Secure Power Allocation with Rate Demands in MIMO Interference Networks

Peyman Siyari[1], Marwan Krunz[1], 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

Technical Report

TR-UA-ECE-2017-1

Last Update: July 16, 2017

Abstract

In this paper, we propose a distributed interference management algorithm for a single-stream MIMO interference network that is tapped by an external eavesdropper. The network consists of multiple, concurrently active links that may interfere with each other. A multi-antenna eavesdropper (Eve) is present in the communications range of these transmissions. Along with its information signal, each legitimate transmitter (Tx) creates a bogus signal, known as *transmit-based friendly jamming* (TxFJ), to confuse Eve. Although generating TxFJ protects the link from eavesdropping, it creates unwanted interference at other unintended but legitimate links, thus degrading their throughput. Using noncooperative game theory, we design a distributed method for reducing interference on legitimate receivers and increasing the aggregate interference at Eve. Each link is a player in the game. It seeks to maximize its secrecy rate subject to a given information-rate constraint. The strategy profile of each player is to control the amount of TxFJ it generates. Because a pure noncooperative game may not always 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 assumption of exact knowledge of eavesdropping channels, we show that the price-based game forces transmitters to reduce their TxFJ. We also show that this game has a comparable secrecy sum-rate to a centralized approach. We then relax the assumption of perfect knowledge of eavesdropping channels at each link, and leverage mixed strategic games to provide robust

solutions to the distributed secrecy sum-rate maximization problem. Simulations are conducted to show that these solutions lead to operating points that are 25% more efficient than those of the pure noncooperative game.

Index Terms

Wiretap interference channel, friendly jamming, pricing, pure and mixed strategic 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.

In contrast to its detrimental role in achieving the capacity limit of a shared wireless channel, interference can play a positive role in providing physical layer (PHY-layer) security for wireless transmissions [1]. The need for PHY-layer security is triggered by emerging applications such as the Internet-of-things (IoT), smart spaces/cities, etc., for which traditional cryptographic methods can be difficult to implement. For example, many IoT devices do not have enough computational power to execute encryption/decryption techniques in a timely manner. Moreover, these devices are vulnerable to security attacks that attempt to break their cryptographic defenses; such attacks rely on high computational capabilities of adversarial systems [2]. In contrast, PHY-layer security offers perfect secrecy, irrespective of the adversary's computational power [3].

As the name suggests, PHY-layer security relies on the characteristics of the Physical layer, including the channel state information (CSI) and signal precoding. While many research works can be classified as

PHY-layer security studies, our main focus in this paper is on information-theoretic secrecy. In particular, we are primarily interested in exploiting/managing interference in the context of information-theoretic PHY-layer secrecy [4]. The main goal of information-theoretic secrecy is to improve the channel state at the legitimate receiver (Rx), relative to the channel state at the eavesdropper (Eve). In his seminal work, Wyner showed that if the channel between a legitimate transmitter (Tx) and its corresponding Rx is better than the channel between the Tx and Eve, then a nonzero rate can be securely communicated between Tx and Rx, irrespective of the computational power of Eve [3]. Thus, the notion of *the degraded wiretap channel* was established to signify the basic setting of an information-theoretic secure communication. There are several scenarios in which the Rx's channel advantage arises naturally, including near-field communications (NFC) and medical communications where the proximity between the legitimate parties can guarantee information-theoretic secrecy.

However, achieving the channel advantage as a requirement of information-theoretic secrecy 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 [5] and references therein) that rely on generating a bogus signal called *friendly jamming (FJ)* signal [6] whose purpose is to confuse a nearby eavesdropper. In this method, the legitimate Tx (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 [6] proposed a simple version of this technique that relies on MIMO zero-forcing to ensure that the FJ signal falls in the null-space of the channel between Alice and Bob.

The interest in using FJ *for a single link* is driven by pragmatic considerations, and not necessarily due to its optimality. In fact, it was shown in [7] that in a degraded wiretap channel and perfect knowledge of Eve's location, it is not optimal to use FJ to secure a single link. It was shown in [6] that under FJ, a nonzero secrecy rate can always be achieved for a sufficiently high transmit power, regardless of Eve's location.

In a multi-link scenario, several transmitters wish to convey their messages simultaneously to several legitimate receivers. Hence, the FJ signal of each transmitter must be designed to not interfere with other unintended (but legitimate) receivers in the network. Such a design imposes centralized optimizations, and hence can be quite 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. Thus the design must ensure that a given link's transmission is secured from other eavesdropping links. 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].

For a two-link ICCM model, general inner and outer bounds for the perfect secrecy capacity region were derived in [8]. The authors in [9] investigated a two-user MIMO ICCM setting, and utilized bargaining methods (i.e., Kalai-Smorodinsky bargaining solution) to provide a framework that balances network performance and fairness. Under the WIC model, the feasibility of achieving positive secure degrees of freedom for each legitimate link in the network was studied in [1] and [10].

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 shown in a scenario where the secrecy of a number of links was enhanced by other active links in the network [11]. For instance, in [12] 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

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

second link. Other instances of exploiting interference for secure communications where only one user can be eavesdropped on are found in [13], [14], and [15]. To provide secrecy for all the links in the network, the authors in [16] studied two transmitter-receiver-eavesdropper triples (i.e., each link is being eavesdropped on by a separate eavesdropper that does not cooperate with the other eavesdropper), and proposed a cooperative beamforming approach to achieve the maximum secure degree of freedom for both users. Given knowledge of co-channel interference at receivers, a cooperative transmission alignment scheme between transmitters was established such that their respective receivers will get interference-free signals and the eavesdropper corresponding to each link will experience interference. Generalizations of interference alignment techniques for PHY-layer secrecy were accomplished in [17], [18], and [19].

The work in [20] studied power control in an interference network to maxmize the secrecy sum-rate. An interference network tapped by an external eavesdropper is considered in [20] where multiple cooperative jammers assist legitimate links by generating friendly jamming signals. A distributed power control scheme was proposed to maximize the secrecy sum-rate of the network. The work in [20] considers cooperative jamming as its main secrecy method. Specifically, a fixed number of nodes are exclusively used for cooperative jamming, and all legitimate links can use these cooperative jammers. However, in our work, we do not consider a node specifically assigned to be a jammer. We allow each legitimate transmitter to generate TxFJ itself. Moreover, the use of cooperative jamming nodes in [20] may not be practical due to deployment costs. On the other hand, it was shown in [21] that cooperative jamming can be challenged if the eavesdropper provides a certain separation between its antennas.

C. Overview of Proposed Approach

We consider a network of multiple links that coexist in the same vicinity and may interfere with one another. The main goal here is to hide the transmission of each link from external eavesdroppers. Although previous studies answer many questions regarding perfect secrecy in interference networks, implementation of these ideas requires full cooperation between the legitimate links in terms of multiuser encoding/decoding. In several scenarios, e.g., IoT devices, nodes cannot perform multiuser encoding/decoding

due to their limited capabilities. Thus, practical methods should allow for a distributed implementation as well as low signaling overhead. On another note, while studies that focus on determining the secrecy degrees of freedom (e.g., [1], [22], [23], [14]) provide valuable insights into interference networks, these studies assume high signal-to-interference-plus-noise-ratio (SINR), limiting their applicability. Hence, the achievable secrecy (sum-)rate of these methods is outperformed by schemes that do not make the assumption of high SINR [14].

In this paper, we present a game-theoretic framework for interference management in a MIMO wiretap interference network. Our main goal here is to develop practical techniques to maximize the sum of secrecy rates over all links; yet reduce interference as much as possible. We consider FJ techniques as a pivotal design method for each legitimate link, where the FJ signal is only generated at the Tx side (as opposed to Rx-based FJ techniques, which require full-duplex capability at legitimate Rx's [24], [25]). In the rest of this paper, we refer to this technique as *transmit-based* FJ (TxFJ). We aim to extend the use of TxFJ in an interference network that is tapped by a multi-antenna eavesdropper. Rich literature regarding the performance of TxFJ can be found in [6], [26], [27], and practical implementations were presented in [28].

We assume that each link performs MIMO *beamforming*, i.e., the covariance matrix of the information signal of a given Tx is of rank one. Such an approach has been shown to be optimal under several channel models (see [29]). 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 noncooperative game theory to design distributed power control algorithms with modest signaling overhead.

Due to possible degradation in network performance, caused by the inherent inefficiency of Nash equilibria of noncooperative 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 also 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 in a way that the interference at each legitimate Rx is reduced, but the aggregate interference at Eve remains high.

The contributions of this paper can be summarized as follows:

- We design a price-based distributed TxFJ power control for a MIMO-capable multi-link interference network with an external eavesdropper. While maximizing the secrecy sum-rate of the network, we impose a lower threshold on the achievable information rate of each link. We show that pricing achieves a locally optimal solution for the secrecy sum-rate maximization problem, and its performance is close to the centralized (exhaustive) solution.
- We derive a lower bound on the TxFJ power needed to achieve a positive secrecy rate and yet produce enough interference to prevent Eve from applying successive interference cancellation. This lower bound also allows us to analyze various aspects of our method, such as deriving the conditions under which iterative computation of optimal TxFJ power for each link using pricing method always converges to a unique point.
- 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 implementation of TxFJ for each link, 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 mechanism that is robust to uncertainties about eavesdropping channels. We show that when the network only involves two links, the robust price-based method can be simplified significantly. Simulations show that the solutions found with/without knowledge of Eve's channel

outperform the greedy TxFJ approach.

The rest of this paper is organized as follows. In Section II the system model is introduced. In Section III we formulate the power control problem and determine the minimum TxFJ power that results in positive secrecy for each link. In Section IV we model the power control problem as a noncooperative game. We then introduce pricing to improve the efficiency of the resulting Nash equilibria. The robust version of the proposed game is presented in Section V. Comparison of signaling overhead between our proposed methods is done in Section VII.

Notation: We use boldface uppercase letters to denote matrices, and boldface lowercase letters to denote vectors. The 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 the trace of a matrix. We indicate the set of complex numbers by $\mathbb{C}$.

II. System Model

Consider Q transmitters, Alice_1, …, Alice_Q, ($Q \geq 2$) that communicate with their respective receivers, Bob_1, …, Bob_Q. Let $\mathcal{Q} = \{1, \ldots, Q\}$. For every $q \in \mathcal{Q}$, Alice_q and Bob_q have N_q and M_q antennas, respectively. A passive Eve with L antennas is also present in the same 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 the qth Rx; 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.

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. 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 $0 \leq \phi_q \leq 1$ is the portion of that power that is 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 $E[\mathbf{v}_q \mathbf{v}_q^\dagger] = \sigma_q \mathbf{I}$. The scalar term $\sigma_q = \frac{(1-\phi_q)P_q}{N_q-1}$ denotes the TxFJ 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 $\tilde{\mathbf{H}}_{qq}$[3]. 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 $\mathbf{V}_q$. This way, the information rate of Alice$_q$ is maximized [6]. Specifically, by setting $\mathbf{T}_q = \mathbf{V}_q^{(1)}$, we carry out a transmit beamforming technique to exploit transmit diversity. 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 (ECSI) components. Hence,

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

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

An illustration of the system model under study is given Fig. 1 for a two-link network. It can be seen that the interference components a each Bob include both information signal and TxFJ of unintended Alices. Eve also receives all information and TxFJ signals of Alices.

[3]Acquiring CSI between a Tx and its corresponding Rx 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 from Bob to Alice, thus lowering the probability of eavesdropping on channel estimates.

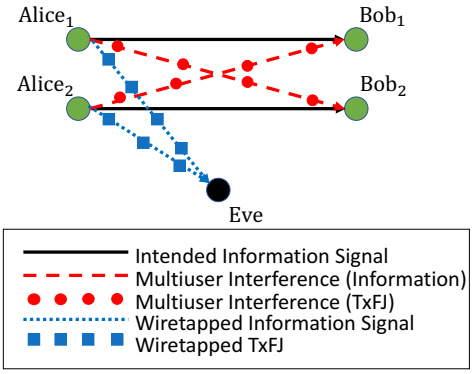


Fig. 1: System model.

After receiving $\mathbf{y}_q$ at Bob$_q$, a linear receiver $\mathbf{d}_q \in \mathbb{C}^{M_q}$ is applied to estimate the transmit signal. The linear estimate $\hat{x}_q$ is

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

The linear receivers $\mathbf{d}_q$, $q \in \mathcal{Q}$, are 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 $\mathbf{U}_q$. In other words, in our model receiver and transmit diversities are both exploited at each link. It can be easily shown that $\mathbf{d}_q^\dagger\mathbf{H}'_{qq}\mathbf{v}_q = \mathbf{d}_q^\dagger\mathbf{U}_q\mathbf{\Sigma_q}\mathbf{V}_q^\dagger\mathbf{V}_q^{(2)}\mathbf{v}_q = 0$, since the vector $\mathbf{d}_q^\dagger\mathbf{U}_q\mathbf{\Sigma_q}$ selects the first row of $\mathbf{\Sigma_q}$, but $\mathbf{V}_q^\dagger\mathbf{V}_q^{(2)}$ selects the $N_q - 1$ rightmost columns of $\mathbf{\Sigma_q}$. Thus, 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, and as Fig. 1 suggests, the TxFJ signal of each Alice is nulled at her corresponding Bob.

The information rate for the qth link can be written as

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

where

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

Assuming a worst-case scenario in which Eve knows the channel between herself and each Alice (obtained by possibly spoofing on the pilot sequences or beaconing signals), Eve applies the linear receiver $\mathbf{r}_q \in \mathbb{C}^L$

while eavesdropping on the qth link's signal so as to obtain the following estimate of the transmit signal

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

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, respectively, and $\mathbf{D}_q$ is the diagonal matrix of singular values. Thus, while eavesdropping on the qth link, Eve chooses $\mathbf{r}_q = \mathbf{L}_q^{(1)}$, where $\mathbf{L}_q^{(1)}$ is the first column of matrix $\mathbf{L}_q$ to perform MRC on the eavesdropped signal. A summary of our notation is given in Table I.

We need to emphasize that the choice of precoders (i.e., beamformers) for TxFJ and information signals in this paper is mainly driven by the fact that acquiring E-CSI knowledge may not be possible in the cases where eavesdropper is a passive node. For a single-link scenario, it was shown in [30] that optimizing the precoders of information and TxFJ signals requires complete 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, which is relatively more practical to achieve.

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 [6], 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 by a specific choice of decoder (i.e., linear receiver) at its receive antennas.

In general, the TxFJ signal from the qth Tx received at the eavesdropper can be written as $\mathbf{r}_q \tilde{\mathbf{G}}_q \mathbf{V}'_q \mathbf{v}_q$ where $\mathbf{V}'_q$ is the N rightmost columns of $\mathbf{V}_q$. Let $\tilde{\mathbf{G}}_q \mathbf{V}'_q = \mathbf{G}'_q = \mathbf{L}'_q \mathbf{D}'_q \mathbf{R}'_q$ be the SVD of the $L \times N$ matrix $\mathbf{G}'_q$, where $\mathbf{L}'_q$ and $\mathbf{R}'_q$ are matrices of left and right singular vectors, respectively, and $\mathbf{D}'_q$ is the diagonal matrix of singular values.

Considering $\mathbf{G}'_q$, if we have $L > N$, indicating that the channel $\mathbf{G}'_q$ is a tall matrix, then eavesdropper has more antennas than the total dimensions considered for the TxFJ signal at the qth Tx. Hence, if eavesdropper knows $\mathbf{G}'_q$ it can choose $\mathbf{r}_q$ to be the rightmost $L - N$ columns of the matrix $\mathbf{L}'_q$. This way,

eavesdropper can nullify the TxFJ signal, i.e., $\mathbf{r}_q\tilde{\mathbf{G}}_q\mathbf{V}'_q = 0$. Therefore, an eavesdropper with sufficiently high number of antennas can nullify the effect of TxFJ on itself. To prevent this, we need to make sure that $L - N \leq 0$, so $N \geq L$. To ensure that $N \geq L$ the qth Tx uses as many dimensions for the TxFJ signal as possible. Hence, we set N to its maximum value, i.e., $N = N_q - 1$. This way, at least we know that the qth Tx cannot do any better to prevent nullification of TxFJ on the eavesdropper. Obviously, by choosing $N = 1$ (i.e., allocating one dimension to the TxFJ precoder), even an eavesdropper with $L = 2$ antennas can nullify the effect of TxFJ on itself.

Hence, the precoder of TxFJ signal $\mathbf{Z}_q$ must include the $N_q - 1$ rightmost columns of $\mathbf{V}_q$. Accordingly, the information signal $\mathbf{s}_q$ 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. With the aforementioned choice of TxFJ beamformer, the beamformer that can maximize the information rate of the qth Tx would be $\mathbf{T}_q = \mathbf{V}_q^{(1)}$, where $\mathbf{V}_q^{(1)}$ is the $N_q - N = N_q - (N_q - 1) = 1$ leftmost column of $\mathbf{V}_q$, i.e., the first column of $\mathbf{V}_q$. Such choices of precoders forces x_q to be a scalar value, signifying that only single-stream signals are allowed to be transmitted.

Overall, with these choices of precoders, we first make sure that our precoders do not require knowledge of E-CSI, then we make sure that our TxFJ signal will not be nullified at an eavesdropper with relatively low number of antennas. Such an approach in assigning precoders was also used in [26], [27]. Notice that in the case of having knowledge of number of antennas at eavesdropper, one can easily choose exact amount of dimensions for the TxFJ beamformer to ensure that eavesdropper is not able to nullify the TxFJ at itself. However, in case of collusion between multiple eavesdroppers, they can form a MIMO receiver with higher number of receive antennas.

Such an approach in assigning precoders was also used in [26], [27]. Notice that in the case of having knowledge of number of antennas at eavesdropper, one can easily choose exact amount of dimensions for the TxFJ beamformer to ensure that eavesdropper is not able to nullify the TxFJ at itself. However, in this paper we assumed that the eavesdropper has close specifications to the legitimate nodes. This forces us to allocate as many dimensions as possible to the TxFJ beamformer, i.e., increase the rank of

TxFJ beamformer as much as possible (to prevent nullification of TxFJ at Eve) and use the remaining dimensions for the precoder of information signal.

III. Problem Formulation

The multiuser channel between the Q Alices and Eve can be modeled as a multiple-access channel because Eve is simultaneously receiving signals from all Alices. If Eve is capable of using successive interference cancellation (SIC), she may be able to simultaneously decode all signals. To illustrate the impact of SIC, consider the example of $Q = 2$. The achievable-rate region of Eve's multi-access channel is shown in Fig. 2, where C_{eq} denotes the achievable rate at Eve while decoding Alice$_q$'s signal ($q = 1, 2$). The points β_q and ψ_q are defined in (7) and (12), respectively, and will be explained shortly. Fig. 2 suggests that to prevent Eve from using SIC, we must have $C_q > \beta_q$ for $q = 1, 2$ [12], 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 other words, if inequality $C_q > \beta_q$ is satisfied, Eve has to decode Alice$_q$'s information signal while considering Alice$_r$'s information signal as interference, $r \neq q$. In this case, the secrecy rate for Alice$_q$, $q = 1, 2$, would be

$$C_q^{sec} = C_q - \mathcal{G}_q. \tag{9}$$

Moreover, since the two links do not coordinate to implement time-sharing, then if the qth link's information rate is higher than the decodable rate at Eve, it can be guaranteed that Eve does not have complete knowledge of the qth information signal. Therefore, Eve cannot subtract this signal and decode Alice$_q$'s signal while eavesdropping on Alice$_r$'s signal. Thus, the achievable 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

$$C_r^{sec} \triangleq \max\{C_r - \beta_r \ , \ 0\} = \log(1 + \frac{\gamma_r}{a_r}) - \log(1 + \frac{\gamma_r}{c_r}). \tag{10}$$

This operating point can be shown in Fig. 2 as the tuple (β_1, β_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

$$C_r^{sec} = \max\{C_r - \psi_r, 0\} \tag{11}$$

where

$$\psi_r \triangleq \log(1 + \frac{\gamma_r}{d_r}) \tag{12}$$

$$d_r = \frac{\left|\mathbf{r}_r^\dagger \mathbf{G}_r'\right| \sigma_r + \left|\mathbf{r}_q^\dagger \mathbf{G}_q'\right|^2 \sigma_q + N_0}{\left|\mathbf{r}_r^\dagger \mathbf{G}_r\right|^2}. \tag{13}$$

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, it can be seen from (10) and (11) that 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 $C_q > \beta_q \ \forall q$, where (with a slight abuse of notation)

$$\beta_q \triangleq \log(1 + \frac{\gamma_q}{c_q}) \tag{14}$$

$$c_q = \frac{\left|\mathbf{r}_q^\dagger \mathbf{G}_q'\right| \sigma_q + \sum_{\substack{r=1 \\ r \neq}}^{Q} \left(\left|\mathbf{r}_q^\dagger \mathbf{G}_r\right|^2 \gamma_r + \left|\mathbf{r}_q^\dagger \mathbf{G}_r'\right|^2 \sigma_r\right) + N_0}{\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2}. \tag{15}$$

$\mathbf{y}_q$	Received Signal at Bob$_q$, $q \in \mathcal{Q} = \{1, \ldots, Q\}$
x_q	Information (Info.) signal of Alice$_q$
$\mathbf{v}_q$	TxFJ signal of Alice$_q$
$\mathbf{s}_q$	Info.-bearing signal transmitted from Alice$_q$
$\mathbf{w}_q$	TxFJ-bearing signal transmitted from Alice$_q$
$\mathbf{T}_q$	Precoder for the info. signal of Alice$_q$
$\mathbf{d}_q$	Linear receiver used at Bob$_q$
$\mathbf{Z}_q$	Precoder for the TxFJ signal of Alice$_q$
$\mathbf{r}_q$	Linear receiver at Eve (eavesdropping on Alice$_q$)
P_q	Total transmit power at Alice$_q$
ϕ_q	Portion of Alice$_q$'s power allocated to info. signal
N_q (M_q)	Number of Tx (Rx) antennas for the qth link
$\mathbf{u}_q$	Transmitted signal from Alice$_q$
$\tilde{\mathbf{H}}_{rq}$	Channel between Alice$_r$ and Bob$_q$
$\mathbf{U}_q$	Matrix of left singular vectors for $\tilde{\mathbf{H}}_{qq}$
$\mathbf{\Sigma_q}$	Diagonal Matrix of singular values for $\tilde{\mathbf{H}}_{qq}$
$\mathbf{V}_q$	Matrix of right singular vectors for $\tilde{\mathbf{H}}_{qq}$
$\mathbf{H}_{rq}$	Beamformed channel between Alice$_r$ and Bob$_q$ (info.)
$\mathbf{H}'_{rq}$	Beamformed channel between Alice$_r$ and Bob$_q$ (TxFJ)
$\mathbf{n}_q$	Noise term at Bob$_q$
L	Number of receive antennas at Eve
$\tilde{\mathbf{G}}_q$	Channel between Alice$_q$ and Eve
$\mathbf{L}_q$	Matrix of left singular vectors for $\tilde{\mathbf{G}}_q$
$\mathbf{D}_q$	Diagonal Matrix of singular values for $\tilde{\mathbf{G}}_q$
$\mathbf{R}_q$	Matrix of right singular vectors for $\tilde{\mathbf{G}}_q$
$\mathbf{G}_q$	Beamformed channel between Alice$_q$ and Eve (info.)
$\mathbf{G}'_q$	Beamformed channel between Alice$_q$ and Eve (TxFJ)
$\mathbf{e}$	Noise term at Eve

TABLE I: Summary of notations used for the system model

Later on, we refer to these constraints while formulating our optimization problems.

We define $C^{sec} \triangleq \sum_{q=1}^{Q} C_q^{sec}$ as the *secrecy sum-rate*, where C_q^{sec} is defined in (9) and β_q is defined in (14). We aim to maximize C^{sec} while ensuring a minimum information rate for all links. This problem can be formally written as:

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

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

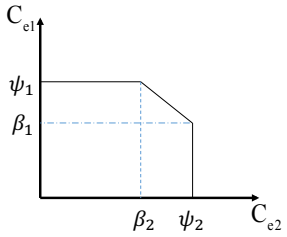


Fig. 2: Achievable rate pairs for a two-user multiple access channel.

each legitimate Tx; and the second constraint ensures a minimum information rate R_q for each link q.

The optimization in (16) is nonconvex, as it can be shown that the Hessian matrix of the objective is not necessarily negative definite w.r.t $[\boldsymbol{\gamma}, \boldsymbol{\sigma}]^T$, thus not ensuring the concavity of the objective function. Hence, solving (16) is prohibitively expensive. We relax this problem by eliminating the dependency on $\boldsymbol{\gamma}$. To do that, we assume 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. The second constraint can now be embedded into the objective function and the first constraint. Hence, (16) is simplified into[4]

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

Considering how we prevent Eve from applying SIC (cf. (14) and the discussion above it), the TxFJ power has to be chosen such that inequality $C_q > \beta_q$ is satisfied for all q. Manipulating $C_q > \beta_q$, we end up with

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

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

where

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

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

Simplifying (18), we can establish the following constraints on σ_q:

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

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

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

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

For the case in (20a), no amount of TxFJ power can prevent Eve from using SIC, and the solution to (17) would be infeasible. 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

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

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

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

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

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

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

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 between the TxFJ powers of transmitters. In other words, Pareto-optimal TxFJ powers of secrecy sum-rate can be found by solving (22)[5]. Unfortunately, the optimization in (22) is still nonconvex. Furthermore, it requires the exact knowledge of ECSI (i.e., $\mathbf{G}_q$ and $\mathbf{G}'_q$).

IV. Game Formulation

A. Greedy FJ

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. In fact, assuming that each player myopically chooses the best strategy for himself, we can formulate this scenario as a noncooperative game, in which the best strategy of each link q is

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

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

[5]To be more specific, the solutions of (22) only correspond to one Pareto-optimal solution on the convex region 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 [31, Section 6], the discussion regarding (52) in Appendix C, and [32]).

may argue that the game formulation in which the strategy of each link is defined by (23) is essentially different than the formulation in (22), such a formulation will later help us 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 nonempty, 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 [33]. Verifying these properties in our game is straightforward, and is thus skipped for brevity. 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 choosing any TxFJ power less than that can degrade the individual secrecy rate of that player. Therefore, the point $\sigma_q = P_q^{jam},\ \forall q$ is the NE. This result is in line with [6] for the single-link case.

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 and maximize the secrecy sum-rate but not to compromise the achievability of positive secrecy at each link.

B. Price-based FJ

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

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

where λ_q is a pricing factor for the qth link, defined in (25) at the top of the next page. The rationale behind pricing was discussed in several previous works (e.g., [34], [35], [36]). In brief, pricing is a mechanism

$$\lambda_q = \sum_{\substack{r=1 \\ r\neq q}}^{Q} \left(\frac{|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2 |\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2 \gamma_r}{\left(\sum_{\substack{t=1 \\ t\neq r}}^{Q} (|\mathbf{d}_r^\dagger \mathbf{H}_{tr}|^2 \gamma_t + |\mathbf{d}_r^\dagger \mathbf{H}'_{tr}|^2 \sigma_t) + N_0\right) \left(\sum_{\substack{t=1 \\ t\neq r}}^{Q} (|\mathbf{d}_r^\dagger \mathbf{H}_{tr}|^2 \gamma_t + |\mathbf{d}_r^\dagger \mathbf{H}'_{tr}|^2 \sigma_t) + |\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2 \gamma_r + N_0\right)} - \right. \tag{25}$$

$$\left. \frac{|\mathbf{r}_r^\dagger \mathbf{G}'_q|^2 |\mathbf{r}_r^\dagger \mathbf{G}_r|^2 \gamma_r}{\left(\sum_{\substack{t=1 \\ t\neq r}}^{Q} (|\mathbf{r}_r^\dagger \mathbf{G}_t|^2 \gamma_t + |\mathbf{r}_r^\dagger \mathbf{G}'_t|^2 \sigma_t) + |\mathbf{r}_r^\dagger \mathbf{G}'_r|^2 \sigma_r + N_0\right) \left(\sum_{\substack{t=1 \\ t\neq r}}^{Q} (|\mathbf{r}_r^\dagger \mathbf{G}_t|^2 \gamma_t + |\mathbf{r}_r^\dagger \mathbf{G}'_t|^2 \sigma_t) + |\mathbf{r}_r^\dagger \mathbf{G}_r|^2 \gamma_r + |\mathbf{r}_r^\dagger \mathbf{G}'_r|^2 \sigma_r + N_0\right)} \right), \ r \neq q, \ \forall q.$$

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

that incentivizes players to spend their TxFJ powers more wisely by charging each player a price per unit of TxFJ power, thus discouraging players from acting selfishly. In our work, we use linear pricing to improve the efficiency of TxFJ control as it can be seen from (24). The optimal TxFJ power can be found by writing the K.K.T. conditions for (24). Hence, a close-form representation of the optimal TxFJ power for the qth link can be written as in (26) at the top of the next page, where the notation $\bullet]_a^b$ means $\max\{\min\{\bullet, a\}, b\}, \ a \leq b$. It is easy to verify that 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 using pricing. 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 Appendix A. ■

Next, we introduce two properties 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:*

- *All links satisfy the bound in* (18)*, i.e.,* $\sigma_q > \frac{A_q}{B_q}, \ \forall q$.

- *Each Bob receives low interference, 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, using (26) *to update TxFJ powers in a sequential manner (i.e., the Gauss-Seidel method in the sense of [37, Chapter 3]) for all* $q \in \mathcal{Q}$ *converges to the unique NE.*

Proof: See Appendix B ■

Remark 1: While we were not able to show the convergence under synchronous updates (i.e., the Jacobi method in the sense of [37, Chapter 3]), where all links update their TxFJ powers simultaneously at each iteration, we verified such convergence in our simulations.

C. Optimality of Greedy FJ Control

It should be noted that if the conditions in Proposition 1 are not met, both the NE uniqueness and convergence of the updates in (26) cannot be verified. Even if the convergence the conditions of Proposition 1 hold, we still assume that the ECSI is known to all the links. Such assumption is not always realizable in practice. Hence, in the rest of this section and the next section, we aim to come up with a method that does not depend on knowledge of ECSI. As a first attempt, we 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 (in terms of power constraint, network topology, etc.) under which there is no need for an iterative optimization. In fact, each Alice can conveniently set her TxFJ power to the maximum available. Feasible conditions on the Pareto-optimality of greedy FJ control is stated in the following property.

Proposition 2. *The greedy FJ approach results in the unique Pareto-optimal operating point 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 nonnegative elements and nonzero rows.*

Proof: See 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, and was already presented in [38], 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 $\lambda_q = -\frac{\partial C_r^{sec}}{\partial \sigma_q},\ q, r = 1, 2$, *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* $\lambda_q = 0$*) if* $\lambda_q \leq 0,\ \forall q$. ■

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, these two schemes will have equal performances. Specifically, under the conditions of Proposition 2, the price-based FJ control reduces to greedy FJ control (i.e., $\lambda_q = 0,\ q \in \mathcal{Q}$), allowing legitimate links to use their maximum available TxFJ powers.

Switching back to the general case of of $Q > 2$, we now aim at finding the conditions that guarantee the optimality of the greedy FJ control, so that once these conditions are met, there will be no need for iterative computation of best responses and message passing between links because legitimate links can simply transmit TxFJ at their maximum powers and still ensure the highest secrecy sum-rate.

Proposition 3. *The Pareto-optimality of the greedy FJ method occurs when each link has a low power left to allocate to TxFJ.*

Proof: See Appendix D. ■

Remark: The result of Proposition 3 is rather intuitive because preserving positive secrecy requires a link has to spend all the remaining power for TxFJ. Therefore, whatever scenario that leaves low power remaining for the TxFJ (e.g., low transmit power, high rate demands or a dense network) can be considered as the scenario where greedy FJ is the optimal operating point.

In the next section, we analyze the case of unknown ECSI for the cases where the greedy FJ control

may not be a unique Pareto-optimal point.

V. Price-based FJ Under ECSI Uncertainties

So far, we have proved that under perfect knowledge of ECSI, price-based FJ control results in locally optimum TxFJ powers. The next question is how to determine the best price in the absence of such knowledge. When the ECSI is unknown, it is difficult to compute σ_q^* and λ_q. Besides, the use of greedy FJ cannot be guaranteed to be a Pareto-optimal point for cases other than those of Proposition 3. In the following, we propose a method to overcome these issues.

Let $R_q(s_q, s_{-q})$ 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 players has infinitely many real numbers. In order to proceed further with our analysis, we need to make this 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 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 an important property of games with finite strategy sets for the players, i.e., *finite games*. It has been shown in [39] that every finite game has a mixed-strategic NE. In the following, we propose an algorithm that can find a mixed-strategic NE of the non-cooperative FJ control game.

A. Mixed Strategic Game Formulation

Definition 1. *A mixed strategy vector for the qth 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 qth player's strategies. In other words, the qth player chooses power level* $i\Delta\sigma_q$ *with probability* $\alpha_{i,q}$.

In the mixed strategic 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

$$E_{s_q}\left[E_{s_{-q}}[R_q(s_q, s_{-q})]\right] \leq E_{s_{-q}}\left[R_q\left(E_{s_q}[s_q], s_{-q}\right)\right], \quad \forall (s_q, s_{-q}) \in \mathcal{S}_q \times \mathcal{S}_{-q} \tag{27}$$

where $\mathcal{S}_{-q} \triangleq \mathcal{S}_1 \times \cdots \times \mathcal{S}_{q-1} \times \mathcal{S}_{q+1} \times \cdots \times \mathcal{S}_Q$. Equation (27) is satisfied with equality if and only if s_q reduces to pure strategies. Hence, using pure strategies is more 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 nonconcave utilities. Unfortunately, to the best of our knowledge, the concept of mixed strategic games has a relatively sparse literature when more than two players are interacting with each other. Hence, we limit our model to $Q = 2$, for which the mixed strategic games are well-understood. While this limits the scalability of our method (only when limited ECSI is available), it turns out that a two-user scenario presents several interesting properties that can be exploited to come up with efficient TxFJ control framework. Such a framework allows for relaxing the knowledge of eavesdropping channel as well as reducing the computational complexity.

Before exploring the application of mixed games, 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) *becomes a decreasing 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 relation 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)

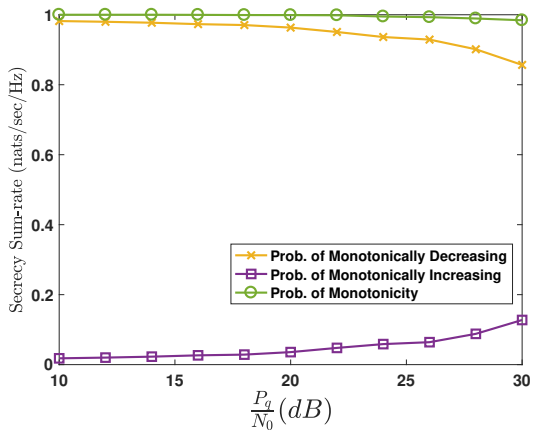


Fig. 3: Probability of monotonicity of σ_q^* w.r.t. $\sigma_r,\ (r,q) = 1,2,\ r \neq q$.

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 increased the number of runs for this simulation. we ran this simulation for a total of 100 placements. For each 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. Lastly, for moderate to low transmit powers the TxFJ power of a link is often a decreasing function of TxFJ of the other link.

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*

$s_1 \backslash s_2$	0	$\Delta\sigma_2$	$\dots$	P_2^{jam}
0	$R_1(0,0), R_2(0,0)$	$R_1(0,\Delta\sigma_2), R_2(0,\Delta\sigma_2)$	$\dots$	$R_1(0,P_2^{jam}), R_2(0,P_2^{jam})$
$\Delta\sigma_1$	$R_1(\Delta\sigma_1,0), R_2(\Delta\sigma_1,0)$	$R_1(\Delta\sigma_1,\Delta\sigma_2), R_2(\Delta\sigma_1,\Delta\sigma_2)$	$\dots$	$R_1(\Delta\sigma_1,P_2^{jam}), R_2(\Delta\sigma_1,P_2^{jam})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
P_1^{jam}	$R_1(P_1^{jam},0), R_2(P_1^{jam},0)$	$R_1(P_1^{jam},\Delta\sigma_2), R_2(P_1^{jam},\Delta\sigma_2)$	$\dots$	$R_1(P_1^{jam},P_2^{jam}), R_2(P_1^{jam},P_2^{jam})$

Table II: Strategy table for the two-link finite jamming game with pricing.

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 Appendix E. ■

For $Q = 2$, we can establish the strategy table for each player. A utility matrix $R_q,\ q = 1,2$, can be obtained such that the (i,j)th entry is $[R_q]_{ij} = \{R_q(i\Delta\sigma_1, j\Delta\sigma_2)|\ (i,j) \in \{0,\dots,M\}^2, r \neq q\}$. Because problem (22) is nonconvex w.r.t the TxFJ powers, the Pareto-optimal points can be found via exhaustive search in Table II. 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 $\mathcal{O}(4n-4)$ because only a small set of TxFJ power tuples comprises the NE points of price-based FJ game, meaning that the locally optimal points of the secrecy sum-rate can be found by searching a small part of Table II. To get more intuition into the order reduction, we discuss a special case of Proposition 4. Recalling the justification of why Eve cannot perform SIC to decode both signals from Alices, if (21c) is always satisfied for both players, then only the rows corresponding to χ_1 and P_1^{jam}, and the columns corresponding to χ_2 and P_2^{jam} need to be searched.

In price-based FJ, the utility function of each player changes at every iteration. Furthermore, the terms $R_1(i\Delta\sigma_1, j\Delta\sigma_2)$ and $R_2(i\Delta\sigma_1, j\Delta\sigma_2), (i,j) \in \{0,\dots,M\}$, in Table II only show the utilities of the two players (at $s_1 = i\Delta\sigma_1$ and $s_2 = j\Delta\sigma_2$), assuming that the iterative application of (26) for both players

converges to $\sigma_1^* = i\Delta\sigma_1$ and $\sigma_2^* = j\Delta\sigma_2$. 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 (22) are met at the NE point of the price-based game. Hence, the utility of each player at the NE point is $R_q(s_1, s_2) = C^{sec}(\sigma_q),\ q \in \{1, 2\}$, which is in general a nonconcave function w.r.t. σ_q. By setting C^{sec} as a function of σ_q, we want to emphasize that each player locally computes its own TxFJ power and checks its effect on the secrecy sum-rate. Considering Proposition 4, the objective of the first player reduces to:

$$\begin{aligned} \underset{\{\alpha_{i,1}\}_{i=1}^{M}, s_2}{\text{maximize}} \quad & \sum_{i=1}^{M} \alpha_{i,1} R_1(i\Delta\sigma_1, s_2) \\ \text{s.t.} \quad & \sum_{i=1}^{M} \alpha_{i,1} = 1 \\ & 0 < \alpha_{i,1} < 1,\ \forall i \\ & s_2 \in \left\{ \left\lceil \frac{\chi_2}{M} \right\rceil \Delta\sigma_2, P_2^{jam} \right\} \end{aligned} \tag{29}$$

where $\{\alpha_{i,1}\}_{i=1}^{M}$ is a probability set and $\lceil \bullet \rceil$ is the ceiling function.

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 (10) depends on C_q and C_{eq}. Because we assumed that Bob can measure his received interference 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; d_{qe} is the distance between Alice$_q$ and Eve in meters,

and η is the path-loss exponent. 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 $\tilde{\mathbf{G}}'_q$ (cf. (2) and Section II). The secrecy rate is now given by

$$C_q^{sec} = C_q - E_{\left[d_{qe},\, \bar{\mathbf{G}}_q, d_{re},\, \bar{\mathbf{G}}_r, \bar{\mathbf{G}}'_q,\, \bar{\mathbf{G}}'_r\right]}\left[C_{eq}\right] = C_q - \tag{30}$$

$$E\left[\log\left(1 + \frac{\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2 \gamma_q}{\left|\mathbf{r}_q^\dagger \mathbf{G}'_q\right|^2 \sigma_q + \left|\mathbf{r}_q^\dagger \mathbf{G}_r\right|^2 \gamma_r + \left|\mathbf{r}_q^\dagger \mathbf{G}'_r\right|^2 \sigma_r + N_0}\right)\right] \tag{31}$$

where $E_{\left[d_{qe},\ldots,\, \bar{\mathbf{G}}'_r\right]}\left[\bullet\right] \triangleq E_{d_{qe}}\left[E_{\bar{\mathbf{G}}_q}\left[\ldots\left[E_{\bar{\mathbf{G}}'_r}\left[\bullet\right]\right]\right]\right]$. We rewrite (31) as

$$E_{\left[d_{qe},\ldots,\, \bar{\mathbf{G}}'_r\right]}\left[C_{eq}\right] = E_{\left[d_{qe},\, \mathbf{W}_q, d_{re},\, \mathbf{Y}_q\right]}\left[\log\left|\frac{\mathbf{W}_q \Gamma_{1q} \mathbf{W}_q^H}{\mathbf{Y}_q \Gamma_{2q} \mathbf{Y}_q^H}\right|\right] \tag{32}$$

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

$$\begin{aligned}\Gamma_{1q} = \text{diag}\Big\{ &\gamma_q, \sigma_q \underbrace{[1,\ldots,1]}_{N_q-1}, \left(\frac{d_{re}}{d_{qe}}\right)^{-\eta} \gamma_r, \\ &\sigma_r \underbrace{[1,\ldots,1]}_{N_r-1} \left(\frac{d_{re}}{d_{qe}}\right)^{-\eta}, d_{qe}^{\eta} N_0 \Big\}\end{aligned} \tag{33}$$

$$\begin{aligned}\Gamma_{2q} = \text{diag}\Big\{ &\sigma_q \underbrace{[1,\ldots,1]}_{N_q-1} \left(\frac{d_{qe}}{d_{re}}\right)^{(-\eta)}, \gamma_r, \\ &\sigma_r \underbrace{[1,\ldots,1]}_{N_r-1}, d_{re}^{\eta} N_0 \Big\}\end{aligned} \tag{34}$$

with $\text{diag}\{\mathbf{f}^T\}$ representing an $m \times m$ diagonal matrix whose diagonal entries are the entries of a vector of size m. The expectation in (32) w.r.t. $\mathbf{W}_q$ and $\mathbf{Y}_q$ can be efficiently computed using the random matrix result in [40, Appendix A, Lemma 2]. However, according to (32) 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 VIII for more details). A similar idea can be found in

[41]. Another example is [42] where the authors assumed that the location of Eve follows a Poisson point process.

Following the same technique used to manipulate (32), we take the expectation of (18) and end up with:

$$\sigma_q > \frac{\left(|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r + N_0\right)}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} E_{[\bar{\mathbf{G}}_q, \bar{\mathbf{G}}'_q]} \left[\frac{|\bar{\mathbf{G}}_q|^2}{|\bar{\mathbf{G}}'_q|^2} \right] - \tag{35}$$

$$E_{[\bar{\mathbf{G}}_r,\, d_q,\, d_r, \bar{\mathbf{G}}'_r,\, \bar{\mathbf{G}}'_q]} \left[\left(\frac{d_{re}}{d_{qe}} \right)^{-\eta} \frac{\left(|\bar{\mathbf{G}}_r|^2 \gamma_r + |\bar{\mathbf{G}}'_r|^2 \sigma_r + N_0\right)}{|\bar{\mathbf{G}}'_q|^2} \right]. \tag{36}$$

The numerator and the denominator inside the first expectation term in (35) correspond to a central Wishart matrix [43]. The numerator inside the second expectation term corresponds to the quadratic form of a Wishart matrix, which preserves the Wishartness property [44]. 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 (35) can be computed using the result in [45, Section 1]. Computing the expectation w.r.t. d_q and d_r can be tackled numerically, as explained above.

Since (30) and (35) are computable, the objective function and third constraint of (29) are defined without knowledge of the eavesdropping channel. Hence, we can establish Table |I to solve (29). The next section discusses an algorithm to perform robust FJ control.

VI. Robust FJ Design and Discussion

We now describe an algorithm that achieves a robust solution for the mixed strategic FJ control in (29) when $Q = 2$. To approximate the expectation of C_{eq} w.r.t. distances, the location of Eve will be assumed to be uniformly distributed within a circle of radius $\hat{r}_e$, whose center coordinates are $(\hat{x}_e, \hat{y}_e)$. The pseudo-code for our algorithm is shown in Algorithm 1. The computation in lines 5 and 6 can be done using the method used to compute (35) (with $\sigma_r = \chi_r$), which requires both links to measure the interference at their receivers and exchange the values of σ_q and γ_q for $q = 1, 2$. Proposition 4 suggests

that the computation in line 5 only sets two power levels for σ_r (i.e., the loop in line 3 will be run once when $\sigma_r = \chi_r$ and once when $\sigma_r = P_r^{jam}$). In the case of exhaustive search, instead of two power levels, we need to search using all power levels in the interval $[\chi_r, P_r^{jam}]$ (cf. Section III.A for more details on exhaustive search).

Line 7 ensures that the selected power in line 4 results in a nonzero utility for the qth player. If the condition in line 7 is not satisfied, the probability assigned to that power level (i.e., $\alpha_{i,q}$) is zero. Hence, one term will be removed from the objective function and constraints of (29). The operation in line 8 (computed using (30)) requires both links to compute their own secrecy rates using their local channels and the method mentioned for computing (30). Then, the rth link should send the value of its own secrecy rate to the qth link in order to compute R_q. After executing lines 2-12, as R_q is already stored in line 8, line 13 chooses the probability set that corresponds to the largest expected utility. The solution found after Line 14 for each player is the probability set $\{\alpha_{i,q}\}_{i=1}^{M},\ q = 1, \ldots, Q$. 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 [46]:

- Generate a uniform random variable $U(0, 1)$.
- Determine the index I such that

$$\sum_{i=1}^{I-1} \alpha_{i,q} \leq U < \sum_{i=1}^{I} \alpha_{i,q} \tag{37}$$

- 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 power assignment[6].

[6]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.

Algorithm 1 Robust Friendly Jamming Control

Input: $N_q, P_q, c_q, M \ \forall q \in \{1, 2\}$

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 $R_q(\sigma_q, \sigma_r)$.

9: **end if**

10: **end for** % do the same loop again but change

11: % line 5 to "Set $\sigma_r = P_r^{jam}$".

12: $R_q(\sigma_q) = \max_{\sigma_r} R_q(\sigma_q, \sigma_r)$.

13: Find $\{\alpha_{i,q}\}_{i=1}^{M}$ by solving (29) (with $R_q(\sigma_q)$ as the summands in the objective function).

14: **end for**

15: **for** $q = 1$ to 2 **do**

16: **if** $C_q < c_q - \epsilon$ **then** Set $\gamma_q = \gamma_q + \delta$.

17: **if** $\gamma_q > P_q$ **then** Set $\gamma_q = P_q$.

18: **end if**

19: **else**

20: **if** $C_q > c_q + \epsilon$ **then** Set $\gamma_q = \gamma_q - \delta$.

21: **end if**

22: **end if**

23: **end for**

24: **until** $c_q - \epsilon < C_q < c_q + \epsilon \quad \forall q$.

Lines 15 to 24 constitute the part of the algorithm that corresponds to satisfying the rate constraints for

both links. 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 [47, 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 extended to the case of multiple links as well. Specifically, the loop between lines 2 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 done in lines 15 and 24 can be done for more than two links. This way, the price-based FJ control can be augmented with the rate adjustment to satisfy the information rate constraints.

Overall, in Algorithm 1, solving the optimization in (29) is done under the assumption that both players have the same utility functions, which allows the qth player, $q = 1, 2$, to find two probability distributions based on the two strategies of the rth player, $r \neq q$, i.e., $\left\lceil \frac{\chi_r}{M} \right\rceil \Delta\sigma_r$ and P_r^{jam}. Hence, the qth player chooses the probability set that maximizes the maximum utility that can be seen by the rth player's action. Algorithm 1 in fact solves the following optimization problem for player 1 (and the same equivalent problem for player 2):

$$\begin{aligned} \underset{\{\alpha_{i,1}\}_{i=1}^{M}}{\text{maximize}} \quad & \max_{s_2} \sum_{i=1}^{M} \alpha_{i,1} R_1(i\Delta\sigma_1, s_2) \\ \text{s.t.} \quad & \sum_{i=1}^{M} \alpha_{i,1} = 1 \\ & 0 < \alpha_{i,1} < 1, \ \forall i \\ & s_2 \in \left\{ \left\lceil \frac{\chi_2}{M} \right\rceil \Delta\sigma_2, P_2^{jam} \right\}. \end{aligned} \tag{38}$$

VII. Comparison of Signaling Overhead

So far, we proposed a distributed price-based approach to achieve locally optimal points of the secrecy sum-rate maximization in (17). It turns out that the pure non-cooperative friendly jamming (FJ) control

game (i.e., greedy FJ control) is a special case of the price-based approach by setting the pricing factor to zero. To enable the price-based scheme, at each given iteration, the objective of links and the pricing factor need to be updated (cf. problem (24)). Hence, in addition to updating the received interference at each link, extra signaling (i.e., coordination) between legitimate links is required to enable distributed implementation of the price-based FJ

Algorithm 2 Robust Friendly Jamming Control

Input: $N_q, P_q, c_q, M \ \forall q \in \{1,2\}$

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**
15: **for** $q = 1$ to 2 **do**
16: **if** $C_q < R_q - \epsilon$ **then** Set $\gamma_q = \gamma_q + \delta$.
17: **if** $\gamma_q > P_q$ **then** Set $\gamma_q = P_q$.
18: **end if**
19: **else**
20: **if** $C_q > R_q + \epsilon$ **then** Set $\gamma_q = \gamma_q - \delta$.
21: **end if**
22: **end if**
23: **end for**
24: **until** $R_q - \epsilon < C_q < R_q + \epsilon \quad \forall q$.

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

Before quantifying the signaling overhead of the proposed schemes in this paper, we need to mention that by distributed implementation of an algorithm, we mean that each link can select its own actions independently, given other players' actions; that is, the algorithm is separable between links such that every link can do part of the optimization independent of other links' strategies. This is in contrast to a non-separable algorithm, where a central authority is needed to find a feasible solution, i.e., the strategies of all links are determined using a centralized algorithm.

A centralized solution should not be confused with the notion of *coordination* (or message passing) between links. The fact that a distributed algorithm needs some coordination between links does not necessarily prevent its distributed implementation (i.e., separability of the problem). Specifically, a link might need some extra information to decide on its own action. Even if this extra information spans every channel gain and all links' strategies (which is of course not ideal at all), an algorithm can still be implemented in a distributed fashion by distributing the steps of the algorithm between various links.

Although the notions of distributed implementation and coordination are two different concepts, both of them greatly affect the practicality of an algorithm. Specifically, in an ideal distributed algorithm, not only the solution approach needs to be separable between the agents, but also the amount of coordination between agents must be kept as little as possible. In the following, we give an overview of our proposed algorithms and quantify the amount of message passing required by each of them.

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 (i.e., the TxFJ power of the qth link) as the decision variable. This means that the qth link is responsible to only find a solution for its own TxFJ power, hence complying with the definition of a distributed approach mentioned earlier in this section. 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.

By analyzing the objective of problem (24), we can quantify the amount of message exchange that is

needed to enable the price-based FJ control. Simplifying λ_q in (25) we have

$$\lambda_q = \sum_{\substack{r=1 \\ r\neq q}}^{Q} |\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2 \left(\frac{1}{\sum_{\substack{t=1 \\ t\neq r}}^{Q} (|\mathbf{d}_r^\dagger \mathbf{H}_{tr}|^2 \gamma_t + |\mathbf{d}_r^\dagger \mathbf{H}'_{tr}|^2 \sigma_t) + N_0} - \frac{1}{\sum_{\substack{t=1 \\ t\neq r}}^{Q} (|\mathbf{d}_r^\dagger \mathbf{H}_{tr}|^2 \gamma_t + |\mathbf{d}_r^\dagger \mathbf{H}'_{tr}|^2 \sigma_t) + |\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2 \gamma_r + N_0} \right) +$$

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

$$\left. \frac{1}{\sum_{\substack{t=1 \\ t\neq r}}^{Q} (|\mathbf{r}_r^\dagger \mathbf{G}_t|^2 \gamma_t + |\mathbf{r}_r^\dagger \mathbf{G}'_t|^2 \sigma_t) + |\mathbf{r}_r^\dagger \mathbf{G}_r|^2 \gamma_r + |\mathbf{r}_r^\dagger \mathbf{G}'_r|^2 \sigma_r + N_0} \right) =$$

$$\sum_{\substack{r=1 \\ r\neq q}}^{Q} |\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2 \left(\frac{1}{b_r} - \frac{1}{b_r(1+\frac{a_r}{b_r})} \right) + |\mathbf{r}_r^\dagger \mathbf{G}'_q|^2 \left(\frac{1}{d_r} - \frac{1}{d_r(1+\frac{c_r}{d_r})} \right) \tag{39}$$

where b_r and d_r are interference (plus noise) levels at the rth link and Eve, respectively. Furthermore, the terms $\frac{a_r}{b_r}$ and $\frac{c_r}{a_r}$ are SINR levels at the rth link and Eve, respectively. Looking at (39), one can deduce that to calculate the price in the objective of (24), the qth link, $q \in \mathcal{Q}$ needs to acquire the interference level and SINR level at its Rx side (to update C_q^{sec}), plus interference and SINR levels at both the rth link and eavesdropper(s) while eavesdropping on the rth link, $r \neq q,\ r \in \mathcal{Q}$ (to update λ_q), plus the the interfering channel gain caused from the TxFJ of the qth link on the rth link and eavesdropper's receptions, i.e., $|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2$ and $|\mathbf{r}_r^\dagger \mathbf{G}'_q|^2,\ \forall r \neq q \in \mathcal{Q}$[7]. Notice that there is no need to know all the channel gains from different transmitters to judge on the optimal value of σ_q. Hence, for the qth link in a given iteration, the values of σ_r, $r \neq q$, are given by measuring interference/SINR levels at the qth link and Eve. On the contrary, the centralized approach aims to solve (17) in one shot, thus cannot assume that the values of TxFJ powers are given. This necessitates knowledge of all channel gains between legitimate nodes and eavesdropper(s) for the centralized approach. 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 (i.e., $|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2$ and $|\mathbf{r}_r^\dagger \mathbf{G}'_q|^2,\ \forall r \in \mathcal{Q}$), which are relatively easier to measure and collect compared to the centralized approach.

In the greedy FJ control, the price $\lambda_q = 0,\ \forall q \in \mathcal{Q}$. Therefore, there is no need to update the objective

[7]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.

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. Hence, there is no need for a link to broadcast its interference and SINR levels to other links. Such an approach in FJ control greatly reduces the amount of message exchange at the cost of losing the performance, i.e., ending up with convergence points that result in lower secrecy sum-rates compared to the ones achieved when the price is not zero. Such a gap in secrecy sum-rate is shown in the next section.

In Section V, we established another framework that relaxes knowledge of E-CSI at legitimate links for cases when such knowledge cannot be obtained (due to e.g., passiveness of eavesdroppers). The mixed strategic game aims to mimic the same capability that exists in price-based FJ control with the assumption of unknown E-CSI. Notice that according to Algorithm 1, which implements the mixed-strategic version of the price-based FJ control for two legitimate links, each link's utility function is set to be $E[C^{sec}]$ 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 expected of leaked rate at Eve where the expectation is w.r.t. E-CSI components.

To summarize, Table II shows the differences between the approaches that we introduced in this paper, where b_r indicates the interference level at the Rx side of the rth link, $\frac{a_r}{b_r} \in \mathbb{R}$ is a real number denoting the SINR level at the Rx side of the rth link; and the terms d_r and $\frac{c_r}{d_r}$ are, respectively, the interference level and SINR level at Eve while eavesdropping on the rth link's communications.

Method	**Utility Functions,** $\forall q \in \mathcal{Q}$	**# of Players** (Q)	**Type of NE** **(How achieved)**	**Amount of Message Exchange** $\forall q \in \mathcal{Q}$
Greedy FJ Control	C_q^{sec}	$Q \geq 2$	Pure NE (iterative)	None
Price-based FJ Control (Full E-CSI)	$C_q^{sec} - \lambda_q \sigma_q$	$Q \geq 2$	Pure NE (iterative)	$b_r,\ \frac{a_r}{b_r},\ d_r,\ \frac{c_r}{d_r},\ \lvert\mathbf{d}_r^{\dagger}\mathbf{H}'_{qr}\rvert^2,$ $\lvert\mathbf{r}_r^{\dagger}\mathbf{G}'_q\rvert^2\ \forall r \neq q,\ r \in \mathcal{Q}$
Price-based FJ Control (Unknown E-CSI)	$E[C_1^{sec} + C_2^{sec}]$	$Q = 2$	Mixed NE (one-shot)	$\frac{a_r}{b_r},\ E[\log(1+\frac{c_r}{d_r})],\ \forall r \neq q,\ r \in \mathcal{Q}$

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

VIII. Numerical Results

In this section, we simulate the TxFJ control methods presented so far.

A. Multi-link Scenario

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

Fig. 4 shows the probability of convergence of the price-based game in (24) under different interference levels. In order to have a better understanding of convergence behavior of the proposed price-based FJ control, we did not consider rate demands for this simulation. We only considered a total of $P_q = 13$ dBm $\forall q \in \mathcal{Q}$, which is equally divided between information signal and TxFJ. All interfering distances $d_{rq},\ (r,q) \in Q, r \neq q$ are equal to each other. Also, all direct distances have the same value. Specifically, $d_{qq} = 10\text{m}, \forall q \in \mathcal{Q}$. The path-loss exponent is set to $\eta = 2.5$. We ran the game (24) iteratively between all links using the Jacobi iterative method. For each point on a curve in Fig. 4, 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

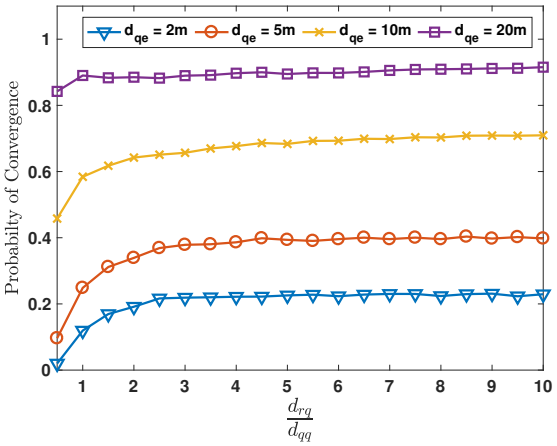


Fig. 4: Probability of convergence of price-based FJ control for different interference levels and different Eve locations, $(Q = 4, \frac{P_q}{N_0} = 30 \text{ dB}, N_q = 5, M_q = 4, L = 4)$.

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 for all runs.

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, a large amount 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. 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.

Compared to current distributed methods, to the best of our knowledge, the approach in [48] is the closest to our goals. This method was also used by several subsequent power control algorithms (e.g., [20], [49]). This work aims to propose distributed optimization algorithms for a set of non-convex/non-concave sum-utility functions. The authors of this work consider that the constraints of their problem are all feasible, and show that under this assumption, their proposed algorithms always converge. Similarly,

in our work, we did not see any convergence issue when our constraints are strictly feasible, i.e., the rate demands are met and every link enjoys positive secrecy. The work in [50] is another example of secure and distributed for interference management algorithms in which the convergence of the distributed algorithms rely on the feasibility of positive secrecy constraint for every link. None of the works mentioned above demonstrated the performance of their algorithms for when some of the constraints are not feasible. In our paper, such a phenomenon is completely possible and depends on the location of the eavesdropper and legitimate links. Hence, if an eavesdropper is sufficiently close to a legitimate link's Tx side that has a high rate demand, then positive secrecy may not be guaranteed. In other words, the nature of the problem we are solving may impose convergence issues for any algorithm due to infeasibility of constraints. We examined such convergence issues in Fig. 4[8].

Fig. 5 shows the resulting secrecy sum-rate of the four aforementioned settings in Fig. 5. We also plotted the secrecy sum-rate of the network when an exhaustive search approach is adopted for finding the optimal solutions[9]. 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 and 5, similar results can be obtained if instead of changing the proximity of Eve to Alices, all links adopt high information rate demands.

Fig. 6 (a) and 6 (b) show the convergence of the 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. 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

[8]While the convergence may be of concern in the case of Fig. 4, it turns out later that in a more realistic scenario the convergence issues (and subsequently performance issues) are less of concern, as the price-based FJ control exhibits an acceptable performance compared to the centralized (exhaustive) approach (cf. Fig. 8 (a)).

[9]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.

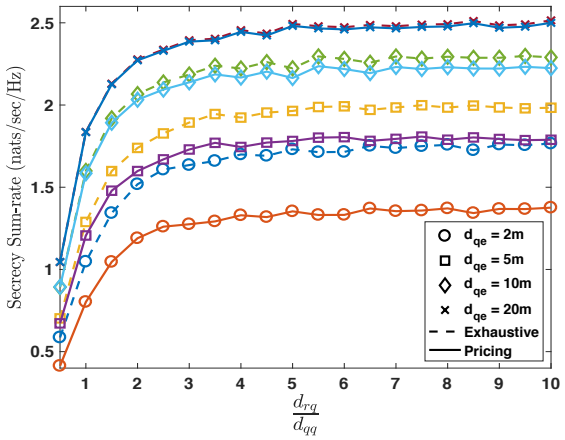
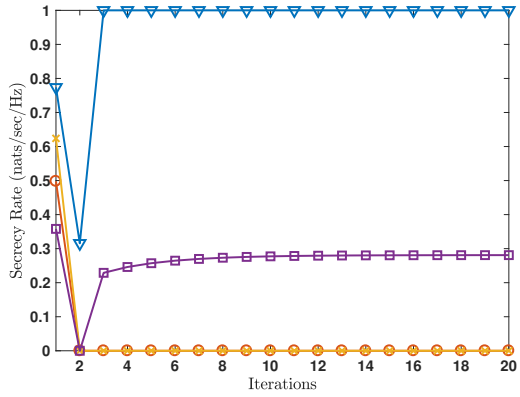


Fig. 5: Secrecy sum-rate of price-based FJ control for different interference levels and different Eve locations, $(Q = 4, \frac{P_q}{N_0} = 30$ dB, $N_q = 5, M_q = 4, L = 4)$.

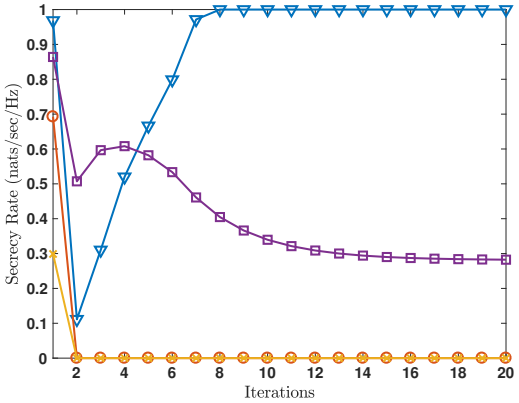
Gauss-Seidel method. Furthermore, the Jacobi method was found to be a bit faster in rate of convergence, as all links simultaneously update their TxFJ powers compared to the Gauss-Seidel method in which at each iteration only one link updates its TxFJ power.

Fig. 7 shows the convergence of the rate adjustment for one channel realization. We randomly initialize $\gamma_q,\ \forall q$, 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. Hence, each iteration of Fig. 7 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 increment of γ_q to $0.2P_q$ 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. 8 (a) and (b) show the secrecy sum-rate of the greedy FJ control compared to the price-based FJ control and exhaustive method for different power constraints of Alices. We assumed that all Alices use the same amount of power constraint. For Fig. 8 (a) 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



(a)



(b)

Fig. 6: Convergence of price-based FJ control for different links, $(Q = 4, \frac{P_q}{N_0} = 30$ dB$, N_q = 5, M_q = 4, L = 4)$

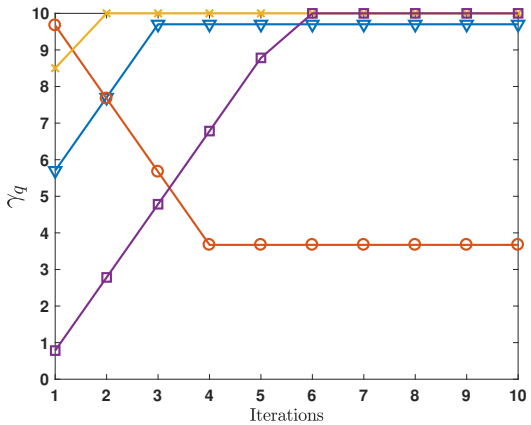
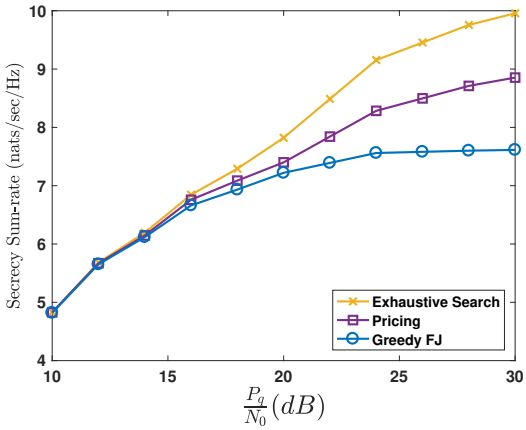


Fig. 7: Convergence of rate demands, $(Q = 4)$.

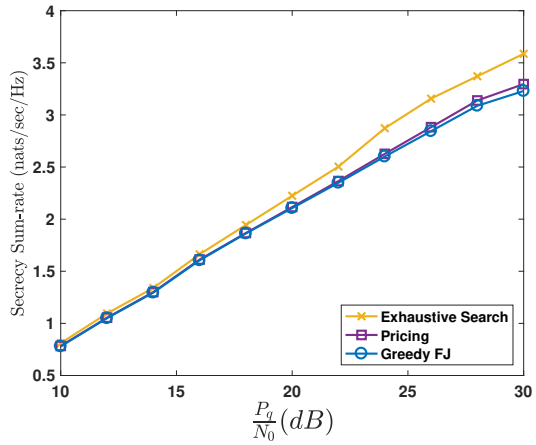
for each link is set to $R_q = 2$nats/sec/Hz, $\forall q \in \mathcal{Q}$. The maximum number of iteration for both the pricing part and rate adjustment is set to 50. We ran each method for a total of 30 placements. For each placement, we tested 100 channel realizations. It can be seen that for low transmit powers, the greedy FJ has a comparable secrecy sum-rate, verifying Proposition 3. As the transmit power increases, the secrecy sum-rate of the greedy method becomes more inferior to the exhaustive and pricing approach, as high interference decreases the information rate of legitimate links, thus lowering the total secrecy in the network. Having low transmit power for each link may compromise the achievability of positive secrecy as well, thus lowering the secrecy sum-rate of the price-based FJ control as previously seen in Fig. 5. However, we see that for this simulation which is a more realistic scenario compared to the settings of Fig. 5, the price-based FJ control has a comparable performance to the exhaustive search for low transmit powers, indicating that positive secrecy is a less concerning issue in more realistic scenarios. Fig. 8 (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 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. 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.

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.



(a)



(b)

Fig. 8: Optimality of the greedy FJ control under different scenarios, $(Q = 4, N_q = 5, M_q = 4, L = 4)$

Fig. 9 depicts the secrecy sum-rate versus Eve's location for a given total power constraint. We compare the performance of the proposed price-based FJ control under complete knowledge of ECSI (indicated by "Pricing (Full ECSI)") with other methods including when every link allocates all its power to information signal (indicated by "No Jamming"), when the Pareto-optimal set of TxFJs is found via exhaustive search (indicated by "Exhaustive Search"), and the greedy FJ method (indicated by "Greedy FJ"). It can be seen that greedy FJ outperforms no-jamming for all of Eve's locations. Furthermore, when $\hat{x}_e \in [-8, -2]$, the performance of price-based FJ is equal to the performance of greedy FJ and that of exhaustive search[10], which indicates that greedy FJ is optimal in these scenarios. Also, for all of Eve's locations, the performance of the pricing scheme is close to that of the exhaustive search approach. Throughout our

[10]For the exhaustive search, we also assume to have complete knowledge of the eavesdropping channels.

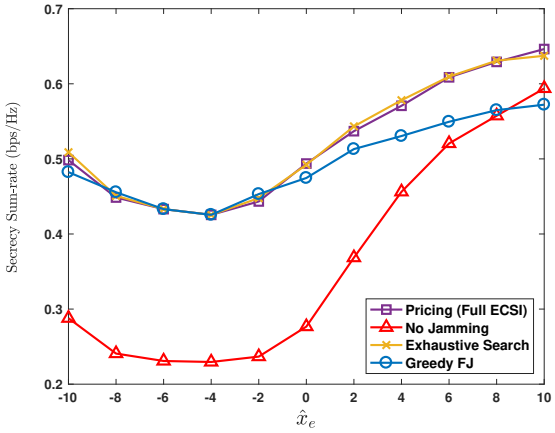


Fig. 9: Effect of Eve's location on the secrecy sum-rate for two links, $(\text{Alice}_1 = (-5, 8),\ \text{Bob}_1 = (5, 8),\ \text{Alice}_2 = (-5, -8),\ \text{Bob}_2 = (5, -8), \hat{y}_e = 3.5, \hat{r}_e = 1.6,\ P_q = -32$ dBm, $N_q = 3,\ M_q = 1,\ L = 1)$.

simulations, the optimality of greedy FJ was observed only at when the power constraints are small.

In Fig. 10 and Fig. 11, we depict, respectively, the secrecy sum-rate and individual secrecy rates for when constraint (18) is taken into account in the pricing method (indicated as "Pricing (Full 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 pricing method can be even lower than the greedy approach with zero secrecy rate for one or both links at some locations of Eve.

In Fig. 12, we compare the performance of Algorithm 1 (indicated as "Robust") with other approaches. The spatial distribution for Eve is the same as in previous simulations, 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 algorithm is used [37, 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

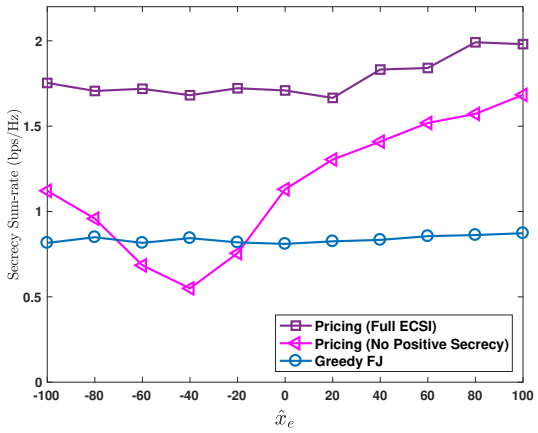
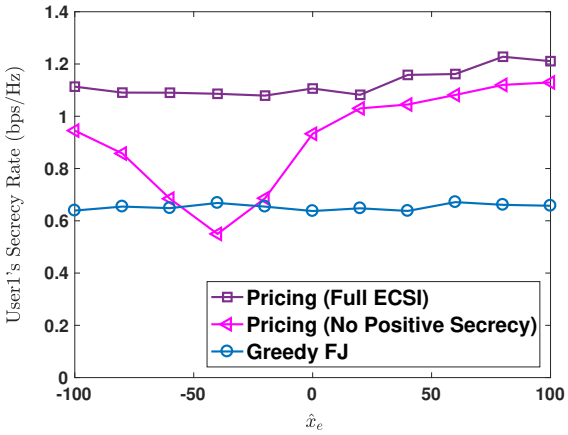


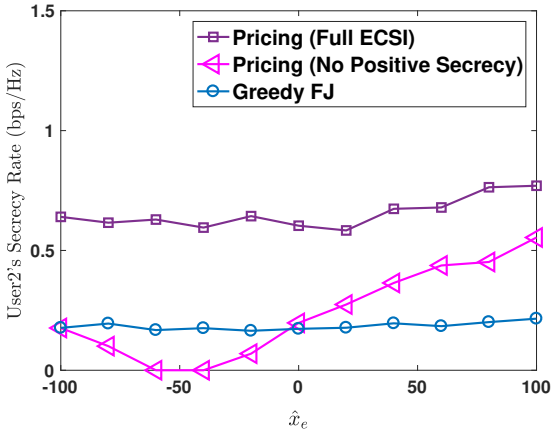
Fig. 10: Effect of Eve's location on the secrecy sum-rate or two links, $(\text{Alice}_1 = (-50, 10),\ \text{Bob}_1 = (5, 10),\ \text{Alice}_2 = (-50, -10),\ \text{Bob}_2 = (50, 10), \hat{y}_e = 0, \hat{r}_e = 10,\ P_q = 0$ dBm, $N_q = 3,\ M_q = 1,\ L = 1)$.

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 runs. 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. 13 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.



(a)



(b)

Fig. 11: Effect of Eve's location on individual secrecy rates for two links (the configurations are the same as Fig. 10.)

IX. Conclusion

In this paper, we studied distributed design of FJ control in an multi-link interference network. We showed that greedy FJ is not an optimal approach in securing the network. Accordingly, we designed a price-based TxFJ control that guarantees a local optimum point for the maximum secrecy sum-rate. Through simulations, we observed a noticeable improvement in the secrecy sum-rate when pricing is leveraged for friendly jamming control. We then introduced uncertainty in the eavesdropping channel and designed a robust method, which was shown via simulations to achieve a higher secrecy sum-rate than the greedy FJ approach.

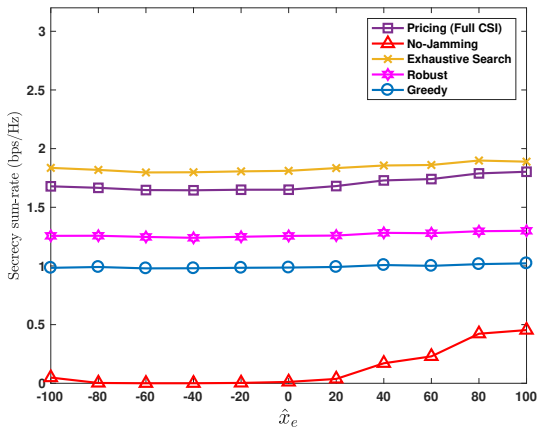


Fig. 12: Effect of Eve's location on the secrecy sum-rate for two links,($\text{Alice}_1 = (-40, 20), \text{Bob}_1 = (40, 20), \text{Alice}_2 = (-40, -20), \text{Bob}_2 = (40, -20), \hat{y}_e = 25, \hat{r}_e = 20,\ P_q = 10$ dBm, $N_q = 3, M_q = L = 1$).

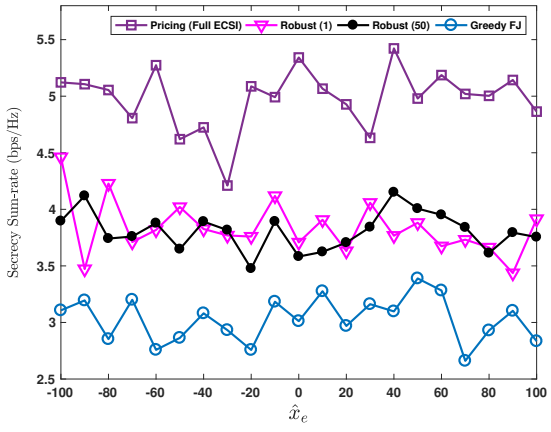


Fig. 13: Effect of number of data transmissions for two links, $(\text{Alice}_1 = (-20, 20), \text{Bob}_1 = (20, 20), \text{Alice}_2 = (-20, -20), \text{Bob}_2 = (20, -20), \hat{y}_e = 10,\ \hat{r}_e = 20,\ P_q = 10$ dBm, $N_q = 4, M_q = L = 1$).

ACKNOWLEDGEMENTS

This research was supported in part by NSF (grants CNS-1409172 and CNS-1513649) and Australian Research Council (Discovery Early Career Researcher Award DE150101092). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF or ARC.

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] D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the cellular message encryption algorithm," in *Proc. 17th Annual International Cryptology Conf.*, B. S. Kaliski, Ed.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[4] 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.

[5] 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.

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

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas part II: The MIMOME wiretap channel," *IEEE Trans. on Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[8] 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.

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

[10] 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.

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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, *IEEE Trans. Inf. Theory", title="Interference Alignment for Secrecy", year=2011, volume=57, number=6, pages="3323–3332", month=june,.*

[18] 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.

[19] K. H. Ha, T. T. Vu, T. Q. Duong, and N.-S. Vo, *On the Interference Alignment Designs for Secure Multiuser MIMO Systems*. [Online]. Available: https://arxiv.org/pdf/1508.00349.pdf

[20] 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.

[21] 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.

[22] J. Xie and S. Ulukus, "Secure degrees of freedom regions of multiple access and interference channels: The polytope structure," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 2044–2069, Apr 2016.

[23] ——, "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.

[24] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[25] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, *IEEE Trans. Signal Process.", title="Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers", year=2013, volume=61, number=20, pages="4962–4974", month=Oct,.*

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

[27] 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.

[28] M. Schulz and A. L. andMatthias Hollick, "Practical known-plaintext attacks against physical layer security in wireless MIMO systems," in *Proc. NDSS Conf.*, Feb. 2014.

[29] 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.

[30] 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 optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

[31] 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.

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

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

[34] D. Schmidt, C. Shi, R. Berry, M. Honig, and W. Utschick, "Distributed resource allocation schemes," *IEEE Signal Processing Mag.*, vol. 26, no. 5, pp. 53–63, Sep. 2009.

[35] D. Nguyen and M. Krunz, "Price-based joint beamforming and spectrum management in multi-antenna cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 11, pp. 2295–2305, Dec. 2012.

[36] G. Scutari, F. Facchinei, J.-S. Pang, and D. Palomar, "Real and complex monotone communication games," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4197–4231, Jul. 2014.

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

[38] 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.

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

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

[41] 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.

[42] 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.

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

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

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

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

[47] 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.

[48] G. Scutari, F. Facchinei, P. Song, D. P. Palomar, and J. S. Pang, "Decomposition by partial linearization: Parallel optimization of multi-agent systems," *IEEE Trans. Signal Process.*, vol. 62, no. 3, pp. 641–656, Feb. 2014.

[49] 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.

[50] 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.

[51] C. Shi, R. A. Berry, and M. L. Honig, "Monotonic convergence of distributed interference pricing in wireless networks," in *Proc. IEEE Int. Symp. Inf. Theory*, 2009, pp. 1619–1623.

[52] S. H. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.

[53] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

[54] R. A. Iltis, S.-J. Kim, and D. A. Hoang, "Noncooperative iterative mmse beamforming algorithms for ad-hoc networks," *IEEE Trans. Commun.*, vol. 54, no. 4, pp. 748–759, Apr. 2006.

[55] G. Scutari, S. Barbarossa, and D. P. Palomar, "Potential games: A framework for vector power control problems with coupled constraints," in *Proc. IEEE ICASSP Conf.*, vol. 4, May 2006, pp. IV–IV.

[56] D. Nguyen and M. Krunz, "Spectrum management and power allocation in mimo cognitive networks," University of Arizona, Tech. Rep. TR-UA-ECE-2011-2, Tech. Rep., 2011. [Online]. Available: http://www.ece.arizona.edu/~krunz/TR/MIMOcognitiveTR_Aug2011.pdf

[57] M. Jakobsson, S. MagnÕe̊sson, C. Fischione, and P. C. Weeraddana, "Extensions of Fast-Lipschitz optimization," *IEEE Trans. Automat. Control*, vol. 61, no. 4, pp. 861–876, Apr 2016.

APPENDIX A

PROOF OF THEOREM 1

Let the Lagrangian of (22) w.r.t $\boldsymbol{\sigma}$ be denoted as $\mathcal{L}(\boldsymbol{\sigma})$. Also, let the Lagrangian of (24) w.r.t σ_q be denoted as $\mathcal{L}_q(\sigma_q),\ \forall q$. For $\boldsymbol{\sigma}^* = [\sigma_q^*]_{q=1}^Q$, with σ_q^* defined in (26), to be a locally optimal solution of (22), the K.K.T. conditions of both (22) and (24) must be equivalent. That is,

$$\frac{\partial \mathcal{L}(\boldsymbol{\sigma}^*)}{\partial \sigma} = \begin{bmatrix} \frac{\partial \mathcal{L}(\boldsymbol{\sigma}^*)}{\partial \sigma_1} \\ \vdots \\ \frac{\partial \mathcal{L}(\boldsymbol{\sigma}^*)}{\partial \sigma_Q} \end{bmatrix} = \begin{bmatrix} \frac{\partial \mathcal{L}_1(\boldsymbol{\sigma}^*)}{\partial \sigma_1} \\ \vdots \\ \frac{\partial \mathcal{L}_Q(\boldsymbol{\sigma}^*)}{\partial \sigma_Q} \end{bmatrix} = 0. \tag{40}$$

Simplifying (40), we have $\lambda_q = -\sum_{\substack{r=1 \\ r\neq q}}^{Q} \frac{\partial C_r^{sec}}{\partial \sigma_q}$ which is the same as (25). Thus, assuming that iterative application of (26) converges to a NE, that NE is a locally optimal solution to (22)

The local optimality of the NE requires proving that (26) converges to the NE . Convergence to NE can be proven following the same approach used in [51, Appendix A]. Basically, once positive secrecy of link q is achieved for all q, then the secrecy rate of the qth link becomes a convex function of σ_r, $r \neq q,\ r \in \mathcal{Q}$. Then, the convergence can be proven using monotonic convergence theorem, i.e., the secrecy sum-rate becomes an upper-bounded and non-decreasing function of the TxFJ powers at each iteration.

APPENDIX B

PROOF OF PROPOSITION 1

Before proving this property, we present a useful lemma. We then leverage the result of this lemma to the game in (24) and prove the uniqueness of its NE[11]. The following lemma sets the conditions that allow us to approximate the secrecy sum-rate as a concave function:

Lemma 1. *For all links that satisfy the bound in* (18)*, in the case of low interference, the secrecy sum-rate* C^{sec} *becomes a concave function of the vector* $\ln \boldsymbol{\sigma} = [\ln \sigma_q]_{q=1}^Q$.

[11]Note that the existence of NE is already known, as the strategy set of each player is a closed and convex set, and the utiltiy of each player is a concave function of his action [33].

$$C_q^{sec} = \log\left(1 + \frac{\left|\mathbf{d}_q^\dagger \mathbf{H}_{qq}\right|^2 \gamma_q}{\sum_{\substack{r=1 \\ r\neq}}^{Q}\left(\left|\mathbf{d}_q^\dagger \mathbf{H}_{rq}\right|^2 \gamma_r + \left|\mathbf{d}_q^\dagger \mathbf{H}'_{rq}\right|^2 \sigma_r\right) + N_0}\right) - \log\left(1 + \frac{\left|\mathbf{d}_q^\dagger \mathbf{H}_{qq}\right|^2 \gamma_q}{\left|\mathbf{d}_q^\dagger \mathbf{H}_{qq}\right|^2 \frac{\left|\mathbf{r}_q^\dagger \mathbf{G}'_q\right|^2}{\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2}\delta_q + \sum_{\substack{r=1 \\ r\neq}}^{Q}\left(\left|\mathbf{d}_q^\dagger \mathbf{H}_{rq}\right|^2 \gamma_r + \left|\mathbf{d}_q^\dagger \mathbf{H}'_{rq}\right|^2 \sigma_r\right) + N_0}\right) \tag{41}$$

Proof: Note that satisfying the bound in (18)*, or* $\sigma_q \in \mathcal{D}_q,\ \forall q$*, with* $\mathcal{D}_q$ *defined in* (22)*, is directly interpreted as either having an eavesdropper that is far enough from the links or having not too demanding rate constraints at the qth link which leaves enough power for TxFJ to satisfy the positive secrecy constraint in* (18) *(i.e., not ending up to the case in* (20a)*). Hence, considering* $\sigma_q \in \mathcal{D}_q,\ \forall q$*, one can set* σ_q *as* $\sigma_q = \frac{A_q}{B_q} + \delta_q$ *where* $\delta_q > 0$ *is upper-bounded until* σ_q *meets its maximum value defined in* (22)[12]*. Note that contrary to* (21) *where* δ_q *is a small positive value, here,* δ_q *can take any positive value as long as* $\sigma_q \in \mathcal{D}_q$*. For example in the case of* $A_q < 0$*, we can set* $\delta_q = -\frac{A_q}{B_q}$*, so that* $\sigma_q = 0$ *as in* (21d)*. Replacing* $\sigma_q = \frac{A_q}{B_q} + \delta_q$ *in the secrecy rate given in* (9)*, wherein* $\mathcal{G}_q$ *is as in* (14)*, we can have a simplified equation for secrecy rate given in* (41)[13]*. It can be easily seen in* (41) *that with* $\sigma_q = \frac{A_q}{B_q} + \delta_q$ *(or equivalently* $\sigma_q \in \mathcal{D}_q$*), positive secrecy is achievable because the second term in* (41) *is always less than the first term as long as* $\delta_q > 0$*. Assume that* $\left|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{qq}\right|^2 \gg \sum_{\substack{r=1 \\ r\neq}}^{Q}\left(\left|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{rq}\right|^2 \gamma_r + \left|\boldsymbol{d}_q^\dagger \boldsymbol{H}'_{rq}\right|^2 \sigma_r\right) + N_0,\ \forall q$*, indicating low interference at each legitimate receiver. Also, assume that* $\left|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{qq}\right|^2 \frac{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}'_q\right|^2}{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}_q\right|^2}\delta_q \gg \sum_{\substack{r=1 \\ r\neq}}^{Q}\left(\left|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{rq}\right|^2 \gamma_r + \left|\boldsymbol{d}_q^\dagger \boldsymbol{H}'_{rq}\right|^2 \sigma_r\right) + N_0,\ \forall q$*, which mainly suggests low interference together with* $\delta_q > 0,\ \forall q$ *such that* $\frac{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}'_q\right|^2}{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}_q\right|^2}\delta_q \geq 1$*. Note that* $\frac{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}'_q\right|^2}{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}_q\right|^2} > 1$ *because the term* $\boldsymbol{r}_q^\dagger \boldsymbol{G}'_q$ *is a vector of i.i.d ZMCSCG random variables and the term* $\boldsymbol{r}_q^\dagger \boldsymbol{G}_q$ *is a scalar ZMCSCG [52], the norm of these two terms is expected to be larger than one*[14]*. Hence, we only*

[12]Note that we do not simply subtract $\frac{A_q}{B_q}$ from $P^{jam} = \frac{P_q - \gamma_q}{N_q - 1}$ to find an upper bound for δ_q, as it is possible that $A_q < 0$.

[13]The details of this simplification is skipped for the sake of brevity. Nevertheless, one can input the secrecy rate in (9) with $\sigma_q = \frac{A_q}{B_q} + \delta_q$ to a mathematical symbolic computation software such as *Mathematica* to obtain the simplified equation in (41).

[14]One can use the law of large numbers as in [11] to prove this for large number of transmit/receive antennas. However, we saw the same trend even for a moderate number of transmit/receive antennas.

require $\delta_q > 1$. Under these assumptions, the secrecy rate C_q^{sce} in (41) *can be approximated to*

$$C_q^{sec} \approx \log\left(\frac{\left|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{qq}\right|^2 \gamma_q}{\sum_{\substack{r=1\\r\neq}}^{Q}\left(\left|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{rq}\right|^2 \gamma_r + \left|\boldsymbol{d}_q^\dagger \boldsymbol{H}'_{rq}\right|^2 \sigma_r\right) + N_0}\right) - \log\left(1 + \frac{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}_q\right|^2 \gamma_q}{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}'_q\right|^2 \delta_q}\right). \tag{42}$$

Let $\boldsymbol{\rho} = [\rho_q]_{q=1}^Q$ where $\rho_q \triangleq \ln \sigma_q$. Hence, (42) *can be rewritten as*

$$C_q^{sec}(\boldsymbol{\rho}) \approx \log\left(\frac{\left|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{qq}\right|^2 \gamma_q}{\sum_{\substack{r=1\\r\neq}}^{Q}\left(\left|\boldsymbol{d}_q^\dagger \boldsymbol{H}_{rq}\right|^2 \gamma_r + \left|\boldsymbol{d}_q^\dagger \boldsymbol{H}'_{rq}\right|^2 e^{\rho_r}\right) + N_0}\right) - \log\left(1 + \frac{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}_q\right|^2 \gamma_q}{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}'_q\right|^2 (e^{\rho_q} - \frac{A_q}{B_q})}\right). \tag{43}$$

It is known that $\log\left(1 + \sum_{q=1}^Q e^{\rho_q}\right)$ is convex in $\mathbb{R}^Q$ [53, Chap. 3.1.5]. Hence, the first term in (43) *is a concave function of $\boldsymbol{\rho} = [\rho_r]_{\substack{r=1\\r\neq q}}^Q$. Also, the second term is a concave function of $\ln \sigma_q$ for $\ln \sigma_q > \frac{1}{2}\ln(\frac{A_q}{B_q}(\frac{A_q}{B_q} - \frac{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}_q\right|^2 \gamma_q}{\left|\boldsymbol{r}_q^\dagger \boldsymbol{G}'_q\right|^2}))$. Because we already have the assumption of $\sigma_q > \frac{A_q}{B_q}$, then the second term in* (43) *is a concave function of $\rho_q = \ln(\sigma_q)$. Therefore, the approximation of C_q^{sec} is a concave function of $\boldsymbol{\rho} = \ln \boldsymbol{\sigma}$.* ■

Now, let us turn our attention to the game in (24). In order to show that there is a unique NE to this game (under the conditions of Proposition 1), we use contradiction. Assume that there are two NEs for the game in (24), namely $\bar{\boldsymbol{\sigma}} = [\bar{\sigma}_q]_{q=1}^Q$ and $\tilde{\boldsymbol{\sigma}} = [\tilde{\sigma}_q]_{q=1}^Q$. Hence, they both satisfy the K.K.T. conditions of (24) for all q, i.e.,

$$\frac{\partial}{\partial \sigma_q} C_q^{sec}(\bar{\boldsymbol{\sigma}}) - \lambda_q + \boldsymbol{\nu}_{q1}^T \frac{\partial}{\partial \sigma_q} \boldsymbol{f}_q(\bar{\boldsymbol{\sigma}}) = 0 \tag{44a}$$

$$\frac{\partial}{\partial \sigma_q} C_q^{sec}(\tilde{\boldsymbol{\sigma}}) - \lambda_q + \boldsymbol{\nu}_{q2}^T \frac{\partial}{\partial \sigma_q} \boldsymbol{f}_q(\tilde{\boldsymbol{\sigma}}) = 0 \tag{44b}$$

where $\boldsymbol{f}_q = [\sigma_q - \chi_q, \frac{P_q - \gamma_q}{N_q - 1} - \sigma_q]^T$, $\boldsymbol{\nu}_{q1} = [\nu_{q1}^{(1)}, \nu_{q1}^{(2)}]^T$, and $\boldsymbol{\nu}_{q2} = [\nu_{q2}^{(1)}, \nu_{q2}^{(2)}]^T$ are the vectors of Lagrange multipliers corresponding to the TxFJ power constraints of Alice$_q$. The result of Theorem 1 suggests that

equations in (44) can be equivalently written as

$$\nabla_{\boldsymbol{\sigma}} C^{sec}(\bar{\boldsymbol{\sigma}}) + \boldsymbol{\Upsilon}_1 \nabla_{\boldsymbol{\sigma}} \boldsymbol{f}(\bar{\boldsymbol{\sigma}}) = \mathbf{0} \tag{45a}$$

$$\nabla_{\boldsymbol{\sigma}} C^{sec}(\tilde{\boldsymbol{\sigma}}) + \boldsymbol{\Upsilon}_2 \nabla_{\boldsymbol{\sigma}} \boldsymbol{f}(\tilde{\boldsymbol{\sigma}}) = \mathbf{0} \tag{45b}$$

where $\nabla_{\boldsymbol{\sigma}} C^{sec}$ is the gradient of C^{sec} w.r.t. $\boldsymbol{\sigma}$, $\boldsymbol{f} = [\boldsymbol{f}_1^T, \ldots, \boldsymbol{f}_Q^T]^T$, $\nabla_{\boldsymbol{\sigma}} \boldsymbol{f}(\boldsymbol{\sigma}) = [\frac{\partial}{\partial \sigma_1} \boldsymbol{f}_1^T(\boldsymbol{\sigma}), \ldots, \frac{\partial}{\partial \sigma_Q} \boldsymbol{f}_Q^T(\boldsymbol{\sigma})]^T$, $\boldsymbol{\Upsilon}_1$ and $\boldsymbol{\Upsilon}_2$ are block diagonal matrices with $[\boldsymbol{\Upsilon}_1]_{qq} = \boldsymbol{\nu}_{q1}^T$ and $[\boldsymbol{\Upsilon}_2]_{qq} = \boldsymbol{\nu}_{q2}^T,\ q \in \mathcal{Q}$ where $[\bullet]_{qq}$ denotes the block on the qth row and the qth column, and finally $\mathbf{0}$ is a vector of zeros (of appropriate size). Multiplying both sides of equations in (45) by $(\tilde{\boldsymbol{\sigma}} - \bar{\boldsymbol{\sigma}})^T$ and subtracting (45b) from (45a) we have

$$\begin{aligned}&(\tilde{\boldsymbol{\sigma}} - \bar{\boldsymbol{\sigma}})^T \nabla_{\boldsymbol{\sigma}} C^{sec}(\bar{\boldsymbol{\sigma}}) + (\bar{\boldsymbol{\sigma}} - \tilde{\boldsymbol{\sigma}})^T \nabla_{\boldsymbol{\sigma}} C^{sec}(\tilde{\boldsymbol{\sigma}}) + \\ &(\tilde{\boldsymbol{\sigma}} - \bar{\boldsymbol{\sigma}})^T \boldsymbol{\Upsilon}_1 \nabla_{\boldsymbol{\sigma}} \boldsymbol{f}(\bar{\boldsymbol{\sigma}}) + (\bar{\boldsymbol{\sigma}} - \tilde{\boldsymbol{\sigma}})^T \boldsymbol{\Upsilon}_2 \nabla_{\boldsymbol{\sigma}} \boldsymbol{f}(\tilde{\boldsymbol{\sigma}}) = 0.\end{aligned} \tag{46}$$

Recalling Theorem 1, at the NE of the price-based method, a locally optimum point of C^{sec} would be found. Thus, both $\bar{\boldsymbol{\sigma}}$ and $\tilde{\boldsymbol{\sigma}}$ satisfy the following unilateral optimality for every player q:

$$C^{sec}(\bar{\sigma}_q, \bar{\boldsymbol{\sigma}}_{-q}) \geq C^{sec}(\sigma_q, \bar{\boldsymbol{\sigma}}_{-q}),\ \forall \sigma_q \in \mathcal{D}_q,\ \forall q \tag{47a}$$

$$C^{sec}(\tilde{\sigma}_q, \tilde{\boldsymbol{\sigma}}_{-q}) \geq C^{sec}(\sigma_q, \tilde{\boldsymbol{\sigma}}_{-q}),\ \forall \sigma_q \in \mathcal{D}_q,\ \forall q \tag{47b}$$

where $\bar{\boldsymbol{\sigma}}_{-q} = (\bar{\sigma}_1, \ldots, \bar{\sigma}_{q-1}, \bar{\sigma}_{q+1}, \ldots, \bar{\sigma}_Q)$ is the set of all TxFJ powers except that of the qth link (equivalent notation also holds for $\tilde{\boldsymbol{\sigma}}_{-q}$). Convexity of each player's strategy set (i.e., concavity of f_q) suggests that the terms in (46) that are related to the constraints can be lower-bounded as

$$\begin{aligned}&(\tilde{\boldsymbol{\sigma}} - \bar{\boldsymbol{\sigma}})^T \boldsymbol{\Upsilon}_1 \nabla_{\boldsymbol{\sigma}} \boldsymbol{f}(\bar{\boldsymbol{\sigma}}) + (\bar{\boldsymbol{\sigma}} - \tilde{\boldsymbol{\sigma}})^T \boldsymbol{\Upsilon}_2 \nabla_{\boldsymbol{\sigma}} \boldsymbol{f}(\tilde{\boldsymbol{\sigma}}) \geq \\ &\boldsymbol{\Upsilon}_1(\boldsymbol{f}(\tilde{\boldsymbol{\sigma}}) - \boldsymbol{f}(\bar{\boldsymbol{\sigma}})) + \boldsymbol{\Upsilon}_2(\boldsymbol{f}(\bar{\boldsymbol{\sigma}}) - \boldsymbol{f}(\tilde{\boldsymbol{\sigma}})) = \\ &\boldsymbol{\Upsilon}_1(\boldsymbol{f}(\tilde{\boldsymbol{\sigma}})) + \boldsymbol{\Upsilon}_2(\boldsymbol{f}(\bar{\boldsymbol{\sigma}})) \geq 0\end{aligned} \tag{48}$$

where we used the complementary slackness conditions, i.e., $\boldsymbol{\nu}_{q_1} \circ f_q(\bar{\boldsymbol{\sigma}}) = \mathbf{0}$ and $\boldsymbol{\nu}_{q_2} \circ f_q(\tilde{\boldsymbol{\sigma}}) = \mathbf{0}$ with $\circ$

and $\mathbf{0}$ denoting the Hadamard product and a vector of zeros (of appropriate size), respectively. Under the conditions of Proposition 1, we can approximate C^{sec} as a concave function of $\ln \bar{\boldsymbol{\sigma}}$ or $\ln \tilde{\boldsymbol{\sigma}}$ where $\ln(\bullet)$ is applied to each element of a vector (cf. Lemma 1). The second term in (43) shows that for all q, the utility of the qth player is a concave function of $\ln \sigma_q$. Moreover, the approximation in (43) is a strictly increasing function of σ_q. Next, the function $\ln \sigma_q$ is concave w.r.t. σ_q. Hence, we can conclude that (43) is a strictly concave function of σ_q[15]. Lastly, the first two terms of (46) can be simplified to

$$\sum_{q=1}^{Q}(\tilde{\sigma}_q - \bar{\sigma}_q)\frac{\partial}{\partial \sigma_q}C^{sec}(\bar{\boldsymbol{\sigma}}) + (\bar{\sigma}_q - \tilde{\sigma}_q)\frac{\partial}{\partial \sigma_q}C^{sec}(\tilde{\boldsymbol{\sigma}}). \tag{49}$$

Therefore,

$$\begin{aligned}&\sum_{q=1}^{Q}(\tilde{\sigma}_q - \bar{\sigma}_q)\frac{\partial}{\partial \sigma_q}C^{sec}(\bar{\boldsymbol{\sigma}}) + (\bar{\sigma}_q - \tilde{\sigma}_q)\frac{\partial}{\partial \sigma_q}C^{sec}(\tilde{\boldsymbol{\sigma}}) > \\ &\sum_{q=1}^{Q}(C^{sec}(\tilde{\sigma}_q, \bar{\boldsymbol{\sigma}}_{-q}) - C^{sec}(\bar{\boldsymbol{\sigma}})) + (C^{sec}(\bar{\sigma}_q, \tilde{\boldsymbol{\sigma}}_{-q}) - C^{sec}(\tilde{\boldsymbol{\sigma}})).\end{aligned} \tag{50}$$

Due to strictly increasing property of C^{sec} w.r.t. σ_q and the inequality in (47), one can consider that if $C^{sec}(\tilde{\sigma}_q, \bar{\boldsymbol{\sigma}}_{-q}) < C^{sec}(\bar{\boldsymbol{\sigma}})$, then $\tilde{\sigma}_q < \bar{\sigma}_q$. On the other hand, as the second term in the right hand side (RHS) of (50) suggests, $C^{sec}(\bar{\sigma}_q, \tilde{\boldsymbol{\sigma}}_{-q}) < C^{sec}(\tilde{\boldsymbol{\sigma}})$ means that $\bar{\sigma}_q < \tilde{\sigma}_q$. This contradiction together with the result obtained in (48) suggests that (46) does not hold except only for the case where $\bar{\sigma}_q = \tilde{\sigma}_q,\ \forall q \in \mathcal{Q}$, which contradicts the assumption of existence of two different NEs. Hence, the NE of this game must be unique. Also, the approximation of C_q^{sec} is a concave function of $\boldsymbol{\rho} = \ln \boldsymbol{\sigma}$, $\forall q \in \mathcal{Q}$. Furthermore, Theorem 1 suggests that every NE of the price-based FJ control is a local optimum of the secrecy sum-rate maximization. Thus, the unique NE of the price-based game is the global maximum of the secrecy sum-rate maximization problem in (22).

The convergence of iterative optimization in (24), wherein C_q^{sec} is written according to (42) and subsequently $\lambda_q = -\sum_{r \neq q} \frac{\partial C_r^{sec}}{\partial \sigma_q}$, can be established by finding a Lyapunov-type function of the TxFJ

[15]Specifically, we use the fact that for a convex function $g(x)$ and a nondecreasing convex function $f(x)$, the composite function $f\left(g(x)\right)$ is convex w.r.t. x [53].

powers for the qth player, $\forall q \in \mathcal{Q}$, and show that it is nondecreasing w.r.t. σ_q and upper-bounded. We do not go through the details of this proof for the sake of brevity (see [54], [55, Section 2.2], and [56, Appendix IV]).

APPENDIX C
PROOF OF PROPOSITION 2

In order to prove this property, we leverage the concept of Fast Lipschitz optimization introduced in [57], defined in the following:

Definition 2. *The following problem is said to be of* Fast Lipschitz *form:*

$$\begin{aligned} &\max_{\boldsymbol{x}} \ \boldsymbol{g}_0(\boldsymbol{x}) \\ &\quad \textit{s.t.} \ x_i \leq g_i(\boldsymbol{x}) \ \ \forall i \in \mathbb{A} \\ &\qquad x_i = g_i(\boldsymbol{x}) \ \ \forall i \in \mathbb{B} \end{aligned} \tag{51}$$

where

- $\boldsymbol{x} = [x_i]_{i=1}^n$ *is the vector of decision variables (not to be confused with the information signals defined in Section II).*
- $\boldsymbol{g}_0 : \mathbb{R}^n \to \mathbb{R}^m$ *is a differentiable scalar ($m = 1$) or vector-valued ($m \geq 2$) function.*
- $\mathbb{A}$ *and* $\mathbb{B}$ *are complementary subsets of* $\{1, 2, \ldots, n\}$.
- $g_i : \mathbb{R}^n \to \mathbb{R}$ *are differentiable functions.*

For the case of $\mathbf{g}_0$ being a vector valued function, the problem in (51) is sometimes called vector optimization, where the aim is to maximize all the elements of $\mathbf{g}_0$ with respect to the nonnegative orthant $\mathbb{R}_+^m$ (i.e., a proper cone [53, Section 4.7]), indicating that all the elements of $\mathbf{g}_0$ must remain positive. A feasible decision vetor $\mathbf{x}^*$ is said to be *Pareto-optimal* if there is no other feasible vector $\tilde{\mathbf{x}}$ such that $\mathbf{g}_0(\mathbf{x}^*) \geq \mathbf{g}_0(\tilde{\mathbf{x}})$ where the inequality is element-wise. If such Pareto-optimal point is unique, then $\mathbf{x}^*$ is the best achievable decision vector. The authors in [57] proved that if some sufficient conditions (derived

in [57, Theorem 7]) hold for the problem in (51), then a unique Pareto-optimal point for the problem in (51) exists and can be found via the iterative computation $\mathbf{x}^* = \mathbf{g}(x^*)$ where $\mathbf{g} = [g_i]_{i=1}^m$.

If the set of feasible vectors is a convex set, then one can convert the objective in (51) to the following form

$$\max_{\mathbf{x}} \ \nu^T \mathbf{g}_0(\mathbf{x}) \tag{52}$$

where ν is a vector of positive weights. It can be shown that any Pareto-optimal point of (51) can be found by a proper choice of weights in (52) [32]. Looking back at the problem where the aim was to solve (17), it turns out that the same scalarization technique used in (52) is actually used in (17) as well where the elements of $\mathbf{g}_0$ where set to individual secrecy rates, the decision vector $\mathbf{x}$ was set to the vector of TxFJ powers, and the weight vector ν's elements were set to 1. Moreover, the uniqueness of the Pareto-optimal point of (17) (i.e., uniqueness of NE of price-based FJ control defined by (24)) was shown in Proposition 1 for the case where the optimal TxFJ power is not necessarily the maximum TxFJ power, i.e., $\sigma_q = P_q^{jam}$.

Here, we would like to show where using maximum TxFJ power is a unique Pareto-optimal operating point, which can be proven by leveraging Fast-Lipschitz optimization problems. In order to write the Fast Lipschitz form of (17), one can observe that because the problem in (17) has no equality constraints, we can assume that its Fast Lipschitz form does not have equality constraints, i.e., $\mathbb{B} = \emptyset$. Furthermore, because in this proof we are trying to prove the optimality of greedy method (i.e., using maximum TxFJ power), we can set the functions $g_q = P_q^{jam}$, $q \in \mathcal{Q}$.

Now that we have converted the greedy method into a Fast-Lipschitz optimization problem, we can use the properties of this class of optimization problems, specifically [57, Theorem 7] to comment on the conditions that guarantee the greedy method is the unique Pareto-optimal point. Because [57, Theorem 7] provides sufficient conditions (for the uniqueness of the Pareto-optimal optimal point) when the functions $g_q(\mathbf{x})$ are assumed to be of general types, we simplify these conditions to the case where $g_q = P_q^{jam}$ are constant values. The general qualifying conditions in [57, Theorem 7] requires the following for the

uniqueness of the Pareto-optimal point:

- $\nabla \mathbf{g}_0(\mathbf{x})$ must have nonnegative elements with nonzero rows where $\nabla \mathbf{g}_0(\mathbf{x})$ is the Jacobian matrix of $\mathbf{g}_0(\mathbf{x})$ w.r.t. $\mathbf{x}$, i.e., the elements in the qth column of $\nabla \mathbf{g}_0(\mathbf{x})$ are denoted as $[\nabla \mathbf{g}_0(\mathbf{x})]_{:,q} = \frac{\partial \mathbf{g}_0(\mathbf{x})}{\partial x_q}$[16], $q \in \mathcal{Q}$.
- $||\nabla \mathbf{g}|| < 1$ where $\nabla \mathbf{g}$ is the Jacobian matrix of $\mathbf{g} = [g_q]_{q=1}^{Q}$ w.r.t $\mathbf{x}$, i.e., the elements in the qth column of $\nabla \mathbf{g}$ are denoted as $[\nabla \mathbf{g}]_{:,q} = \frac{\partial \mathbf{g}}{\partial x_q}$; and $||\bullet||$ is an arbitrary matrix norm.

  There exists a $k < \infty$ such that
- The kth power of $\nabla \mathbf{g}$, i.e., $(\nabla \mathbf{g})^k$ has nonnegative elements.
- When $k > 1$, then $||\sum_{l=1}^{k-1} (\nabla \mathbf{g})^l|| < z(\mathbf{x}) = \min_q \frac{\min_r [\nabla \mathbf{g}_0(\mathbf{x})]_{rq}}{\max_r [\nabla \mathbf{g}_0(\mathbf{x})]_{rq}}$ where $[\nabla \mathbf{g}_0(\mathbf{x})]_{rq}$ refers to the element in the rth row and qth column of $\nabla \mathbf{g}_0(\mathbf{x})$.

Considering that in our case the elements of $\mathbf{g}_0(\mathbf{x})$ are assumed to represent the individual secrecy rates for all $q \in \mathcal{Q}$, $\mathbf{x}$ is the vector of all links' TxFJ powers, and $\mathbf{g} = [P_q^{jam}]_{q=1}^{Q}$, then the last three items of general qualifying conditions are automatically satisfied (assuming that $z(\mathbf{x}) = 1$ in case of having zeros at both its nominator and denominator). Hence, we only need to satisfy the first item of general qualifying conditions, indicating that $[\nabla \mathbf{g}_0(\mathbf{x})]_{rq} = \frac{\partial C_r^{sec}}{\partial \sigma_q} > 0, r, q \in \mathcal{Q}$, is the only requirement to guarantee that the greedy FJ control is of Fast-Lipschitz form. Hence, the property is proved.

APPENDIX D

PROOF OF PROPOSITION 3

In order to prove this property, we need to make use of the reformulation of the secrecy rate in (41) that we previously utilized in the proof of Proposition 1. According to the proof of Proposition 2, in order for the greedy FJ –which results in using the maximum TxFJ power at each link– to be the unique Pareto-optimal operating point, we only require every element of $\nabla \mathbf{g}_0(\mathbf{x})$ to be nonnegative with nonzero row where $[\nabla \mathbf{g}(\mathbf{x})]_{rq} = \frac{\partial C_r^{sec}}{\partial \sigma_q}, r, q \in \mathcal{Q}$. Given that the secrecy rate of the qth user is a strictly increasing

[16]Note that $\mathbf{g}_0(\mathbf{x})$ is in general a vector. Thus the derivative $\frac{\partial \mathbf{g}_0(\mathbf{x})}{\partial x_q}$ is a vector whose elements are denoted by individual derivative of each element of $\mathbf{g}_0(\mathbf{x})$ w.r.t. $\mathbf{x}$.

function of its own TxFJ, then $\frac{\partial C_r^{sec}}{\partial \sigma_q} > 0, r = q$. For the case of $r \neq q$, the term $\frac{\partial C_r^{sec}}{\partial \sigma_q}$ can be written as

$$\frac{\partial C_r^{sec}}{\partial \sigma_q} = \frac{-\frac{|\mathbf{d}_r \mathbf{H}'_{qr}|^2}{|\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2}\gamma_r}{a_r\left(a_r+\gamma_r\right)} + \frac{\left(\frac{|\mathbf{r}_r^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_r^\dagger \mathbf{G}_r|^2}\delta'_r + \frac{|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2}{|\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2}\right)\gamma_r}{\left(\frac{|\mathbf{r}_r^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_r^\dagger \mathbf{G}_r|^2}\delta_r + a_r\right)\left(\frac{|\mathbf{r}_r^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_r^\dagger \mathbf{G}_r|^2}\delta_r + a_r + \gamma_r\right)} \tag{53}$$

where $\delta_r = \sigma_r - \frac{A_r}{B_r}$ with A_r and B_r defined in (19); and $\delta'_r = \frac{\partial \delta_r}{\partial \sigma_q}$. Note that A_r and B_r are functions of σ_q, so δ'_r is well-defined and is not trivially zero. Let $\frac{|\mathbf{r}_r^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_r^\dagger \mathbf{G}_r|^2} = f_r$ and set $\delta_r = \sigma_r - \frac{A_r}{B_r}$ in (53). Hence, $f_r\delta'_r + \frac{|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2}{|\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2} = \frac{|\mathbf{d}_r^\dagger \mathbf{G}'_q|^2}{|\mathbf{d}_r^\dagger \mathbf{G}_r|^2} > 0$, indicating that the nominator of the second term in the RHS of (53) is always positive. Set the nominator of the second term to $Z > 0$. Given that the first term in the RHS of (53) is always negative, replacing δ_r with $\delta_r = \sigma_r - \frac{A_r}{B_r}$, the following cases can be considered for $\frac{\partial C_r^{sec}}{\partial \sigma_q}$:

1) If $\frac{A_r}{B_r} > 0$, and $|\frac{A_r}{B_r}| < \frac{a_r}{f_r}$: In this case the second term in the RHS of (53), namely $h(\sigma_r)$ which is a function of σ_r, can be written as

$$h(\sigma_r) = \frac{Z}{(\sigma_r + W)(\sigma_r + E)} \tag{54}$$

where both $Z > 0$, $W > 0$, $E > 0$ and $E > W$[17]. The plot of $h(\sigma_r)$ is shown in Fig. 14.

It can be seen that if σ_r is reasonably low (which refers to a low power constraint on TxFJ), then we may have $\frac{\partial C_r^{sec}}{\partial \sigma_q} = \frac{-\frac{|\mathbf{d}_r \mathbf{H}'_{qr}|^2}{|\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2}\gamma_r}{a_r(a_r+\gamma_r)} + h(\sigma_r) > 0$. Note that it could be the case that if W is too large as is shown in Fig. 15, indicating large interference at the rth legitiamte receiver or close proximity of Alice$_r$ to Eve, then even a low value for σ_r cannot be enough to guarantee $\frac{\partial C_r^{sec}}{\partial \sigma_q} > 0$. Note also that for the case of $\frac{A_r}{B_r} < 0$, although we can set $\sigma_r = 0$ by following the procedure in (21), we can still use the above analysis to show that lower values of σ_r (in this case the lowest value) is more probable to make $\frac{\partial C_r^{sec}}{\partial \sigma_q}$.

[17]We do not show the process of simplifying the second term in RHS of (53) to end up with (54) for the sake of brevity. One can use $\delta_r = \sigma_r - \frac{A_r}{B_r}$ in (53) to end up with the same result in (54) for the second term in RHS of (53)

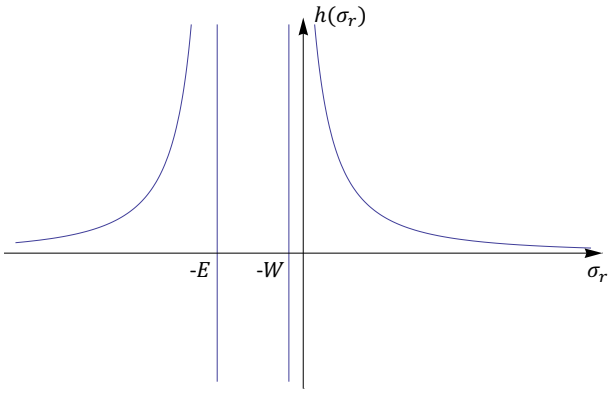


Fig. 14: Plot of $h(\sigma_r)$ when W is small.

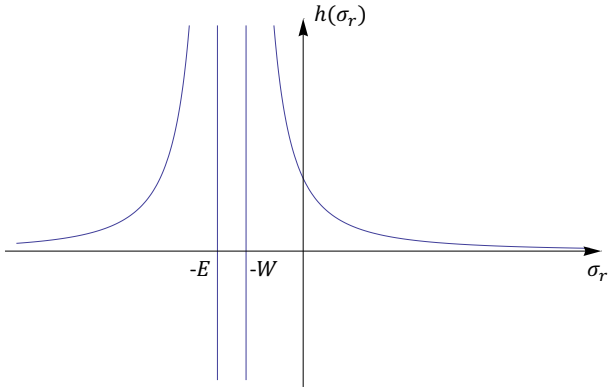


Fig. 15: Plot of $h(\sigma_r)$ when W is large.

2) If $\frac{A_r}{B_r} > 0$ and $\frac{a_r}{f_r} < |\frac{A_r}{B_r}| < \frac{(a_r+\gamma_r)}{f_r}$ or $|\frac{A_r}{B_r}| > \frac{(a_r+\gamma_r)}{f_r}$: In this case the second term in the RHS of (53), namely $h(\sigma_r)$ which is a function of σ_r, can be written as

$$h(\sigma_r) = \frac{Z}{(\sigma_r + W)(\sigma_r + E)} \tag{55}$$

where $W < 0$, but $E > 0$. The plot of $h(\sigma_r)$ is the same as Fig. 14 with the rightmost root shifted to the right side of $\sigma_r = 0$ axis because now W is considered a negative value. It can be easily deduced that for a large value of $|W|$ a moderate/high value of σ_r can make $\frac{\partial C_r^{sec}}{\partial \sigma_q} > 0$. However, it is unlikely to have $\frac{a_r}{f_r} < |\frac{A_r}{B_r}|$. This can be seen from the definition of A_r and B_r in (19), where $\frac{A_r}{B_r}$ has $\frac{a_r}{f_r}$ as its first term which is then subtracted by a positive term. Thus, the case where $\frac{a_r}{f_r} < |\frac{A_r}{B_r}|$ or $|\frac{A_r}{B_r}| > \frac{(a_r+\gamma_r)}{f_r}$ will never occur.

Therefore, once we ensure a low constraint on σ_r, i.e., the maximum TxFJ power, we can have $\frac{\partial C_r^{sec}}{\partial \sigma_q} > 0,\ \forall r, q \in \mathcal{Q}$, and thus according to Proposition 2, the greedy FJ control approach becomes the unique Pareto-optimal operating point in the network.

APPENDIX E

PROOF OF PROPOSITION 4

Without loss of generality, assume that σ_q^* is a decreasing function of σ_r and χ_q defined in (26) satisfies $\Delta\sigma_q < \chi_q < \frac{P_q - \gamma_q}{N_q - 1}$, $q = 1, 2$. Furthermore, assume that the iterative use of (26) is done sequentially, i.e., Gauss-Seidel algorithm in the sense of [37, Chapter 3] is used, meaning that only one player is updating his TxFJ power at each iteration. More specifically, let the initial TxFJ power for the qth player be $\sigma_q^{*^{(1)}}$, where the superscript $^{(1)}$ represents the iteration index. In the second iteration σ_r gets updated using (26) and $\sigma_q^{*^{(2)}} = \sigma_q^{*^{(1)}}$. In the third iteration, $\sigma_r^{*^{(3)}} = \sigma_r^{*^{(2)}}$, and σ_q gets updated, and so on. Since σ_q^* is assumed to be a decreasing function of σ_r. Hence, if $\sigma_q^{*^{(1)}} < \sigma_q^{*^{(3)}}$ the rth player will select a smaller TxFJ power in the fourth iteration compared to the second iteration (i.e., $\sigma_r^{*^{(2)}} > \sigma_r^{*^{(4)}}$). Consequently, in the fifth iteration, the qth player selects a higher TxFJ power comparing to the third iteration. This trend continues until either the qth player reaches P_q^{jam} or the rth player reaches to χ_r. Depending on which player reaches to either of the extreme points faster than the other, the first four forms in the RHS of (28) are expected to be achieved. For the case of (χ_1, χ_2) and (P_1^{jam}, P_2^{jam}), we first derive the price above which we always have $\sigma_q^* = \chi_q$. Let this price be $\lambda_{q,1}$. Reducing the inequality $\sigma_q^* \leq \chi_q$, we end up with an inequality in the form of $\lambda_q \geq \lambda_{q,1}$. Next, we find a price below which we have $\sigma_q^* = P_q^{jam}$. Let this price be $\lambda_{q,2}$. Reducing the inequality $\sigma_q^* \geq P_q^{jam}$, we end up with an inequality in the form of $\lambda_{q,2} \geq \lambda_q$[18]. Because σ_q is a decreasing function of λ_q, if $P_q^{jam} > \chi_q$ then $\lambda_{q,1} > \lambda_{q,2}$. Thus, the tuples (χ_1, χ_2) and (P_1^{jam}, P_2^{jam}) happen when $\lambda_q > \lambda_{q,1},\ \forall q \in \{1, 2\}$ and $\lambda_q < \lambda_{q,2},\ \forall q \in \{1, 2\}$, respectively. An equivalent proof for when σ_q^* is an increasing function of σ_r can be given, which is skipped for the sake of brevity.

[18]Note that when $0 < \lambda_q \leq \lambda_{q,2}$, greedy FJ is optimal in terms of secrecy sum-rate, but it may not always be beneficial for both of the links unless $\lambda_q \leq 0$. The condition $\lambda_q \leq 0,\ \forall q$ found in Proposition 2 can also guarantee the optimality of greedy FJ in terms of individual secrecy rates.