Price-based Friendly Jamming in a MISO Interference Wiretap Channel

Peyman Siyari
Department of Electrical and Computer Engineering
University of Arizona, USA
Email: psiyari@email.arizona.edu

Marwan Krunz
Department of Electrical and Computer Engineering
University of Arizona, USA
Email: krunz@email.arizona.edu

Diep N. Nguyen
Faculty of Engineering and Information Technology
University of Technology Sydney, Australia
Email: diep.nguyen@uts.edu.au

***Abstract*—In this paper, we expand the scope of PHY-layer security by investigating TX-based friendly jamming (FJ) for the wiretap channel in multi-link settings. For the single-link scenario, creating a TX-based FJ is an effective and practical method in improving the secrecy rate. In a multi-link setting, several information signals must be transmitted simultaneously. Thus, the design must guarantee that the FJ signal of a given transmitter does not interfere with unintended but legitimate receivers. Under the assumption of exact knowledge of the eavesdropping channel, we first propose a distributed price-based approach to improve the secrecy sum-rate of a two-link network with one eavesdropper while satisfying an information-rate constraint for both link. Simulations show that price-based FJ control outperforms greedy FJ, and is close to the performance of a centralized approach. Next, we propose a method based on mixed strategic games that can offer robust solutions to the distributed secrecy sum-rate maximization problem under the assumption of an unknown eavesdropping channel. Lastly, we use simulations to show that in addition to outperforming the greedy approach, our robust optimization also satisfies practical network considerations. In particular, the transmission time for the robust optimization can be determined flexibly to match the channel's coherence time.**

Keywords*—*Interference wiretap channel, friendly jamming, pricing, pure and mixed strategic games.

I. Introduction

The broadcast nature of wireless communications makes them vulnerable to wiretapping activities. Physical-layer security provides cost-effective solutions to this problem through keyless secret communications that do not require a hand-shaking mechanism between the communicating parties [1], [2]. Several approaches in the area of PHY-layer security have been proposed in the last decade (see [3] and the references therein). Among these is the use of artificial noise as a friendly jamming (FJ) signal, which guarantees a non-zero secrecy rate for a link without requiring the knowledge of the eavesdropper's location [4]. In this method, the transmitter (Alice) uses multiple antennas to generate a FJ signal along with the information signal, increasing the interference at the eavesdropper (Eve) but without interfering with the legitimate receiver (Bob).

In a multi-link scenario, to accommodate the simultaneous transmission of several information signals, the FJ signal of each transmitter must be designed to not interfere with other legitimate receivers in the network. To avoid such interference and yet prevent the leakage of users' information, one can exploit MIMO precoding, which ensures that the null space of any FJ signal includes the locations of all legitimate receivers but excludes potential eavesdropping locations. This solution, however, is not practical when coordination between transmitters is challenging (e.g., mobile ad-hoc networks). Therefore, the need for distributed interference management is crucial to guarantee a secure yet non-interfering communications.

Interference management roots back to the power control problem in interference-channel networks, which has been extensively investigated. The main challenge there is to manage the interference at all receivers so as to maximize the sum of individual rates. In an analogous manner, in the interference wiretap channel, the unwanted interference from one transmitter degrades the received signal at unintended receivers, reducing the security of the network in terms of the secrecy rate. However, the possibility of increasing the interference at Eve makes the unwanted interference potentially useful in terms of improving the security of the communications. This idea was first introduced in [5] and [6]. The effect of interference alignment in providing secure transmissions was investigated in [7] and [8]. In some studies, a particular user was assumed to be eavesdropped on, and the other users coordinate with each other to increase interference at Eve while maintaining their own rate requirements. As an example, in [9] the authors considered a two-link SISO interference channel with one Eve. By jointly optimizing the transmission powers of the two users (without FJ), the authors tried to maximize the secrecy rate for one link while maintaining a given quality of service (QoS) for the other link. In [10], the authors studied this problem in a two-tier downlink heterogeneous network comprised of one macrocell and several femtocells. They proposed a transmit beamforming method for the signals intended to macrocell and femtocell users so as to maximize the secrecy rate of one eavesdropped macrocell user. This maximization is subject to satisfying the rate requirements of all other macrocell users.

In other works, PHY-layer security was studied when users have confidential messages and there is no Eve in the network. The transmission of one user is not to be captured by unintended receivers. In [11] game theory was used to study the trade-off between the network performance and fairness in a MIMO interference channel with confidential messages. The work in [12] considered the secrecy-rate region of the interference channel when users transmit FJ signal along

with their information signal. They showed that by using FJ, the secrecy-rate region will be larger than when FJ is not employed.

In this paper, we present a game-theoretic framework for FJ-based interference management in a MISO wiretap channel. The selfish nature of contending links makes game theory an appropriate tool for such a study. We consider a network of two interfering MISO links in the presence of one eavesdropper. Our approach is based on pricing; a well-known concept in game theory. Contrary to intuition, we show that there is a possibility that if one or both transmitters reduce their FJ powers, the sum of the secrecy rates of the two links can be increased. The reduction in FJ power must be done in a way that the interference at each legitimate receiver is reduced, but the aggregate interference at Eve remains high.

The contributions of this paper are as follows:

- We design a price-based distributed FJ mechanism for a multi-link MISO system. We show that the pricing method achieves a locally optimal solution for the secrecy sum-rate maximization problem, and its performance is close to the centralized solution.
- While maximizing the secrecy sum-rate, we consider an additional constraint for each link, whereby a certain level of information rate is to be satisfied.
- We derive a lower bound on the FJ power that achieves a positive secrecy rate and guarantees the maximum possible interference that prevents Eve from using successive interference cancellation.
- Lastly, we relax the assumption of exact knowledge of the eavesdropping channel and derive a robust price-based FJ method. Simulations show that the locally optimal solutions found with/without the knowledge of Eve's channel outperform the greedy FJ.

The rest of this paper is organized as follows. In Section II, we introduce the system model. In Section III, we formulate the FJ control problem as a game. In Section IV the robust jamming control is proposed. In Section V the jamming control algorithm is given and practical considerations are discussed. In Section VI simulation results assess the performance of our algorithm. Finally, Section VII concludes the paper.

II. System Model

We consider the communication scenario in Fig. 1, where two transmitters, Alice1 and Alice2 communicate with two respective receivers, Bob1 and Bob2. Each transmitter $q,\ q = 1, 2$, has N_q transmit antennas, and each receiver $q,\ q = 1, 2$, has one antenna. A passive eavesdropper (Eve) with one antenna exists in the range of communication. The received signal by the qth receiver, y_q is:

$$y_q = \tilde{H}_{qq}u_q + \tilde{H}_{rq}u_r + n_q, \quad r, q \in \{1, 2\},\ r \neq q \qquad (1)$$

where $\tilde{H}_{qr}$ is the $1 \times N_q$ channel matrix between the qth transmitter and the rth receiver, u_q is the transmitted signal from the qth transmitter, and n_q is the complex AWGN with the power $N_0\ dBm$. We assume that $\tilde{H}_{qr}$ is a zero mean complex Gaussian matrix. Let $\tilde{G}_q$ denote the $1 \times N_q$ complex

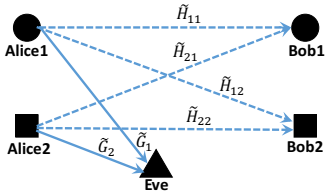

Fig. 1: System model.

channel matrix from the qth transmitter to Eve. Eve's received signal is

$$z = \tilde{G}_q u_q + \tilde{G}_r u_r + e \qquad (2)$$

where e has the same characteristics of n_q. We assume that channels remain stationary during each transmission. The signal $u_q = s_q + w_q$ consists of an information bearing signal s_q and FJ signal w_q. For the FJ signal, we write $w_q = Z_q v_q$, where Z_q is an orthonormal basis for the null space of $\tilde{H}_{qq}$ ($\tilde{H}_{qq}w_q = 0$) and v_q is a vector of i.i.d. complex Gaussian random variables with covariance matrix $E[v_q v_q^H] = \sigma_q I_{(N_q-1)}$. The scalar value σ_q denotes the FJ power and I_{N_q} is the $N_q \times N_q$ identity matrix. Let $\tilde{H}_{qq} = U_q \Sigma_q V_q^H$ be the singular value decomposition (SVD) of $\tilde{H}_{qq}$. We set $Z_q = V_q^{(2)}$ where $V_q^{(2)}$ is the matrix of $N_q - 1$ rightmost columns of V_q. Thus, the FJ signal $w_q = Z_q v_q$ lies in the null space of $\tilde{H}_{qq}$. For the information bearing signal, $s_q = T_q x_q$ where T_q is the precoder and x_q is the information signal. We assume that a Gaussian codebook is used[1]. Furthermore, let $\gamma_q = \text{tr}\{E[x_q x_q^H]\}$ denote the information signal's power, where tr$\{.\}$ is the trace operator and $(.)^H$ is the Hermitian of a matrix. The power budget for transmitter q is written as

$$\begin{aligned} &E[|u_q|^2] = \text{tr}\left\{E[u_q u_q^H]\right\} \leq P_q, \\ &\Rightarrow \text{tr}\{E[v_q v_q^H]\} + \gamma_q \leq P_q \end{aligned} \qquad (3)$$

where $P_q \triangleq \sigma_q(N_q - 1) + \gamma_q$ is a scalar value representing the total power budget at the qth transmitter. We assume that the qth receiver is able to estimate the channel $\tilde{H}_{qq}$ and feed it back to the qth transmitter. Also, the process of acquiring channel state information (CSI) is assumed to be done securely, so that we can only focus on the secrecy of the data transmission phase. To maximize the secrecy rate, the precoder T_q is set to $T_q = V_q^{(1)}$, where $V_q^{(1)}$ is the first column of V_q [4].

III. Problem Formulation

Given that $\tilde{H}_{qq}V_q^{(2)} = 0$, we set $H_{qq} \triangleq \tilde{H}_{qq}V_q^{(1)}$, $H_{qr} \triangleq \tilde{H}_{qr}V_q^{(1)}$, $H_{j_q} \triangleq \tilde{H}_{qr}V_q^{(2)}$, $G_q \triangleq \tilde{G}_q V_q^{(1)}$, $G_{j_q} \triangleq \tilde{G}_q V_q^{(2)}$, where $(q, r) \in \{1, 2\},\ q \neq r$. The terms G_q and G_{j_q} indicate the eavesdropping channel components. Hence,

$$y_q = H_{qq}x_q + H_{rq}x_r + H_{j_r}v_r + n_q \qquad (4)$$

$$z_q = G_q x_q + G_{j_q} v_q + G_r x_r + G_{j_r} v_r + e_q. \qquad (5)$$

The information rate for the qth link can be written as

$$C_q = \log\left(1 + \frac{|H_{qq}x_q|^2}{|H_{rq}x_r|^2 + |H_{j_r}|^2 \sigma_r + N_0}\right). \qquad (6)$$

The channel between the two Alices and Eve can be modeled as a multiple-access channel because Eve is simultaneously

[1]In the case of finite codebooks (e.g., QAM), the (secrecy) rate can be approximated using the gap approximation [13, Chapter 9].

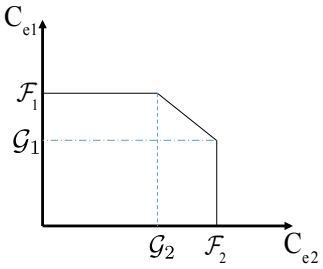

Fig. 2: Achievable rate pairs for a two-user multiple access channel.

receiving signals from both Alices. If Eve is capable of using successive interference cancellation (SIC), she might be able to simultaneously decode both signals. The achievable-rate region of Eve's multi-access channel is shown in Fig. 2, where C_{eq} denotes the the achievable rate at Eve while decoding the qth signal ($q = 1, 2$). The points $\mathcal{G}_q$ and $\mathcal{F}_q$ are defined in the following. Fig. 2 suggests that to prevent Eve from using SIC, we must have $C_q > \mathcal{G}_q$ for $q = 1, 2$ [9], i.e.,

$$\log\left(1 + \frac{|H_{qq}x_q|^2}{|H_{rq}x_r|^2 + |H_{j_r}|^2\sigma_r + N_0}\right) > \mathcal{G}_q \tag{7}$$

where

$$\mathcal{G}_q \triangleq \log\left(1 + \frac{|G_q x_q|^2}{|G_{j_q}|^2\sigma_q + |G_r x_r|^2 + |G_{j_r}|^2\sigma_r + N_0}\right). \tag{8}$$

More specifically, 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 of 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 the other signal without interference. In other words, if inequality (7) is satisfied, Eve has to decode the second information signal while considering the first information signal as interference. Thus, the achievable rate at Eve while decoding rth signal, $r = 1, 2$, is $C_{er} = \mathcal{G}_r$ and the secrecy rate of rth link is

$$C_r^{sec} \triangleq \max\{C_r - C_{er}\ ,\ 0\} = \tag{9}$$
$$\log\left(1 + \frac{|H_{rr}x_r|^2}{|H_{qr}x_q|^2 + |H_{j_q}|^2\sigma_q + N_0}\right) -$$
$$\log\left(1 + \frac{|G_r x_r|^2}{|G_{j_r}|^2\sigma_r + |G_q x_q|^2 + |G_{j_q}|^2\sigma_q + N_0}\right),\ r \neq q.$$

If (7) is not satisfied, Eve has complete knowledge of the first signal (i.e., the qth signal, $q = 1, 2$). Hence, Eve can consider the second signal (i.e., the rth signal, $r \neq q$) as interference and decodes the first signal. Knowledge of the first signal allows Eve to deduct the first signal from the received signal and obtain the second signal without interference. Hence, $C_{er} = \mathcal{F}_r$ and

$$C_r^{sec} = \max\left\{\log\left(1 + \frac{|H_{rr}x_r|^2}{|H_{qr}x_q|^2 + |H_{j_q}|^2\sigma_q + N_0}\right) - \mathcal{F}_r, 0\right\} \tag{10}$$

where

$$\mathcal{F}_r \triangleq \log\left(1 + \frac{|G_r x_r|^2}{|G_{j_q}|^2\sigma_q + |G_{j_r}|^2\sigma_r + N_0}\right). \tag{11}$$

It is obvious from (7) and (10) that in order to achieve the maximum secrecy, the two transmitters have to choose a transmission rate higher than Eve's decodable rate. As can be seen in (9) and (10), the interference caused by the FJ signal can degrade the received SINR at unintended receivers, but it also adds interference at Eve. This creates a conflicting situation. The performance of the network is comprised of the performance of both links. Hence, we define the term secrecy sum-rate to be $C^{sec} = C_1^{sec} + C_2^{sec}$. We aim to maximize C^{sec} while ensuring a minimum information rate for both links. This problem can be formally written as:

$$\underset{\{\gamma_1,\gamma_2,\sigma_1,\sigma_2\}}{\text{maximize}}\ C^{sec} \tag{12}$$
$$\text{s.t.} \begin{cases} \gamma_q + \sigma_q(N_q - 1) \leq P_q \\ C_q \geq c_q \end{cases},\ \forall q \in \{1, 2\}$$

where the second constraint ensures a minimum information rate c_q for each link q.

The optimization in (12) is non-convex. Thus, solving it is prohibitively expensive. One relaxation to this problem is to eliminate the dependency of the problem on γ_1 and γ_2. To do that, we assume that the rate constraint in (12), is satisfied with equality, i.e., $C_q = c_q$. Considering that this rate constraint is satisfied for some γ_q, the second constraint can be embedded into the objective function and the first constraint. Hence, we have[2]

$$\underset{\{\sigma_1,\sigma_2\}}{\text{maximize}}\ C^{sec} \tag{13}$$
$$\text{s.t.}\quad \sigma_q \leq \frac{P_q - \gamma_q}{N_q - 1},\ \forall q \in \{1, 2\}.$$

Considering how we prevent Eve from applying SIC in (7), the FJ power has to be chosen such that inequality (7) is satisfied. Reducing (7), we have

$$\sigma_q > \frac{A_q}{B_q}, \tag{14}$$

where

$$A_q \triangleq |G_q|^2\gamma_q\left(|H_{rq}|^2\gamma_r + |H_{j_r}|^2\sigma_r + N_0\right) - \tag{15}$$
$$|H_{qq}|^2\gamma_q(|G_r|^2\gamma_r + |G_{j_r}|^2\sigma_r + N_0),$$
$$B_q \triangleq |G_{j_q}|^2|H_{qq}|^2\gamma_q.$$

Simplifying (14), we can establish the following constraints on σ_q:

$$\sigma_q = \frac{P_q - \gamma_q}{N_q - 1} \quad \text{if} \quad \frac{A_q}{B_q} > \frac{P_q - \gamma_q}{N_q - 1} \tag{16}$$
$$\sigma_q > \frac{A_q}{B_q} \quad \text{if} \quad A_q > 0\ \ \&\ \ \frac{A_q}{B_q} < \frac{P_q - \gamma_q}{N_q - 1}, \tag{17}$$
$$\sigma_q > 0 \quad \text{if} \quad A_q < 0. \tag{18}$$

For the case in (16), no power can prevent Eve from using SIC to decode two information messages, and the solution to (13) would be infeasible. Hence, we assume that if (16) is true for any of the links, they will not start any communications. Since the inequality in (18) strictly suggests that the FJ power has to be positive, we define $\Delta\sigma_q$ to be the smallest value that

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

$$\lambda_q = \frac{|H_{j_q}H_{rr}|^2\gamma_r}{(|H_{qr}|^2\gamma_q + |H_{j_q}|^2\sigma_q + N_0)(|H_{qr}|^2\gamma_q + |H_{j_q}|^2\sigma_q + |H_{rr}|^2\gamma_r + N_0)} - \frac{|G_{j_q}G_r|^2\gamma_r}{(|G_q|^2\gamma_q + |G_{j_q}|^2\sigma_q + |G_{j_r}|^2\sigma_r + N_0)(|G_q|^2\gamma_q + |G_{j_q}|^2\sigma_q + |G_r|^2\gamma_r + |G_{j_r}|^2\sigma_r + N_0)}, \quad r \neq q,\ (r,q) \in \{1,2\}^2. \tag{22}$$

$$\sigma_q^* = \left[\frac{1}{|G_{j_q}|^2}\left(\sqrt{|G_qG_{j_q}|^2\frac{\gamma_q}{\lambda_q} + \frac{|G_q|^4\gamma_q^2}{4}} - \frac{|G_q|^2\gamma_q}{2} - \left(|G_r|^2\gamma_r + |G_{j_r}|^2\sigma_r + N_0\right)\right)\right]_{\chi_q}^{\frac{P_q-\gamma_q}{N_q-1}}. \tag{23}$$

σ_q can take. Considering that we can have either of (17) or (18), the optimization in (13) becomes

$$\begin{aligned} \underset{\{\sigma_1,\sigma_2\}}{\text{maximize}} \quad & C^{sec} \\ \text{s.t.} \quad & \sigma_q \in D_q,\ \forall q \in \{1,2\} \end{aligned} \tag{19}$$

where $D_q \triangleq \left[\max\left\{\frac{A_q}{B_q}, \Delta\sigma_q\right\}, \frac{P_q-\gamma_q}{N_q-1}\right]$ and $[a,b]$ represents a continuous interval between a and b. The optimization in (13) aims to find the best tradeoff between the FJ powers of the two transmitters. In other words, the Pareto-optimal FJ powers can be found by solving (19)[3]. Unfortunately, the optimization in (19) is still non-convex. Furthermore, it requires the exact knowledge of the eavesdropping channel components (i.e., G_q and G_{j_q}).

A. Game Formulation

1) Greedy FJ: One solution to reduce the complexity of (13) is to let each Tx maximize its own secrecy rate and ignore the effect of its FJ on the unintended Rx. This locally optimized FJ control leads to a game theoretic interpretation of this network. Assuming that each player myopically chooses the best strategy for itself, we formulate this scenario as a non-cooperative game, in which the best strategy of each link $q,\ q = 1, 2$, is

$$\begin{aligned} \underset{\sigma_q}{\text{maximize}} \quad & C_q^{sec} \\ \text{s.t.} \quad & \sigma_q \in D_q. \end{aligned} \tag{20}$$

In this game, the utility function of each player (link) is its secrecy rate and his strategy is to choose the best FJ power to maximize its utility subject to a power constraint (i.e., strategy set). The existence of Nash equilibrium (NE) in this game can be proven by showing that the strategy set of each player is a non-empty, compact, and convex subset of $\mathbb{R}$, and the utility function of each player is a continuous and quasi-concave function of the FJ power. Verifying these properties in our game is straightforward and is skipped for brevity. Since the objective function in (20) is strictly concave in σ_q, the best strategy that maximizes the secrecy rate of the qth player is to select the maximum available FJ power, i.e., $\sigma_q = P_q^{jam} = \frac{P_q-\gamma_q}{N_q-1},\ q = 1, 2$. When $\sigma_q = P_q^{jam}\ \forall q$, no player will be willing to unilaterally change its own strategy because choosing any FJ 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 [4] 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. As an intuitive explanation, consider the case where the interference from Alice2 is large enough such that it interferes with Bob1's reception; the interference from Alice1 is not large enough to affect Bob2; and Eve is much closer to Alice1 than to Alice2. Considering almost equal FJ power constraints, if both players select the maximum FJ power, Alice1 can make its transmission more secure by applying maximum FJ power without affecting Bob2. However, although Alice2 is not that much in the risk of being eavesdropped, it chooses the maximum possible FJ power which has little impact on its own secrecy rate, but can degrade the received SINR at Bob1. Degradation of C_1 makes the transmission of Alice1 less secure, so the secrecy sum-rate of the network will be reduced.

2) Price-based FJ: The efficiency of the NE in the greedy FJ approach can be improved by using appropriate pricing policies. Hence, for $q \in \{1, 2\}$, the objective function of player q in (20) would be modified into:

$$\begin{aligned} \underset{\sigma_q}{\text{maximize}} \quad & \left\{C_q^{sec} - \lambda_q\sigma_q\right\} \\ \text{s.t.} \quad & \sigma_q \in D_q \end{aligned} \tag{21}$$

where λ_q is a pricing factor for the qth link, defined in (22). The rationale behind pricing has been discussed in many works (e.g., [15]–[17]). In brief, pricing is a mechanism that incentivizes players to spend their FJ powers more wisely by charging each player a price per unit of FJ power, thus discouraging players from acting selfishly. In this work, a linear pricing will be used to improve the efficiency of FJ control. The optimal FJ power can be found by writing the K.K.T conditions for (21). Hence, close-form representation of the optimal FJ power for the qth link can be written as in (23), where $[\bullet]_b^a \triangleq \min\{\max\{\bullet, b\}, a\}$ and $\chi_q \triangleq \min\left\{\max\{\frac{A_q}{B_q}, \Delta\sigma_q\}, P_q^{jam}\right\}$. It is easy to verify that by setting $\lambda_q = 0$, we end up with the previously mentioned greedy FJ approach.

By iteratively using (23) to set the FJ power for both players, the games converges to a NE from which neither player is willing to deviate. In what follows, 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 (22).

Theorem 1. *The NE of the game wherein the players use* (22) *as the pricing factor to solve the optimization in* (21) *equals to that of a locally optimal solution of* (19)*.*

Proof: See Appendix A. ■

Next, we introduce two properties of the price-based FJ control.

Proposition 1. *The greedy FJ approach is the optimal FJ control if* $\lambda_q \leq 0,\ \forall q \in \{1, 2\}$.

[3]Details of the relationship between the Pareto-optimal points and sum utility optimization can be found in [14].

$s_1 \backslash s_2$	$\Delta\sigma_2$	$2\Delta\sigma_2$	$\dots$	P_2^{jam}
$\Delta\sigma_1$	$R_1(\Delta\sigma_1, \Delta\sigma_2), R_2(\Delta\sigma_1, \Delta\sigma_2)$	$R_1(\Delta\sigma_1, 2\Delta\sigma_2), R_2(\Delta\sigma_1, 2\Delta\sigma_2)$	$\dots$	$R_1(\Delta\sigma_1, P_2^{jam}), R_2(\Delta\sigma_1, P_2^{jam})$
$2\Delta\sigma_1$	$R_1(2\Delta\sigma_1, \Delta\sigma_2), R_2(2\Delta\sigma_1, \Delta\sigma_2)$	$R_1(2\Delta\sigma_1, 2\Delta\sigma_2), R_2(2\Delta\sigma_1, 2\Delta\sigma_2)$	$\dots$	$R_1(2\Delta\sigma_1, P_2^{jam}), R_2(2\Delta\sigma_1, P_2^{jam})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
P_1^{jam}	$R_1(P_1^{jam}, \Delta\sigma_2), R_2(P_1^{jam}, \Delta\sigma_2)$	$R_1(P_1^{jam}, 2\Delta\sigma_2), R_2(P_1^{jam}, 2\Delta\sigma_2)$	$\dots$	$R_1(P_1^{jam}, P_2^{jam}), R_2(P_1^{jam}, P_2^{jam})$

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

Proof: See Appendix B. ∎

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

$$(\sigma_1, \sigma_2) = (\sigma_{int}, \chi_2) \text{ or } (\sigma_{int}, P_2^{jam}) \text{ or } (\chi_1, \sigma_{int}) \text{ or } (P_1^{jam}, \sigma_{int}) \text{ or} (\chi_1, \chi_2) \text{ or} (P_1^{jam}, P_2^{jam}), \tag{24}$$

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

Proof: See Appendix C. ∎

IV. Robust Optimization Procedure

So far, we proved that price-based FJ control results in locally optimum FJ powers. The next challenging question is how to determine the best price without having exact knowledge of the eavesdropping channel.

When such knowledge is available, iterative computation of σ_q^* in (23) converges to the NE. Also, the price-based FJ results in locally optimal solutions of the secrecy sum-rate. However, the unknown eavesdropping channel makes it difficult to compute σ_q^* and λ_q. In the following, we propose a method to overcome this issue.

Let $R_q(s_1, s_2)$ be the utility of the qth player, where s_1 and s_2 represent the strategy taken by player 1 and player 2, respectively. The strategy space for each player q is a continuous interval that can be written as $\sigma_q \in [\Delta\sigma_q, P_q^{jam}]$. The strategy set of the players has infinitely many real numbers. If we are to analyze this game using strategy tables, then the strategy set of each player should be countable and finite. In order to create a finite strategy set, we discretize the FJ power. Assuming that we have n bits to convey $M = 2^n$ power levels, the power level increment is $\Delta\sigma_q = \frac{P_q^{jam}}{2^n}$. Hence, the strategy set would be $S_q = \{\Delta\sigma_q, 2\Delta\sigma_q, \dots, (M-1)\Delta\sigma_q, P_q^{jam}\}$. Considering that $s_q \in S_q$, a utility matrix $R_q,\ q = 1, 2$, can be obtained such that its (i, j) entry is $[R_q]_{ij} = \left\{R_q(i\Delta\sigma_q, j\Delta\sigma_q) |\ (i, j) \in \{1, \dots, M\}^2\right\}$.

Since the problem in (13) is non-convex w.r.t the FJ powers, the Pareto-optimal points can be found via exhaustive search in Table I. Considering a finite jamming game, the complexity of this optimization is in the order of $\mathcal{O}(n^2)$. Proposition 2 reduces the complexity to $\mathcal{O}(4n - 4)$ because only a small set of FJ power tuples comprise the NE points of price-based FJ, meaning that the locally optimal points of the secrecy sum-rate can be found by searching a small part of Table I. To get more intuition into the order reduction, we discuss a special case of Proposition 2. Recalling the explanation used to justify why Eve cannot use SIC to decode both signals from Alices, if (18) is always satisfied for both players, then only the rows corresponding to $\Delta\sigma_1$ and P_1^{jam}, and the columns corresponding to $\Delta\sigma_2$ and P_2^{jam} need to be searched.

In order to proceed further with designing a robust optimization framework, we introduce the concept of mixed strategic games.

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

In the mixed strategic jamming game, both players choose their FJ power level based on probability distributions. Hence, the best response of each player is to maximize the expected value of its own utility. We should 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. its strategy, then using Jensen's inequality, we deduce that

$$E_{s_1}\left[E_{s_2}[R_1(s_1, s_2)]\right] \le E_{s_2}\left[R_1\left(E_{s_1}[s_1], s_2\right)\right], \quad \forall (s_1, s_2) \in S_1 \times S_2. \tag{25}$$

The inequality in (25) is satisfied with equality if and only if s_1 reduces to pure strategies. Hence, whatever the strategies of other players are, every NE of the game is achieved using pure strategies [14]. Sufficiency of pure strategies cannot be guaranteed if the utility function of a player is not concave w.r.t. its action. Hence, mixed strategies should also be investigated for non-concave utilities.

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 $R_2(i\Delta\sigma_1, j\Delta\sigma_2), (i, j) \in \{1, \dots, M\}$, in Table I only show the utilities of both players (at $s_1 = i\Delta\sigma_1$ and $s_2 = j\Delta\sigma_2$) assuming that iteratively using (23) for both players converges to $\sigma_1^* = i\Delta\sigma_1$ and $\sigma_2^* = j\Delta\sigma_2$. Hence, it is not possible to use the objective function in (21) as a utility function in the strategy table. In order to establish the strategy table, we inspect (19) again. Theorem 1 suggests that the K.K.T. conditions of (19) are met at the NE point, so 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 a non-concave 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 FJ power and checks its effect on the secrecy sum-rate. Recalling Proposition 2, at a locally optimal point, only one tuple of FJ powers at the corner entries of Table I happens. Hence, the objective of the first player is

$$\begin{aligned} \underset{\{\alpha_{i,1}\}_{i=1}^M}{\text{maximize}} \quad & \sum_{i=1}^{M} \alpha_{i,1} R_1(i\Delta\sigma_1, s_2), \\ \text{s.t.} \quad & \sum_{i=1}^{M} \alpha_{i,1} = 1, \\ & 0 < \alpha_{i,1} < 1, \forall i, \\ & s_2 \in \left\{\left\lceil \frac{\chi_2}{M} \right\rceil \Delta\sigma_2, P_2^{jam}\right\} \end{aligned} \tag{26}$$

where $\{\alpha_{i,1}\}_{i=1}^M$ is the probability set, and $\lceil \bullet \rceil$ is the ceiling function. Problem (26) is a linear program, which can be solved efficiently using numerical techniques. The second player's strategy can be found accordingly.

So far, all the derivations are based on complete knowledge of the eavesdropping channel. However, if Eve is a passive device in the network , this assumption is unrealistic. For the qth player, the computation of the secrecy rate defined in (9) depends on C_q and C_{eq}. Since we assumed that Bob can measure his received interference and Alice is aware of the channel between her and her corresponding Bob, the computation of C_q can be done locally. However, the eavesdropping channel is unknown, its components can be equivalently shown as the product of some large-scale and small-scale fading, so $G_q = \bar{G}_q({d_q}^{-\eta})$ and $G_{j_q} = \bar{G}_{j_q}({d_{j_q}}^{-\eta})$, where $\bar{G}_q$ and $\bar{G}_{j_q}$ are scalar and $1 \times (N_q - 1)$ matrix, respectively, and the entries of both are i.i.d. standard complex Gaussian random variables with unit variance (the same representation can be done for H_{qr} and H_{j_q}). The terms $d_q^{-\eta}$ and $d_{j_q}^{-\eta}$ are the corresponding distances where $d_q^{-\eta}$ is a scalar and $d_{j_q}^{-\eta}$ is an $(N_q - 1) \times (N_q - 1)$ diagonal matrix, and η is the equivalent path-loss exponent. The secrecy rate in such a setting is given by

$$C_q^{sec} = C_q - E_{[d_q,\, \bar{G}_q, d_r,\, \bar{G}_r, \bar{G}_{j_q},\, \bar{G}_{j_r}]}\left[C_{eq}\right] = C_q - \tag{27}$$

$$E\left[\log\left(1 + \frac{|G_q|^2 \gamma_q}{|G_{j_q}|^2 \sigma_q + |G_r|^2 \gamma_r + |G_{j_r}|^2 \sigma_r + N_0}\right)\right] \tag{28}$$

where $E_{[d_q, \bar{G}_q, \ldots, \bar{G}_{j_r}]}[\bullet] \triangleq E_{d_q}\left[E_{\bar{G}_q}\left[\ldots\left[E_{\bar{G}_{j_r}}[\bullet]\right]\right]\right]$. We rewrite (28) as

$$E_{[d_q,\, \bar{G}_q, d_r,\, \bar{G}_r, \bar{G}_{j_q},\, \bar{G}_{j_r}]}\left[C_{eq}\right] = E_{[d_q,\, W_q, d_r,\, Y_q]}\left[\log\left|\frac{W_q \Gamma_{1q} W_q^H}{Y_q \Gamma_{2q} Y_q^H}\right|\right] \tag{29}$$

where $W_q \triangleq [\bar{G}_q, \bar{G}_{j_q}, \bar{G}_r, \bar{G}_{j_r}, e_q]$, $Y_q \triangleq [\bar{G}_{j_q}, \bar{G}_r, \bar{G}_{j_r}, e_q]$, and

$$\Gamma_{1q} = \mathrm{diag}\Big\{\gamma_q, \sigma_q \underbrace{[1, \ldots, 1]}_{N_q - 1}\left(\frac{d_{j_q}}{d_q}\right)^{-2\eta}, \left(\frac{d_r}{d_q}\right)^{-2\eta}\gamma_r, \tag{30}$$

$$\sigma_r \underbrace{[1, \ldots, 1]}_{N_r - 1}\left(\frac{d_{j_r}}{d_q}\right)^{-2\eta}, (d_q)^{2\eta} N_0\Big\},$$

$$\Gamma_{2q} = \mathrm{diag}\Big\{\sigma_q \underbrace{[1, \ldots, 1]}_{N_q - 1}\left(\frac{d_{j_q}}{d_r}\right)^{(-2\eta)}, \gamma_r, \tag{31}$$

$$\sigma_r \underbrace{[1, \ldots, 1]}_{N_r - 1}\left(\frac{d_{j_r}}{d_r}\right)^{-2\eta}, (d_r)^{2\eta} N_0\Big\}$$

with $\mathrm{diag}\{F^T\}$ representing an $m \times m$ diagonal matrix whose diagonal entries are the entries of F (F is a vector of size m). The expectation in (29) w.r.t. W_q and Y_q can be efficiently computed using the random matrix result in [18, Appendix A, Lemma 2]. However, according to (29) C_{eq} is still a random variable over the distances d_q and d_r, which corresponds to the spatial distribution of Eve. Since we were not able to analytically formulate this distribution, we numerically approximate the expectation of C_{eq} w.r.t. the distances. To do this approximation, in simulations, we assume that Eve is uniformly distributed within a circle of a given radius, and the center of this circle is determined depending on our simulation scenario (see Section VI for more details). A similar idea can be found in [19]. Another example is [20] where the authors assumed that the location of Eve follows a Poisson point process.

Following the same technique used to manipulate (29), we take the expectation of (14) and end up with:

$$\sigma_q > \frac{\left(|H_{rq}|^2 \gamma_r + |H_{j_r}|^2 \sigma_r + N_0\right)}{|H_{qq}|^2} E_{[G_q, G_{j_q}]}\left[\frac{|G_q|^2}{|G_{j_q}|^2}\right] - \tag{32}$$

$$E_{[\bar{G}_r,\, d_q,\, d_r, \bar{G}_{j_r},\, \bar{G}_{j_q}]}\left[\frac{\left(|G_r|^2 \gamma_r + |G_{j_r}|^2 \sigma_r + N_0\right)}{|G_{j_q}|^2}\right].$$

The numerator and the denominator inside the first expectation term in (32) correspond to a central Wishart matrix. The numerator inside the second expectation term corresponds to the quadratic form of a Wishart matrix, which preserves Wishartness property [21]. Hence, both of the expectations correspond to the ratio of two Wishart matrices. Since we assumed a MISO system, all of the Wishart matrices are in fact scalars. Hence, the expectations in (32) can be computed using the result in [22, section 1]. Computing the expectation w.r.t. d_q and d_r can be tackled numerically, as explained above.

Since (27) and (32) are computable, the objective function and third constraint of (26) are defined without knowledge of the eavesdropping channel. Hence, we can establish Table I to solve (26). The next section describes an algorithm that achieves a robust solution for (26).

V. Algorithm Design

We now describe an algorithm that achieves a robust solution for the FJ control. In order to approximate the expectation of C_{eq} w.r.t. the distances, the location of Eve will be assumed to be uniformly distributed within a circle of radius $\hat{r}_e$, and the center coordinates are $(\hat{x}_e, \hat{y}_e)$. The pseudocode for our algorithm is shown below as Algorithm 1. The computation in lines 5 and 6 can be done using the method used to compute (32) (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 2 suggests that the computation of 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 $\sigma_r = P_r^{jam}$). For the case of exhaustive search, instead of two power levels, we should search using all power levels in the interval $[\chi_r, P_r^{jam}]$ (cf. Section IV for more details on exhaustive search).

Line 7 ensures that the selected power in line 4 results in a non-zero 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 (26). The operation in line 8 (computed using (27)) requires that both links compute their own secrecy rates using their local channel and the method mentioned for (27). Then, the rth link should send the value of its own secrecy rate to the qth link in order to compute R_q. After doing the operations of lines 2-12, two different solutions for $\{\alpha_{i,q}\}_{i=1}^{M}$ will be found for the qth link (one for when $\sigma_r = \chi_r$ and one for when $\sigma_r = P_r^{jam}$). As R_q is already stored in line 8, line 14 chooses the probability set corresponding to the largest expected utility. Creating a probabilistic FJ power assignment is done by converting the uniform distribution to a probability mass function corresponding to $\{\alpha_{i,q}\}_{i=1}^{M}$ for $q = 1, 2$ [23]. Compared to the price-based solution with complete knowledge of the eavesdropping channel, the robust FJ control algorithm only needs exchanging secrecy rates, FJ powers, and information signal powers.

Algorithm 1 Robust Friendly Jamming Control

Input:
- $N_q, P_q, \phi_q = \frac{p_q}{\sigma_q(N_q-1)}, c_q, M \quad \forall q \in \{1,2\}$
- $\hat{r}_e$ % The radius of the circle within which % Eve is uniformly distributed.
- $(\hat{x}_e, \hat{y}_e)$ % The center of the circle within which % Eve is uniformly distributed.

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.
9: **end if**
10: **end for** % do the same loop again but change
11: % line 5 to "Set $\sigma_r = P_r^{jam}$".
12: Find $\{\alpha_{i,q}\}_{i=1}^{M}$ by solving (26). % once for $\sigma_r = \chi_r$ and
13: % once for $\sigma_r = P_r^{jam}$.
14: Choose the probability set (i.e., $\{\alpha_{i,q}\}_{i=1}^{M}$) that corresponds to the largest expected utility.
15: **end for**
16: **for** $q = 1$ to 2 **do**
17: **if** $C_q < c_q - \epsilon$ **then** Set $\gamma_q = \gamma_q + \delta$.
18: **if** $\gamma_q > P_q$ **then** Set $\gamma_q = P_q$.
19: **end if**
20: **else**
21: **if** $C_q > c_q + \epsilon$ **then** Set $\gamma_q = \gamma_q - \delta$.
22: **end if**
23: **end if**
24: **end for**
25: **until** $c_q - \epsilon < C_q < c_q + \epsilon \quad \forall q$.

Lines 16 to 25 constitute the outer loop of the algorithm that corresponds to satisfying the rate constraints of both links. For some choice of δ and ϵ, as long as the rate requirements are feasible, the linear adjustment used in lines 17 and 21 converges without the need for central control (similar procedure can be found in [24, Algorithm 1]). Hence, this linear adjustment ensures each link achieves its minimum target rate. If the target rates are not achievable, then the line 18 limits the links to their maximum total transmit powers.

VI. Numerical Results

In this section, we simulate the FJ control methods presented before. In all of the simulations, the variance of additive noise at both receivers and at Eve (i.e., noise floor) is set to $N_0 = -50$ dBm. The information rate constraints are chosen such that the transmitters use no more than $1/3$ of their total transmit powers for the information signal. The horizontal axis in all figures is the horizontal coordinate for the center of the circle within which Eve is uniformly distributed. Each point on the plots is the result of averaging over 10 random locations of Eve (in order to approximate (27) w.r.t. distances). At each random location, 500 channel realizations are simulated and then averaged.

Fig. 3 shows the variation of the secrecy sum-rate with of Eve's location for a given total power constraint. 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[4], which indicates that greedy FJ is optimal in these scenarios. Also, in all of Eve's locations, the pricing scheme has a performance close to the exhaustive search approach. Throughout our simulations, the optimality of greedy FJ was observed only at very low power constraints.

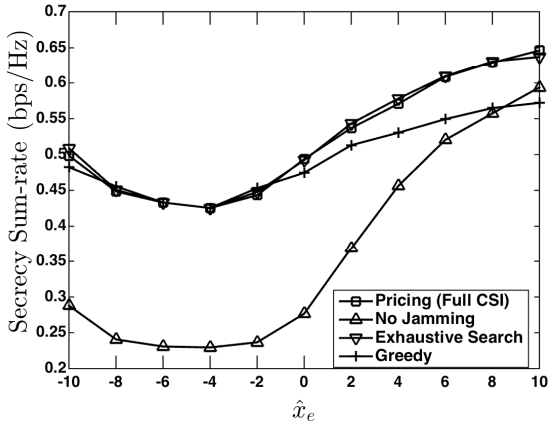

Fig. 3: Effect of Eve's location on the secrecy sum-rate, $(\text{Alice}_1 = (-5, 8),\ \text{Bob}_1 = (5, 8),\ \text{Alice}_2 = (-5, -8),\ \text{Bob}_2 = (5, -8), \hat{y}_e = 3.5, \hat{r}_e = 1.6,\ P_q = -32$ dBm, $N_q = 3)$.

In Fig. 4 and Fig. 5, we show the secrecy sum-rate as well as individual secrecy rates for when constraint (14) is into account in pricing method (indicated as "Pricing (Full CSI) and for when it is not (indicated as "Pricing (No Positive Secrecy)"). It can be seen that considering (14) in our jamming 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 at some locations of Eve. Furthermore, satisfying (14) guarantees non-zero secrecy rate for each link. However, if it is ignored, zero secrecy rate happens to one or both links for some locations of Eve.

In Fig. 6, 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 (23) to optimize their FJ powers (i.e., the Gauss-Seidel algorithm is used [16]). Note that since the performance of the pricing method depends on the starting point for the iterative procedure, 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 FJ control algorithm, we use 8 bits to quantize of power levels. After finding the probability set $\{\alpha_{i,q} : i = 1, \ldots, \}$ that maximizes the expected utility in (26), probabilistic assignment of the FJ powers in robust jamming control is done as follows. The qth player generates a sample from the $\{\alpha_{i,q} : i = 1, \ldots, \}$. Depending on the value of this sample, player q selects FJ power, say $i\Delta\sigma_q$, and starts transmission. Lastly, the achievable rate is computed using the method in (27). This procedure is repeated 50 times per channel realization and the expected utility in (26) is approximated by averaging over these samples. 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.

[4]Note that we assume to have complete knowledge of eavesdropping channel components in the exhaustive search approach.

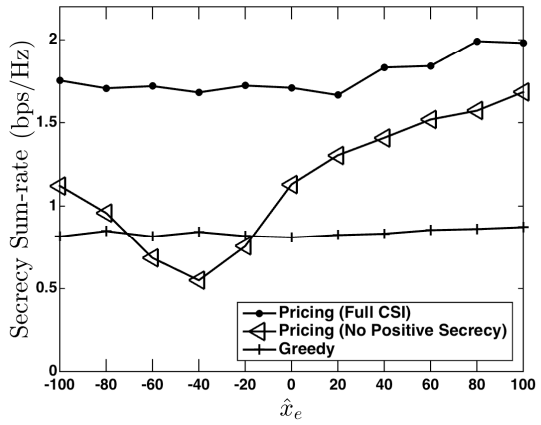

Fig. 4: Effect of Eve's location on the secrecy sum-rate, $(\text{Alice}_1 = (-50, 10),\ \text{Bob}_1 = (5, 10),\ \text{Alice}_2 = (-50, -10),\ \text{Bob}_2 = (50, 10), \hat{y}_e = 0, \hat{r}_e = 10,\ P_q = 0$ dBm, $N_q = 3)$.

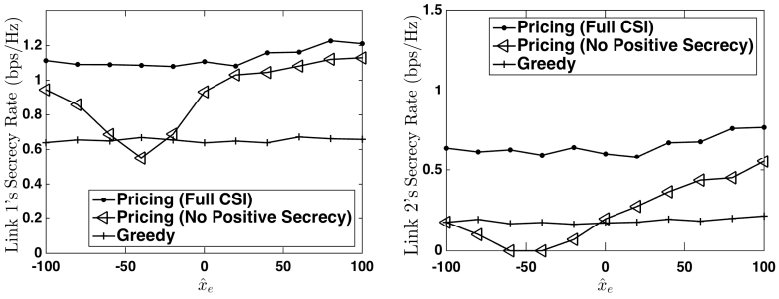

Fig. 5: Effect of Eve's location on individual secrecy rates, The configurations are the same as Fig. 4.

The expected value in (26) must be computed after averaging over several samples of data transmissions within 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 compute the expected utility in (26). Furthermore, in order to fix the other parameters that might affect this comparison, we simulated 50 channel realizations at each location of Eve. It can be seen in Fig. 7 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.

VII. Conclusion

In this paper, we studied distributed design of friendly jamming control in a 2-link wireless network. We showed that greedy friendly jamming is not an optimal approach to secure network. Accordingly, we designed a price-based FJ 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 used for jamming control. We then introduced uncertainty in the eavesdropping channel and designed a robust method that can be used when this channel is known only in probabilistic terms. Extension of this framework to more than two interfering links or to the case of MIMO-enabled links is left for future research.

Acknowledgements

This research was supported in part by NSF (grants CNS-1409172 and CNS-1513649), the Army Research Office (grant W911NF-13-1-0302), 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, ARO, or ARC.

References

[1] 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.

[2] S. Vasudevan, D. Goeckel, and D. F. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. ACM MobiHoc Symp.*, 2010, pp. 21–30.

[3] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Commun. Mag.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

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

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

[6] A. Rabbachin, A. Conti, and M. Win, "The role of aggregate interference on intrinsic network secrecy," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2012, pp. 3548–3553.

[7] 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.

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

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

[10] 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.

[11] 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.

[12] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 885–887, Oct. 2010.

[13] A. Goldsmith and S.-G. Chua, "Variable-rate variable-power MQAM for fading channels," *IEEE Trans. Commun.*, vol. 45, no. 10, pp. 1218–1230, Oct. 1997.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

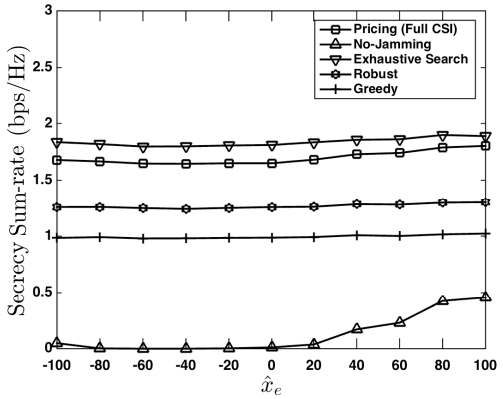

Fig. 6: Effect of Eve's location on the secrecy sum-rate,($\text{Alice}_1 = (-40, 20), \text{Bob}_1 = (40, 20), \text{Alice}_2 = (-40, -20),$ $\text{Bob}_2 = (40, -20), \hat{y}_e = 25, \hat{r}_e = 20,\ P_q = 10$ dBm, $N_q = 3\ \forall q$).

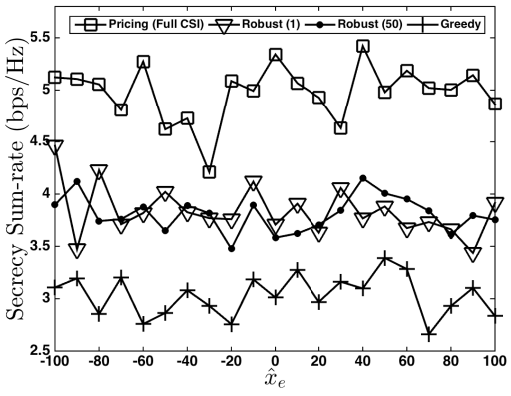

Fig. 7: Effect of number of data transmissions, $(\text{Alice}_1 = (-20, 20), \text{Bob}_1 = (20, 20), \text{Alice}_2 = (-20, -20)$ $\text{Bob}_2 = (20, -20), \hat{y}_e = 10,\ \hat{r}_e = 20,\ P_q = 10$ dBm, $N_q = 4\ \forall q$).

[19] 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.

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

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

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

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

[24] 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.

APPENDIX A
PROOF OF THEOREM 1

Let the Lagrangian of (19) w.r.t (σ_1, σ_2) be denoted as $\mathcal{L}(\sigma) = \mathcal{L}(\sigma_1, \sigma_2)$. Also, let the Lagrangian of (21) w.r.t σ_q be denoted as $\mathcal{L}_q(\sigma_q),\ q = 1, 2$. For (σ_1^*, σ_2^*) defined in (23) to be a locally optimal solution of (19), the K.K.T conditions of both (19) and (21) must be equivalent. That is

$$\frac{\partial \mathcal{L}(\sigma^*)}{\partial \sigma} = \begin{bmatrix} \dfrac{\partial \mathcal{L}(\sigma_1^*, \sigma_2^*)}{\partial \sigma_1} \\ \dfrac{\partial \mathcal{L}(\sigma_1^*, \sigma_2^*)}{\partial \sigma_2} \end{bmatrix} = \begin{bmatrix} \dfrac{\partial \mathcal{L}_1(\sigma_1^*, \sigma_2^*)}{\partial \sigma_1} \\ \dfrac{\partial \mathcal{L}_2(\sigma_1^*, \sigma_2^*)}{\partial \sigma_2} \end{bmatrix} = 0. \quad (33)$$

Simplifying (33), we have $\lambda_q = -\frac{\partial C_r^{sec}}{\partial \sigma_q}$ which is the same as (22). Assuming that iteratively application of (23) converges, the NE of the pricing method is a locally optimal solution to (19) [5].

APPENDIX B
PROOF OF PROPOSITION 1

Given that $\lambda_q = -\frac{\partial C_r^{sec}}{\partial \sigma_q}$ for $\lambda_q > 0$, then $\frac{\partial C_r^{sec}}{\partial \sigma_q} < 0$. Hence, the positive price is effective as long as the increase in one player's FJ power reduces the secrecy rate for the other. Thus, the positive price λ_q can make a player reduce its FJ power if this reduction is beneficial for the other player. Now, considering $\lambda_q \leq 0$, the increase in one player's FJ power results in either no change (i.e., $\lambda_q = 0$) or increase (i.e., $\lambda_q < 0$) in the other player's secrecy rate. Therefore, whenever $\lambda_q \leq 0$ the right decision would be using the maximum FJ power (i.e., setting $\lambda_q = 0$).

[5]Local optimality of the NE requires proving that using (23) converges to the NE . In Proposition 2, convergence to NE is proved.

APPENDIX C
PROOF OF PROPOSITION 2

Without loss of generality, assume that w.l.o.g. χ_q defined in (23) satisfies $\Delta\sigma_q < \chi_q < \frac{P_q - \gamma_q}{N_q - 1}$. Furthermore, assume that the iterative use of (23) is done sequentially, meaning that only one player is updating its FJ power at each iteration. Let the initial FJ 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 (23) and $\sigma_q^{*^{(2)}} = \sigma_q^{*^{(1)}}$. In the third iteration, $\sigma_r^{*^{(3)}} = \sigma_r^{*^{(2)}}$, and σ_q gets updated. According to (23), σ_q^* is a decreasing function of σ_r. Hence, if $\sigma_q^{*^{(1)}} < \sigma_q^{*^{(3)}}$ the rth player will select a smaller FJ power in the fourth iteration comparing to the second iteration (i.e., $\sigma_r^{*^{(2)}} > \sigma_r^{*^{(4)}}$). Consequently, in the fifth iteration, the qth player selects a higher FJ 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 right hand side of (24) 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 $\lambda_{q,2} \geq \lambda_q$ [6]. Since 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 $\lambda_q > \lambda_{q,1},\ \forall q$ and $\lambda_q < \lambda_{q,2},\ \forall q$, respectively [7].

[6]Note that when $0 < \lambda_q \leq \lambda_{q,2}$, greedy FJ is optimal in terms of secrecy sum-rate, but it might not always be beneficial for both of the links unless we have $\lambda_q \leq 0$. The bound $\lambda_q \leq 0,\ \forall q$ found in proposition 1 can also guarantee the optimality of greedy FJ in terms of individual secrecy rates.

[7]Note that the effect of λ_q is negligible on the convergence behavior of (23) because λ_q is a sublinear function of FJ powers. We did not see any case where the effect of λ_q could be seen.