Power Games for Secure Communications in Single-stream MIMO Interference Networks

Peyman Siyari[1], Marwan Krunz[1,2], and Diep N. Nguyen[2]
[1]Department of Electrical and Computer Engineering, University of Arizona, USA
[2]Faculty of Engineering and Information Technology, University of Technology Sydney, Australia
{psiyari, krunz}@email.arizona.edu, diep.nguyen@uts.edu.au

***Abstract*—We propose a distributed interference management method for a single-stream MIMO interference network that is tapped by an external eavesdropper. Along with its information signal, each legitimate transmitter creates a bogus signal, known as *transmit-based friendly jamming* (TxFJ), to confuse the eavesdropper. Although generating TxFJ protects the link from eavesdropping, it creates interference at other unintended but legitimate links. Using non-cooperative game theory, we design a distributed method for maximizing the sum of secrecy rates. Each link is a player in the game. It seeks to maximize its secrecy rate subject to a given information-rate constraint and power budget. The strategy profile of each player is to control the amount of TxFJ it generates. Because a pure non-cooperative game may not have Nash equilibria that result in (Pareto-)optimal secrecy sum-rate, we propose a modified *price-based* game, in which each link is penalized for generating interference on other legitimate links. Under the exact knowledge of eavesdropping channels, we show that the price-based game has a comparable secrecy sum-rate to a centralized approach. We then relax the assumption of knowledge of eavesdropping channels, and leverage mixed-strategy games to provide robust solutions to the distributed secrecy sum-rate maximization problem.**

***Index Terms*—Wiretap interference network, friendly jamming, pricing, pure and mixed-strategy games.**

I. Introduction

A. Motivation

Interference has typically been considered an undesirable phenomenon when the goal is to boost the throughput of a shared wireless channel. Accordingly, many studies have been conducted to allow two or more wireless links to coexist in the same vicinity while inflicting minimum interference on each other. Examples include schemes that coordinate access through orthogonality in time, frequency, or code domain. The scarcity of the RF spectrum together with the increasing wireless demand led to introducing new schemes in which interference is generated in every domain, thus making interference management a key design issue. Contrary to its harmful role in achieving the capacity limit of a shared wireless channel, interference can be leveraged to provide physical-layer (PHY-layer) security [1].

In this paper, we are primarily interested in exploiting/managing interference in the context of information-theoretic PHY-layer secrecy [2]. The main goal here is to improve the channel state at the legitimate receiver (Rx), relative to the channel state at the eavesdropper (Eve). However, achieving this channel advantage may not always be possible, as is the case in cellular systems or WiFi networks where Eve may have a better channel state than the legitimate Rx. Accordingly, several techniques for PHY-layer security have been proposed (see [3]) that rely on generating a bogus signal called *friendly jamming (FJ)* signal [4] whose purpose is to confuse a nearby eavesdropper. In this method, the legitimate transmitter (Alice) uses multiple antennas to generate an FJ signal along with the information signal, thereby increasing the interference at Eve, but without affecting the reception at the legitimate Rx (Bob). The authors in [4] proposed a simple version of this technique ensuring that the FJ signal falls in the null-space of the channel between Alice and Bob. It was shown in [4] that under FJ, a non-zero secrecy rate can always be achieved for a sufficiently high transmit power, regardless of Eve's location.

In a multi-link scenario, several transmitters convey their messages simultaneously to several legitimate receivers. Hence, the FJ signal of each transmitter must not interfere with other unintended (but legitimate) receivers in the network. Such a design imposes centralized optimizations, and hence can be challenging when no central entity exists in the network or when no coordination is possible between links. Therefore, the need for distributed interference management with minimal coordination is crucial to guarantee secure yet non-interfering communications.

B. Related Work

To account for PHY-layer security in interference networks, two types of system models have been considered in the literature: *interference channel with confidential messages* (ICCM) and *wiretap interference channel* (WIC). In the ICCM model, each link may be curious about the transmissions of its neighboring links [5], [6]. Under WIC, an external eavesdropper(s) is present and the transmissions of links must be kept secure from these Eve(s), i.e., Bobs are not considered malicious eavesdroppers [1], [7][1].

An interesting observation about secret communications in interference networks was made in [1], where it was shown that interference caused by information signals can be exploited to confuse nearby eavesdroppers. A similar result was observed in a scenario where the secrecy of a number of links was enhanced by other active links in the network [8].

An abridged version of this paper was presented at IEEE INFOCOM 2016.

[1]A combination of the two models can also be considered.

In [9] the authors considered a two-link SISO WIC with one eavesdropper. By jointly optimizing the transmission powers of the two links, the authors attempted to maximize the secrecy rate for one link while maintaining a given throughput for the second link. Other instances of exploiting interference for secure communications can be found in [10], [11], and [12]. To provide secrecy for all the links in the network, the authors in [13] studied two transmitter-receiver-eavesdropper triplets (i.e., each link is being eavesdropped on by a separate eavesdropper) and proposed a cooperative beamforming approach to achieve the maximum secure degree of freedom for both links. Generalizations of interference alignment for PHY-layer secrecy were accomplished in [14].

An interference network under the WIC model was considered in [15] where dedicated cooperative jammers assist legitimate links by generating FJ signals. A distributed power control scheme was proposed to maximize the secrecy sum-rate of the network subject to a power budget for cooperative jammers. In contrast to [15], we allow each legitimate transmitter (Tx) to generate both the information and TxFJ signals itself. The use of cooperative jamming nodes in [15] may not be practical due to deployment costs. Furthermore, it was shown in [16] that cooperative jamming can be challenged if the eavesdropper has a certain separation between its antennas.

C. Overview of Proposed Approach

We consider a network of multiple legitimate links that coexist in the same vicinity and may interfere with one another. An eavesdropper snoops on ongoing communications (i.e., WIC model). Although previous studies (e.g., [1], [17], [11]) answer many questions regarding secrecy in interference networks, implementation of these ideas requires full coordination between legitimate links.

In the network under our study, all nodes are equipped with multiple antennas (i.e., MIMO WIC). Our main goal is to develop distributed power control schemes to maximize the sum of secrecy rates over all links. We consider FJ as the main technique used at each legitimate link, where the FJ signal is generated at the Tx side [4], [18], [19].

We assume that each link performs MIMO *beamforming*, i.e., the covariance matrix of the information signal of a given Alice is rank one. Such an approach has been shown to be optimal under several channel models (see [20]). Although in our case beamforming is a suboptimal approach, it helps us gain a valuable insight into solving the underlying optimization problems. We further assume that legitimate nodes cannot implement multiuser (secure) encoding. Hence, the problem reduces to controlling the power distribution between the information and TxFJ signals at each link. Each contending link acts selfishly, motivating us to leverage non-cooperative game theory for distributed power control.

Due to possible degradation in network performance, caused by the inherent inefficiency of Nash equilibria of non-cooperative games, we later augment our design using *pricing*, a well-known concept in game theory. Specifically, each legitimate link is charged a price for generating interference. Such a penalty is expected to lower interference in the network. However, interference reduction may result in a less noisy environment for Eve, allowing her to easily wiretap on ongoing communications. Contrary to such intuition, we show that there is a possibility that if one or more Tx's reduce their TxFJ powers, the sum of the secrecy rates over various links can actually increase. The reason is that the reduction in TxFJ power is done such that the interference at each legitimate Rx is reduced, but the aggregate interference at Eve remains high.

Overall, our contributions can be summarized as follows:

- We derive a lower bound on the TxFJ power to achieve a positive secrecy rate and produce enough interference to prevent Eve from applying successive interference cancellation. This lower bound also allows us to analyze various properties of our subsequent methods.
- We design a price-based distributed TxFJ power control for the MIMO WIC under our study. We show that pricing achieves a locally optimal solution for the secrecy sum-rate maximization problem. We also derive conditions whereby the price-based FJ control achieves the global optimum of the secrecy sum-rate maximization problem.
- We derive the conditions under which the use of the maximum possible TxFJ power leads to a unique Pareto-optimal point on the secrecy capacity region of the network. This result simplifies the design of the network, as no extra signaling is needed to regulate TxFJ powers.
- Lastly, we relax the assumption of exact knowledge of the eavesdropping channel and design a price-based TxFJ control that is robust to uncertainties about eavesdropping channels.

Notation: Boldface uppercase/lowercase letters denote matrices/vectors. Matrix $\mathbf{I}$ denotes the identity matrix of appropriate size. $E[\bullet]$, $\bullet^\dagger$, and $\mathrm{Tr}(\bullet)$ are, respectively, the expected value, complex conjugation (with transposition in case of vectors and matrices), and trace operators. The sets of real and complex numbers are indicated by $\mathbb{R}$ and $\mathbb{C}$, respectively.

II. System Model

Consider Q transmitters, $\text{Alice}_1, \ldots, \text{Alice}_Q$, ($Q \geq 2$) that communicate with their respective receivers, $\text{Bob}_1, \ldots, \text{Bob}_Q$. Let $\mathcal{Q} = \{1, \ldots, Q\}$. Alice_q and Bob_q, $q \in \mathcal{Q}$, have N_q and M_q antennas, respectively. A passive Eve with L antennas is also present in the network[2]. The received signal at Bob_q is

$$\mathbf{y}_q = \tilde{\mathbf{H}}_{qq}\mathbf{u}_q + \sum_{\substack{r=1 \\ r\neq q}}^{Q} \tilde{\mathbf{H}}_{rq}\mathbf{u}_r + \mathbf{n}_q \tag{1}$$

where $\tilde{\mathbf{H}}_{rq} \in \mathbb{C}^{M_q \times N_r}$, $r \in \mathcal{Q}$, is the $M_q \times N_r$ complex channel matrix between Alice_r and Bob_q, $\mathbf{u}_q \in \mathbb{C}^{N_q}$ is the transmitted signal from Alice_q. The term $\mathbf{n}_q \in \mathbb{C}^{M_q}$ is the complex AWGN at Bob_q; its power is N_0 and its covariance matrix is $E[\mathbf{n}_q\mathbf{n}_q^\dagger] = \frac{N_0}{M_q}\mathbf{I}$. The received signal at Eve is

$$\mathbf{z} = \tilde{\mathbf{G}}_q\mathbf{u}_q + \sum_{\substack{r=1 \\ r\neq q}}^{Q} \tilde{\mathbf{G}}_r\mathbf{u}_r + \mathbf{e} \tag{2}$$

[2]Though we assume a single eavesdropper, L can capture the case of multiple (multi-antenna) colluding eavesdroppers.

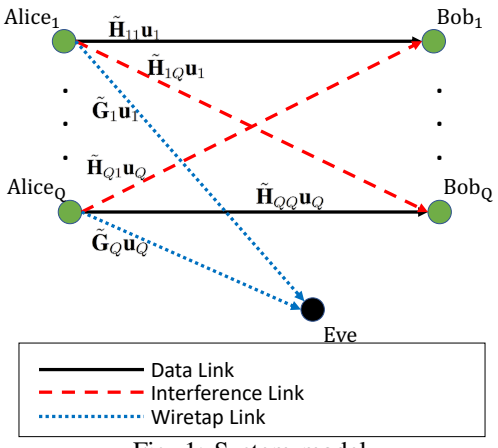


Fig. 1: System model.

where $\tilde{\mathbf{G}}_q \in \mathbb{C}^{L\times N_q}$, $q \in \mathcal{Q}$ denotes the channel matrix between Alice$_q$ and Eve, and $\mathbf{e}$ is the noise term. Fig. 1 depicts a visual representation of our system model defined by (1) and (2). The signal $\mathbf{u}_q = \mathbf{s}_q + \mathbf{w}_q$ consists of the information-bearing signal $\mathbf{s}_q$ and TxFJ signal $\mathbf{w}_q$. $\mathbf{s}_q$ can be written as $\mathbf{s}_q = \mathbf{T}_q x_q$, where $\mathbf{T}_q$ is the precoding matrix (precoder) and x_q is the information signal. Assume that a Gaussian codebook is used for x_q, i.e., x_q is a zero mean circularly symmetric complex Gaussian (ZMCSCG) random variable with $E[x_q x_q^\dagger] = \phi_q P_q \triangleq \gamma_q$, where P_q is the total transmit power of Alice$_q$ and $0 \le \phi_q \le 1$ is the portion of that power allocated to the information signal. For the TxFJ signal, we write $\mathbf{w}_q \triangleq \mathbf{Z}_q\mathbf{v}_q$, where $\mathbf{Z}_q \in \mathbb{C}^{N_q\times(N_q-1)}$ is the precoder of the TxFJ signal, $\mathbf{v}_q \in \mathbb{C}^{N_q-1}$ is a vector of i.i.d. ZMCSCG random variables, and $E[\mathbf{v}_q\mathbf{v}_q^\dagger] = \sigma_q\mathbf{I}$[3]. The scalar term $\sigma_q = \frac{(1-\phi_q)P_q}{N_q-1}$ denotes the power allocated to each dimension of $\mathbf{v}_q$. Let $\tilde{\mathbf{H}}_{qq} = \mathbf{U}_q\mathbf{\Sigma_q}\mathbf{V}_q^\dagger$ denote the singular value decomposition (SVD) of $\tilde{\mathbf{H}}_{qq}$, where $\mathbf{\Sigma_q}$ is the diagonal matrix of singular values, and $\mathbf{U}_q$ and $\mathbf{V}_q$ are left and right matrices of singular vectors, respectively. We set $\mathbf{Z}_q = \mathbf{V}_q^{(2)}$, where $\mathbf{V}_q^{(2)}$ is the matrix of N_q-1 rightmost columns of $\mathbf{V}_q$. We assume that Alice$_q$ knows the channel state information (CSI)[4]. The precoder $\mathbf{T}_q$ is set to $\mathbf{T}_q = \mathbf{V}_q^{(1)}$, where $\mathbf{V}_q^{(1)}$ is the first column of $\mathbf{V}_q$. Let $\mathbf{H}_{qq} \triangleq \tilde{\mathbf{H}}_{qq}\mathbf{V}_q^{(1)}$, $\mathbf{H}'_{qq} \triangleq \tilde{\mathbf{H}}_{qq}\mathbf{V}_q^{(2)}$, $\mathbf{H}_{qr} \triangleq \tilde{\mathbf{H}}_{qr}\mathbf{V}_q^{(1)}$, $\mathbf{H}'_{qr} \triangleq \tilde{\mathbf{H}}_{qr}\mathbf{V}_q^{(2)}$, $\mathbf{G}_q \triangleq \tilde{\mathbf{G}}_q\mathbf{V}_q^{(1)}$, and $\mathbf{G}'_q \triangleq \tilde{\mathbf{G}}_q\mathbf{V}_q^{(2)}$. The terms $\mathbf{G}_q$ and $\mathbf{G}'_q$ indicate the eavesdropping channel state information (E-CSI) components. Hence,

$$\mathbf{y}_q = \mathbf{H}_{qq}x_q + \mathbf{H}'_{qq}\mathbf{v}_q + \sum_{\substack{r=1\\r\neq q}}^{Q}(\mathbf{H}_{rq}x_r + \mathbf{H}'_{rq}\mathbf{v}_r) + \mathbf{n}_q$$

$$\mathbf{z} = \mathbf{G}_q x_q + \mathbf{G}'_q\mathbf{v}_q + \sum_{\substack{r=1\\r\neq q}}^{Q}(\mathbf{G}_r x_r + \mathbf{G}'_r\mathbf{v}_r) + \mathbf{e}.$$

[3]It was shown in [21] that *structured signaling* can have a better secrecy compared to Gaussian signaling when channel gains are real numbers. However, to the best of our knowledge, proving the usefulness of structured codes for the case of complex channels and interference networks is still an open problem.

[4]Acquiring CSI between Alice and her corresponding Bob is assumed to be done securely. For example, implicit channel estimation (i.e., Bob sending pilot signals to Alice) can be used to avoid having to send explicit CSI feedback.

The choice of precoders (i.e., beamformers) for TxFJ signals in this paper is mainly driven by the fact that acquiring E-CSI knowledge may not be always possible. For a single-link scenario, it was shown in [22] that optimizing the precoders of information and TxFJ signals requires knowledge of E-CSI. However, in this paper, the beamforming vector of TxFJ signal for each link depends only on the channel between the two nodes comprising that link. Our choice of beamforming vector of information signal for each link comes from the fact that the number of antennas at eavesdropper(s) may not be known in some cases. As pointed out in [4], the main limitation of the TxFJ method is that if the eavesdropper has more antennas than the legitimate Tx, then the eavesdropper may be able to nullify the effect of TxFJ on itself[5].

After receiving $\mathbf{y}_q$ at Bob$_q$, a linear receiver $\mathbf{d}_q \in \mathbb{C}^{M_q}$ is applied to estimate x_q. $\mathbf{d}_q$, $q \in \mathcal{Q}$, is assumed to be chosen according to the maximum ratio combining (MRC) method. Hence, $\mathbf{d}_q = \mathbf{U}_q^{(1)}$, where $\mathbf{U}_q^{(1)}$ is the first column of $\mathbf{U}_q$. Hence, the estimate $\hat{x}_q$ can be described as

$$\hat{x}_q \triangleq \mathbf{d}_q^\dagger(\mathbf{H}_{qq}x_q + \mathbf{H}'_{qq}\mathbf{v}_q + \sum_{\substack{r=1\\r\neq q}}^{Q}(\mathbf{H}_{rq}x_r + \mathbf{H}'_{rq}\mathbf{v}_r) + \mathbf{n}_q). \quad (3)$$

The terms $\mathbf{d}_q^\dagger\mathbf{U}_q\mathbf{\Sigma_q}$ and $\mathbf{V}_q^\dagger\mathbf{V}_q^{(2)}$ are orthogonal to each other. Hence, $\mathbf{d}_q^\dagger\mathbf{H}'_{qq}\mathbf{v}_q = \mathbf{d}_q^\dagger\mathbf{U}_q\mathbf{\Sigma_q}\mathbf{V}_q^\dagger\mathbf{V}_q^{(2)}\mathbf{v}_q = 0$. The information rate for the qth link can be written as

$$C_q = \log(1 + \frac{\gamma_q}{a_q}) \quad (4)$$

where

$$a_q \triangleq \frac{\sum_{\substack{r=1\\r\neq q}}^{Q}\left(\left|\mathbf{d}_q^\dagger\mathbf{H}_{rq}\right|^2\gamma_r + \left|\mathbf{d}_q^\dagger\mathbf{H}'_{rq}\right|^2\sigma_r\right) + N_0}{\left|\mathbf{d}_q^\dagger\mathbf{H}_{qq}\right|^2} \quad (5)$$

is the normalized interference received at Bob$_q$. Assuming a worst-case scenario in which Eve knows the channel between herself and each Alice (obtained by possibly spoofing on the pilot sequences), Eve applies the linear receiver $\mathbf{r}_q \in \mathbb{C}^L$ while eavesdropping on the qth link's communications so as to obtain the following estimate of x_q

$$\hat{z}_q = \mathbf{r}_q^\dagger(\mathbf{G}_q x_q + \mathbf{G}'_q\mathbf{v}_q) + \sum_{\substack{r=1\\r\neq q}}^{Q}(\mathbf{G}_r x_r + \mathbf{G}'_r\mathbf{v}_r) + \mathbf{e}). \quad (6)$$

Let $\tilde{\mathbf{G}}_q = \mathbf{L}_q\mathbf{D}_q\mathbf{R}_q$ be the SVD of $\tilde{\mathbf{G}}_q$, where $\mathbf{L}_q$ and $\mathbf{R}_q$ are matrices of left and right singular vectors, and $\mathbf{D}_q$ is the diagonal matrix of singular values. Eve chooses $\mathbf{r}_q = \mathbf{L}_q^{(1)}$, where $\mathbf{L}_q^{(1)}$ is the first column of $\mathbf{L}_q$, to perform MRC.

III. Problem Formulation

The multiuser channel between the Q Alices and Eve can be modeled as a multiple-access channel. If Eve is capable of using successive interference cancellation (SIC), she may be able to simultaneously decode all signals. To illustrate the

[5]A detailed explanation on how Eve is able to perform nullification of TxFJ is given in [23, Section II].

impact of SIC, consider the example of $Q = 2$. The rate region of Eve's multi-access channel is shown in Fig. 2, where C_{eq} denotes the rate at Eve while decoding Alice$_q$'s signal ($q = 1, 2$). The points β_q and ψ_q are defined later on in (7) and (10), respectively. Fig. 2 suggests that to prevent Eve from using SIC, we must have $C_q > \beta_q$ for $q = 1, 2$ [9], where

$$\beta_q \triangleq \log(1 + \frac{\gamma_q}{c_q}) \tag{7}$$

$$c_q = \frac{\left|\mathbf{r}_q^\dagger \mathbf{G}_q'\right| \sigma_q + \left(\left|\mathbf{r}_q^\dagger \mathbf{G}_r\right|^2 \gamma_r + \left|\mathbf{r}_q^\dagger \mathbf{G}_r'\right|^2 \sigma_r\right) + N_0}{\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2} \tag{8}$$

where $r \neq q$ (c_q is not to be confused with C_q defined in (4)). In this case, the secrecy rate for Alice$_q$, $q = 1, 2$, would be $C_q^{sec} = \max\{C_q - \beta_q, 0\}$ [9]. Because $C_q > \beta_q$, it can be guaranteed that Eve does not have complete knowledge of the qth information signal. Thus, the rate at Eve while eavesdropping on Alice$_r$'s signal, $r \neq q$, is $C_{er} = \beta_r$, and the secrecy rate of the rth link is

$$C_r^{sec} \triangleq \max\{C_r - \beta_r\ ,\ 0\} = \max\left\{\log(1 + \frac{\gamma_r}{a_r}) - \log(1 + \frac{\gamma_r}{c_r}), 0\right\}. \tag{9}$$

This operating point is shown as the tuple (β_1, β_2) in Fig. 2. If $C_q \leq \beta_q$, Eve has complete knowledge of Alice$_q$'s signal, $q = 1, 2$. Hence, Eve can consider Alice$_r$'s signal, $r \neq q$, as interference and decode Alice$_q$'s signal. Knowledge of Alice$_q$'s signal allows Eve to remove it from the total received signal and obtain Alice$_r$'s signal without interference. Hence, $C_{er} = \psi_r$ and $C_r^{sec} = \max\{C_r - \psi_r, 0\}$ where

$$\psi_r \triangleq \log(1 + \frac{\gamma_r}{d_r}) \tag{10}$$

$$d_r = \frac{\left|\mathbf{r}_r^\dagger \mathbf{G}_r'\right| \sigma_r + \left|\mathbf{r}_q^\dagger \mathbf{G}_q'\right|^2 \sigma_q + N_0}{\left|\mathbf{r}_r^\dagger \mathbf{G}_r\right|^2}. \tag{11}$$

This operating point can be shown as the tuple (ψ_1, β_2) or (β_1, ψ_2) in Fig. 2, depending on which Alice is targeted first by Eve. Overall, in order to achieve the maximum secrecy, both transmitters have to choose a transmission rate higher than Eve's decodable rate. For $Q > 2$, in order to prevent Eve from using SIC, we must have $C_q > \zeta_q\ \forall q$, where

$$\zeta_q \triangleq \log(1 + \frac{\gamma_q}{f_q}) \tag{12a}$$

$$f_q = \frac{\left|\mathbf{r}_q^\dagger \mathbf{G}_q'\right| \sigma_q + \sum_{\substack{r=1 \\ r\neq q}}^{Q} \left(\left|\mathbf{r}_q^\dagger \mathbf{G}_r\right|^2 \gamma_r + \left|\mathbf{r}_q^\dagger \mathbf{G}_r'\right|^2 \sigma_r\right) + N_0}{\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2}. \tag{12b}$$

Hence,

$$C_q^{sec} = \max\{C_q - \zeta_q, 0\}. \tag{13}$$

We define $C^{sec} \triangleq \sum_{q=1}^{Q} C_q^{sec}$ as the *secrecy sum-rate*, where C_q^{sec} is defined in (13) and ζ_q is defined in (12a). We aim to maximize C^{sec} while ensuring a minimum information rate for all links. This problem can be formally written as:

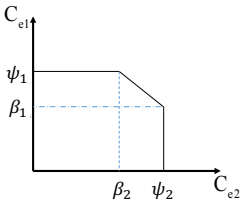


Fig. 2: Rate pairs for a two-user multiple access channel.

$$\underset{\boldsymbol{\gamma},\boldsymbol{\sigma}}{\text{maximize}}\ C^{sec} \quad \text{s.t.} \begin{cases} \gamma_q + \sigma_q(N_q - 1) \leq P_q \\ C_q \geq R_q \end{cases}, \ \forall q \tag{16}$$

where $\boldsymbol{\gamma} \triangleq [\gamma_q]_{q=1}^{Q} = [\gamma_1, \ldots, \gamma_Q]$ and $\boldsymbol{\sigma} \triangleq [\sigma_q]_{q=1}^{Q}$. The first constraint imposes a power constraint on each legitimate Tx; and the second constraint ensures a minimum information rate R_q for each link q. The optimization in (16) is non-convex. We relax this problem by assuming that the second constraint in (16) is satisfied with equality for some amount of power for the information signal, i.e., $C_q = R_q$ for some γ_q^*, for all q[6]. The second constraint can now be embedded into the objective function and the first constraint. Hence, (16) is simplified into[7]

$$\underset{\boldsymbol{\sigma}}{\text{maximize}}\ \ C^{sec} \quad \text{s.t.} \quad \sigma_q \leq \frac{P_q - \gamma_q^*}{N_q - 1},\ \forall q. \tag{17}$$

Recalling how we prevent Eve from applying SIC in (12a), σ_q is chosen such that $C_q > \zeta_q$ is satisfied for all q, i.e.,

$$\sigma_q > \frac{A_q}{B_q} \tag{18}$$

where

$$A_q \triangleq \left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2 \left(\sum_{\substack{r=1 \\ r\neq q}}^{Q} (\left|\mathbf{d}_q^\dagger \mathbf{H}_{rq}\right|^2 \gamma_r + \left|\mathbf{d}_q^\dagger \mathbf{H}_{rq}'\right|^2 \sigma_r) + N_0\right) - \left|\mathbf{d}_q^\dagger \mathbf{H}_{qq}\right|^2 \left(\sum_{\substack{r=1 \\ r\neq q}}^{Q} \left(\left|\mathbf{r}_q^\dagger \mathbf{G}_r\right|^2 \gamma_r + \left|\mathbf{r}_q^\dagger \mathbf{G}_r'\right|^2 \sigma_r\right) + N_0\right) \tag{19a}$$

$$B_q \triangleq \left|\mathbf{r}_q^\dagger \mathbf{G}_q'\right| \left|\mathbf{d}_q^\dagger \mathbf{H}_{qq}\right|^2. \tag{19b}$$

Simplifying (18), the following constraints can be established:

$$\sigma_q = \frac{P_q - \gamma_q^*}{N_q - 1} \quad \text{if} \quad \frac{A_q}{B_q} \geq \frac{P_q - \gamma_q^*}{N_q - 1} \tag{20a}$$

$$\sigma_q > \frac{A_q}{B_q} \quad \text{if} \quad A_q > 0 \ \ \& \ \ \frac{A_q}{B_q} < \frac{P_q - \gamma_q^*}{N_q - 1} \tag{20b}$$

$$\sigma_q > 0 \quad \text{if} \quad A_q = 0. \tag{20c}$$

$$\sigma_q = 0 \quad \text{if} \quad A_q < 0. \tag{20d}$$

[6]Later on, when we propose our FJ control algorithm, we devise a procedure for finding γ_q^*.

[7]Later, as we present our TxFJ control algorithm, we provide more explanation of this simplification.

For the case in (20a), no amount of TxFJ power can prevent Eve from using SIC. Because the inequalities in (20b) and (20c) are strict, we define $\delta_q > 0$ to denote an arbitrarily small positive value, so that we can have

$$\sigma_q = \frac{P_q - \gamma_q^*}{N_q - 1} \quad \text{if} \quad \frac{A_q}{B_q} \geq \frac{P_q - \gamma_q^*}{N_q - 1} \tag{21a}$$

$$\sigma_q \geq \frac{A_q}{B_q} + \delta_q \quad \text{if} \quad A_q > 0 \;\; \& \;\; \frac{A_q}{B_q} < \frac{P_q - \gamma_q^*}{N_q - 1} \tag{21b}$$

$$\sigma_q \geq \delta_q \quad \text{if} \quad A_q = 0. \tag{21c}$$

$$\sigma_q = 0 \quad \text{if} \quad A_q < 0. \tag{21d}$$

Considering that any of (20b), (20c), or (20d) holds, the optimization in (17) becomes

$$\begin{aligned} \underset{\boldsymbol{\sigma}}{\text{maximize}} \;\; & C^{sec} \\ \text{s.t.} \;\; & \sigma_q \in \mathcal{D}_q \triangleq \left[\chi_q, \frac{P_q - \gamma_q^*}{N_q - 1}\right], \; \forall q \end{aligned} \tag{22}$$

where $\chi_q \triangleq \min\left\{\max\left(\delta_q \frac{A_q}{|A_q|}, \frac{A_q}{B_q} + \delta_q \frac{A_q}{|A_q|}, 0\right), \frac{P_q - \gamma_q^*}{N_q - 1}\right\}$ and $[a, b]$ denotes a continuous interval between a and b. The optimization in (22) aims to find the best tradeoff (i.e., Pareto-optimal solutions) of secrecy sum-rate[8]. Unfortunately, the optimization in (22) is still non-convex. Furthermore, it requires the knowledge of E-CSI (i.e., $\mathbf{G}_q$ and $\mathbf{G}'_q$).

IV. Game Formulation

A. Greedy FJ control

One method to reduce the complexity of (22), and at the same time enable distributed implementation with low signaling overhead, is to let each Alice maximize the secrecy of her transmission to the corresponding Bob and ignore the effect of her TxFJ on unintended Bobs. This locally optimized TxFJ control leads to a game theoretic interpretation of this network. That is, a non-cooperative game can be formulated in which the best strategy of each link q is

$$\begin{aligned} \underset{\sigma_q}{\text{maximize}} \;\; & C_q^{sec} \\ \text{s.t.} \;\; & \sigma_q \in \mathcal{D}_q. \end{aligned} \tag{23}$$

In this game, the utility function of each player (link) is his secrecy rate and his strategy is to choose the best TxFJ power to maximize his utility subject to a power constraint (i.e., strategy set). Although one may argue that the game formulation in (23) is essentially different from the formulation in (22), we use (23) to build foundations on how we find suitable solutions for (22).

The existence of a Nash equilibrium (NE) for game (23) can be proven by showing that the strategy set of each player is a non-empty, compact, and convex subset of $\mathbb{R}$, and the utility function of each player is a continuous and quasi-concave function of the TxFJ power [26]. Verifying these properties in our game is straightforward, and is thus skipped for brevity.

[8]To be more specific, the solutions of (22) only correspond to one Pareto-optimal solution on the convex portion of the secrecy rate region. We skip the details of the relationship between the Pareto-optimal points and (weighted) sum utility optimization for the sake of brevity (see [24, Section 6], [23, Appendix C], and [25]).

Since the objective function in (23) is strictly concave in σ_q, the best strategy that maximizes the secrecy rate of the qth player is to select the maximum available TxFJ power, i.e., $\sigma_q = P_q^{jam} \triangleq \frac{P_q - \gamma_q^*}{N_q - 1}, \; q = 1, 2$. When $\sigma_q = P_q^{jam} \; \forall q$, no player will be willing to unilaterally change his own strategy because any other strategy can degrade the secrecy rate of that player. Therefore, the point $\sigma_q = P_q^{jam}, \; \forall q$ is the NE.

This NE point, however, may not always be efficient, because selfish maximization of the secrecy rate by each player is not always guaranteed to be Pareto-optimal. Hence, we seek a modification that prevents legitimate links from using all their TxFJ powers, so as to reduce interference in the network.

B. Price-based FJ control

The efficiency of the NE in the greedy FJ approach can be improved by using pricing policies. Specifically, for all q, the utility of player q in (23) would be modified into:

$$\begin{aligned} \underset{\sigma_q}{\text{maximize}} \;\; & C_q^{sec} - \lambda_q \sigma_q \\ \text{s.t.} \;\; & \sigma_q \in \mathcal{D}_q \end{aligned} \tag{24}$$

where λ_q is a pricing factor for the qth link, defined as

$$\lambda_q \triangleq \sum_{\substack{r=1 \\ r \neq q}}^{Q} -\frac{\partial C_r^{sec}}{\partial \sigma_q} \tag{25}$$

The optimal TxFJ power can be found by writing the K.K.T. conditions for (24). A close-form representation of the optimal TxFJ power for the qth link can be written as (26) at the top of the next page, where $\bullet]_a^b$ denotes $\min\{\max\{\bullet, a\}, b\}, \; a \leq b$. It is easy to verify that in (26), by setting $\lambda_q = 0$, we end up with the greedy TxFJ approach. By iteratively using (26) to set the TxFJ power for all players, the game converges to a NE from which neither player is willing to deviate. Later on, we further explain the feasibility of converging to a NE. The following theorem clarifies the reason for setting the pricing factor as in (25).

Theorem 1. *The NE of the game* (24) *where players apply* (25) *as the pricing factor equals to that of a locally optimal solution to* (22)*.*

Proof: See [23, Appendix A]. ∎

Next, we introduce an important property of the price-based FJ control.

Proposition 1. *The price-based FJ control admits a unique NE that is the global optimum of the secrecy sum-rate maximization problem in* (22) *if the following conditions are satisfied:*

- *All links have feasible strategies, i.e., they satisfy the bound in* (18)*, i.e.,* $\sigma_q > \frac{A_q}{B_q}, \; \forall q$.
- *Low interference at each Bob, i.e.,* $\left|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{qq}\right|^2 \gg \sum_{\substack{r=1 \\ r \neq}}^{Q} (|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{rq}|^2 \gamma_r + |\boldsymbol{d}_q^\dagger \boldsymbol{H}'_{rq}|^2 \sigma_r) + N_0, \; \forall q$.

Furthermore, assuming only feasible strategies for all links, using (26) *to update TxFJ powers in a sequential manner (i.e., the Gauss-Seidel method in the sense of [27, Chapter 3]) for all* $q \in \mathcal{Q}$ *converges to a (unique) NE.*

$$\sigma_q^* = \frac{1}{|\mathbf{r}_q^\dagger \mathbf{G}_q'|^2} \left(\sqrt{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 |\mathbf{r}_q^\dagger \mathbf{G}_q'|^2 \frac{\gamma_q^*}{\lambda_q} + |\mathbf{r}_q^\dagger \mathbf{G}_q|^4 \frac{{\gamma_q^*}^2}{4}} - |\mathbf{r}_q^\dagger \mathbf{G}_q|^2 \frac{\gamma_q^*}{2} - \sum_{\substack{r=1 \\ r \neq q}}^{Q} \left(|\mathbf{r}_q^\dagger \mathbf{G}_r|^2 \gamma_r + |\mathbf{r}_q^\dagger \mathbf{G}_r'|^2 \sigma_r + N_0 \right) \right)\Bigg]_{\chi_q}^{\frac{P_q - \gamma_q^*}{N_q^{-1}}} . \quad (26)$$

Proof: See [23, Appendix B]. ∎

Remark: While we were not able to show the convergence under synchronous updates (i.e., the Jacobi method in the sense of [27, Chapter 3]), where all links update their actions simultaneously at each iteration, we verified it in our simulations.

C. Optimality of Greedy FJ Control

As a first attempt, w We now analyze the situation where the use of greedy FJ control results in a unique Pareto-optimal point for the secrecy sum-rate maximization in (17). This analysis allows us to find the conditions under which there is no need for an iterative price-based FJ control optimization (and subsequently, no need for knowledge of E-CSI) because each Alice sets her TxFJ power to the maximum available.

Proposition 2. *The greedy FJ approach results in the unique Pareto-optimal operating point for problem* (17) *if the matrix* ∇C^{sec}*, whose* (i,j) *element is given by* $\frac{\partial C_i^{sec}}{\partial \sigma_j}, i,j \in \mathcal{Q}$*, has non-negative elements and non-zero rows.*

Proof: See [23, Appendix C]. ∎

Remark: In the following, we give a simple side result of Proposition 2, which serves as an intuitive example to understand Proposition 2. This side result was already presented in [28], but now extended to multiple links in this paper.

Corollary 1. *For a network of two legitimate links, the greedy FJ control results in a unique Pareto-optimal point if* $\lambda_q \leq 0$*,* $q = 1, 2$*.*

Proof: Given that $\lambda_q = -\frac{\partial C_r^{sec}}{\partial \sigma_q}$*,* $q, r = 1, 2$ *(see* (25)*), for* $\lambda_q > 0$*, then* $\frac{\partial C_r^{sec}}{\partial \sigma_q} < 0$*. Hence, a positive price is effective as long as the increase in one player's TxFJ power reduces the secrecy rate for the other link. Now, considering* $\lambda_q \leq 0$*, the increase in one player's TxFJ power results in either no change (i.e.,* $\lambda_q = 0$*) or an increase (i.e.,* $\lambda_q < 0$*) in the other player's secrecy rate. Therefore, whenever* $\lambda_q \leq 0$ *the right decision would be to use the maximum TxFJ power (i.e., setting* $\lambda_q = 0$*).* ∎

Remark: We would like to clarify that in general, the efficiency of the Greedy FJ control is not superior to that of the pricing-based approach. However, under some special conditions, detailed in Proposition 2, the price-based FJ control reduces to greedy FJ control (i.e., $\lambda_q = 0,\ \forall q \in \mathcal{Q}$).

For the general case of $Q > 2$, we now aim at making sense out of the conditions in Proposition 2, i.e., what would be the physical interpretation of these conditions.

Proposition 3. *The Pareto-optimality of the greedy FJ method occurs when* $\frac{\gamma_q}{\sigma_q} >> 1,\ \forall q$*.*

Proof: See [23, Appendix D]. ∎

Remark: The result of Proposition 3 is rather intuitive because preserving positive secrecy requires a link to spend a portion of its power for TxFJ. Therefore, whatever scenario that leaves low power to the TxFJ of all Alices (e.g., low transmit power, high rate demands or a dense network) can be the scenario where $\frac{\gamma_q}{\sigma_q} >> 1,\ \forall q$.

V. Price-based FJ Under E-CSI Uncertainties

When the E-CSI is unknown, it is difficult to compute σ_q^* and λ_q. Besides, the use of greedy FJ cannot be always guaranteed to be a Pareto-optimal point. In the following, we propose a method to overcome the issue of not having complete knowledge of E-CSI. We first need to introduce some new definitions for our game.

Let $U_q(s_q, s_{-q})$ be the utility of the qth player, where s_q and s_{-q} denote the strategy taken by player q and by other players except q, respectively. Without loss of generality, assume that the lower bound on σ_q for guaranteeing positive secrecy (as in (20)) has not been taken into account yet. Hence, the strategy space for each player q is a continuous interval, which can be written as $\sigma_q \in [0, P_q^{jam}]$. The strategy set of each player has infinitely many real numbers. In order to proceed further with our analysis, we need to make the strategy sets countable and finite. Hence, we discretize the TxFJ power. Assuming that we have n bits to convey $M = 2^n$ power levels, the power level increment is $\Delta\sigma_q = \frac{P_q^{jam}}{2^n}$. The strategy set of the qth player now becomes $\mathcal{S}_q = \{0, \Delta\sigma_q, 2\Delta\sigma_q, \ldots, (M-1)\Delta\sigma_q, P_q^{jam}\}$. Discretizing the players' strategies allows us to leverage a property of games with finite strategy sets for the players (i.e., *finite games*): Every finite game has a mixed-strategic NE [29].

A. Mixed-Strategy Game Formulation

Definition 1. *A mixed-strategy vector for the* q*th player* $\mathcal{A}_q = \left\{ [\alpha_{i,q}]_{i=1}^M \mid 0 \leq \alpha_{i,q} \leq 1,\ \sum_i \alpha_{i,q} = 1,\ \forall q \right\}$ *is a probability distribution of the* q*th player's strategies. In other words, the* q*th player chooses power level* $i\Delta\sigma_q$ *with probability* $\alpha_{i,q}$*.*

In the mixed-strategy jamming game, players choose their TxFJ powers based on probability distributions. Hence, the best response of each player is to maximize the expected value of his own utility. We note that some games can be limited to only pure strategies. In particular, if the utility function of a player is concave w.r.t. his strategy, then using Jensen's inequality, we deduce that $\forall (s_q, s_{-q}) \in \mathcal{S}_q \times \mathcal{S}_{-q}$, where $\mathcal{S}_{-q} \triangleq \mathcal{S}_1 \times \cdots \times \mathcal{S}_{q-1} \times \mathcal{S}_{q+1} \times \cdots \times \mathcal{S}_Q$, we must have

$$E_{s_q}\left[E_{s_{-q}}[U_q(s_q, s_{-q})] \right] \leq E_{s_{-q}}\left[U_q\left(E_{s_q}[s_q], s_{-q} \right) \right]. \quad (27)$$

Equation (27) is satisfied with equality if and only if s_q reduces to pure strategies. Hence, using pure strategies is more

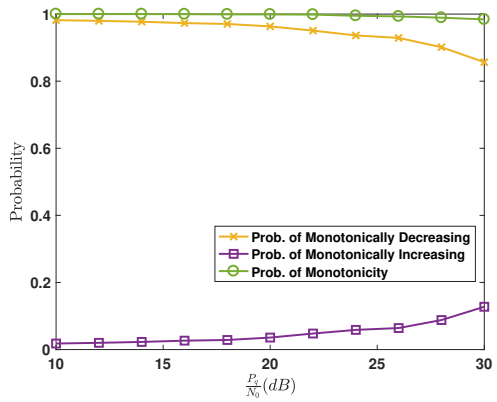


Fig. 3: Probability of monotonicity of σ_q^* w.r.t. σ_r, $(r,q) = 1,2,\ r \neq q$.

efficient than using mixed strategies. However, sufficiency of pure strategies cannot be guaranteed if the utility function of a player is not concave w.r.t. his action. Hence, mixed strategies should also be investigated for non-concave utilities. Unfortunately, to the best of our knowledge, even though the existence of a mixed NE in games with finite strategy spaces is guaranteed regardless of concavity of utility functions [30], finding the mixed NE in games with non-concave utilities is in general difficult. In our case, we limit our study to $Q = 2$, for which the mixed-strategy games are well-understood.

Before exploring the application of mixed-strategy games in our FJ control problem, we present an important observation related to the behavior of price-based FJ control when $Q = 2$. Assume now that the constraints imposed on σ_q in (20) are taken into account.

Conjecture 1. *When $Q = 2$, the optimal update of one player in* (26) *is a monotonic function of the TxFJ power of the other player's action, i.e., σ_q^* is a monotonic function of σ_r^* for $q = 1,2$ and $r \neq q$.*

Although we were not able to analytically prove the above relationship between the two TxFJ powers, we verified it via the following simulation. We replaced the term λ_q in (26) with the right hand side (RHS) of (25) and examined whether the optimal update on TxFJ of one link is a monotonic function of TxFJ of another link. We randomly placed both links as well as the eavesdropper in a circle with radius $r_{circ} = 25$ m. The distance between the transmitter and the receiver of each link is set to be a constant $d_{link} = 15$ m. Due to the importance of this conjecture, we have a high number of runs for this simulation. we ran this simulation for a total of 100 random link placements. For each link placement, we created 1000 channel realizations. Then, the probability of monotonicity of TxFJ powers w.r.t each other can be calculated by counting the number of times that σ_q^* is a monotonic function of σ_r, $r, q \in \mathcal{Q}$ and dividing this number by $100 * 1000$. This simulation is done for different transmit powers at both Alices. We assumed that both Alices use the same amount of transmit power for each run. It can be seen in Fig. 3 that the monotonicity of TxFJ powers w.r.t. each other occurs almost every time we run this simulation. We ended up with the same results for different values of r_{circ} and d_{link} as well. Such verification of Conjecture 1 allows us to conclude the following:

Proposition 4. *If $Q = 2$ and $\lambda_q > 0$, the NE tuple of TxFJ powers (σ_1, σ_2) will take one of the following forms:*

$$(\sigma_1,\sigma_2) = (\sigma_{int},\chi_2) \text{ or } (\sigma_{int},P_2^{jam}) \text{ or } (\chi_1,\sigma_{int}) \text{ or } (P_1^{jam},\sigma_{int}) \text{ or } (\chi_1,\chi_2) \text{ or } (P_1^{jam},P_2^{jam}) \tag{28}$$

where $\chi_q < \sigma_{int} < P_q^{jam}$.

Proof: See [23, Appendix E]. ∎

For $Q = 2$, we can establish the strategy table shown in Table I. A utility matrix $\mathbf{U}_q$, $q = 1,2$, can be obtained such that the (i,j)th entry is $[\mathbf{U}_q]_{ij} = \left\{U_q(i\Delta\sigma_1, j\Delta\sigma_2)|\ (i,j) \in \{0,\dots,M\}^2, r \neq q\right\}$ where U_q is the utility function of the qth player and will be characterized shortly. Because problem (22) is non-convex w.r.t the TxFJ powers, the Pareto-optimal points can be found via exhaustive search in Table I. Considering a finite jamming game, the complexity of this optimization is in the order of $\mathcal{O}(n^2)$, where n is the number of strategies for each player. Proposition 4 reduces the complexity to $\mathcal{O}(4n-4)$ signifying that only a small set of TxFJ power tuples comprises the NE points of price-based FJ game

In price-based FJ, the utility function of each player changes at every iteration due to the price updates. However, such update cannot be shown in a strategy table, i.e., the terms $U_1(i\Delta\sigma_1, j\Delta\sigma_2)$ and $U_2(i\Delta\sigma_1, j\Delta\sigma_2), (i,j) \in \{0,\dots,M\}$, in Table I can only show the utilities of the two players (at $s_1 = i\Delta\sigma_1$ and $s_2 = j\Delta\sigma_2$) for one iteration. Hence, it is not possible to designate the objective function in (24) as a utility function in the strategy table. In order to establish the strategy table, we inspect (22) again. Theorem 1 suggests that the K.K.T. conditions of secrecy sum-rate maximization in (22) are met at the NE point of the price-based game. Hence, we consider the utility of each player at the NE point to be $U_q(s_1,s_2) = C^{sec}(\sigma_q),\ q \in \{1,2\}$, which is in general a non-concave function w.r.t. σ_q. Because the two players have the same utility, it is reasonable for the qth player, $q = 1,2$ to assume that the rth player $(r \neq q, r = 1,2)$ chooses a strategy that is towards maximizing the utility of the qth player. Considering this fact and Proposition 4, the objective of player 1 (and equivalently for player 2) in the mixed-strategy FJ control game can be written as:

$$\begin{aligned} \underset{\{\alpha_{i,1}\}_{i=1}^M}{\text{maximize}} \quad & \max_{s_2} \sum_{i=1}^{M} \alpha_{i,1} U_1(i\Delta\sigma_1, s_2) \\ \text{s.t.} \quad & \sum_{i=1}^{M} \alpha_{i,1} = 1 \\ & 0 < \alpha_{i,1} < 1,\ \forall i \end{aligned} \tag{29}$$

where $\{\alpha_{i,1}\}_{i=1}^M$ is a probability set and $s_2 \in \left\{\left\lceil \frac{\chi_2}{M} \right\rceil \Delta\sigma_2, P_2^{jam}\right\}$ with $\lceil \bullet \rceil$ denoting the ceiling function. In other words, the qth player mixes his strategies to maximize the maximum utility that is seen from rth player's action.

TABLE I: Strategy table for the two-link finite jamming game with pricing.

$s_1 \backslash s_2$	0	$\Delta\sigma_2$	$\dots$	P_2^{jam}
0	$U_1(0,0), U_2(0,0)$	$U_1(0,\Delta\sigma_2), U_2(0,\Delta\sigma_2)$	$\dots$	$U_1(0,P_2^{jam}), U_2(0,P_2^{jam})$
$\Delta\sigma_1$	$U_1(\Delta\sigma_1,0), U_2(\Delta\sigma_1,0)$	$U_1(\Delta\sigma_1,\Delta\sigma_2), U_2(\Delta\sigma_1,\Delta\sigma_2)$	$\dots$	$U_1(\Delta\sigma_1,P_2^{jam}), U_2(\Delta\sigma_1,P_2^{jam})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
P_1^{jam}	$U_1(P_1^{jam},0), U_2(P_1^{jam},0)$	$U_1(P_1^{jam},\Delta\sigma_2), U_2(P_1^{jam},\Delta\sigma_2)$	$\dots$	$U_1(P_1^{jam},P_2^{jam}), U_2(P_1^{jam},P_2^{jam})$

B. Robust Solutions

So far, our derivations are based on complete knowledge of the eavesdropping channel. However, if Eve is a passive device, this assumption is unrealistic. For the qth player, the computation of the secrecy rate defined in (9) depends on C_q and C_{eq}. Because we assumed that Bob can measure his received interference level and Alice is aware of the channel between herself and her corresponding Bob, the computation of C_q can be done locally. Each component of (unknown) eavesdropping channel can be equivalently shown as the product of some large-scale and small-scale fading parts, so $\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2 = |\bar{\mathbf{G}}_q|^2 {d_{qe}}^{-\eta}$ and $|\mathbf{r}^\dagger \mathbf{G}_q'|^2 = |\bar{\mathbf{G}}_q'|^2 d_{qe}^{-\eta}$, where $\bar{\mathbf{G}}_q$ and $\bar{\mathbf{G}}_q'$ represent the small-scale fading parts, and are, respectively, scalar and $1\times(N_q-1)$ matrix with i.i.d. standard complex Gaussian entries[9]; d_{qe} is the distance between Alice$_q$ and Eve in meters, and η is the path-loss exponent. The secrecy rate is now given by

$$C_q^{sec} = C_q - E_{\left[d_{qe},\, \bar{\mathbf{G}}_q, d_{re},\, \bar{\mathbf{G}}_r, \bar{\mathbf{G}}_q', \bar{\mathbf{G}}_r'\right]}\left[C_{eq}\right] = C_q - E\left[\log\left(1+\frac{\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2 \gamma_q}{\left|\mathbf{r}_q^\dagger \mathbf{G}_q'\right|^2 \sigma_q + \left|\mathbf{r}_q^\dagger \mathbf{G}_r\right|^2 \gamma_r + \left|\mathbf{r}_q^\dagger \mathbf{G}_r'\right|^2 \sigma_r + N_0}\right)\right] \tag{30}$$

where $E_{\left[d_{qe},\dots,\, \bar{\mathbf{G}}_r'\right]}[\bullet] \triangleq E_{d_{qe}}\left[E_{\bar{\mathbf{G}}_q}\left[\dots\left[E_{\bar{\mathbf{G}}_r'}[\bullet]\right]\right]\right]$. We rewrite (30) as

$$E_{\left[d_{qe},\dots,\, \bar{\mathbf{G}}_r'\right]}\left[C_{eq}\right] = E_{\left[d_{qe},\, \mathbf{W}_q, d_{re},\, \mathbf{Y}_q\right]}\left[\log\left|\frac{\mathbf{W}_q \Gamma_{1q} \mathbf{W}_q^H}{\mathbf{Y}_q \Gamma_{2q} \mathbf{Y}_q^H}\right|\right] \tag{31}$$

where $\mathbf{W}_q \triangleq [\bar{\mathbf{G}}_q, \bar{\mathbf{G}}_q', \bar{\mathbf{G}}_r, \bar{\mathbf{G}}_r', 1]$, $Y_q \triangleq [\bar{\mathbf{G}}_q', \bar{\mathbf{G}}_r, \bar{\mathbf{G}}_r', 1]$, and

$$\Gamma_{1q} = \text{diag}\Big\{\big[\gamma_q, \sigma_q \underbrace{[1,\dots,1]}_{N_q-1}, \left(\frac{d_{re}}{d_{qe}}\right)^{-\eta}\gamma_r, \sigma_r \underbrace{[1,\dots,1]}_{N_r-1}\left(\frac{d_{re}}{d_{qe}}\right)^{-\eta}, d_{qe}^{\eta/2}\sqrt{N_0}\big]^T\Big\} \tag{32}$$

$$\Gamma_{2q} = \text{diag}\Big\{\big[\sigma_q \underbrace{[1,\dots,1]}_{N_q-1}\left(\frac{d_{qe}}{d_{re}}\right)^{-\eta}, \gamma_r, \sigma_r \underbrace{[1,\dots,1]}_{N_r-1}, d_{re}^{\eta}\sqrt{N_0}\big]^T\Big\} \tag{33}$$

with diag$\{\mathbf{f}^T\}$ representing an $m\times m$ diagonal matrix whose diagonal entries are the entries of $\mathbf{f}$ with size m. The expectation in (31) w.r.t. $\mathbf{W}_q$ and $\mathbf{Y}_q$ can be efficiently computed using the random matrix result in [31, Appendix A, Lemma 2]. However, according to (31) C_{eq} is still a random variable over the distances d_{qe} and d_{re}. Since we were not able to analytically formulate this distribution, we numerically approximate the expectation of C_{eq} w.r.t. distances. To do this approximation, in simulations, we assume that Eve is uniformly distributed within a circle of a given radius. The center of this circle is determined depending on our simulation scenario (see Section VII for more details). A similar idea can be found in [32]. Another example is [33] where the authors assumed that the location of Eve follows a Poisson point process.

Following the same technique used to manipulate (31), we take the expectation of (18) and end up with:

$$\sigma_q > \frac{\left(|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2\gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}_{rq}'|^2\sigma_r + N_0\right)}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} E_{\left[\bar{\mathbf{G}}_q, \bar{\mathbf{G}}_q'\right]}\left[\frac{|\bar{\mathbf{G}}_q|^2}{|\bar{\mathbf{G}}_q'|^2}\right] - E_{\left[\bar{\mathbf{G}}_r,\, d_q,\, d_r, \bar{\mathbf{G}}_r', \bar{\mathbf{G}}_q'\right]}\left[\left(\frac{d_{re}}{d_{qe}}\right)^{-\eta}\frac{(|\bar{\mathbf{G}}_r|^2\gamma_r + |\bar{\mathbf{G}}_r'|^2\sigma_r + N_0)}{|\bar{\mathbf{G}}_q'|^2}\right]. \tag{34}$$

The numerator and the denominator inside the first expectation term in (34) correspond to a central Wishart matrix [34]. The numerator inside the second expectation term corresponds to the quadratic form of a Wishart matrix, which preserves the Wishartness property [35]. Hence, both expectation terms correspond to the ratio of two Wishart matrices. Since we assumed a MIMO single-stream system, all Wishart matrices are in fact scalars. Hence, the expectations in (34) can be computed using the result in [36, Section 1]. Computing the expectation w.r.t. $d_{qe},\ \forall q$ can be tackled numerically as explained above.

Since (30) and (34) are computable, we can set $U_q(s_1,s_2) = E[C^{sec}(\sigma_q)],\ q\in\{1,2\}$, where the expectation is w.r.t. eavesdropping channel components. Hence, the objective function of (29) can be defined without knowledge of E-CSI. Hence, we can establish Table I to solve (29). A summary of the procedure to solve (29) is given in Algorithm 1 (Line 3 to 14). The solution found after Line 14 for each player is the probability set $\{\alpha_{i,q}\}_{i=1}^M,\ q=1,\dots,Q$. Creating a probabilistic TxFJ power assignment is done by converting the uniform distribution to a probability mass function corresponding to $\{\alpha_{i,q}\}_{i=1}^M$ for $q=1,2$, which is as follows [37]: 1) Generate a uniform random variable $U(0,1)$; 2) Determine the index I such that $\sum_{i=1}^{I-1}\alpha_{i,q} \le U < \sum_{i=1}^{I}\alpha_{i,q}$; 3) Use the TxFJ power $I\Delta\sigma_q$. Such a probabilistic TxFJ power assignment must be done several times to approximate the probability mass $\{\alpha_{i,q}\}_{i=1}^M$. The expected value of secrecy sum-rate can be calculated by averaging achieved secrecy rates using the probabilistic TxFJ

[9]Note that the transmit precoders $\mathbf{T}_q$ and $\mathbf{Z}_q,\ \forall q\in\mathcal{Q}$ are unitary matrices that do not change the characteristics of the original channel matrices $\tilde{\mathbf{H}}_{rq}$, $\tilde{\mathbf{G}}_q$, and $\tilde{\mathbf{G}}_q'$ (see (2) and Section II).

Algorithm 1 Robust Friendly Jamming Control

Initialize: $0 < \gamma_q < P_q,\ \Delta\sigma_q = \frac{P_q^{jam}}{M} \quad \forall q$

1: **repeat**
2: **for** $q = 1$ to 2 **do**
3: **for** $i = 1$ to M **do**
4: Set $\sigma_q = i\Delta\sigma_q$.
5: Compute $\sigma_r = \chi_r, \quad r \neq q$.
6: Compute χ_q.
7: **if** $\sigma_q < \chi_q$ **then** Set $\alpha_{i,q} = 0$.
8: **else** Compute and store $U_q(\sigma_q, \sigma_r)$.
9: **end if**
10: **end for** % do the same loop again but change
11: % line 5 to "Set $\sigma_r = P_r^{jam}$".
12: $U_q(\sigma_q) = \max_{\sigma_r} U_q(\sigma_q, \sigma_r)$.
13: Find $\{\alpha_{i,q}\}_{i=1}^{M}$ by solving (29) (with $U_q(\sigma_q)$ as the summands in the objective function).
14: **end for** % Choose the probability set that maximizes the
15: % secrecy sum-rate.
16: **for** $q = 1$ to 2 **do** % Rate adjustment procedure:
17: **if** $C_q < R_q - \epsilon$ **then** Set $\gamma_q = \gamma_q + \delta$.
18: **if** $\gamma_q > P_q$ **then** Set $\gamma_q = P_q$.
19: **end if**
20: **else**
21: **if** $C_q > R_q + \epsilon$ **then** Set $\gamma_q = \gamma_q - \delta$.
22: **end if**
23: **end if**
24: **end for** % γ_q^* is found.
25: **until** $R_q - \epsilon < C_q < R_q + \epsilon \quad \forall q$.

power assignment[10].

Lines 15 to 24 of Algorithm 1 aim at satisfying the rate constraints for both links, i.e., finding γ_q^* mentioned in (17). For some choice of δ and ϵ, as long as the rate requirements are feasible, the linear adjustment used in lines 16 and 20 converges without the need for central control (similar procedure can be found in [38, Algorithm 1]). Hence, this linear adjustment ensures that each link achieves its minimum target rate. If the target rates are not achievable, then line 17 limits the links to their maximum total transmit powers, i.e., no power will be allocated to TxFJ. The linear adjustments used in line 16 and 20 can be easily added to the price-based game for multiple links in (24) as well. Specifically, the loop between lines 3 and 14 can be replaced with the game (24). Then, at the convergence point of the game (24) or after reaching the maximum iteration number, the rate adjustments in lines 15 and 24 (to satisfy the information rate constraints) can be done for price-based game as well.

VI. Comparison of Signaling Overhead

In this section, we compare the signaling overhead requirement of our proposed distributed schemes.

In the case of price-based FJ control where the links' actions are defined by (24), notice that compared to (17), problem (24) only sets σ_q as the decision variable. This means that the qth link is responsible to only find a solution for its own TxFJ power. Each link needs to solve (24) and start transmission with the obtained solutions. This makes up one iteration of price-based FJ control. At the next iteration, each link q needs to recalculate the pricing factor λ_q and update the parameters of its objective function. This update procedure taken before solving individual problems is the *message exchange* phase of our distributed algorithm. Simplifying λ_q in (25) we have

$$\lambda_q = \sum_{\substack{r=1 \\ r\neq q}}^{Q} |\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2 \frac{(1+\frac{\gamma_r}{a_r})-1}{b_r(1+\frac{\gamma_r}{a_r})} + |\mathbf{r}_r^\dagger \mathbf{G}'_q|^2 \frac{(1+\frac{\gamma_r}{f_r})-1}{g_r(1+\frac{\gamma_r}{f_r})} \tag{35}$$

where

$$b_r = \frac{\sum_{\substack{t=1 \\ t\neq r}}^{Q} (|\mathbf{d}_r^\dagger \mathbf{H}_{tr}|^2 \gamma_t + |\mathbf{d}_r^\dagger \mathbf{H}'_{tr}|^2 \sigma_t) + N_0}{|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2} \tag{36}$$

$$g_r = \frac{\sum_{\substack{t=1 \\ t\neq r}}^{Q} (|\mathbf{r}_r^\dagger \mathbf{G}_t|^2 \gamma_t + |\mathbf{r}_r^\dagger \mathbf{G}'_t|^2 \sigma_t) + |\mathbf{r}_r^\dagger \mathbf{G}'_r|^2 \sigma_r + N_0}{|\mathbf{r}_r^\dagger \mathbf{G}'_q|^2} \tag{37}$$

are interference (plus noise) levels at the rth link and Eve, respectively. Furthermore, the terms $\frac{\gamma_r}{a_r}$ and $\frac{\gamma_r}{f_r}$ are SINR levels at the rth link and Eve, respectively. From (35), one can deduce that to calculate the price in (25) and the optimal TxFJ power in (26), the qth link, $q \in \mathcal{Q}$, needs to acquire the following: 1) interference and SINR levels at both the rth link and eavesdropper(s) while eavesdropping on the rth link, $r \neq q,\ r \in \mathcal{Q}$, and 2) the the equivalent channel gains (after beamforming) caused from the information and TxFJ signals of the qth link on the rth link and eavesdropper's receptions, i.e., $|\mathbf{r}_q^\dagger \mathbf{G}_q|^2, |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2$ and $|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2, |\mathbf{r}_r^\dagger \mathbf{G}'_q|^2,\ \forall r \neq q \in \mathcal{Q}$[11]. On the contrary, a centralized approach aims to solve (17) in one shot. This necessitates knowledge of all channel gains between legitimate nodes and eavesdropper(s). By distributing the problem between links in the price-based approach, the problem can be solved iteratively and the message exchange reduces to interference and SINR levels plus a portion of channel gains, which are relatively easier to obtain.

In the greedy FJ control, the price $\lambda_q = 0,\ \forall q \in \mathcal{Q}$. Therefore, there is no need to update the objective function of the qth link, $q \in \mathcal{Q}$, after each iteration because we showed that the maximum available TxFJ power maximizes the secrecy rate of the qth link in the greedy approach. This greatly reduces the amount of message exchange at the cost of losing the performance.

In Section V, we established another framework that relaxes knowledge of E-CSI at legitimate links. Notice that a According to Algorithm 1, each link's utility function is set to $E[C^{sec}]$, where $E[\bullet]$ is the expectation over eavesdropping channels. As for the amount of message exchange, this approach requires SINR levels of both links (which is the same as that of price-based scheme) plus the expectation of leaked rate at Eve where the expectation is w.r.t. E-CSI components.

[10]Such a procedure for practical implementation of mixed solutions may not be of interest because all probabilistic transmissions have to be done in one channel realization. However, in practical scenarios, the coherence time is not long enough to accommodate more than a few transmissions. We examine this deficiency in the simulation section.

[11]Clearly, recalculation of pricing factor and the objective function requires a link to know the eavesdropper's CSI (E-CSI), which is not practical when eavesdroppers are passive nodes. The explanation regarding how to relax such knowledge is discussed in detail in Section V.

TABLE II: Comparison of message exchange requirements for the proposed approaches.

Method	**Utility Functions,** $\forall q \in \mathcal{Q}$	**# of Players** (Q)	**Type of NE (How achieved)**	**Local optimality of the solution**	**Amount of Message Exchange** $\forall q$
Greedy FJ Control	C_q^{sec}	$Q \geq 2$	Pure NE (one-shot)	Not guaranteed	None
Price-based FJ Control (Full E-CSI)	$C_q^{sec} - \lambda_q \sigma_q$	$Q \geq 2$	Pure NE (iterative)	Guaranteed	$b_r,\ \frac{a_r}{b_r},\ d_r,\ \frac{c_r}{d_r},\ \lvert\mathbf{d}_r^\dagger \mathbf{H}'_{qr}\rvert^2,$ $\lvert\mathbf{r}_r^\dagger \mathbf{G}'_q\rvert^2\ \forall r \neq q,\ r \in \mathcal{Q}$
Price-based FJ Control (Unknown E-CSI)	$E[C_1^{sec} + C_2^{sec}]$	$Q = 2$	Mixed NE (one-shot)	Guaranteed	$\frac{a_r}{b_r},\ E[\log(1 + \frac{c_r}{d_r})],\ \forall r \neq q,\ r \in \mathcal{Q}$
[39]	C^{sec}	$Q \geq 2$	Pure NE (Iterative)	Guaranteed	Same as Price-based FJ control under Full E-CSI + Calculation of Lagrange multipliers to satisfy cooperative jammers' power budgets
[40]	C_q^{sec}	$Q \geq 2$	Pure NE (iterative)	Not guaranteed	$b_r,\ \frac{a_r}{b_r},\ d_r,\ \frac{c_r}{d_r},$ $\forall r \neq q,\ r \in \mathcal{Q}$

In what follows, we have provided a detailed analysis of the messaging overhead of the techniques in [39], [41], [40] and compare them to ours[12]. One important note about the works in [39], [40] is that both of these works assume full knowledge of E-CSI in their analyses. Hence, we compare these schemes with our price-based FJ method for which full knowledge of E-CSI must be available. We first give a summary of each of these works and then characterize the amount of messaging overhead they impose on the network.

The authors in [39] investigated the secrecy sum-rate maximization problem in an interference network with cooperative jammers. The decision variables for their optimization problem are the powers of legitimate links and the powers of cooperative jammers. The work in [39] also imposes a constraint on the total power budget of the cooperative jammers. This is a shared constraint between the legitimate links, and cannot be decomposed to enable distributed implementation.

The work in [41] studied power control for a dense network of small cells that coexist with some macrocells. They focused on the uplink communication of small-cell networks and proposed a distributed power optimization to maximize the sum of uplink rates subject to constraints on transmission powers as well as a tolerable interference level at macrocell users. The solution method in [41] closely follows the work in [39]. The constraint on interference level at macrocell users is a shared constraint and cannot be decomposed to enable distributed implementation. Thus, the amount of overhead in [41] is comparable to [39].

The work in [40] considers the Physical-layer security for a multi-channel interference network with full-duplex-enabled nodes. The authors did not assume that Alices are capable of generating TxFJ and only focused on the power allocation of information signals to study the problem of greedy secrecy-rate maximization. They proposed a water-filling-like power allocation to different channels of a given link. While the system model in [40] is quite different from ours in terms of adopting multi-channel and full-duplex communications, due to the greedy nature of this algorithm, we can compare this method to our proposed greedy method. In other words, no pricing model (i.e., any attempt on secrecy sum-rate maximization) was considered in [40]. We found out that the method in [40] requires each link to know the interference and SINR at the receiver as well as the interference and SINR at Eve. In contrast, in our work, due to the adoption of TxFJ, no messaging is needed to implement the greedy algorithm.

[12]It is difficult to compare our approach to those in [9], [12], [13], [42], as such works differ in the system model and/or optimization variables.

Table II shows a more unified comparison between our methods (greedy FJ control, price-based FJ control with perfect E-CSI and imperfect E-CSI) and those in [39] and [40] in terms of messaging overhead.

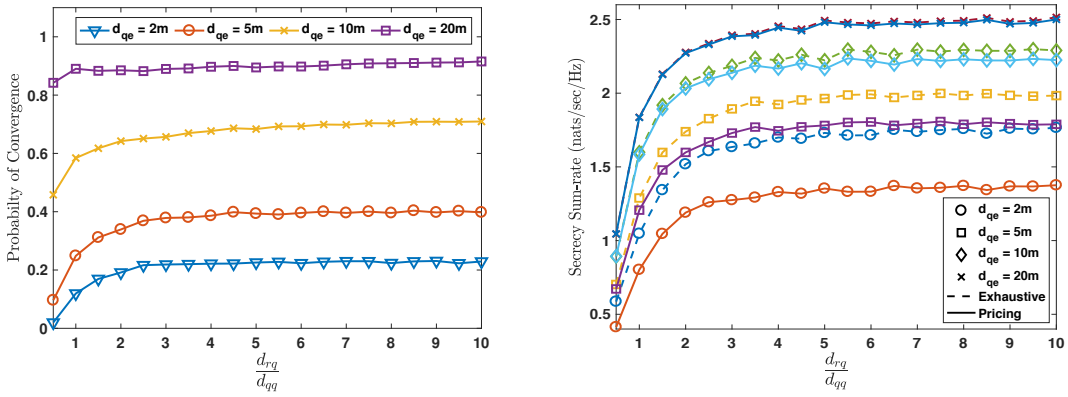
VII. Numerical Results

A. Multi-link Scenario

We consider a four-link network with one eavesdropper. To assess different aspects of our method, we manipulate the placement of these links as well as the eavesdropper from one simulation to another.

Fig. 4 (a) shows the probability of convergence of the price-based game in (24) under different interference levels. The total power of each Alice is $P_q = 13$ dBm $\forall q \in \mathcal{Q}$. We also set the rate demands such that $\gamma_q = 10$ dBm $\forall q \in \mathcal{Q}$. All interfering distances $d_{rq},\ (r,q) \in Q, r \neq q$ are equal to each other. Also, the direct distance between Alice$_q$ and Bob$_q$ is set to $d_{qq} = 10$ m, $\forall q \in \mathcal{Q}$. The path-loss exponent is set to $\eta = 2.5$, and $N_0 = 0$ dBm. We ran the game (24) iteratively between all links using the Jacobi iterative method. For each point on a curve in Fig. 4 (a), we calculate the probability of convergence by counting the number of times that solving (24) iteratively for all links converges to a point, and divide this number by a total of 1000 times running the iterative optimization. Each run creates a different realization of small scale-fading components of all channels. The maximum number of iterations was set to 50. We plotted the the probability of convergence of our algorithm vs. the ratio $\frac{d_{rq}}{d_{qq}}$ for four different locations of Eve. Same as interfering distances, the distance between all Alices and Eve, d_{qe} $\forall q \in \mathcal{Q}$ are equal to each other.

It can be seen that when Eve is close to Alices, the probability of convergence is very low, such that for $\frac{d_{rq}}{d_{qq}} = 10, \forall (r,q) \in \mathcal{Q}$ only a convergence probability of 0.2 can be expected. The reason is that when Eve is close to Alices, large amounts of TxFJ is needed to guarantee positive secrecy. In some realizations where the required TxFJ power exceeds the maximum available power at Alice, achieving positive secrecy for some or all Alices becomes infeasible, which also violates the first condition of Proposition 1. Thus, the NE uniqueness and consequently the convergence of iterations cannot be guaranteed. However, it can be seen that as Eve becomes farther from Alices, the convergence probability increases.



(a) (b)

Fig. 4: (a) Probability of convergence (b) Secrecy sum-rate of price-based FJ control for different interference levels and different Eve locations, $(Q = 4, \frac{P_q}{N_0} = 30$ dB$, N_q = 5, M_q = 4, L = 4)$.

Lastly, it can be seen that the second condition in Proposition 1 is not very strict, as for $\frac{d_{qq}}{d_{rq}} > 3$, no noticeable improvement in convergence can be seen.

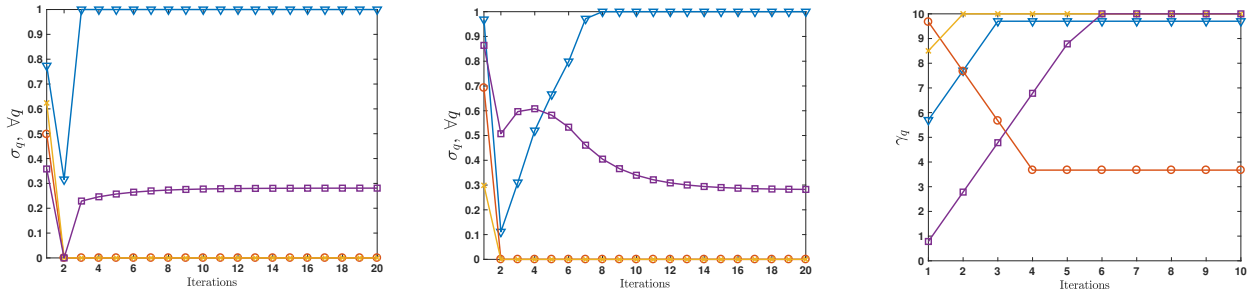
Fig. 4 (b) shows the resulting secrecy sum-rate of the four curves plotted in Fig. 4 (a). We compared the performance of our price-based FJ control with that of an exhaustive search method which solves (17). All solid/dashed curves show the resulting secrecy sum-rate of the price-based/exhaustive approach[13]. A pair of curves with the same markings show the performance of the two methods for a certain value of d_{qe}. It can be seen that for a relatively far Eve, which satisfies the first condition of Proposition 1, there is not much difference between the price-based approach and the exhaustive search approach. This indicates that the local optimum point(s) of the secrecy-sum-rate becomes the global optimum when the conditions of Proposition 1 are satisfied. It should be noted that for both Fig. 4 (a) and (b), similar results can be obtained if instead of changing the proximity of Eve to Alices, all links adopt high information rate demands.

Fig. 5 (a) and (b) show the convergence of the TxFJ power of each link for price-based FJ control under Jacobi and Gauss-Seidel methods, respectively. Both figures are plotted in the same channel realization with the same placement of links. The initial TxFJ power is set randomly for each link. Each curve shows the value of TxFJ of a link normalized by the maximum available TxFJ of that link over 20 iterations. Although the Jacobi method was not proved to be convergent in our analyses, we did not find any case where Jacobi method does not follow the same convergence behavior as the Gauss-Seidel method. Furthermore, the Jacobi method was found to be a bit faster in rate of convergence, as all links simultaneously update their TxFJ powers compared to the Gauss-Seidel method in which at each iteration only one link updates its TxFJ power.

Fig. 5 (c) shows the convergence of the rate adjustment for one channel realization. We randomly initialize γ_q, $\forall q$, and then the rate adjustments are done the same way as it is shown in lines 15 to 24 of Algorithm 1. The maximum value of γ_q in this simulation is 10 dBm. Each iteration of Fig. 5 (c) consists of running the game (24) until the convergence. Then, the qth $q \in \mathcal{Q}$, link adjusts γ_q by increasing or decreasing it. During our simulation, we found out that setting δ (as the increment of γ_q) to $0.2\gamma_q$ gives us a fast and reliable convergence for all links. We terminate these iterations once the information rate of a link is within a tight neighborhood of its rate demand (e.g., $0.95R_q < \log(1+\frac{\gamma_q}{a_q}) < 1.05R_q$). It can be seen that the convergence of rate adjustments is fairly quick once a suitable increment for the power of information signal and a suitable neighborhood around rate demands is considered.

Fig. 6 (a) and (b) show the secrecy sum-rate of the greedy FJ control compared to the price-based FJ control and exhaustive search method for different power constraints of Alices. We assumed that all Alices use the same amount of power constraint. For both figures of Fig. 6, all Q links as well as the eavesdropper are randomly placed in a circle, namely, the simulation region with radius $r_{circ} = 25$ m. The distance between the transmitter and the receiver of each link is set to be a constant $d_{link} = 5$ m. The required rate demand for each link is set to $R_q = 2$ nats/sec/Hz, $\forall q \in \mathcal{Q}$. The maximum number of iteration for both the pricing part and rate adjustment is set to 50. We ran each method for a total of 30 link placements. For each placement, we tested 100 channel realizations. It can be seen that for low transmit powers, the greedy FJ has a comparable secrecy sum-rate to the exhaustive approach, verifying Proposition 3. As the transmit power increases, the secrecy sum-rate of the greedy method becomes more inferior to the exhaustive and pricing approaches, as high interference decreases the information rate of legitimate links, thus lowering the total secrecy in the network. We see that for the simulation in Fig. 6 (a) which is a more realistic scenario compared to the settings of Fig. 4 (b), the price-based FJ control has a comparable performance to the exhaustive search for low transmit powers, indicating that convergence is a less concerning issue in more realistic scenarios. Fig. 6 (b) shows the same comparison with the difference that now the four links' placements is done in a circle with $r_{circ} = 20$ m and $d_{link} = 15$ m. It can be seen that the secrecy sum-rate of greedy FJ control is very close to that of the exhaustive search. The reason is that this simulation is done in a denser network in which each link experiences more interference on links and

[13]To do exhaustive search, we discretize TxFJ powers of all links to very small increments and find the combination that results in the highest secrecy sum-rate.



(a) (b) (c)

Fig. 5: Convergence of (a) price-based FJ control (Jacobi Method) (b) price-based FJ control (Gauss-Seidel) (c) rate demands, $(Q = 4, \frac{P_q}{N_0} = 30$ dB$, N_q = 5, M_q = 4, L = 4)$

each Bob receives a weaker information signal. Thus, each link has to spend a lot of its power on the information signal to meet its rate demand ($R_q = 2$ nats/sec/Hz, $\forall q \in \mathcal{Q}$). The rest of the power left for TxFJ is small, forcing each user to spend all the remaining power on TxFJ to preserve positive secrecy. Such network conditions satisfy the conditions of Proposition 2, allowing the greedy FJ control to have a performance close to that of the exhaustive search method.

B. Two-link Scenario

In all simulations of this part, the noise floor at both Bobs and at Eve is set to $N_0 = -50$ dBm. The information rate constraints are chosen such that Alices allocate no more than $1/3$ of their total transmit powers for the information signal. In all figures, the horizontal axis is the horizontal coordinate for the center of the circle within which Eve is uniformly distributed. Each point on every plot is the result of averaging over 10 random locations for Eve (in order to approximate (30) w.r.t. distances). At each random location, 500 channel realizations are simulated and then averaged. We compare the performance of the proposed price-based FJ control under complete/partial knowledge of E-CSI (indicated by "Pricing (Full E-CSI)"/"Robust") with other methods including when every link allocates all its power to information signal (indicated by "No Jamming"), exhaustive search (indicated by "Exhaustive Search"), and the greedy FJ control (indicated by "Greedy FJ").

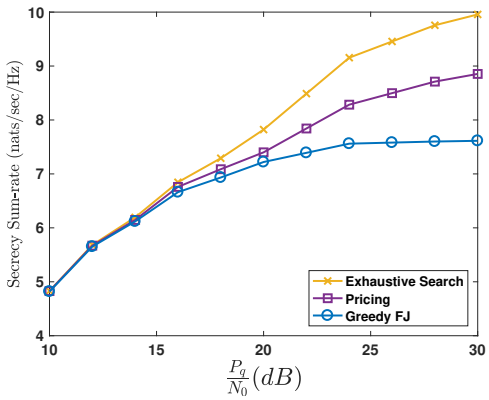
In Fig. 7, we depict, individual secrecy rates for when constraint (18) is taken into account in the price-based FJ control (indicated as "Pricing (Full E-CSI) and for when it is not (indicated as "Pricing (No Positive Secrecy)"). It can be seen that applying constraint (18) in the price-based FJ control significantly affects the secrecy sum-rate such that if it is overlooked, the performance of the price-based FJ control can be even lower than the greedy approach with zero secrecy rate for one or both links at some locations of Eve.

In Fig. 8 (a), we compare the performance of Algorithm 1 (indicated as "Robust") with other approaches. The spatial distribution for Eve is the same as in previous simulation, but with $P_q = 10$ dBm. For the pricing method with full CSI, transmitters sequentially apply (26) to optimize their TxFJ powers (i.e., the Gauss-Seidel method is used [27, Chapter 3]). Note that because the performance of the pricing method generally depends on the starting point for the iterative procedure (except for when the conditions of Proposition 1 hold), for each channel realization, the performance of the pricing method is the result of averaging the convergence point of Gauss-Seidel method over 30 different starting points. For the robust TxFJ control algorithm, we use 8 bits to quantize power levels. After finding the probability set $\{\alpha_{i,q} : i = 1, \ldots, M\}$ that maximizes the expected utility in (29), probabilistic assignment of the TxFJ powers in robust jamming control is done as follows. The qth player generates a sample from the probability set $\{\alpha_{i,q} : i = 1, \ldots, \}$. Depending on the value of this sample, player q selects TxFJ power, say $i\Delta\sigma_q$, and starts transmitting. This procedure is repeated 50 times per channel realization and the expected utility in (29) is approximated by averaging over these repeats. It can be seen that the robust approach is 25% better than the greedy approach. When the eavesdropping channel is known, the advantage of price-based FJ becomes more significant.

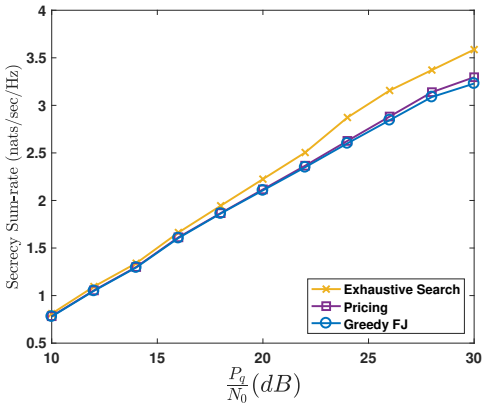
The expected value in (29) must be computed after averaging over several samples of data transmissions for one channel realization. However, in practical scenarios, the coherence time is not long enough to accommodate more than a few transmissions. In order to test this limitation, we compare the performance of robust optimization between 50 data transmissions and 1 data transmission per each channel realization so as to approximate the expected utility in (29). To reduce the effect of other parameters on this comparison, we simulated 50 channel realizations at each location of Eve. It can be seen in Fig. 8 (b) that averaging over 1 data transmission (indicated as "Robust(1)") does not affect the secrecy sum-rate very much, compared to averaging over 50 data transmissions (indicated as "Robust(50)"). Therefore, the robust jamming control can also be implemented in channels with low coherence times.

VIII. Conclusions

In this paper, we studied distributed design of FJ control in a MIMO wiretap interference network. We showed that greedy FJ is not an optimal approach in terms of total network secrecy rate. Accordingly, we designed a price-based TxFJ control that guarantees a local optimum point in maximizing the secrecy sum-rate. Through simulations, we observed a noticeable improvement in the secrecy sum-rate when pricing is leveraged for FJ control. We then introduced uncertainty in the eavesdropping channel and designed a robust method.



(a)



(b)

Fig. 6: Optimality of the greedy FJ control under different scenarios, $(Q = 4, N_q = 5, M_q = 4, L = 4)$

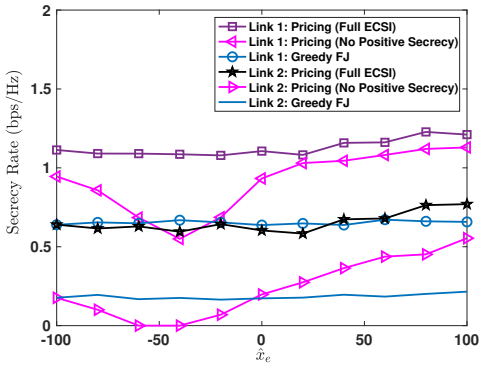


Fig. 7: Effect of SIC on individual secrecy rates: $\big(\text{Alice}_1 = (-50, 10),\ \text{Bob}_1 = (5, 10),\ \text{Alice}_2 = (-50, -10), \text{Bob}_2 = (50, 10), \hat{y}_e = 0, \hat{r}_e = 10,\ P_q = 0$ dBm, $N_q = 3, M_q = L = 1\big)$.

We showed via simulations that the robust method achieves a higher secrecy sum-rate than the greedy FJ approach.

ACKNOWLEDGEMENTS

This research was supported in part by the National Science Foundation (grants # CNS-1409172, CNS-1513649, IIP-1265960, and CNS-1617335), Australian Research Council (Discovery Early Career Researcher Award DE150101092), and Qatar Foundation (grant # NPRP 8-052-2-029). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the NSF, ARC and QF.

REFERENCES

[1] O. Koyluoglu, H. El Gamal, L. Lai, and H. Poor, "On the secure degrees of freedom in the k-user gaussian interference channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 384–388.

[2] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[3] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.

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

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

[6] S. Fakoorian and A. Swindlehurst, "MIMO interference channel with confidential messages: Game theoretic beamforming designs," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Nov. 2010, pp. 2099–2103.

[7] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling," in *Proc. IEEE Globecom Conf.*, Nov. 2009, pp. 1–6.

[8] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Interference-assisted secret communication," in *Proc. IEEE Inf. Theory Workshop*, May 2008, pp. 164–168.

[9] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3810–3823, Jul. 2015.

[10] D. Park, "Secrecy rate improvement based on joint decoding in MIMO wiretap channels with a helping interferer," *To appear in IEEE Transactions on Vehicular Technology*, 2016.

[11] L. Li, A. P. Petropulu, Z. Chen, and J. Fang, "Improving wireless physical layer security via exploiting co-channel interference," *IEEE J. Select. Topics Signal Process.*, vol. 10, no. 8, pp. 1433–1448, Dec. 2016.

[12] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[13] L. Li, C. Huang, and Z. Chen, "Cooperative secrecy beamforming in wiretap interference channels," *IEEE Signal Process Lett.*, vol. 22, no. 12, pp. 2435–2439, Dec. 2015.

[14] L. Ruan, V. K. N. Lau, and M. Z. Win, "Generalized interference alignment ;part II: Application to wireless secrecy," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2688–2701, May 2016.

[15] A. Alvarado, G. Scutari, and J. S. Pang, "A new decomposition method for multiuser DC-programming and its applications," *IEEE Trans. Signal Process.*, vol. 62, no. 11, pp. 2984–2998, 2014.

[16] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *2013 IEEE Symp. Security and Privacy*, May 2013, pp. 160–173.

[17] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

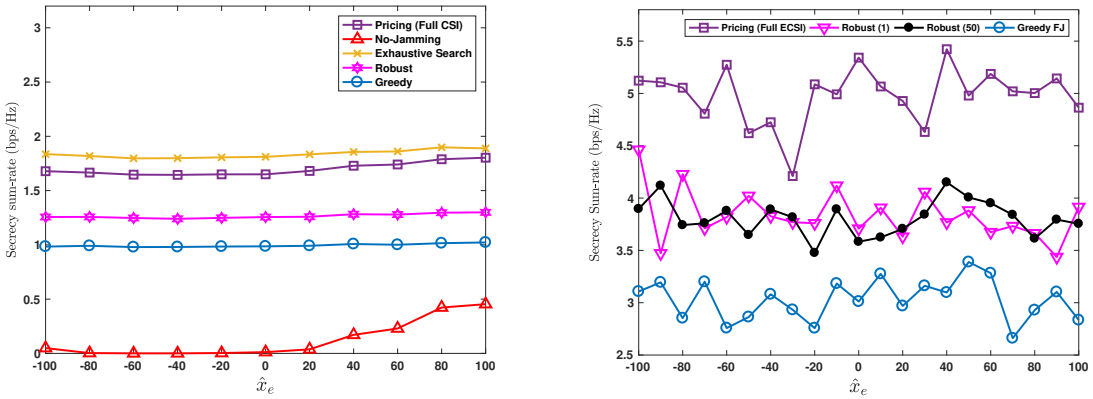
[18] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP Conf.*, Apr. 2009, pp. 2437–2440.

[19] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[20] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *IEEE J. Select. Areas Commun.*, vol. 21, no. 5, pp. 684–702, June 2003.

[21] X. He and A. Yener, "The interference wiretap channel with an arbitrarily varying eavesdropper: Aligning interference with artificial noise," in *Proc. 50th Annu. Allerton Conf. Commun., Contr., and Comput.*, Oct. 2012, pp. 204–211.

[22] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating opti-



(a) (b)

Fig. 8: Effect of (a) Eve's location (b) number of transmissions on the secrecy sum-rate for two links:
(a) : $\text{Alice}_1 = (-40, 20), \text{Bob}_1 = (40, 20), \text{Alice}_2 = (-40, -20), \text{Bob}_2 = (40, -20), \hat{y}_e = 25,\ \hat{r}_e = 20,\ P_q = 10$ dBm.
(b) : $\text{Alice}_1 = (-20, 20), \text{Bob}_1 = (20, 20), \text{Alice}_2 = (-20, -20), \text{Bob}_2 = (20, -20), \hat{y}_e = 10,\ \hat{r}_e = 20,\ P_q = 10$ dBm.

mization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

[23] P. Siyari, M. Krunz, and D. N. Nguyen, "Secure power allocation with rate demands in MIMO interference networks," University of Arizona Department of ECE, Tech. Rep., 2017. [Online]. Available: http://wireless.ece.arizona.edu/sites/default/files/techrep_Peyman_2017.pdf

[24] G. Scutari, D. Palomar, and S. Barbarossa, "Optimal linear precoding strategies for wideband noncooperative systems based on game theory, part I: Nash equilibria," *IEEE Trans. Signal Process.*, vol. 56, no. 3, pp. 1230–1249, Mar. 2008.

[25] G. Eichfelder and J. Jahn, *Vector and Set Optimization*. New York, NY: Springer New York, 2016.

[26] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave N-person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, 1965.

[27] D. P. Bertsekas and J. N. Tsitsiklis, Eds., *Parallel and Distributed Computation: Numerical Methods*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1989.

[28] P. Siyari, M. Krunz, and D. N. Nguyen, "Price-based friendly jamming in a MISO interference wiretap channel," in *Proc. IEEE INFOCOM Conf.*, Apr 2016, pp. 1–9.

[29] J. F. Nash, "Equilibrium points in N-person games," *National Academy of Sciences*, vol. 36, no. 1, pp. 48–49, 1950.

[30] H. Peters, *Finite Games*. Berlin, Heidelberg: Springer Berlin, 2015.

[31] A. Lozano, A. Tulino, and S. Verdu, "High-snr power offset in multi-antenna communication," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4134–4151, Dec. 2005.

[32] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.

[33] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers," in *Proc. IEEE ICC Conf.*, Jun. 2011, pp. 1–5.

[34] Y. Fujikoshi, V. V. Ulyanov, and R. Shimizu, *Wishart Distribution*. John Wiley & Sons, Inc., 2011, pp. 29–46.

[35] C. Rao, *Linear statistical inference and its applications*, 2nd ed. New York, NY: Wiley, 1973.

[36] G. Pederzoli, "On the ratio of generalized variances," *Commun. in Stat. - Theory and Methods*, vol. 12, no. 24, pp. 2903–2909, Jan. 1983.

[37] M. Boon, *Generating random variables*. [Online]. Available: http://www.win.tue.nl/~marko/2WB05/lecture8.pdf

[38] W. Yu, G. Ginis, and J. Cioffi, "Distributed multiuser power control for digital subscriber lines," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 5, pp. 1105–1115, Jun. 2002.

[39] A. Alvarado, G. Scutari, and J.-S. Pang, "A new decomposition method for multiuser dc-programming and its applications," *IEEE Trans. Signal Process.*, vol. 62, no. 11, pp. 2984–2998, Jun. 2014.

[40] X. Tang, P. Ren, and Z. Han, "Distributed power optimization for security-aware multi-channel full-duplex communications: A variational inequality framework," *Accepted in IEEE Trans. Commun.*, 2017.

[41] J. Zheng, Y. Wu, N. Zhang, H. Zhou, Y. Cai, and X. Shen, "Optimal power control in ultra-dense small cell networks: A game-theoretic approach," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4139–4150, 2017.

[42] D. Park, "Weighted sum rate maximization of MIMO broadcast and interference channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 1742–1753, Mar. 2016.

Peyman Siyari received the M.Sc. degree of Electrical Engineering from AmirKabir University of Technology, Iran, in 2013. He is working toward his Ph.D. at the University of Arizona. His research interests include physical-layer security, convex optimization in signal processing, and game theory.

Marwan Krunz is the Kenneth VonBehren Endowed Professor in the Department of ECE at the University of Arizona. He is also an affiliated faculty with the University Technology Sydney. He co-directs the Broadband Wireless Access and Applications Center, a multi-university industry-focused NSF center that includes 16+ industry affiliates. He received his Ph.D. degree in electrical engineering from Michigan State University in 1995 and joined the University of Arizona in January 1997, after a postdoctoral stint at the University of Maryland. In 2010, he was a Visiting Chair of Excellence at the University of Carlos III de Madrid. He previously held various visiting research positions at University Technology Sydney, INRIA-Sophia Antipolis, HP Labs, University of Paris VI, University of Paris V, University of Jordan, and US West Advanced Technologies. He has published more than 250 journal articles and peer-reviewed conference papers, and is a co-inventor on several US patents. He is an IEEE Fellow, an Arizona Engineering Faculty Fellow (2011-2014), and an IEEE Communications Society Distinguished Lecturer (2013 and 2014). He was the recipient of the 2012 IEEE TCCC Outstanding Service Award. He received the NSF CAREER award in 1998. He has served and continues to serve as the editorial board of several IEEE journals, the steering and advisory committee of numerous conferences, and the panel member of several funding agencies. Effective January 2017, he will be the next EiC for IEEE Transactions on Mobile Computing. He was a keynote speaker, an invited panelist, and a tutorial presenter at numerous conferences. See http://www2.engr.arizona.edu/∼ krunz/ for more details.

Diep N. Nguyen is a faculty member of the School of Computing and Communications, University of Technology Sydney (UTS). He received M.E. and Ph.D. in Electrical and Computer Engineering from University of California, San Diego and The University of Arizona, respectively. Before joining UTS, he was a DECRA Research Fellow at Macquarie University, a member of technical staff at Broadcom (California), ARCON Corporation (Boston), consulting the Federal Administration of Aviation on turning detection of UAVs and aircraft, US Air Force Research Lab on anti-jamming.