictly increasing and positive w.r.t. $J_i > \bar{J}_i$. Thus, it can be seen that

$$\lim_{J_i \rightarrow +\infty} c_i(J_i) = \frac{A_i(J_i)}{B_i(J_i)} = -0,$$

and it can be proved by the mean value theorem that there exists a point $\tilde{J}_i \in (\bar{J}_i, +\infty)$ such that $\frac{d}{dJ_i} c_i(\tilde{J}_i) = 0$. Moreover, $\tilde{J}_i$ is actually the unique solution to $\frac{d}{dJ_i} c_i(J_i) = 0$ w.r.t. $J_i \in [0, +\infty)$ given the properties of $A_i(J_i)$ and $B_i(J_i)$. Since $c_i(J_i)$ is decreasing at $J_i = \bar{J}_i$, it can also be verified that $c_i(J_i)$ is strictly decreasing in $[\bar{J}_i, \tilde{J}_i]$, and then strictly increasing in $(\tilde{J}_i, +\infty)$. In summary, for $J_i \in [0, +\infty)$, $c_i(J_i)$ has the following properties as shown in Fig. 1b:

- $c_i(J_i) \geq 0$, $\forall J_i \in [0, \bar{J}_i]$, and $c_i(J_i) < 0$, $\forall J_i \in (\bar{J}_i, +\infty)$.
- $c_i(J_i)$ is strictly decreasing w.r.t. $J_i \in [0, \tilde{J}_i]$, and is strictly increasing w.r.t. $J_i \in (\tilde{J}_i, +\infty)$.

Recall that $c_i(J_i) = \frac{d}{dJ_i} C_{S_i}(J_i)$ by definition, so $C_{S_i}(J_i)$ is concave w.r.t. $J_i \in [0, \tilde{J}_i]$, since $c_i(J_i)$ is strictly decreasing w.r.t. $J_i \in [0, \tilde{J}_i]$. In summary, for $J_i \in [0, +\infty)$, $C_{S_i}(J_i)$ has the following properties as shown in Fig. 1a:

- $C_{S_i}(J_i) > 0$, $\forall J_i \in [0, +\infty)$.
- $C_{S_i}(J_i)$ is concave w.r.t. $J_i \in [0, \tilde{J}_i]$ and reaches its maximum at $J_i = \bar{J}_i < \tilde{J}_i$.
- $C_{S_i}(J_i)$ is convex and decreasing w.r.t. $J_i \in (\tilde{J}_i, +\infty)$.

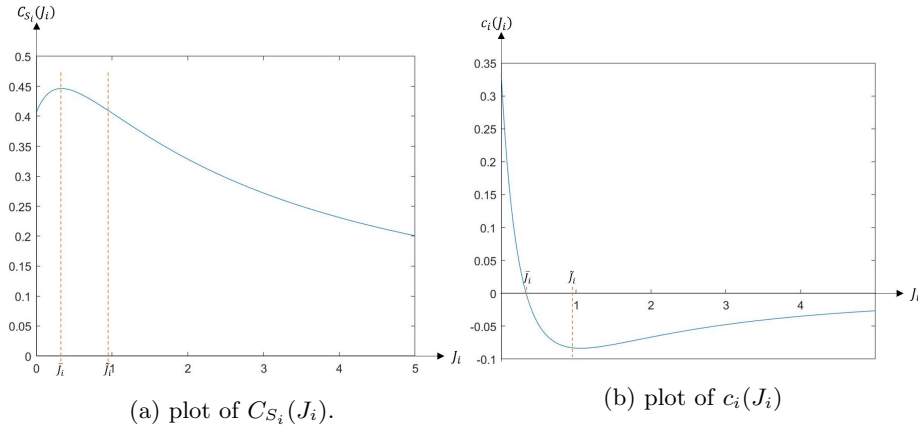


Fig. 1: plots of $C_{S_i}(J_i)$ and $c_i(J_i)$, with $g_i^L = 2, g_i^E = 1, h_i^L = 1, h_i^E = 2, T_i = 1, \sigma = 1$.

2.2 The Optimal Power Allocation Policy

To find the optimal power allocation policy for the network, the friendly jammer needs to solve the following problem:

$$\begin{aligned} \max_{\mathbf{J}} \quad & v_J(\mathbf{J}) = \sum_{i=1}^n C_{S_i}(J_i) = \sum_{i=1}^n \left[\ln \left(1 + \frac{g_i^L T_i}{\sigma + h_i^L J_i} \right) - \ln \left(1 + \frac{g_i^E T_i}{\sigma + h_i^E J_i} \right) \right] \\ \text{s.t.} \quad & \sum_{i=1}^n J_i \leq J, \\ & 0 \leq J_i \leq \bar{J}_i, \quad \forall i = 1, \dots, n. \end{aligned} \quad (1)$$

Note that $v_J(\mathbf{J})$ is a concave function on $\mathbf{J} \in \mathcal{J}$ where $\mathcal{J}$ is the feasible region of optimization problem 1. To prove it, simply let $v_i(\mathbf{J}) := C_{S_i}(J_i)$, then $v_i(\mathbf{J})$ is concave on $\mathbf{J} \in \mathcal{J}$ since $C_{S_i}(J_i)$ is concave on $J_i \in [0, \bar{J}_i]$. Thus, $v_J(\mathbf{J})$ is concave on $\mathbf{J} \in \mathcal{J}$ since it is a sum of $v_i(\mathbf{J})$'s. So optimization problem 1 is a convex optimization problem.

Theorem 1. *The considered convex optimization problem has a unique optimal solution $\mathbf{J}^* = (J_1^*, \dots, J_n^*)$ that is subject to water-filling scheme. Let the sequence of sender-receiver links be ordered according to $c_i(0)$ such that $c_1(0) > \dots > c_n(0)$ assuming $c_i(0) \neq c_j(0), \forall i \neq j$ for the sake of simplicity.*

a) *If $\sum_{i=1}^n \bar{J}_i \geq J$, then there exists $w \geq 0$ and a threshold integer $k > 0$ such that*

$$\begin{cases} c_1(J_1^*) = \dots = c_k(J_k^*) = w, \\ \sum_{i=1}^k J_i^* = J, \\ c_i(0) \leq w, J_i^* = 0, \quad \forall k < i \leq n. \end{cases} \quad (2)$$

and $\mathbf{J}^*$ is the solution of equations system 2.

b) *If $\sum_{i=1}^n \bar{J}_i < J$, then $k = n, w = 0$, and $\mathbf{J}^*$ is the solution to*

$$c_1(J_1^*) = \dots = c_n(J_n^*) = w = 0. \quad (3)$$

6 Zhifan Xu and Melike Baykal-Gürsoy

and $\sum_{i=1}^n J_i^* < J$.

Proof. We provide a proof in the appendix. $\square$

Based on Theorem 1, the optimal value of w in the system of equations 2 can be determined using numerical methods such as bisection search.

3 A Friendly Interference Game

This section considers another scenario where the attacker can eavesdrop on only one of n channels due to resource constraints. To intercept as much information as possible, the attacker tries to maximize the expected eavesdropping capacity. Let the attack strategy of the eavesdropper be $\mathbf{y} = (y_1, \dots, y_n)$ where y_i represents the probability that the eavesdropper picks channel i as target. Naturally, we have $y_i \geq 0$, $\forall i = 1, \dots, n$ and $\sum_{i=1}^n y_i = 1$. Thus, the payoff for the attacker under interference signals is

$$v_E(\mathbf{J}, \mathbf{y}) = \sum_{i=1}^n y_i C_{E_i}(J_i) = \sum_{i=1}^n y_i \ln \left(1 + \frac{g_i^E T_i}{\sigma + h_i^E J_i} \right). \quad (4)$$

Meanwhile, the friendly jammer still tries to maximize the total capacity that can be used to transmit messages securely, so the friendly jammer's payoff is

$$\begin{aligned} v_J(\mathbf{J}, \mathbf{y}) &= \sum_{i=1}^n [C_{L_i}(J_i) - y_i C_{E_i}(J_i)] \\ &= \sum_{i=1}^n \left[\ln \left(1 + \frac{g_i^L T_i}{\sigma + h_i^L J_i} \right) - y_i \ln \left(1 + \frac{g_i^E T_i}{\sigma + h_i^E J_i} \right) \right], \end{aligned} \quad (5)$$

and the friendly jammer's power allocation strategy $\mathbf{J}$ is still subject to the total power constraint.

Now, we have a non-zero sum game with two players, namely the friendly jammer and the eavesdropper. We shall look for the Nash Equilibrium, that is, we want to find a strategy pair $(\mathbf{J}^*, \mathbf{y}^*)$ such that

$$\begin{aligned} v_J(\mathbf{J}, \mathbf{y}^*) &\leq v_J(\mathbf{J}^*, \mathbf{y}^*), \quad \forall \mathbf{J} \in \mathcal{J}, \\ v_E(\mathbf{J}^*, \mathbf{y}) &\leq v_E(\mathbf{J}^*, \mathbf{y}^*), \quad \forall \mathbf{y} \in \mathcal{Y}, \end{aligned}$$

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

3.1 Theoretical Analysis

Consider the friendly jammer's problem given a fixed attack strategy $\mathbf{y}^*$ of the adversary. It can be seen that $\frac{\partial v_J(\mathbf{J}, \mathbf{y}^*)}{\partial J_i}$ share similar properties with $c_i(J_i)$, and interfering any channel i where $\frac{\partial v_J(\mathbf{J}, \mathbf{y}^*)}{\partial J_i}|_{J_i=0} \leq 0$ will be a dominated strategy for the friendly jammer. Let I be the set of channels where $\frac{\partial v_J(\mathbf{J}, \mathbf{y}^*)}{\partial J_i}|_{J_i=0} > 0$,

let $\bar{J}_i(\mathbf{y}^*) > 0$ be a real value such that $\frac{\partial v_J(\mathbf{J}, \mathbf{y}^*)}{\partial J_i} \big|_{J_i=\bar{J}_i(\mathbf{y}^*)} = 0, \forall i \in I$, then the friendly jammer needs to solve the following optimization problem:

$$\begin{aligned} \max_{J_i, \forall i \in I} \quad & \sum_{i \in I} \left[\ln \left(1 + \frac{g_i^L T_i}{\sigma + h_i^L J_i} \right) - y_i^* \ln \left(1 + \frac{g_i^E T_i}{\sigma + h_i^E J_i} \right) \right] \\ \text{s.t.} \quad & \sum_{i \in I} J_i \leq J, \\ & 0 \leq J_i \leq \bar{J}_i(\mathbf{y}^*), \quad \forall i \in I. \end{aligned} \quad (6)$$

Optimization problem 6 is similar to optimization problem 1 but with a subset of channels as targets and with smaller coefficients $y_i^* \leq 1$ in the objective function. So the objective function of optimization problem 6 is concave w.r.t. its feasible region. Thus, an optimal power allocation strategy $\{J_i^*, i \in I\}$ should still have the properties implied by KKT conditions. That is,

$$\begin{aligned} \frac{\partial v_J(\mathbf{J}^*, \mathbf{y}^*)}{\partial J_i} &= \frac{y_i^* g_i^E h_i^E T_i}{(g_i^E T_i + \sigma + h_i^E J_i^*)(\sigma + h_i^E J_i^*)} - \frac{g_i^L h_i^L T_i}{(g_i^L T_i + \sigma + h_i^L J_i^*)(\sigma + h_i^L J_i^*)} \\ &\begin{cases} = w_D, & \text{for } J_i^* > 0, \quad \forall i \in I, \\ \leq w_D, & \text{for } J_i^* = 0, \quad \forall i \in I, \end{cases} \end{aligned} \quad (7)$$

where $w_D \geq 0$, and $w_D(\sum_{i \in I} J_i^* - J) = 0$.

Similarly, given the friendly jammer's strategy $\mathbf{J}^*$, the eavesdropper can find his optimal strategy by solving a convex optimization problem where an optimal solution $\mathbf{y}^*$ should satisfy

$$\frac{\partial v_E(\mathbf{J}^*, \mathbf{y}^*)}{\partial y_i} = \ln \left(1 + \frac{g_i^E T_i}{\sigma + h_i^E J_i^*} \right) \begin{cases} = w_A, & \text{for } y_i^* > 0, \quad \forall i = 1, \dots, n, \\ \leq w_A, & \text{for } y_i^* = 0, \quad \forall i = 1, \dots, n, \end{cases} \quad (8)$$

where $w_A \geq 0$ and $\sum_{i=1}^n y_i^* = 1$.

Theorem 2. Define $\Theta_i(J_i) := \frac{\partial v_E(\mathbf{J}, \mathbf{y})}{\partial y_i}$. Let the sequence of sender-receiver links be ordered according to $\Theta_i(0)$ such that $\Theta_1(0) > \dots > \Theta_n(0)$ assuming $\Theta_i(0) \neq \Theta_j(0), \forall i \neq j$ for the sake of simplicity. Let $k > 0$ be the largest integer such that

$$\begin{cases} \Theta_1(J_1) = \dots = \Theta_k(J_k) = w_A \geq 0, \\ \sum_{i=1}^k J_i = J, \\ \Theta_i(0) \leq w_A, \quad J_i = 0, \quad \forall k < i \leq n. \end{cases} \quad (9)$$

Let $\mathbf{J}' = (J'_1, \dots, J'_n)$ be the solution of system of equations 9.

Define $\Delta_{J'_i}(y_i) := \frac{\partial v_J(\mathbf{J}, \mathbf{y})}{\partial J_i} \big|_{J_i=J'_i}$. Let $m > 0$ be the largest integer such that

$$\begin{cases} \Delta_{J'_1}(y_1) = \dots = \Delta_{J'_m}(y_m) = w_D \geq 0, \\ \sum_{i=1}^m y_i \leq 1. \end{cases} \quad (10)$$

a) If $k \leq m$, a Nash Equilibrium strategy pair $(\mathbf{J}^*, \mathbf{y}^*)$ can be found by solving

$$\begin{cases} \mathbf{J}^* = \mathbf{J}', \\ \Delta_{J'_1}(y_1^*) = \dots = \Delta_{J'_k}(y_k^*) = w_D \geq 0, \\ \sum_{i=1}^k y_i^* = 1. \end{cases} \quad (11)$$

b) If $k > m$, there exists a positive integer $h \leq k$ such that a Nash Equilibrium strategy pair $(\mathbf{J}^*, \mathbf{y}^*)$ can be found where $\mathbf{J}^*$ is the solution of

$$\begin{cases} \Theta_1(J_1^*) = \dots = \Theta_h(J_h^*) = w'_A > w_A, \\ J_i^* = 0, \quad \forall h < i \leq n, \\ \Theta_h(0) > w'_A \geq \Theta_{h+1}(0), \end{cases} \quad (12)$$

and $\mathbf{y}^*$ is the solution of

$$\begin{cases} \Delta_{J_1^*}(y_1^*) = \dots = \Delta_{J_h^*}(y_h^*) = 0, \\ y_{h+1}^* = 1 - \sum_{i=1}^h y_i^*, \quad \Delta_{J_{h+1}^*}(y_{h+1}^*) \leq 0, \\ y_{h+1}^* = 0, \quad \text{if } w'_A \neq \Theta_{h+1}(0), \\ y_i^* = 0, \quad \forall h+1 < i \leq n. \end{cases} \quad (13)$$

Proof. We provide a proof in the appendix. $\square$

3.2 Algorithm to Find $(\mathbf{J}^*, \mathbf{y}^*)$

This sections presents an algorithm based on the bisection methods and Theorem 2 to approximate a pair of Nash Equilibrium strategies $(\mathbf{J}^*, \mathbf{y}^*)$ within a given tolerance factor, δ . An explicit value for δ is used to make the algorithm terminate within reasonable CPU time.

Algorithm

Inputs. Parameters of the communication network: $T_i, g_i^L, g_i^E, h_i^L, h_i^E, \forall i = 1, \dots, n$. The background noise σ . And the explicit tolerance $\delta \leq 0.01$.

Step 1. Let k, w_A and $\mathbf{J}'$ be the solution of system of equations 9.

Step 2. Let m, w_D and $\mathbf{y}^*$ be the solution of system of equations 10.

Step 3. If $k \leq m$. Let $\mathbf{J}^* \leftarrow \mathbf{J}'$. Let $\mathbf{y}^*$ be the solution of system of equations 11. $(\mathbf{J}^*, \mathbf{y}^*)$ is a pair of NE strategies and the algorithm is terminated. Otherwise, go to step 4.

Step 4. If $k > m$. Let $h \leftarrow k$. Let $w_A^{LB} \leftarrow w_A$.

Step 4a. Let $h \leftarrow h - 1$ and then $w'_A \leftarrow \Theta_{h+1}(0)$.

Step 4b. Let $\mathbf{J}'$ be the solution of system of equations 12. Let $w_D \leftarrow 0$. Let m and $\mathbf{y}^*$ be the solution of system of equations 10 with the value of $\mathbf{J}'$. Go to step 5.

Step 5. If $h = m$. Let $\mathbf{J}^* \leftarrow \mathbf{J}'$, then $(\mathbf{J}^*, \mathbf{y}^*)$ is a pair of NE strategies and the algorithm is terminated. Otherwise, go to step 6.

Step 6. If $h > m$. Let $w_A^{LB} \leftarrow \Theta_{h+1}(0)$. Go to step 4a. Otherwise, go to step 7.

Step 7. If $h < m$. Let $w_A^{UB} \leftarrow \Theta_{h+1}(0)$ and then $h \leftarrow h + 1$.

Step 7a. Let $w'_A \leftarrow \frac{1}{2}(w_A^{UB} + w_A^{LB})$. Let $\mathbf{J}'$ be the solution of system of equations 12. Let $w_D \leftarrow 0$. Let m and $\mathbf{y}^*$ be the solution of system of equations 10 with the value of $\mathbf{J}'$.

Step 7b. If $h = m$ and $y_{h+1}^* \leq \delta$. Let $\mathbf{J}^* \leftarrow \mathbf{J}'$ and $y_{h+1}^* \leftarrow 0$. Then $(\mathbf{J}^*, \mathbf{y}^*)$ is NE strategies and the algorithm is terminated. Otherwise, go to step 7c.

Step 7c. If $h = m$ and $y_{h+1}^* > \delta$, or if $h < m$. Let $w_A^{UB} \leftarrow w_A'$. Go to step 7a. Otherwise, go to step 7d.
Step 7d. If $h > m$. Let $w_A^{LB} \leftarrow w_A'$. Go to step 7a.

4 Numerical Illustrations

This section presents a few numerical examples. First, consider a 5 parallel channel communication network with $g_i^L = p^{i-1}$ for $i \in [1, 5]$ where $p \in (0, 1)$, which corresponds to Rayleigh fading in orthogonal frequency-division multiplexing (OFDM) systems. Similarly, let $g_i^E = q^{i-1}$ for $i \in [1, 5]$ where $q \in (0, 1)$ for the eavesdropper. Let $p = 0.65$ and $q = 0.5$ such that the assumption $g_i^L > g_i^E$, $\forall i = 1, \dots, 5$ is satisfied. Also set $\delta = 0.1$ and $T_i = 1$, $\forall i = 1, \dots, 5$. Finally, we set $h_i^E = 0.45$, $h_i^L = 0.05$ for all $i = 1, \dots, 5$ and $J = 1$ for the sake of simplicity. The assumption $c_i(0) > 0$, $\forall i = 1, \dots, 5$ is satisfied.

Following the algorithm in section 3.2, we get $k = 3$ and $m = 4$. So the threshold index is $h = 3$. The approximated NE strategies are found in 0.0313 CPU time, with $\mathbf{J}^* = (0.731, 0.254, 0.016, 0, 0)$, $\mathbf{y}^* = (0.535, 0.305, 0.16, 0, 0)$, $w_A = 1.204$ and $w_D = 0.074$. It can be clearly seen that $(\mathbf{J}^*, \mathbf{y}^*)$ is subject to water-filling scheme where both players focus on the channels with higher initial eavesdropping capacities.

Now increase h_i^L 's by 50%, meaning that the legitimate users suffer more from the interference signals. Using the algorithm in section 3.2, we get $k = 3$ and $m = 2$ in 0.0469 CPU time. And the final threshold index is $h = 2$, with $\mathbf{J}^* = (0.667, 0.222, 0, 0, 0)$, $\mathbf{y}^* = (0.541, 0.339, 0.12, 0, 0)$, $w_A = 1.253$ and $w_D = 0$. Compared to the previous example, the friendly jammer protects fewer channels and leaves channel 3 with no protection under attack even though there is unused jamming power.

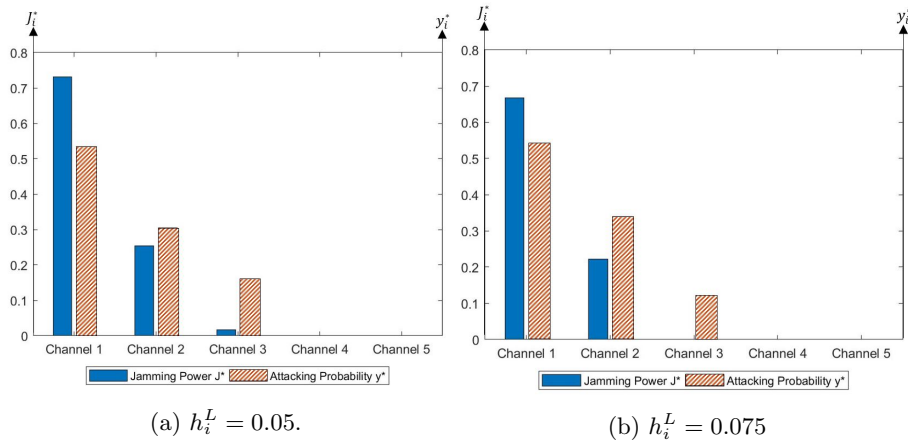


Fig. 2: plots of $\mathbf{J}^*$ and $\mathbf{y}^*$.

5 Conclusions and Future Research

In this paper, we consider a friendly interference game where a friendly jammer is employed to interfere eavesdroppers in a wireless network. We prove the existence of the optimal power allocation strategy of the friendly jammer as part of a pair of Nash Equilibrium strategies in a non-zero sum game. It turns out that the optimal power allocation strategy will be subject to a water-filling scheme. An algorithm to approximate the optimal power allocation strategy to within a given tolerance is presented. We also show that the effect of interference signals on legitimate users is a key parameter that affect the performance of this approach. The interference signals should be carefully tuned such that no interference power will be wasted.

Of interest for future research is an extension of this model to include the legitimate users as decision makers. For instance, a base station controlling transmission power among multiple channels may cooperate with a friendly jammer.

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.: Closed form solutions for water-filling problems in optimization and game frameworks. *Telecommunication Systems* **47**(1-2), 153–164 (2011)
3. 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)
4. 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)
5. 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)
6. Goel, S., Negi, R.: Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications* **7**(6) (2008)
7. Lai, L., El Gamal, H.: The water-filling game in fading multiple-access channels. *IEEE Transactions on Information Theory* **54**(5), 2110–2122 (2008)
8. Leung-Yan-Cheong, S., Hellman, M.: The Gaussian wire-tap channel. *IEEE Transactions on Information Theory* **24**(4), 451–456 (1978)
9. 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)
10. Shannon, C.E.: Communication theory of secrecy systems. *Bell System Technical Journal* **28**(4), 656–715 (1949)
11. Tang, X., Liu, R., Spasojevic, P., Poor, H.V.: Interference assisted secret communication. *IEEE Transactions on Information Theory* **57**(5), 3153–3167 (May 2011)
12. 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)

13. Wyner, A.D.: The wire-tap channel. Bell System Technical Journal **54**(8), 1355–1387 (1975)

Appendix

Proof of Theorem 1. Consider the KKT conditions of convex optimization problem 1. A vector $\mathbf{J}^* = (J_1^*, \dots, J_n^*)$ is the optimal solution if there exists a group of non-negative numbers $w, \lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n$ such that

$$\begin{cases} \sum_{i=1}^n J_i^* - J \leq 0, \\ w(J - \sum_{i=1}^n J_i^*) = 0, \\ \lambda_i J_i^* = 0, \quad \mu_i(\bar{J}_i - J_i^*) = 0, \quad \forall i = 1, \dots, n, \\ w = c_i(J_i^*) + \lambda_i - \mu_i, \quad \forall i = 1, \dots, n. \end{cases} \quad (14)$$

It should be noted that actually we must have $\mu_i = 0$ for all $i = 1, \dots, n$. To show that, suppose $\mu_i > 0$ for some i , then we have $J_i^* = \bar{J}_i$, which leads to $\lambda_i = 0$. Thus, we must have $w = c_i(\bar{J}_i) - \mu_i = -\mu_i < 0$, which is impossible. Thus, the KKT condition can be simplified to

$$\begin{cases} \sum_{i=1}^n J_i^* - J \leq 0, \\ w(J - \sum_{i=1}^n J_i^*) = 0, \\ \lambda_i J_i^* = 0, \quad \forall i = 1, \dots, n, \\ w = c_i(J_i^*) + \lambda_i, \quad \forall i = 1, \dots, n. \end{cases} \quad (15)$$

a) Given $\sum_{i=1}^n \bar{J}_i \geq J$, it must be true that $\sum_{i=1}^n J_i^* - J = 0$. To show that, suppose $\sum_{i=1}^n J_i^* - J < 0$, then $w = 0$. Thus, $\lambda_i = 0, c_i(J_i^*) = 0, \forall i = 1, \dots, n$. Then $J_i^* = \bar{J}_i, \forall i = 1, \dots, n$ follows. Hence, $\sum_{i=1}^n J_i^* = \sum_{i=1}^n \bar{J}_i \geq J$, which is against the assumption $\sum_{i=1}^n J_i^* - J < 0$. So $\sum_{i=1}^n J_i^* - J = 0$ must be true given $\sum_{i=1}^n \bar{J}_i \geq J$.

The equality condition $\sum_{i=1}^n J_i^* - J = 0$ implies that there must exist some i 's such that $J_i^* > 0$. Let $k > 0$ be the largest index i such that $J_i^* > 0$, then we have $\lambda_k = 0$ and

$$0 \leq w = c_k(J_k^*) < c_k(0) < c_j(0), \quad \forall 1 \leq j < k.$$

Now, to satisfy $w = c_j(J_j^*) + \lambda_j, \forall j = 1, \dots, k-1$ knowing $\lambda_j \geq 0$, we must have $J_j^* > 0, \forall j = 1, \dots, k-1$, which leads to $\lambda_j = 0, \forall j = 1, \dots, k-1$ and $w = c_k(J_k^*), j = 1, \dots, k-1$. So $\mathbf{J}^*$ can be an optimal solution when system of equations 2 has a solution with $w \geq 0$. It is easy to verify that the solution will be unique if it exists.

b) Given $\sum_{i=1}^n \bar{J}_i < J$, it must be true that $\sum_{i=1}^n J_i^* - J < 0$ since $J_i^* \leq \bar{J}_i, \forall i = 1, \dots, n$. Then $w = 0$ follows, and $\mathbf{J}^*$ must satisfy $0 = c_i(J_i^*) + \lambda_i, \forall i = 1, \dots, n$, which leads to $J_i^* > 0, \forall i = 1, \dots, n$ and $\lambda_i = 0, \forall i = 1, \dots, n$. So $\mathbf{J}^*$ can be an optimal solution when system of equations 3 has a solution and it is easy to verify that you can't have a solution of system of equations 2 at the same time.

Proof of Theorem 2. We will first show that a NE strategy pair $(\mathbf{J}^*, \mathbf{y}^*)$ of this non-zero sum game will be subject to a water-filling scheme.

Let $(\mathbf{J}^*, \mathbf{y}^*)$ be a NE strategy pair and let h be the largest integer such that $J_h^* > 0$. According to condition 7, it is true that $h \in I$ and $y_h^* > 0$. Then, by condition 8,

$$w_A = \Theta_h(J_h^*) < \Theta_h(0) < \Theta_i(0), \quad \forall i = 1, \dots, h-1,$$

which implies $J_i^* > 0$, $\forall i = 1, \dots, h-1$, in order for condition 8 to be satisfied. Then, by condition 7 again, one has $y_i^* > 0$, $\forall i = 1, \dots, h-1$.

In summary, a NE strategy pair $(\mathbf{J}^*, \mathbf{y}^*)$ should be subject to a water-filling scheme with a threshold index h such that

$$\begin{cases} J_i^* > 0, & y_i^* > 0, & \forall i = 1, \dots, h, \\ J_i^* = 0, & \forall i = h+1, \dots, N. \end{cases} \quad (16)$$

a) If $k \leq m$, the solution to system of equations 9 and 11 satisfy conditions 7, 8 and 16, which defines the NE strategy pair $(\mathbf{J}^*, \mathbf{y}^*)$ of this game. Thus, $I = \{1, \dots, k\}$ in this case.

b) If $k > m$, there is no feasible solution to system of equations 9 and 11 since it is impossible to have $\Delta_{J_k^*}(y_k^*) = w_D \geq 0$. Besides, by the definition of k , it is impossible to have $h > k$.

Notice that solving system of equations 9 instead with $w_A' > w_A$ and $\sum_{i=1}^k J_i \leq J$ will provide solutions containing smaller J_i' 's and threshold index $h \leq k$, and smaller J_i' 's lead to larger m as defined by system of equations 10. Thus, one can find a NE strategy pair $(\mathbf{J}^*, \mathbf{y}^*)$ by increasing the value of w_A until conditions 7, 8 and 16 are satisfied.

Now, one can search for the threshold index $h \leq k$ with an increased $w_A' > w_A$ as shown in system of equations 12. Clearly, $\sum_{i=1}^n J_i^* < J$ in this case, which leads to $w_D = 0$ by constraint $w_D(\sum_{i=1}^n J_i^* - J) = 0$. Also, under condition 8, it is possible to have $y_{h+1}^* = 1 - \sum_{i=1}^h y_i^* > 0$ if and only if $w_A' = \Theta_{h+1}(0)$, but the constraint $\Delta_{J_{h+1}^*}(y_{h+1}^*) \leq w_D = 0$ must be satisfied at the same time as implied by condition 7 and $J_{h+1}^* = 0$.

In summary, the solution of system of equations 12 and 13 form a Nash Equilibrium strategy pair $(\mathbf{J}^*, \mathbf{y}^*)$ of this game in this case.