A Game-Theoretic Approach for Probabilistic Cooperative Jamming Strategies over Parallel Wireless Channels

Zhifan Xu, Melike Baykal-Gürsoy
Department of Industrial and Systems Engineering
Rutgers University
Piscataway, NJ, USA
zhifan.xu@rutgers.edu, gursoy@soe.rutgers.edu

Predrag Spasojević
Department of Electrical and Computer Engineering
Rutgers University
Piscataway, NJ, USA
spasojev@winlab.rutgers.edu

2021 IEEE Conference on Communications and Network Security (CNS) | 978-1-6654-4496-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/CNS53000.2021.9705044

***Abstract*—Considered is a network of parallel wireless channels in which individual parties are engaged in secret communication under the protection of cooperative jamming. A strategic eavesdropper selects the most vulnerable channels to attack. Existing works usually suggest the defender allocate limited cooperative jamming power to various channels. However, it usually requires some strong assumptions and complex computation to find such an optimal power control policy. This paper proposes a probabilistic cooperative jamming scheme such that the defender focuses on protecting randomly selected channels. Two different cases regarding each channel's eavesdropping capacity are discussed. The first case studies the general scenario where each channel has different eavesdropping capacity. The second case analyzes an extreme scenario where all channels have the same eavesdropping capacity. Two non-zero-sum Nash games model the competition between the network defender and an eavesdropper in each case. Furthermore, considering the case that the defender does not know the eavesdropper's channel state information (CSI) leads to a Bayesian game. For all three games, we derive conditions for the existence of a unique Nash equilibrium (NE), and obtain the equilibria and the value functions in closed form.**

***Index Terms*—wireless communication network, eavesdropping, cooperative jamming, security game, Bayesian equilibrium.**

I. Introduction

THE broadcast nature of wireless communication allows for the transmitted messages to be eavesdropped by unintended receivers who are within the communication range. Over the years, efforts have been made to facilitate the security of wireless communication channels, and game-theoretic models naturally arise in such resource allocation problems [1]. Garnaev and Trappe [2] solved a power allocation problem of a transmitter working against nature, which decides on the transmission and eavesdropping gains using a zero-sum game. Yüksel *et al.* [3] investigated a rate allocation game between a source and a hostile jammer helping an eavesdropper. As suggested in [4]–[6], eavesdroppers, through different means, may also strategically manipulate the secrecy performance of wireless networks. Various game theoretic models with eavesdroppers as decision makers have been investigated, such as the stochastic game studied in [7] and [8], in which a sender and an attacker can both switch between multiple working modes. In [9], the authors suggested a game against an attacker who can choose which one of multiple parallel channels to eavesdrop on.

Research on interference channels has led to the introduction of using artificial noise to enhance the secrecy of a communication channel (see [10], [11]). Tekin and Yener [12], [13] showed that the secrecy of a wireless wire-tap channel consisting of multiple sender-receiver links can be increased when some of the senders transmit jamming signals to the eavesdropper. The authors coined the term *Cooperative Jamming* for the proposed scheme. Other researchers have investigated different aspects of friendly interference since then. For instance, Tang *et al.* [14], [15] investigated the achievable secrecy rate when a friendly interferer is employed to jam passive eavesdroppers. Rabbachin *et al.* [16] studied a wireless network assisted by multiple friendly interferers. Comprehensive reviews of cooperative jamming and friendly interference can be found in [17], [18].

The effect of interference has been introduced into games against eavesdroppers as well, such as the information secrecy game in [19] in which a second legitimate user tries to jam the eavesdropper in a cognitive network, and the relay selection game in [20] with multiple users interfering with each other when they use the same relay. Game theoretic models have also been used to study the interaction between users and friendly interferers, such as the Stackelberg pricing game by Han *et al.* [21] for a single communication pair and friendly jammers. Zhong *et al.* [22] extended this game to the case of power sharing between the sender and friendly interferers. Wang *et al.* [23] investigated another pricing game in which a single friendly interferer protects all sub-channels of an OFDMA network. Garnaev *et al.* [24] analyzed a game between a friendly interferer and a strategic eavesdropper in which each player could target a single channel. The authors showed that both players adopted threshold type equilibrium

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

policies.

In this paper, we consider using cooperative jamming to protect a network of parallel wireless channels against a strategic eavesdropper who selects a limited number of channels as targets. Existing works, such as [25] and [26], usually focus on hard-to-compute power allocation strategies and rely on strong assumptions. In [25], Zhang *et al.* proposed a Lagrange dual method with the help of exhaustive search to find the optimal power allocation strategy. In [26], Xu and Baykal-Gürsoy restricted discussions to the situation where the eavesdropping channels are the degraded versions of the wire-tapped communication channels, and used bi-section search algorithms to find a Nash equilibrium. However, those assumptions may not be realistic since CSIs are essentially random variables that may change from time to time. In this paper, we propose a probabilistic cooperative jamming scheme such that the defender focuses on protecting channels selected randomly from time to time. We develop a game-theoretic approach to study the channel selection strategy without assuming the relationships between the intended receiver's CSI and the eavesdropper's CSI. We introduce two games corresponding to different possibilities of eavesdroppers' CSI. Moreover, we present a Bayesian game in which the eavesdropper's CSI is private information. The analysis demonstrates that the equilibrium and the value of each game are derived in closed form equations without the need for iterative computations.

The rest of this paper is organized as follows. Section II introduces the basic notation and the utility function of the defender. Section III presents two non-zero-sum games associated with two cases of eavesdroppers' CSI, and derives the closed form solutions of equilibrium strategies. Section IV suggests a Bayesian game that takes into account the uncertainty of eavesdroppers' CSIs. Section V demonstrates numerical examples. Sections VI summarizes the conclusions and makes suggestions for future research. Finally, Appendices A and B contain the proofs of Theorems 1 through 3.

II. Formulation of the Problem

A. System Model

Consider a parallel wireless communication network consisting of N independent sender-receiver channels, such as the frequency-division-multiplexing (FDM) communication network shown in Fig. 1, or an orthogonal-frequency-division-multiplexing (OFDM) network discussed in [23] and [25]. Each channel works at a non-overlapping frequency and the inter-channel interference is mitigated via techniques like pulse-shaping filters. Confidential messages are transmitted through these channels in blocks of T length of time. For each channel i, the communication capacity is

$$C_{L_i} = \log_2\left(1 + \frac{h_{L_i} P_i}{\sigma_i^2}\right), \tag{1}$$

with h_{L_i} denoting the channel gain between sender i (Alice i) and legitimate receiver i (Bob i), P_i, σ_i^2 denoting the transmission power and the noise, respectively, on channel i.

Meanwhile, an eavesdropper (Eve) tries to intercept the communication between senders and receivers. Due to budget limitation, or to reduce the risk of Local Oscillator (LO) leakage that may be caught by Intrusion Detection Systems (see, e.g., [8]), Eve can only use hardware with limited capability to listen on n_E of N different frequencies at the same time. The eavesdropping capacity of channel i is

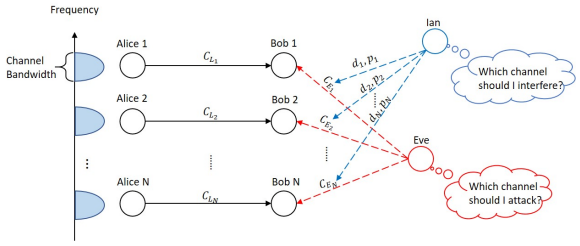


Fig. 1. Interference Assisted Parallel Communication Network

$$C_{E_i} = \log_2\left(1 + \frac{h_{E_i} P_i}{\sigma_i^2}\right), \tag{2}$$

with h_{E_i} denoting Eve's channel gain at eavesdropping channel i. Under an eavesdropping attack, channel i's achievable transmission rate is equal to its secrecy capacity [27]–[29]

$$C_{S_i} = (C_{L_i} - C_{E_i})^+ = (C_{L_i} - C_{E_i}) + \Delta_{\mathrm{I}_i}, \tag{3}$$

where $x^+ = \max\{x, 0\}$ and $\Delta_{\mathrm{I}_i} = (C_{E_i} - C_{L_i})^+$. In this paper, we consider the scenario where Alice and Bob will only send information when the default secrecy capacity, C_{S_i}, is positive, that is, $\Delta_{\mathrm{I}_i} = 0$.

A friendly interferer (Ian), with total power J at hand, can send out cooperative jamming signals to decrease eavesdropping capacities. If Ian chooses to jam channel i that Eve also picks, channel i's eavesdropping capacity will be reduced to

$$C'_{E_i} = \log_2\left(1 + \frac{h_{E_i} P_i}{\sigma_i^2 + g_{E_i} J}\right), \tag{4}$$

where g_{E_i} is the channel gain on i between Ian and Eve [16]. This paper adopts the worst case scenario where cooperative jamming may not be perfectly mitigated by Bob i. Thus, the communication capacity of channel i will also be decreased to

$$C'_{L_i} = \log_2\left(1 + \frac{h_{L_i} P_i}{\sigma_i^2 + g_{L_i} J}\right), \tag{5}$$

where g_{L_i} is the channel gain between Ian and Bob i. Therefore, the secrecy capacity of channel i with the help of cooperative jamming becomes

$$C'_{S_i} = \left(C'_{L_i} - C'_{E_i}\right)^+, \quad \forall i = 1, ..., N. \tag{6}$$

This paper adopts the common assumption that the instantaneous CSI of intended users, h_{L_i}s and g_{L_i}s, are perfectly known to both Ian and Eve (see, e.g., [25], [30], [31]). Meanwhile, h_{E_i}s and g_{E_i}s may be instantaneous values if eavesdropper's CSIs are also known; otherwise, since Eve is typically listening passively, h_{E_i}s and g_{E_i}s denote some approximate value such as mean or mode when only statistical CSI of eavesdropping channels is available [32]–[34].

It is clear that Ian should not interfere with channels with $C'_{S_i} \leq C_{S_i}$. Also, applying cooperative jamming to a channel i that is not under attack will only harm the network's throughput. In practice, it is hard for Ian to know the target chosen by Eve ahead of time. Similarly, Eve is unlikely to

identify all the channels protected by Ian within T time due to her limited eavesdropping capability. Hence, assume that Ian and Eve make their choices simultaneously and thus, they are engaged in a one-shot simultaneous play Nash game.

B. Game Formulation

In this paper, we consider a probabilistic cooperative jamming scheme such that Ian protects a single channel, i.e., $n_I = 1$, at every transmission block and will select the channel strategically. Also, we focus on a limited-capability Eve with $n_E = 1$, and leave the more general case for future research.

The other parameters are as follows:

- $d_i \in (0, 1]$: efficiency of cooperative jamming on eavesdropping channel i, where $d_i = (C_{E_i} - C'_{E_i})/C_{E_i}$.
- $p_i \in (0, 1]$: detrimental effect of cooperative jamming on Bob i, where $p_i = (C_{L_i} - C'_{L_i})/C_{L_i}$.
- $x_i \in [0, 1]$: probability of Ian defending channel i for $i \leq N$, and probability of not interfering at all for $i = N+1$. Let $\boldsymbol{x} = (x_1, ..., x_{N+1})^\intercal$ represent Ian's mixed strategy and $X = \{\boldsymbol{x} | \boldsymbol{x} \geq \mathbf{0}, \ \sum_{i=1}^{N+1} x_i = 1\}$.
- $y_i \in [0, 1]$: probability of Eve attacking channel i for $i \leq N$. $\boldsymbol{y} = (y_1, ..., y_N)$ represents Eve's mixed strategy and $Y = \{\boldsymbol{y} | \boldsymbol{y} \geq \mathbf{0}, \ \sum_{i=1}^{N} y_i = 1\}$.

With probabilistic strategies x_i and y_i, the achievable transmission rate for secret communication at channel i is a random variable, say R_{S_i}, where

$$R_{S_i} = \begin{cases} C'_{S_i} & \text{with probability } x_i y_i, \\ C_{S_i} & \text{with probability } (1 - x_i) y_i, \\ (1 - p_i) C_{L_i}, & \text{with probability } x_i (1 - y_i), \\ C_{L_i}, & \text{otherwise.} \end{cases} \tag{7}$$

Ian, working as a helper to improve the overall secrecy of the network, aims to maximize the expected achievable transmission rate of the whole network [9]. Thus, Ian's payoff under arbitrary mixed strategies $(\boldsymbol{x}, \boldsymbol{y})$ is

$$\begin{aligned} \mu^D(\boldsymbol{x},\boldsymbol{y}) &= \mathbb{E}\left[\sum_{i=1}^{N} R_{S_i}\right] = \sum_{i=1}^{N} \mathbb{E}[R_{S_i}] \\ &= \sum_{i=1}^{N} x_i \left[\left(\sum_{k=1}^{N} C_{L_k} - \sum_{j=1}^{N} y_j \left(C_{E_j} - \Delta_{\mathrm{I}_j} \right) \right) - p_i C_{L_i} + y_i d_i C_{E_i} \right. \\ &\quad \left. - y_i \Delta_{\mathrm{I}_i} \right] + x_{N+1} \left[\sum_{k=1}^{N} C_{L_k} - \sum_{j=1}^{N} y_j \left(C_{E_j} - \Delta_{\mathrm{I}_j} \right) \right]. \end{aligned} \tag{8}$$

Note that we have omitted the positive operation $(\cdot)^+$ for C'_{S_i} in function (8), which is due to the fact that the optimal value of x_i must be 0 if $C'_{S_i} = 0$, and thus Ian's payoffs with and without the positive operation have the same optimal value.

The next section introduces two types of Eve with different configurations of CSI. Type I Eve has distinct eavesdropping capacities at each channel, while Type II Eve has the same eavesdropping capacity at all channels. We present a non-zero-sum game for each type, and show that the eavesdropper has different behavioral patterns under each situation. The Nash equilibrium (NE) strategy for each type of Eve, namely type $h = \mathrm{I}, \mathrm{II}$, together with the corresponding interference strategy $\boldsymbol{x}^*$, i.e., the strategy pair $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\boldsymbol{h}})$, satisfies

$$\begin{aligned} v_h^D &\equiv \mu^D(\boldsymbol{x}^*, \boldsymbol{y}^*_{\boldsymbol{h}}) \geq \mu^D(\boldsymbol{x}, \boldsymbol{y}^*_{\boldsymbol{h}}), \ \ \forall \boldsymbol{x} \in X, \\ v_h^A &\equiv \mu_h^A(\boldsymbol{x}^*, \boldsymbol{y}^*_{\boldsymbol{h}}) \geq \mu_h^A(\boldsymbol{x}^*, \boldsymbol{y}_{\boldsymbol{h}}), \ \ \forall \boldsymbol{y}_{\boldsymbol{h}} \in Y, \end{aligned}$$

where v_h^D and v_h^A denote the game value of the two players.

III. Complete Information Games: Two Basic Cases

A. Against Type I Eve

In this scenario, we consider the general case where Eve's eavesdropping capacities are all distinct and call this Eve as Type I Eve. For the sake of simplicity, assume that all C_{E_i}'s are arranged in decreasing order, that is,

$$C_{E_1} > C_{E_2} > \cdots > C_{E_N} > 0.$$

With probabilistic strategies x_i and y_{I_i}, the eavesdropping capacity utilized by Eve at channel i is a random variable, say R_{E_i}, where

$$R_{E_i} = \begin{cases} C'_{E_i} & \text{with probability } x_i y_{\mathrm{I}_i}, \\ C_{E_i} & \text{with probability } (1 - x_i) y_{\mathrm{I}_i}, \\ 0, & \text{with probability } 1 - y_{\mathrm{I}_i}. \end{cases} \tag{9}$$

Thus, the expected payoff for Type I Eve under arbitrary mixed strategies $(\boldsymbol{x}, \boldsymbol{y}_{\mathbf{I}})$, is

$$\mu_{\mathrm{I}}^A(\boldsymbol{x}, \boldsymbol{y}_{\mathbf{I}}) = \sum_{i=1}^{N} \mathbb{E}\left[R_{E_i}\right] = \sum_{i=1}^{N} y_{\mathrm{I}_i} C_{E_i} \left(1 - x_i d_i\right). \tag{10}$$

The following theorem demonstrates the water-filling form [35] of the equilibrium, $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{I}})$.

Theorem 1. *Consider the non-zero-sum game against Type I Eve. Let k be a positive integer such that $\phi_k < 1 < \phi_{k+1}$ where ϕ_i is a strictly increasing sequence defined as $\phi_i = \sum_{j=1}^{i} \frac{C_{E_j} - C_{E_i}}{d_j C_{E_j}}$, $\forall i = 1, .., N$ and $\phi_{N+1} = \infty$. Let m be a non-negative integer such that $\psi_m < 1 < \psi_{m+1}$, where ψ_i is a strictly increasing sequence defined as $\psi_i = \sum_{j=1}^{i} \frac{p_j C_{L_j}}{d_j C_{E_j}}$, $\forall i = 1, .., N$ and $\psi_{N+1} = \infty$.*

(a) If $k \leq m$, then the game has a unique NE $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{I}})$ with

$$x_j^* = \begin{cases} \frac{\frac{1}{d_j C_{E_j}}}{\sum_{i=1}^{k} \frac{1}{d_i C_{E_i}}} \left(1 - \sum_{i=1}^{k} \frac{C_{E_i} - C_{E_j}}{d_i C_{E_i}}\right), & \forall j \leq k, \\ 0, & \forall k < j \leq N + 1, \end{cases} \tag{11}$$

$$y_{\mathrm{I}_j}^* = \begin{cases} \frac{\frac{1}{d_j C_{E_j}}}{\sum_{i=1}^{k} \frac{1}{d_i C_{E_i}}} \left(1 - \sum_{i=1}^{k} \frac{p_i C_{L_i} - p_j C_{L_j}}{d_i C_{E_i}}\right), & \forall j \leq k, \\ 0, & \forall k < j \leq N. \end{cases} \tag{12}$$

(b) If $m < k$, then the game has a unique NE $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{I}})$ with

$$x_j^* = \begin{cases} \frac{C_{E_j} - C_{E_{m+1}}}{d_j C_{E_j}}, & \forall j \leq m, \\ 0, & \forall m < j \leq N, \\ 1 - \sum_{i=1}^{m} \frac{C_{E_i} - C_{E_{m+1}}}{d_i C_{E_i}}, & j = N + 1, \end{cases} \tag{13}$$

$$y_{\mathrm{I}_j}^* = \begin{cases} \frac{p_j C_{L_j}}{d_j C_{E_j}}, & \forall j \leq m, \\ 1 - \sum_{i=1}^{m} \frac{p_i C_{L_i}}{d_i C_{E_i}}, & j = m + 1, \\ 0, & \forall j > m + 1. \end{cases} \tag{14}$$

Proof. We provide a proof in Appendix A. □

Remark. Note the assumptions that $\phi_k \neq 1$ and $\psi_m \neq 1$. In case $\phi_k = 1$ and $\psi_m \neq 1$, the defender, in case $\phi_k \neq 1$ and $\psi_m = 1$, the attacker may have infinitely many solutions, depending on $k \leq m$ or $m < k$, respectively.

The value of m will be smaller if $p_j C_{L_j}$s are close to $d_j C_{E_j}$s. This means that when the intended receivers suffer more from interference, the number of channels that will be protected by Ian gets smaller. Besides, if $m < k$, Ian will not even expand his resources fully into interference.

B. Against Type II Eve

In this scenario, we consider an extreme case in which Eve's eavesdropping capacities at different channels are similar to each other. That is,

$$C_{E_1} \approx C_{E_1} \approx \cdots \approx C_{E_N} \approx C_E,$$

where C_E is the average value of all C_{E_i}'s. It will be shown that the equilibrium strategies are no longer of threshold type. Using C_E instead of C_{E_i} in equation (10), the expected payoff for Type II Eve under arbitrary mixed strategies, $(\boldsymbol{x}, \boldsymbol{y_{II}})$, can be characterized as

$$\mu^A_{\rm II}(\boldsymbol{x}, \boldsymbol{y_{II}}) = C_E \sum_{i=1}^{N} y_{{\rm II}_i}\Big(1 - x_i d_i\Big). \tag{15}$$

Since all channels' eavesdropping capacities are the same, Type II Eve can focus on avoiding strong interference signals with high d_i. Ian also approximates each channel's eavesdropping capacity C_{E_i} using C_E, so the defender's payoff in this scenario changes to

$$\begin{aligned}\mu^D(\boldsymbol{x},\boldsymbol{y_{II}}) = \sum_{i=1}^{N} x_i \Bigg[\Big(\sum_{k=1}^{N} C_{L_k} - C_E + \sum_{j=1}^{N} y_{{\rm II}_j} \Delta_{{\rm II}_j}\Big) \\ - p_i C_{L_i} + y_{{\rm II}_i} d_i C_E - y_{{\rm II}_i} \Delta_{{\rm II}_i} \Bigg] \\ + x_{N+1} \Bigg[\sum_{k=1}^{N} C_{L_k} - C_E + \sum_{j=1}^{N} y_{{\rm II}_j} \Delta_{{\rm II}_j} \Bigg],\end{aligned} \tag{16}$$

where $\Delta_{{\rm II}_j} = \big(C_E - C_{L_j}\big)^+$. We still consider that all channels to be protected has positive default secrecy capacity, that is, $\Delta_{{\rm II}_j} = 0$ in this paper.

The following theorem provides analytical expressions for the equilibrium strategies $\boldsymbol{x}^*$ and $\boldsymbol{y}^*_{\rm II}$, and reveals an all-or-nothing defending pattern.

Theorem 2. *Consider the non-zero-sum game against Type II Eve. Let* $\xi_N = \sum_{j=1}^{N} \frac{p_j C_{L_j}}{d_j C_E}$.

(a) If $\xi_N < 1$, *then the game has a unique equilibrium strategy for both players as*

$$x^*_j = \begin{cases} \frac{\frac{1}{d_j}}{\sum_{i=1}^{N} \frac{1}{d_i}}, & \forall j = 1, ..., N, \\ 0, & j = N+1, \end{cases} \tag{17}$$

$$y^*_{{\rm II}_j} = \frac{\frac{1}{d_j}}{\sum_{i=1}^{N} \frac{1}{d_i}} \Big(1 - \sum_{i=1}^{N} \frac{p_i C_{L_i} - p_j C_{L_j}}{d_i C_E}\Big), \forall j \leq N. \tag{18}$$

(b) If $\xi_N > 1$, *then the game has a unique equilibrium strategy for the defender but a continuum of equilibrium strategies for the eavesdropper, as given below.*

$$x^*_j = \begin{cases} 0, & \forall j \leq N, \\ 1, & j = N+1, \end{cases} \quad \textit{and} \quad y^*_{{\rm II}_j} \leq \frac{p_j C_{L_j}}{d_j C_E}, \ \forall j \leq N. \tag{19}$$

Proof. We provide a proof in Appendix A. □

Remark. Here we assume $\xi_N \neq 1$ to focus on the cases in which Ian has unique equilibrium strategies. When $\xi_N = 1$, Ian may have infinitely many solutions.

The condition $\xi_N < 1$ actually implies that $p_j C_{L_j}$ is much smaller than $d_j C_E$ for all $j < N$. In this situation, Ian will interfere with all channels probabilistically but pay more attention to the channels with small d_js since Type II Eve tries to avoid strong interference. But, if $\xi_N > 1$, Ian will not interfere at all since the attacker can always eavesdrop on channels with relatively large $d_j C_E$.

IV. Bayesian Game with Uncertainty about Eavesdropper's CSI

This section considers the scenario where the instantaneous CSI of eavesdropping channels is privately known by the eavesdropper, while the defender has distributional knowledge that the eavesdropping capacities are $\{C^k_{E_i}, \forall i\}$ with probability α_k, where $\sum_{k=1}^{K} \alpha_k = 1$. That is, the defender needs to use one consistent cooperative jamming strategy to counter the attack initiated by possibly K different eavesdroppers. We propose a Bayesian game theoretic model in which the defender's expected payoff is characterized as

$$\mu^D(\boldsymbol{x}, \boldsymbol{y}_{h_1}, ..., \boldsymbol{y}_{h_K}) = \sum_{k=1}^{K} \alpha_k \mu^D(\boldsymbol{x}, \boldsymbol{y}_{h_k}), \tag{20}$$

where $\boldsymbol{y}_{h_k}$ is the strategy adopted by a type k eavesdropper.

In this paper, we focus on the scenario where Ian will encounter either a Type I or a Type II Eve with probability $\alpha \in (0, 1)$ and $1 - \alpha$, respectively, and we leave more complicated scenarios for future discussion. The expected payoff for Ian, μ^D, under a mixed policy triple $(\boldsymbol{x}, \boldsymbol{y}_{\rm I}, \boldsymbol{y}_{\rm II})$, of Ian, Type I Eve and Type II Eve, respectively, is

$$\begin{aligned}\mu^D(\boldsymbol{x},\boldsymbol{y}_{\rm I},\boldsymbol{y}_{\rm II}) &= \alpha \mu^D(\boldsymbol{x},\boldsymbol{y}_{\rm I}) + (1-\alpha)\mu^D(\boldsymbol{x},\boldsymbol{y}_{\rm II}) \\ &= \sum_{i=1}^{N} x_i \Bigg[\sum_{k=1}^{N} C_{L_k} - \alpha \sum_{j=1}^{N} y_{{\rm I}_j} C_{E_j} - (1-\alpha) C_E \Bigg] \\ &\quad + \sum_{i=1}^{N} x_i \Big(- p_i C_{L_i} + \alpha y_{{\rm I}_i} d_i C_{E_i} + (1-\alpha) y_{{\rm II}_i} d_i C_E \Big) \\ &\quad + x_{N+1} \Bigg[\sum_{k=1}^{N} C_{L_k} - \alpha \sum_{j=1}^{N} y_{{\rm I}_j} C_{E_j} - (1-\alpha) C_E \Bigg].\end{aligned} \tag{21}$$

Meanwhile, Eve is playing a game with complete information. Let $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\rm I}, \boldsymbol{y}^*_{\rm II})$ be the Bayesian equilibrium such that

$$v^D_B \equiv \mu^D(\boldsymbol{x}^*, \boldsymbol{y}^*_{\rm I}, \boldsymbol{y}^*_{\rm II}) \geq \mu^D(\boldsymbol{x}, \boldsymbol{y}^*_{\rm I}, \boldsymbol{y}^*_{\rm II}), \ \ \forall \boldsymbol{x} \in X,$$

$$v^A_{\rm I} \equiv \mu^A_{\rm I}(\boldsymbol{x}^*, \boldsymbol{y}^*_{\rm I}) \geq \mu^A_{\rm I}(\boldsymbol{x}^*, \boldsymbol{y}_{\rm I}), \ \ \forall \boldsymbol{y_{\rm I}} \in Y,$$

$$v^A_{\rm II} \equiv \mu^A_{\rm II}(\boldsymbol{x}^*, \boldsymbol{y}^*_{\rm II}) \geq \mu^A_{\rm II}(\boldsymbol{x}^*, \boldsymbol{y_{\rm II}}), \ \ \forall \boldsymbol{y_{\rm II}} \in Y,$$

where v^D_B, $v^A_{\rm I}$ and $v^A_{\rm II}$ denote the game value of Ian, Type I Eve and Type II Eve, respectively.

The following lemma reveals a channel sharing structure for Type I and Type II Eves. The equilibrium target sets of two Eves have at most one channel in common.

Lemma 1. *For the Nash equilibrium* $(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{I}}^*, \boldsymbol{y}_{\mathbf{II}}^*)$*, if* $y_{\mathrm{I}_i}^* > 0$*, then* $y_{\mathrm{II}_j}^* = 0, \ \forall j < i$*.*

Proof. Let S_i^A be a pure policy of Eve attacking channel i with probability 1. Given $y_{\mathrm{I}_i}^* > 0$, it holds that

$$\mu_{\mathrm{I}}^A(\boldsymbol{x}^*, S_i^A) \geq \mu_{\mathrm{I}}^A(\boldsymbol{x}^*, S_j^A), \quad \forall j = 1, ..., N,$$

implying

$$C_{E_i} - x_i^* d_i C_{E_i} \geq C_{E_j} - x_j^* d_j C_{E_j}, \quad \forall j = 1, ..., N.$$

This inequality, then, provides the following bound on the payoff function of Type II Eve under the pure policy of attacking channel j, i.e., $\mu_{\mathrm{II}}^A(\boldsymbol{x}^*, S_j^A)$, as

$$\begin{aligned}\mu_{\mathrm{II}}^A(\boldsymbol{x}^*, S_j^A) &= C_E(1 - x_j^* d_j) \\ &\leq \frac{C_{E_i}}{C_{E_j}} C_E(1 - x_i^* d_i), \quad \forall j = 1, ..., N \\ &< C_E(1 - x_i^* d_i) = \mu_{\mathrm{II}}^A(\boldsymbol{x}^*, S_i^A), \quad \forall j < i\end{aligned}$$

since $C_{E_j} > C_{E_i}, \ \forall j < i$. This means that S_j^As are not Type II Eve's best responses for all $j < i$. □

According to lemma 1, there must exist an integer n such that $y_{\mathrm{I}_i}^* > 0, \ \forall 1 \leq i \leq n$, $y_{\mathrm{I}_i}^* = 0, \forall n+1 \leq i \leq N$ and $y_{\mathrm{II}_i}^* = 0, \ \forall 1 \leq i \leq n-1$, $y_{\mathrm{II}_i}^* \geq 0 \ \forall n \leq i \leq N$. Let $\bar{\mu}_{B_i}^D \equiv \mu^D(S_i^D, \boldsymbol{y}_{\mathbf{I}}^*, \boldsymbol{y}_{\mathbf{II}}^*) - \mu^D(S_{N+1}^D, \boldsymbol{y}_{\mathbf{I}}^*, \boldsymbol{y}_{\mathbf{II}}^*)$ is the benefit of interfering with channel i as opposed to not interfering at all. It is equal to

$$\bar{\mu}_{B_i}^D = \begin{cases} -p_i C_{L_i} + \alpha y_{\mathrm{I}_i}^* d_i C_{E_i}, & \forall i = 1, ..., n-1, \\ -p_i C_{L_i} + \alpha y_{\mathrm{I}_i}^* d_i C_{E_i} + (1-\alpha) y_{\mathrm{II}_i}^* d_i C_E, & i = n, \\ -p_i C_{L_i} + (1-\alpha) y_{\mathrm{II}_i}^* d_i C_E, & \forall i = n+1, ..., N, \\ 0, & i = N+1. \end{cases}$$

This implies that Ian will confront only Type I Eve from channels 1 to $n-1$, only Type II Eve from channels $n+1$ to N, and a mix of Type I Eve and Type II Eve at channel n in the Bayesian equilibrium.

The next theorem provides an analytical solution $(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{I}}^*, \boldsymbol{y}_{\mathbf{II}}^*)$ to this Bayesian game.

Theorem 3. *Consider the Bayesian game described above. Let* $\tilde{v}_B^D$ *be the solution to*

$$\begin{cases} \tilde{v}_B^D = \bar{\mu}_{B_1}^D = \cdots = \bar{\mu}_{B_N}^D, \\ \sum_{i=1}^n y_{\mathrm{I}_i}^* = 1, \\ \sum_{i=n}^N y_{\mathrm{II}_i}^* = 1. \end{cases} \tag{22}$$

Let k *and* ϕ_k *be defined as in Theorem 1. Let* m *be a non-negative integer such that* $\zeta_m < 1 < \zeta_{m+1}$ *where* ζ_i *is a strictly increasing sequence defined as*

$$\zeta_i = \frac{1}{\alpha} \sum_{j=1}^{i} \frac{p_j C_{L_j} + \max\{\tilde{v}_B^D, 0\}}{d_j C_{E_j}}, \quad \forall i = 1, ..., N, \tag{23}$$

and $\zeta_{N+1} = \infty$*.*

(a) If $k \leq m$*, then the game has unique equilibrium strategies for the defender and for Type I Eve, and a continuum of equilibrium strategies for Type II Eve, given as*

$$x_j^* = \begin{cases} \frac{\frac{1}{d_j C_{E_j}}}{\sum_{i=1}^k \frac{1}{d_i C_{E_j}}} (1 - \sum_{i=1}^k \frac{C_{E_i} - C_{E_j}}{d_i C_{E_i}}), & \forall j \leq k, \\ 0, & \forall j > k, \end{cases} \tag{24}$$

$$y_{\mathrm{I}_j}^* = \begin{cases} \frac{\frac{1}{d_j C_{E_j}}}{\sum_{i=1}^k \frac{1}{d_i C_{E_i}}} \left(1 - \frac{1}{\alpha} \sum_{i=1}^k \frac{p_i C_{L_i} - p_j C_{L_j}}{d_i C_{E_i}}\right), & \forall j \leq k, \\ 0, & \forall j > k, \end{cases} \tag{25}$$

$$y_{\mathrm{II}_j}^* \begin{cases} = 0, & \forall j \leq k, \\ \leq \frac{\alpha}{1-\alpha} \frac{\frac{1}{d_j C_E}}{\sum_{i=1}^k \frac{1}{d_i C_{E_i}}} (1 - \frac{1}{\alpha} \sum_{i=1}^k \frac{p_i C_{L_i} - p_j C_{L_j}}{d_i C_{E_i}}), & \forall j > k. \end{cases} \tag{26}$$

(b) If $k > m$*, and*

(b - 1) $\tilde{v}_B^D < 0$*, then the game again has unique equilibrium strategies for the defender and for Type I Eve, and a continuum of equilibrium strategies for Type II Eve, given as*

$$x_j^* = \begin{cases} \frac{C_{E_j} - C_{E_{m+1}}}{d_j C_{E_j}}, & \forall j \leq m, \\ 0, & \forall m < j \leq N, \\ 1 - \sum_{i=1}^m \frac{C_{E_i} - C_{E_{m+1}}}{d_i C_{E_i}}, & j = N+1, \end{cases} \tag{27}$$

$$y_{\mathrm{I}_j}^* = \begin{cases} \frac{1}{\alpha} \cdot \frac{p_j C_{L_j}}{d_j C_{E_j}}, & \forall j \leq m, \\ 1 - \frac{1}{\alpha} \sum_{i=1}^m \frac{p_i C_{L_i}}{d_i C_{E_i}}, & j = m+1, \\ 0, & \forall j > m+1, \end{cases} \tag{28}$$

$$y_{\mathrm{II}_j}^* = \begin{cases} 0, & \forall j < m, \\ \leq \frac{1}{1-\alpha} \cdot \frac{p_j C_{L_j}}{d_j C_E} - \frac{\alpha C_{E_j}}{(1-\alpha) C_E} (1 - \frac{1}{\alpha} \sum_{i=1}^m \frac{p_j C_{L_j}}{d_i C_i}), & j = m+1, \\ \leq \frac{1}{1-\alpha} \cdot \frac{p_j C_{L_j}}{d_j C_E}, & \forall j > m+1. \end{cases} \tag{29}$$

(b - 2) $\tilde{v}_B^D > 0$*, then all players have unique equilibrium strategies as*

$$y_{\mathrm{I}_j}^* = \begin{cases} \frac{1}{\alpha} \cdot \frac{p_j C_{L_j} + \tilde{v}_B^D}{d_j C_{E_j}}, & \forall j \leq m, \\ 1 - \frac{1}{\alpha} \sum_{i=1}^m \frac{p_i C_{L_i} + \tilde{v}_B^D}{d_i C_{E_i}}, & j = m+1, \\ 0, & \forall j > m+1, \end{cases} \tag{30}$$

$$y_{\mathrm{II}_j}^* = \begin{cases} 0, & \forall j < m, \\ 1 - \frac{1}{1-\alpha} \sum_{i=m+1}^N \frac{p_i C_{L_i} + \tilde{v}_B^D}{d_i C_E}, & j = m+1, \\ \frac{1}{1-\alpha} \cdot \frac{p_j C_{L_j} + \tilde{v}_B^D}{d_j C_E}, & \forall j > m+1. \end{cases} \tag{31}$$

$$x_j^* = \begin{cases} \frac{C_{E_j} - v_{\mathrm{I}}^A}{d_j C_{E_j}}, & \forall j \leq m_I, \\ \frac{C_E - v_{\mathrm{II}}^A}{d_j C_E}, & \forall m_I < j \leq N, \\ 0, & j = N+1, \end{cases} \tag{32}$$

where

$$v_{\mathrm{I}}^A = \frac{1}{\sum_{i=1}^m \frac{1}{d_i C_{E_i}} + \sum_{i=m+1}^N \frac{1}{d_i C_{E_{m+1}}}} \left(\sum_{i=1}^N \frac{1}{d_i} - 1\right), \tag{33}$$

$$v_{\mathrm{II}}^A = \frac{C_E}{C_{E_{m+1}}} v_{\mathrm{I}}^A. \tag{34}$$

Proof. We provide a proof in Appendix B. □

Remark. Here we assume that $\tilde{v}_B^D \neq 0, \phi_k \neq 1$ and $\zeta_m \neq 1$ to focus on the cases in which most players have unique equilibrium strategies.

Note that Ian's optimal strategy in this scenario becomes a mixture of optimal defense strategies from scenarios in section III. The cut-off index m is positively correlated with Ian's belief α, that is, when α is larger, it is likely that more channels will be attacked by Type I Eve. Indices k and m decide whether Ian should intercept type II Eve. So Theorem 3 case (a) with $k \leq m$ is similar to Theorem 1 case (a), in the sense that all defense resources are used to counter type I Eve. When $k > m$, the value of $\tilde{v}_B^D$ indicates whether it is beneficial for Ian to intercept Type II Eve. Thus, Theorem 3 case (b - 1) is similar to Theorem 1 case (b) combined with Theorem 2 case (b), in which Ian has additional resources after defending type I Eve but is not willing to defend type II Eve since $\tilde{v}_B^D < 0$. While in case (b - 2), Ian will intercept both type I and type II Eve.

V. Numerical Illustration

In this section we present three numerical examples corresponding to each game model. For all three examples, consider a wireless communication network with $N = 5$ parallel channels with the thermal noise $\sigma_i^2 = 1,\ \forall i = 1, ..., 5$, and channel communication capacities $\{C_{L_i}, i = 1, ..., 5\} = (0.9, 1.1, 0.7, 0.6, 0.8)$. Also, let $\{d_i\}$ = {70%, 40%, 50%, 60%, 45%} such that some eavesdropping channels are more resistant to friendly interference.

The first and second examples demonstrate how the detrimental effects of interference on the intended receivers, i.e., p_i, affect the NE. For every i, p_i is positively correlated with user i's channel gain of the jamming signal, i.e., g_{L_i}. Specifically, if $g_{L_i} = 0$, then $p_i = 0\%$; if $g_{L_i} \to +\infty$, then $p_i \to 100\%$.

The third example visualizes the NE of the Bayesian game as α and p_i changes. One can clearly see the load sharing structure between Type I and Type II Eves.

A. Game against Type I Eavesdropper

Assume the eavesdropping capacity of each channel to be $\{C_{E_i}, i = 1, ..., 5\} = (0.5, 0.45, 0.4, 0.35, 0.3)$. For the sake of simplicity, let $p_i = p,\ \forall i = 1, ..., 5$ and let p vary between 0% to 15%.

Fig. 2(a) displays the optimal defense strategies in NE. Clearly, the optimal defense strategies are always of threshold type such that Ian only needs to work on channels with high eavesdropping capacity. As p increases from 0% to 15%, the number of protected channels decreases from 3 to 2, and Ian starts not to expand the full power for $p \geq 8.21\%$. In general, as p increases, the friendly interferer uses less time for protection, and the eavesdropper focuses more on channels with higher eavesdropping capacity.

Fig. 2(c) illustrates the average total secrecy capacity against Type I Eve, when Ian uses the game theoretic model backed Algorithm 1 (GT Algorithm), uses an Equal Proportion algorithm (EP Algorithm) that protects every channel with the same frequency, and does nothing (Without CJ), respectively. Eve is assumed to always apply her best response. As p increases, the GT Algorithm always outperforms the others. More importantly, using the naive EP Algorithm is even worse than not sending cooperative jamming signals at all when p is large.

B. Game against Type II Eavesdropper

In this example, let the eavesdropping capacity of each channel be $C_{E_i} = 0.45,\ \forall i = 1, ..., 5$ for a type II Eve. Still, let $p_i = p,\ \forall i = 1, ..., 5$. As shown in Fig. 3(a) and 3(b), there is a clear all-or-nothing structure for the friendly interferer's optimal defense strategy as p increases. All channels are under protection when $p \leq 5.48\%$, but it is not worthwhile for the friendly interferer to protect any channel when $p > 5.48\%$.

Fig. 3(c) depicts the average total secrecy capacity against Type II Eve when Ian uses the game theoretic model backed Algorithm 2 (GT Algorithm), uses an EP Algorithm, and adopts Without CJ, respectively. As p increases, the GT Algorithm outperforms the Without CJ method until it stops sending cooperative jamming signals. Still, using the naive EP Algorithm is worse than Without CJ for large p.

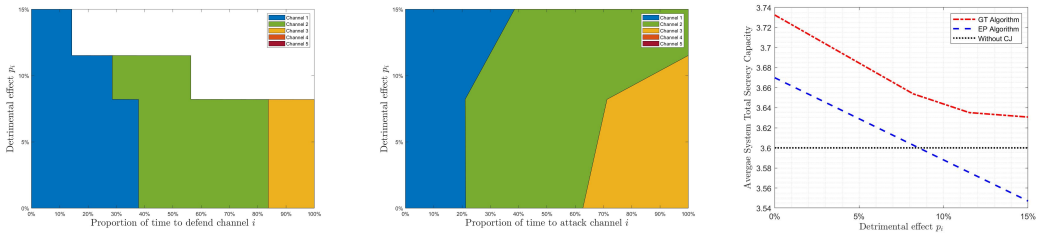
C. Bayesian Game with Uncertainty about the Attacker's Type

Let $\{C_{E_i}, i = 1, ..., 5\}$ = (0.5, 0.45, 0.40, 0.35, 0.30) for Type I Eve, and $C_E = 0.45$ for Type II Eve. Still assume $p_i = p,\ \forall i = 1, ..., 5$. Let $\alpha = 60\%$ be fixed.

Fig. 4 demonstrates the equilibrium strategies as p increases. When $p \leq 5.49\%$, Theorem 3 gives $k = 3$, $m = 2$ and $\tilde{v}_B^D > 0$. So the Bayesian equilibrium falls in the Theorem 3 case (b - 2), and Ian uses up all his resources to have all channels under protection. As $p \geq 5.49\%$, k is still larger than m but $\tilde{v}_B^D < 0$. Hence, the Bayesian equilibrium falls in the Theorem 3 case (b - 1), and Ian's defense resources are not fully utilized. Moreover, Ian is not willing to intercept Type II Eve anymore. As p increases, the number of protected channels decreases to 1, and Ian will not protect some channels even though they are at risk of being attacked by Type I Eve. When p is large, Type I Eve can focus more on attacking channels with higher eavesdropping capacity, while type II Eve has the flexibility to attack more channels. Therefore, reducing interference caused by cooperative jamming on legitimate users is still important when the eavesdropper's type is unknown.

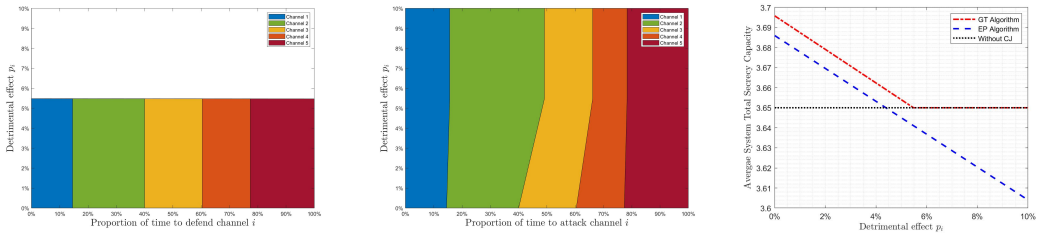
Fig. 4(d) displays the simulated expected total secrecy capacity against unknown type eavesdroppers with $\alpha = 60\%$. It presents the comparison between Ian's Bayesian game based Algorithm 3 (BG Algorithm), EP Algorithm, and Without CJ decision. As observed in both Type I and Type II games, as p increases, the BG Algorithm outperforms the others, and using the naive EP Algorithm is worse than Without CJ when p is large.

As seen in Fig. 4(b,c), the attackers' NE strategies have a clear load sharing structure. Notice that an eavesdropper can indeed exploit the friendly interferer's incorrect belief about the attacker's type. Hence, an accurate inference on the type of upcoming attackers is crucial.



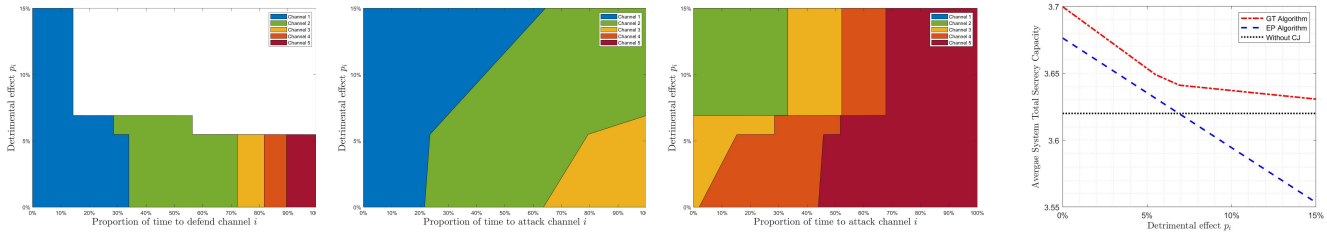
(a) Optimal defense strategy as p increases (b) Optimal attack strategy as p increases (c) Expected total secrecy capacity

Fig. 2. NE strategies against Type I eavesdropper.



(a) Optimal defense strategy as p increases (b) Optimal attack strategy as p increases (c) Expected total secrecy capacity

Fig. 3. NE strategies against Type II eavesdropper.



(a) Optimal defense strategy (b) Type I Eve's optimal strategy (c) Type II Eve's optimal strategy (d) Expected total secrecy capacity

Fig. 4. NE strategies for Bayesian game against unknown types of Eavesdroppers as p increases.

VI. Conclusion

This paper investigates game theoretic probabilistic channel selection strategies for cooperative jamming to protect a network of parallel wireless channels against intelligent eavesdroppers. Eavesdroppers with two types of CSI configuration are discussed; I) either she has distinct eavesdropping capacity at each channel, or II) all eavesdropping channels have the same capacity. Two non-zero-sum games model the problem for each type of eavesdropping CSI. Analytical expressions for the equilibrium strategies derived demonstrate that the defender should use a threshold type strategy against a type I eavesdropper and an all-or-nothing strategy against a type II eavesdropper. The level of interference on legitimate receivers, which is represented by $\{p_i\}$, is critical in deciding how to select channels for protection. The results imply that the interferer must carefully configure the interfere signals to make then beneficial to achieving communication secrecy.

In the case that eavesdropping CSIs are privately known to the attacker, a Bayesian game model is proposed and analytical expressions for NE strategies are provided when the eavesdropping capacity is either of Type I or Type II. The defender's best strategy can be considered as a mixture of the threshold type policy against Type I Eve and the all-or-nothing policy against type II Eve, depending on his belief about the type of eavesdropper's CSIs. The attackers' best policy reveals a load sharing structure, in which a Type I attacker will focus on a few channels with high eavesdropping capacities, while a Type II attacker attacks the rest.

Of interest for future research is to complete the discussion of the Bayesian game when there are K scenarios of different eavesdropping CSI. Another interest for future research is to consider investment or pricing decisions associated with reducing the detrimental effect of friendly interference on legitimate users. For instance, the defender may be involved in a pricing game with legitimate users such that the user at each channel may agree to pay a price for decreasing g_{L_i}.

Appendix A
Proof of Theorem 1 and Theorem 2

Consider the network of parallel channels as a network of heterogeneous nodes, where C_{E_i} and C_E are rewards paid to a Type I attacker and a Type II attacker if an attack

is successfully initiated at node i, respectively. d_i is the effectiveness of applying cooperative jamming to intercept the attacker at node i. And $g_i = p_i C_{L_i}$ represents the cost of intercepting the attacker at channel i. Then the NE solutions of the Type I and Type II game follow Theorem 1 and Theorem 2 of [36], respectively.

APPENDIX B
PROOF OF THEOREM 3

One can interpret the discussed Bayesian game in the following way: the defender is playing against a Type I attacker from channel 1 to channel n and is playing against a Type II attacker from channel n to channel N where the two games intersect at channel n. The Bayesian game should have similar properties to the previous games including:

- Property 1, if $y^*_{\mathrm{I}_i} > 0$, then $x^*_j > 0,\ \forall j < i$.
- Property 2, if $x^*_i > 0$, then $y^*_{\mathrm{I}_i} > 0$.
- Property 3, either $x^*_i > 0,\ \forall i \geq n$, or $x^*_i = 0,\ \forall i \geq n$, will be true between the defender and Type II Eve.

Let $S^D_i, i = 1, ..., N$, be the pure policy that the defender selects channel i with probability one, and let $S^D_{N=1}$ be the pure policy of not using cooperative jamming. Let $\bar{v}^D_B = v^D_B - \mu^D(S^D_{N+1}, \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}})$. The next proposition will be essential for constructing an upper bound for n.

Proposition. $\bar{v}^D_B \geq \tilde{v}^D_B$.

Proof. If $\tilde{v}^D_B \leq 0$, then $\bar{v}^D_B \geq \tilde{v}^D_B$ since $\bar{v}^D_B \geq 0$ by definition. If $\tilde{v}^D_B > 0$, consider the following optimization problem:

$$\min_{\bar{v}^D_B, \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}}} \quad \bar{v}^D_B$$
$$\text{s.t.} \quad \bar{v}^D_B \geq \bar{\mu}^D_{B_i} \quad \forall i = 1, ..., N,$$

with $\sum_{i=1}^{n} y^*_{\mathrm{I}_i} = 1$ and $\sum_{i=n}^{N} y^*_{\mathrm{II}_i} = 1$. It is easy to show that the optimal value of this minimization problem is $\tilde{v}^D_B$. □

Hence, it holds that $\bar{v}^D_B \geq \max\{\tilde{v}^D_B, 0\}$. This in turn suggests an upper bound for the cut-off index n, given the indices m and k defined in Theorem 3.

Proposition. $n \leq \min\{k, m+1\}$.

Proof. By the definition of n, $y^*_{\mathrm{I}_n} > 0$. Then, property 1 implies that $x^*_j \geq \frac{C_{E_j} - C_{E_n}}{d_j C_{E_j}} \geq 0,\ \forall i = 1, ..., n$. Moreover, because $x_j = 0,\ \forall j = n+1, ..., N$, $\sum_{j=1}^{n} x^*_j = 1 - x^*_{N+1} \leq 1$. Hence, $\sum_{j=1}^{n} \frac{C_{E_j} - C_{E_n}}{d_j C_{E_j}} \leq \sum_{j=1}^{n} x^*_j \leq 1$, and $n \leq k$ follows. By property 1 and 2, clearly, $x^*_i > 0$, $y^*_{\mathrm{I}_i} > 0,\ \forall i \leq n-1$, and $\bar{\mu}^D_{B_i} = \bar{v}^D_B,\ \forall i \leq n-1$, giving $y^*_{\mathrm{I}_i} = \frac{\bar{v}^D_B + p_i C_{L_i}}{\alpha d_i C_{E_i}} > 0,\ \forall i \leq n-1$. Since it is also true that $y^*_{\mathrm{I}_n} > 0$ and $\bar{v}^D_B \geq \max\{\tilde{v}^D_B, 0\}$, then $\sum_{i=1}^{n-1} \frac{\tilde{v}^D_B + p_i C_{L_i}}{\alpha d_i C_{E_i}} \leq \sum_{i=1}^{n-1} \frac{\bar{v}^D_B + p_i C_{L_i}}{\alpha d_i C_{E_i}} \leq 1$ holds, and by definition, $n \leq m+1$ follows. □

The final value of n and the explicit solution of $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}})$ depends on the value of k, m and $\tilde{v}^D_B$ as defined in Theorem 3. There are three possible cases: (a) $k \leq m$, (b - 1) $m < k$ and $\tilde{v}^D_B < 0$, (b - 2) $m < k$ and $\tilde{v}^D_B > 0$.

(a) The case $k \leq m$ is similar to case (a) in Theorem 1, where the defender will use up all his attention to intercept Type I Eve at the first k channels with $n = k$ and will not interfere with Type II Eve. Meanwhile, a Type I attacker will also focus on channels 1 through k. The equilibrium strategies for the defender and Type I attacker are the solution to

$$\begin{cases} v^A_{\mathrm{I}} = \mu^A_{\mathrm{I}}(\boldsymbol{x}^*, S^A_1) = \cdots = \mu^A_{\mathrm{I}}(\boldsymbol{x}^*, S^A_k), \\ \bar{v}^D_B = \bar{\mu}^D_{B_1} = \cdots = \bar{\mu}^D_{B_k}, \\ \sum_{i=1}^{k} x^*_i = 1, \quad \sum_{i=1}^{k} y^*_{\mathrm{I}_i} = 1, \end{cases} \tag{35}$$

which gives $C_{E_{k+1}} < v^A_{\mathrm{I}} < C_{E_k}$, $\bar{v}^D_B > \max\{\tilde{v}^D_B, 0\}$ and $x^*_i > 0,\ \forall i = 1, ..., k$. Since $x_i = 0,\ \forall i = k+1, ..., N+1$, it holds that

$$v^A_{\mathrm{II}} = \mu^A_{\mathrm{II}}(\boldsymbol{x}^*, S^A_{k+1}) = \cdots = \mu^A_{\mathrm{I}}(\boldsymbol{x}^*, S^A_N) = C_E$$
$$> \mu^A_{\mathrm{II}}(\boldsymbol{x}^*, S^A_i), \quad \forall i = 1, ..., k.$$

So in equilibrium, a Type II attacker attacks channels $k+1$ to N and makes sure that it is always more beneficial for the defender to intercept a Type I attacker. Any strategy that satisfies $\bar{\mu}^D_{B_i} \leq \bar{v}^D_B,\ \forall i = k+1, ..., N$, and $\sum_{i=k+1}^{N} y^*_{\mathrm{II}_i} = 1$, is a NE strategy of a Type II attacker.

(b) The case $k > m$ can be imagined as case (b) of Theorem 1 combined with the Type II game. The defender has extra resources to fight against a Type II attacker, but whether the defender will interfere with a Type II attacker depends on the value of an indicator, $\tilde{v}^D_B$.

Proposition. Given $k > m$, if $\tilde{v}^D_B < 0$, then $x^*_i = 0,\ \forall i = n \geq N$; but, if $\tilde{v}^D_B > 0$, then $x^*_i > 0,\ \forall i = n \geq N$.

Proof. Assume $x^*_i \neq 0$ for some $i = n \geq N$ given $\tilde{v}^B_D < 0$. By property 3, $x^*_i > 0,\ \forall i = n \geq N$. Moreover, by property 1 and 2, it is also true that $x^*_i > 0,\ \forall i \leq n-1$. That requires,

$$\bar{\mu}^D_{B_i} = \bar{v}^D_B \geq 0, \quad \forall i = 1, ..., N.$$

However, it is impossible to find such $\bar{\mu}^D_{B_i}\ \forall i = 1, ..., N$, since $\tilde{v}^B_D < 0$. Hence, the assumption cannot be true.
Assume $x^*_i = 0$ for some $i = n \geq N$, under the constraint $\tilde{v}^B_D > 0$. Then, property 3 implies $x^*_i = 0,\ \forall i = n \geq N$. Furthermore, $x^*_{N+1} = 0$ since $\bar{v}^D_B \geq \tilde{v}^D_B > 0 = \bar{\mu}^D_{B_{N+1}}$. That will lead to $\sum_{i=1}^{n-1} x^*_i = 1$. Meanwhile, if $x^*_i > 0$ for an integer $i \leq n$, then $y^*_i > 0$ by property 2 and $\mu^A_{\mathrm{I}}(\boldsymbol{x}^*, S^A_i) = v^A_{\mathrm{I}}$. Moreover, $v^A_{\mathrm{I}} \geq C_{E_n}$ since $x^*_n = 0$. It can be seen that it is impossible to find a solution of $\sum_{i=1}^{n-1} x^*_i = 1$ given $n-1 \leq m$, $k > m$ and the constraint $\mu^A_{\mathrm{I}}(\boldsymbol{x}^*, S^A_i) \geq C_{E_n},\ \forall i \leq n-1$. Hence, the assumption cannot be true. □

(b - 1) If $k > m$ and $\tilde{v}^D_B < 0$, this case is similar to case (b) of Theorem 1 combined with case (b) of Theorem 2. One can use similar techniques to show that the cut-off index is equal to $m+1$, i.e., $n = m+1$. A Type I attacker will focus on channels 1 to $m+1$, while the defender can protect more than m channels but it is beneficial not to protect the remaining channels so that $x^*_i = 0,\ \forall i = m+1, ..., N$ by lemma 6 and has $x^*_{N+1} > 0$. Thus, the equilibrium strategies of the defender and a Type I attacker are solutions to

$$\begin{cases} v^A_{\mathrm{I}} = \mu^A_{\mathrm{I}}(\boldsymbol{x}^*, S^A_1) = \cdots = \mu^A_{\mathrm{I}}(\boldsymbol{x}^*, S^A_m) = C_{E_{m+1}}, \\ \bar{v}^D_B = \bar{\mu}^D_{B_1} = \cdots = \bar{\mu}^D_{B_m} = 0, \\ x^*_{N+1} = 1 - \sum_{i=1}^{m} x^*_i, \quad y^*_{\mathrm{I}_{m+1}} = 1 - \sum_{i=1}^{m} y^*_{\mathrm{I}_i}. \end{cases}$$

Note that $x^*_i > 0,\ \forall i = 1, ..., m$ and $x_i = 0,\ \forall i = m+$

$1, ..., N$. Thus, any strategy that satisfies $\bar{\mu}_{B_i}^D \leq 0, \ \forall i = m+1, ..., N$, and $\sum_{i=m+1}^{N} y_{\mathrm{II}_i}^* = 1$, can be a NE strategy of a Type II attacker.

(b - 2) If $k > m$ and $\tilde{v}_B^D > 0$, this case can be regarded as case (b) of Theorem 1 combined with case (a) of Theorem 2. The attackers' equilibrium strategies $(\boldsymbol{y}_{\mathbf{I}}^*, \boldsymbol{y}_{\mathbf{II}}^*)$ are solutions to the system of equations 22 since $x_i^* > 0, \ \forall i = 1, ..., N$, which gives $\bar{v}_B^D = \tilde{v}_B^D$ and $n = m + 1$. Thus, $(\boldsymbol{y}_{\mathbf{I}}^*, \boldsymbol{y}_{\mathbf{II}}^*)$ need

$$\begin{cases} y_{\mathrm{I}_i}^* > 0, y_{\mathrm{II}_i}^* = 0, & \forall 1 \leq i < n, \\ y_{\mathrm{I}_n}^* > 0, y_{\mathrm{II}_n}^* > 0, & \\ y_{\mathrm{I}_i}^* = 0, y_{\mathrm{II}_i}^* > 0, & \forall n < i \leq N. \end{cases}$$

Hence, $\boldsymbol{x}^*$ is the solution to

$$\begin{cases} v_{\mathrm{I}}^A = \mu_{\mathrm{I}}^A(\boldsymbol{x}^*, S_1^A) = \cdots = \mu_{\mathrm{I}}^A(\boldsymbol{x}^*, S_{m+1}^A), \\ v_{\mathrm{II}}^A = \mu_{\mathrm{II}}^A(\boldsymbol{x}^*, S_{m+1}^A) = \cdots = \mu_{\mathrm{II}}^A(\boldsymbol{x}^*, S_N^A), \\ \sum_{i=1}^{N} x_i^* = 1, \end{cases}$$

which is unique.

REFERENCES

[1] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, pp. 1–39, 2013.

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

[3] 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.

[4] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "Physical layer security in wireless networks with passive and active eavesdroppers," in *2012 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2012, pp. 4868–4873.

[5] L. Li, A. P. Petropulu, and Z. Chen, "Mimo secret communications against an active eavesdropper," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2387–2401, 2017.

[6] S. Allipuram, P. Mohapatra, and S. Chakrabarti, "Secrecy performance of an artificial noise assisted transmission scheme with active eavesdropper," *IEEE Communications Letters*, vol. 24, no. 5, pp. 971–975, 2020.

[7] A. Garnaev, M. Baykal-Gürsoy, and H. V. Poor, "A game theoretic analysis of secret and reliable communication with active and passive adversarial modes," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2155–2163, 2015.

[8] A. Salem, X. Liao, Y. Shen, and X. Lu, "Provoking the adversary by dual detection techniques: A game theoretical framework," in *2017 International Conference on Networking and Network Applications (NaNA)*. IEEE, 2017, pp. 326–329.

[9] A. Garnaev and W. Trappe, "Secret communication when the eavesdropper might be an active adversary," in *International Workshop on Multiple Access Communications*. Springer, 2014, pp. 121–136.

[10] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE vehicular technology conference*, vol. 62, no. 3. Citeseer, 2005, p. 1906.

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

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

[17] X. He and A. Yener, "Cooperative jamming: The tale of friendly interference for secrecy," in *Securing Wireless Communications at the Physical Layer*. Springer, 2009, pp. 65–88.

[18] 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 and Tutorials*, vol. 21, no. 3, 2019.

[19] Y. Wu and K. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 831–842, 2011.

[20] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Başar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in *2011-MILCOM 2011 Military Communications Conference*. IEEE, 2011, pp. 119–124.

[21] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *2009 International Conference on Game Theory for Networks*. IEEE, 2009, pp. 287–294.

[22] Y. Zhong, F. Zhou, Y. Wang, X. Deng, and N. Al-Dhahir, "Cooperative jamming-aided secure wireless powered communication networks: A game theoretical formulation," *IEEE Communications Letters*, vol. 24, no. 5, pp. 1081–1085, 2020.

[23] 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.

[24] 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.

[25] 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.

[26] Z. Xu and M. Baykal-Gürsoy, "A friendly interference game in wireless secret communication networks," in *The 10th International Conference on NETwork Games, COntrol and OPtimization (NETGCOOP)*, 2021.

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

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

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] L. Wang, H. Wu, and G. L. Stüber, "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.

[34] 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.

[35] 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.

[36] Z. Xu and M. Baykal-Gürsoy, "Efficient network protection games against multiple types of strategic attackers," in *ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2021, pp. 2620–2624.