Secure Communications in a MIMO Wiretap Interference Channel with Full-duplex Receivers

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*—We consider an interference network tapped by external eavesdropper(s) in which each legitimate transmit-receive pair conceals its communications by using joint transmit-based friendly jamming (TxFJ) and receiver-based friendly jamming (RxFJ). Specifically, TxFJ is realized at the transmit side using MIMO precoding while RxFJ is achieved at the receiver side of each link by leveraging the state-of-the-art self-interference-suppression techniques (allowing a radio to cancel the self-interference effect of its transmit signal). We show that with a careful power allocation between the information signal and TxFJ at the transmit side of each link, the corresponding receiver is able decide on using RxFJ independent of any multi-user interference factor. This ability sets the receivers free from having to measure multi-user interference at eavesdropper(s). With every link following such strategy, we model this interaction as a non-cooperative game. We derive sufficient conditions under which the game admits a unique Nash equilibrium. We then propose a robust version of the game that requires only statistical knowledge of eavesdropping channel.**

Keywords*—*Wiretap interference network, friendly jamming, full-duplex, Nash equilibrium, contraction mapping, receiver-based jamming.

I. Introduction

Among the proposed methods for physical-layer (PHY-layer) security[1], the use of artificial noise (or friendly jamming) is shown to be the closest to a practical implementation. In this method (proposed in [2]), along with the information signal, a transmitter, called Alice, uses multiple antennas and a portion of total transmit power to inject a bogus signal, known as transmit-based friendly jamming (TxFJ), into the channel to confuse the nearby eavesdropper(s). Assuming that Alice knows the channel state information between herself and the legitimate receiver, called Bob, she constructs the TxFJ signal (using precoding techniques) that falls in the null-space of Alice-Bob channel, hence not affecting Bob's reception.

It is possible that an eavesdropper, called Eve, appears very close to Bob, making Alice-Bob channel and Alice-Eve channel highly correlated, thus increasing the possibility that the TxFJ signal to also become nullified at Eve. With recent advances in self-interference suppression (SIS) that allows a radio to cancel the self-interference effect of its own transmit signal, Bob can enhance its secrecy by emitting a jamming signal while he is receiving information from Alice [3]. Note that the latest attempt in realizing full-duplex radios [4] allows a radio to transmit and receive using the same antenna array and on the same frequency (i.e., in-band full-duplex MIMO).

In this paper, we study an interference channel that is tapped by external eavesdropper(s). The legitimate links in the network are all equipped with multiple antennas at both transmitter and receiver side, and can use both TxFJ and RxFJ. Our design parameters are the power of RxFJ signal and the power allocation (PA) between information signal and TxFJ signal of all links.

We assume that legitimate links do not cooperate with each other to decide on design parameters, and there is no centralized authority responsible for computations and optimizations. Hence, links have to make decisions in a distributed fashion. Of course, such design inevitably produces interference at several links, but since Eve(s) is also receiving the interference from all of the links, a careful design can guarantee that the interference at the legitimate links is properly managed while the interference at Eve is kept high as much as possible. We model such an interaction between the legitimate links using non-cooperative games. We then relax the requirement of the eavesdropping channel in our optimizations to propose the robust version of our game.

The works in [5] and [6] are the closest studies to our work. However, both of the aforementioned works consider full knowledge of eavesdropping channel which is not a practical assumption. Regarding the PA between information signal and TxFJ signal, the works in [7] and [8] focused only on the single-link scenario, making their approaches not extendable to the case of multiple links. Furthermore, the authors in [9] investigate optimal PA in a broadcast channel. Here, we investigate the more challenging scenario (i.e., interference channel) where distributed optimization approaches are required.

II. System Model

Consider Q transmitters ($Q \geq 2$), $\text{Alice}_1, \ldots, \text{Alice}_Q$ that communicate with their respective receivers, $\text{Bob}_1, \ldots, \text{Bob}_Q$. Alice_q, $q = 1, \ldots, Q$, has N_q transmit antennas, and Bob_q , $q = 1, \ldots, Q$, has M_q antennas. A passive Eve with L antennas also exists in the range of legitimate links' communications[2]. The received signal at Bob_q, $\mathbf{y}_q$ is:

$$\mathbf{y}_q = \tilde{\mathbf{H}}_{qq}\mathbf{u}_q + \sqrt{\tau_q}\mathbf{H}'_{qq}\mathbf{m}_q + \sum_{\substack{r=1 \\ r\neq q}}^{Q}(\tilde{\mathbf{H}}_{rq}\mathbf{u}_r + \mathbf{H}'_{rq}\mathbf{m}_r) + \mathbf{n}_q$$

where $\tilde{\mathbf{H}}_{rq} \in \mathbb{C}^{M_q \times N_r}$, $r = 1, \ldots, Q$, 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. $\tau_q \in \mathbb{R}^+$ and $\mathbf{H}'_{qq} \in \mathbb{C}^{M_q \times M_q}$ are respectively the positive-real-valued SIS factor and the self interference channel at Bob_q due to the imperfect SIS

[1] See [1] (and references therein) for a complete survey.

[2] Note that L can be assumed to be large enough to represent multiple multi-antenna colluding eavedroppers. However, in this paper, for ease of presentation, we consider the L-antenna Eve as a single entity.

at Bob$_q$. $\mathbf{m}_q \in \mathbb{C}^{M_q}$ is the RxFJ signal created by Bob$_q$, which is a zero mean circularly symmetric complex Gaussian (ZMCSCG) random variable with variance $E[\mathbf{m}_q\mathbf{m}_q^\dagger] = p'_q\mathbf{I}_{M_q}$ where $p'_q \leq P'_q$ with P'_q denoting the total power of Bob$_q$ to be used for RxFJ; $\mathbf{I}_{M_q}$ denotes the $M_q \times M_q$ identity matrix; and $E[\bullet]$ and $\dagger$ respectively denote the expected value and complex conjugation (with transposition in case of vectors and matrices). $H'_{rq} \in \mathbb{C}^{M_q \times M_r}$, $r \neq q$, is the channel from Bob$_r$ to Bob$_q$ because the jamming signals created by other Bobs interfere with Bob$_q$'s reception. $\mathbf{n}_q \in \mathbb{C}^{M_q}$ is the complex AWGN whose power is N_0 and whose covariance matrix is $E[\mathbf{n}_q\mathbf{n}_q^\dagger] = N_0\mathbf{I}_{M_q}$.

We assume that $\tilde{\mathbf{H}}_{rq} = \bar{\mathbf{H}}_{rq}{d_{rq}}^{-\eta/2}$ where $\bar{\mathbf{H}}_{rq} \in \mathbb{C}^{M_q \times N_r}$ represents the small-scale fading, d_{rq} is the distance between Alice$_r$ and Bob$_q$ in meters and η is the path-loss exponent. The same equivalent assumption holds for $\mathbf{H}'_{rq}$, $r \neq q$, i.e., $\mathbf{H}'_{rq} = \bar{\mathbf{H}}'_{rq}{d'_{rq}}^{-\eta/2}$ where $\bar{\mathbf{H}}'_{rq} \in \mathbb{C}^{M_q \times M_r}$ and d'_{rq} is the distance from Bob$_r$ to Bob$_q$. The received signal by Eve is

$$\mathbf{z} = \tilde{\mathbf{G}}_q\mathbf{u}_q + \mathbf{G}'_q\mathbf{m}_q + \sum_{\substack{r=1\\r\neq q}}^{Q}(\tilde{\mathbf{G}}_r\mathbf{u}_r + \mathbf{G}'_r\mathbf{m}_r) + \mathbf{e}$$

where $\tilde{\mathbf{G}}_q \in \mathbb{C}^{L\times N_q}$, $q = 1,\ldots,Q$ denotes the complex channel matrix between Alice$_q$ and Eve, and $\tilde{\mathbf{G}}_q = \bar{\mathbf{G}}_q d_{qe}^{-\eta/2}$ where $\bar{\mathbf{G}}_q \in \mathbb{C}^{L\times N_q}$ and d_{qe} is the distance between Alice$_q$ and Eve; $\mathbf{G}'_q \in \mathbb{C}^{L\times M_q}$, $q = 1,\ldots,Q$, is the channel between Bob$_q$ and Eve. $\mathbf{G}'_q = \bar{\mathbf{G}}'_q {d'_{qe}}^{-\eta/2}$ where $\bar{\mathbf{G}}'_q \in \mathbb{C}^{L\times M_q}$ and d'_{qe} is the distance from Bob$_q$ to Eve, and finally, $\mathbf{e}$ has the same characteristics as $\mathbf{n}_q$. The signal $\mathbf{u}_q = \mathbf{s}_q + \mathbf{w}_q$ consists of the information signal $\mathbf{s}_q$ and the TxFJ signal $\mathbf{w}_q$. As in [10], we only consider the case of single stream data transmission using multiple antennas. That is, we set $\mathbf{s}_q \triangleq \mathbf{T}_q x_q$ where $\mathbf{T}_q \in \mathbb{C}^{N_q}$ is the precoder and $x_q \in \mathbb{C}$ is the information signal.

Assume that a Gaussian codebook is used for x_q, i.e., x_q is distributed as a ZMCSCG random variable with $E[x_q x_q^\dagger] = \phi_q P_q$ where P_q is the total transmit power of Alice$_q$ and $0 \leq \phi_q \leq 1$ is the portion of transmit power allocated to the information signal. For the TxFJ signal, we write $\mathbf{w}_q \triangleq \mathbf{Z}_q\mathbf{v}_q$, where $\mathbf{Z}_q \in \mathbb{C}^{N_q\times(N_q-1)}$ is an orthonormal basis for the null space of $\tilde{\mathbf{H}}_{qq}$ ($\tilde{\mathbf{H}}_{qq}\mathbf{w}_q = 0$) and $\mathbf{v}_q \in \mathbb{C}^{(N_q-1)}$ is a vector with i.i.d. ZMCSCG entries and $E[\mathbf{v}_q\mathbf{v}_q^\dagger] = \sigma_q\mathbf{I}_{(N_q-1)}$. The scalar value $\sigma_q = \frac{(1-\phi_q)P_q}{N_q-1}$ denotes the TxFJ power. 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 V_q, to form a transmit beamforming technique. Let $\mathbf{H}_{qq} \triangleq \tilde{\mathbf{H}}_{qq}\mathbf{V}_q^{(1)}$, $\mathbf{H}_{j_{qq}} \triangleq \tilde{\mathbf{H}}_{qq}\mathbf{V}_q^{(2)}$, $\mathbf{H}_{qr} \triangleq \tilde{\mathbf{H}}_{qr}\mathbf{V}_q^{(1)}$, $\mathbf{H}_{j_{qr}} \triangleq \tilde{\mathbf{H}}_{qr}\mathbf{V}_q^{(2)}$, $\mathbf{G}_q \triangleq \tilde{\mathbf{G}}_q\mathbf{V}_q^{(1)}$, $\mathbf{G}_{j_q} \triangleq \tilde{\mathbf{G}}_q\mathbf{V}_q^{(2)}$. The terms $\mathbf{G}_q$ and $\mathbf{G}_{j_q}$ denote the eavesdropping channel components. Hence,

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

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

After receiving $\mathbf{y}_q$ at Bob$_q$, a linear receiver $\mathbf{d}_q \in \mathbb{C}^{M_q}$ is applied. Given that $\mathbf{d}_q^\dagger\mathbf{H}_{j_{qq}}\mathbf{v}_q = 0$, the linear estimate $\hat{\mathbf{y}}_q$ is

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

Hence, the information rate for the qth link can be written as

$$C_q = \log(1 + \frac{\phi_q P_q}{a_q + b_q p'_q}) \tag{2}$$

where

$$a_q = \frac{\sum_{\substack{r=1\\r\neq}}^{Q}\left(\left|\mathbf{d}_q^\dagger\mathbf{H}_{rq}\right|^2\phi_r P_r + \left|\mathbf{d}_q^\dagger\mathbf{H}_{j_{rq}}\right|^2\frac{(1-\phi_r)P_r}{N_r-1} + |\mathbf{d}_q^\dagger\mathbf{H}'_{rq}|^2 p'_r\right) + N_0}{\left|\mathbf{d}_q^\dagger\mathbf{H}_{qq}\right|^2}, \tag{3a}$$

$$b_q = \tau_q\frac{|\mathbf{d}_q^\dagger\mathbf{H}'_{qq}|^2}{|\mathbf{d}_q^\dagger\mathbf{H}_{qq}|^2}. \tag{3b}$$

Eve also applies the linear receiver $\mathbf{r}_q \in \mathbb{C}^L$ while eavesdropping on qth link's signal to obtain

$$\hat{\mathbf{z}}_q = \mathbf{r}_q^\dagger(\mathbf{G}_q x_q + \mathbf{G}_{j_q}\mathbf{v}_q + \mathbf{G}'_q\mathbf{m}_q + \sum_{\substack{r=1\\r\neq q}}^{Q}(\mathbf{G}_r x_r + \mathbf{G}_{j_r}\mathbf{v}_r + \mathbf{G}'_r\mathbf{m}_r) + \mathbf{e}). \tag{4}$$

Thus, the rate at Eve while eavesdropping on Alice$_q$ (i.e., leaked rate of Alice$_q$) is

$$C_{eq} = \log(1 + \frac{\phi_q P_q}{c_q + d_q p'_q}) \tag{5}$$

where

$$c_q = \frac{\left|\mathbf{r}_q^\dagger\mathbf{G}_{jq}\right|\frac{(1-\phi_q)P_q}{N_q-1}}{\left|\mathbf{r}_q^\dagger\mathbf{G}_q\right|^2} + \frac{\sum_{\substack{r=1\\r\neq}}^{Q}\left(\left|\mathbf{r}_q^\dagger\mathbf{G}_r\right|^2\phi_r P_r + \left|\mathbf{r}_q^\dagger\mathbf{G}_{j_r}\right|^2\frac{(1-\phi_r)P_r}{N_r-1} + |\mathbf{r}_q^\dagger\mathbf{G}'_r|^2 p'_r\right) + N_0}{\left|\mathbf{r}_q^\dagger\mathbf{G}_q\right|^2}, \tag{6a}$$

$$d_q = \frac{|\mathbf{r}_q^\dagger\mathbf{G}'_q|^2}{|\mathbf{r}_q^\dagger\mathbf{G}_q|^2}. \tag{6b}$$

Finally, the secrecy rate of Alice$_q$ can be written as

$$C_q^{sec} = \max\{C_q - C_{eq}, 0\}. \tag{7}$$

The linear receivers $\mathbf{d}_q$, $q = 1,\ldots,Q$, and $\mathbf{r}$ are assumed to be chosen according maximal ratio combining (MRC) method. Hence, $\mathbf{d}_q = \mathbf{U}_q^{(1)}$ where $\mathbf{U}_q^{(1)}$ is the first column of $\mathbf{U}_q$. Let the SVD of $\tilde{\mathbf{G}}_q$ be denoted as $\tilde{\mathbf{G}}_q = \mathbf{L}_q\mathbf{D}_q\mathbf{R}_q$ 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 qth link, $\mathbf{r} = \mathbf{L}_q^{(1)}$ where $\mathbf{L}_q^{(1)}$ is the first column of matrix $\mathbf{L}_q$.

[3]Acquiring channel state information (CSI) is assumed to be done securely. For example, implicit channel estimation can be used to lower the probability of eavesdropping on channel estimates.

III. Problem Formulation

In this section, we state the main objectives and present the necessary bounds to guarantee positive secrecy. From here on, wherever we use RxFJ, we are referring to the power of RxFJ, and wherever TxFJ is mentioned, we are referring to the power of TxFJ signal.

The main objective for each link q is as follows

$$\begin{aligned} \underset{\phi_q, p'_q}{\text{maximize}} \quad & C_q^{sec} \\ \text{s.t.} \quad & 0 \leq \phi_q \leq 1, \\ & 0 \leq p'_q \leq P'_q. \end{aligned} \tag{8}$$

Due to the non-concavity of the objective function in (8) w.r.t. decision variables, the optimization in (8) is non-convex[4]. To find a tractable (and yet suboptimal) solution, we decompose the analysis of RxFJ and PA into two sub-problems. We first propose a tractable solution for RxFJ that results in not only maintaining positive secrecy, but also alleviating the need for knowledge of interference at Eve. The secrecy maximization w.r.t. only p'_q can be written as

$$\begin{aligned} \underset{p'_q}{\text{maximize}} \quad & \frac{1+\frac{\phi_q P_q}{a_q+b_q p'_q}}{1+\frac{\phi_q P_q}{c_q+d_q p'_q}} \\ \text{s.t.} \quad & 0 \leq p'_q \leq P'_q. \end{aligned} \tag{9}$$

Positive secrecy in (7), imposed via the $\max\{\bullet\}$ function, can be equivalently achieved in (9) iff the objective in (9) is larger than 1. A sufficient condition to achieve positive secrecy is to solve the following optimization:

$$\begin{aligned} \underset{p'_q}{\text{maximize}} \quad & f(p'_q) \triangleq \frac{\frac{\phi_q P_q}{a_q+b_q p'_q}}{\frac{\phi_q P_q}{c_q+d_q p'_q}} = \frac{c_q+d_q p'_q}{a_q+b_q p'_q} \\ \text{s.t.} \quad & 0 \leq p'_q \leq P'_q. \end{aligned} \tag{10}$$

Specifically, if the solution to (10) is greater than 1 then this solution guarantees the positive secrecy. The first and second derivatives of $f(p'_q)$ are as follows

$$\frac{df(p'_q)}{dp'_q} = -\frac{b_q c_q - a_q d_q}{(a_q+b_q p'_q)^2}, \tag{11a}$$

$$\frac{d^2 f(p'_q)}{dp'^2_q} = 2b_q \frac{b_q c_q - a_q d_q}{(a+bp'_q)^3}. \tag{11b}$$

Hence, the optimal value of p'_q, i.e., p'^*_q, is as follows:

$$p'^*_q = \begin{cases} P'_q & \text{if } b_q < \frac{a_q d_q}{c_q}, \\ 0 & \text{if } b_q > \frac{a_q d_q}{c_q}. \end{cases} \tag{12}$$

Simplifying the first condition of (12), a threshold for SIS factor is as follows[5]

$$\tau_q < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2} \frac{a_q d_q}{c_q}. \tag{13}$$

Hence, (12) offers an on-off method that can maintain positive secrecy (if $f(p'^*_q) > 1$). It can be seen in (12) that the optimal value of RxFJ that solves (10) is dependent on two factors: the multi-user interference that Bob_q is receiving (i.e., a_q) and the interference that the eavesdropper is receiving while eavesdropping the qth link (i.e., c_q). Because multi-user interference is subject to vary (due to the behavior of other links), it is not usually desirable to change the RxFJ accordingly, as it imposes additional computations on Bob.

Another way to achieve positive secrecy is to allocate a fair amount of power at the transmit side to TxFJ and information signal. Thus, the objective in (8) is assumed to be larger than one, which reduces to

$$\frac{\phi_q P_q}{a_q+b_q p'_q} > \frac{\phi_q P_q}{c_q+d_q p'_q}. \tag{14}$$

Simplifying this inequality, we end up with the following

$$c_q > a_q + (b_q - d_q) p'_q. \tag{15}$$

The inequality in (15) is a preliminary bound on the PA factor ϕ_q because the term c_q includes ϕ_q, and reducing (15) gives us a bound for ϕ_q. Combining (15) and (12) we have

$$\begin{cases} c_q > a_q + (b_q - d_q) P'_q, & \text{if } \ b_q < \frac{a_q d_q}{c_q}, \\ c_q > a_q, & \text{if } \ b_q > \frac{a_q d_q}{c_q}. \end{cases} \tag{16}$$

Since the inequalities in (16) are strict, we write the following:

$$\begin{cases} c_q = a_q + (b_q - d_q) P'_q + \delta, & \text{if } \ b_q < \frac{a_q d_q}{c_q}, \\ c_q = a_q + \delta, & \text{if } \ b_q > \frac{a_q d_q}{c_q} \end{cases} \tag{17}$$

where $\delta \geq 0$ is a small value that Alice_q can allocate to TxFJ such that (16) is satisfied. Note that (according to (6a)), the term c_q includes the TxFJ of Alice_q. Hence, simplifying the left hand sides (LHS) of equalities in (17), one can find a lower bound on TxFJ, or equivalently on $(1-\phi_q)P_q$[6]. To make use of the lower bound on TxFJ derived from (17), we first introduce a property of the secrecy rate of Alice_q

Lemma 1. *If positive secrecy is achieved, the secrecy rate C_q^{sec} is a monotonically increasing function of P_q and ϕ_q, respectively.*

Proof: Considering the increment δ in transmit power, the lower bound in (15) can be written as

$$c_q = a_q + (b_q - d_q) p'_q + \delta \tag{18}$$

where p'_q is set according to (12). Replacing the term c_q in (7) with the right hand side (RHS) of (18), and taking the derivative of (7) w.r.t. P_q and ϕ_q, we have

$$\frac{dC_q^{sec}}{d_q P_q} = \frac{\phi_q \delta}{(a_q+\phi_q P_q+b_q p'_q)(a_q+\phi_q P_q+b_q p'_q+\delta)}, \tag{19a}$$

$$\frac{dC_q^{sec}}{d\phi_q} = \frac{P_q \delta}{(a_q+\phi_q P_q+b_q p'_q)(a_q+\phi_q P_q+b_q p'_q+\delta)} \tag{19b}$$

which are both positive and prove the Property. ∎

In order to mitigate the knowledge of multi-user interference (i.e., a_q and c_q) in evaluating $\frac{a_q d_q}{c_q}$ in (13), we examine the following alternative conditions for TxFJ, or equivalently the

[4]The non-concavity of objective function can be easily seen by examining the Hessian matrix of the objective function

[5]Although when $p'_q = 0$ the benefits of RxFJ are not present, one can set a minimum RxFJ power to prevent RxFJ to go to zero such that if in the worst-case, TxFJ fails, the received rate of Eve cannot exceed a threshold.

[6]Later on, we derive this lower bound on TxFJ to do further analysis on the power allocation.

term c_q:

$$\begin{cases} c_q = a_q + (b_q - d_q)P'_q + \delta, & \text{if } \ b_q < d_q, \\ c_q = a_q + \delta, & \text{if } \ b_q > d_q. \end{cases} \tag{20}$$

The following property shows the sufficiency of (20) for concluding (17).

Lemma 2. *Provided that* $(b_q - d_q)P'_q + \delta < 0$ *and* $\delta > 0$*, the condition in* (20) *is sufficient for satisfying* (17)*.*

Proof: For when $b_q < d_q$, we replace the term c_q of $\frac{a_q d_q}{c_q}$ with the RHS of (20). If $(b_q - d_q)P'_q + \delta < 0$, one can conclude that $a_q > a_q + (b_q - d_q)P'_q + \delta$. Hence, $b_q < d_q$ is sufficient to deduce $b_q < \frac{a_q d_q}{c_q}$. Regarding $b_q > d_q$ the same argument cannot be used to satisfy $b_q > \frac{a_q d_q}{c_q}$. However, since ${p'_q}^* = 0$ when $b_q > \frac{a_q d_q}{c_q}$, then if $\delta > 0$ –which is a required constraint in order to satisfy the results obtained in (19a) and (19b)– we have $c_q > a_q$. Hence, $b_q > d_q$ is sufficient to satisfy $b_q > \frac{a_q d_q}{c_q}$. ■

Using Lemma 2, one can conclude that in calculating the value of RxFJ in (20), contrary to (17), there is no requirement to know the multi-user interference at Bob_q (i.e., a_q) or at Eve(i.e., c_q). Specifically, Bob_q only has to check whether or not $b_q < d_q$, or equivalently

$$\tau_q < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_q|^2}. \tag{21}$$

The assumption $(b_q - d_q)P'_q + \delta < 0$ sets an upper bound on δ, i.e., $0 < \delta < (d_q - b_q)P'_q$. We choose $\delta = \frac{1}{2}\,|d_q - b_q|\,P'_q$ for both when $b_q < d_q$ and when $b_q > d_q$[7]. In the next section, we use the derived conditions to model a power control game.

IV. Game Formulation

The condition in (20) can be written in general form as

$$\begin{cases} c_q \geq a_q + (b_q - d_q)P'_q + \delta, \text{if } \ b_q < d_q, \\ c_q \geq a_q + \delta, \text{if } \ b_q > d_q. \end{cases} \tag{22}$$

Using (3) and (6), an upper bound on ϕ_q is shown in (23) at the top of the next page where

$$A_{q,r} = \frac{N_q - 1}{N_r - 1} \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2} \left((N_r - 1)|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{jr}|^2 \right), \tag{24a}$$

$$B_{q,r} = \frac{N_q - 1}{N_r - 1} \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2} \left((N_r - 1)|\mathbf{r}_q^\dagger \mathbf{G}_r|^2 - |\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2 \right), \tag{24b}$$

$$C_{q,r} = \frac{N_q - 1}{N_r - 1} \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{jr}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}, \tag{24c}$$

$$D_{q,r} = (N_q - 1) \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}, \tag{24d}$$

$$E_q = (N_q - 1) \frac{\tau_q |\mathbf{r}_q^\dagger \mathbf{G}_q|^2 |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}. \tag{24e}$$

[7]While by no means this assignment is optimal, it turns out in simulations that network-wide, the effect of such assignment is minmal. Note that the optimal assignment of δ is in fact as difficult as assigning the optimal value of ϕ_q back in (8), which we tried to avoid earlier in this paper.

Hence, link q's optimization problem, where $q = 1, \ldots, Q$, is

$$\begin{aligned} \underset{\phi_q}{\text{maximize}} \ \ & C_q^{sec} \\ \text{s.t.} \ \ & (23). \end{aligned} \tag{25}$$

Notice that in establishing (25), the value of c_q (or equivalently power of TxFJ) is already set according to (20). Hence, in (25), only those ϕ_q's that exist in the numerators of C_q and C_{eq} are treated as variables. Using the condition in (19b), the maximum amount of ϕ_q in (23) solves (25) because the condition in (20) guarantees the secrecy rate being a monotonically increasing function of ϕ_q (cf. Lemma 1). Hence, the best-response of the qth link, $q = 1, \ldots, Q$, is when ϕ_q meets its upper bound in (23) with equality. Otherwise, the secrecy rate is not maximized. With every link following such strategy, the interaction between the legitimate links can be modeled as non-cooperative game [11] where the players are the links, the strategy set of the qth player is the constraint in (25), and the utility of each player is his secrecy rate. The Nash equilibrium is a point at which no player is willing to unilaterally change his strategy given the strategies of other players [11]. A NE exists if the strategy set of each player is non-empty, compact, and convex and the utility function of each player is a continuous and (quasi-)concave function of its action. Replacing c_q with RHS of (20), C_q^{sec} becomes concave w.r.t ϕ_q. Specifically,

$$\frac{d^2 C_q^{sec}}{d\phi_q^2} = P_q^2 \left(\frac{1}{a + \delta + \phi_q P_q + b p'_q} - \frac{1}{a + \phi_q P_q + b p'_q} \right) \tag{26}$$

which is always negative indicating that C_q^{sec} is concave w.r.t. ϕ_q. The compactness of strategy sets is also obvious. Hence, at least one NE exists in this game. A necessary and sufficient condition for the uniqueness of NE is proven in the following theorem.

Theorem 1. *The game defined in* (25) *for all* $q = 1, \ldots, Q$ *has a unique NE iff the following condition is satisfied:*

$$\rho(\mathbf{A} + \mathbf{B}) < 1 \tag{27}$$

where $\rho(\bullet)$ *indicates the spectral radius of a matrix,* $\mathbf{A}$ *is a* $Q \times Q$ *matrix whose entires are written as*

$$\mathbf{A} = \begin{cases} -\frac{P_r}{P_q} A_{q,r} \ , & r \neq q, \\ 0 \ , & r = q \end{cases}, \forall q \in \{1, \ldots, Q\}, \tag{28}$$

and $\mathbf{B}$ *is as follows:*

$$\mathbf{B} = \begin{cases} \frac{P_r}{P_q} B_{q,r} \ , & r \neq q, \\ 0 \ , & r = q \end{cases}, \forall q \in \{1, \ldots, Q\}. \tag{29}$$

Proof: The uniqueness of NE can be proven by leveraging the concept of fixed point theorem. In fact, if the iterative computation of each player's best-response (i.e., ϕ_q meeting its upper bound in (23) with equality for all q) has a fixed point, the convergence point is the NE of the game [12]. We first analyze the existence of fixed point of the argument inside $\max\{\min\{\bullet, 1\}, 0\}$. Then, we extend the analysis to include $\max\{\min\{\bullet, 1\}, 0\}$. Concatenating the constraint in (23) for all q (without considering $\max\{\min\{\bullet, 1\}, 0\}$), the following fixed point problem in its tth iteration can be established:

$$\Phi(t+1) = \mathcal{T}(\Phi(t)) = \mathbb{1} + (\mathbf{A} + \mathbf{B})\Phi(t) + \mathbf{f} \tag{30}$$

where $\Phi = [\phi_1, \ldots, \phi_Q]^T$ and $\mathbb{1}$ is a vector whose entries are 1, $\mathbf{f}$ is a vector constructed by concatenating other terms in (23) for all q. The rest of the proof is presented in Appendix

$$\phi_q \leq \max\{\min\{1-\frac{1}{P_q}\sum_{\substack{r=1\\r\neq q}}^{Q}\left\{\left(A_{q,r}-B_{q,r}\right)\phi_r P_r + C_{q,r}P_r + D_{q,r}p'_r\right\} - \frac{p'_q}{P_q}E_q - \delta, 1\}, 0\} \tag{23}$$

A. ■

Remark 1: Using this condition, the convergence of Jacobi iterative method in the sense of [12, Ch. 2, Proposition 6.8] is guaranteed. In fact, at every iteration, every player updates its action corresponding to the observed action of other players in the previous iteration. Hence, we choose Jacobi method as our main iterative power control algorithm.

Although (27) is a tight condition, evaluating it requires the knowledge of the whole matrix $\mathbf{A}+\mathbf{B}$ which is not desirable for distributed implementation. We introduce a sufficient condition which can be evaluated in distributed fashion. It is shown in [12, Proposition A.20] that for any induced matrix norm[8] $||\bullet||$ and any square matrix $\mathbf{M}$ we have $\rho(\mathbf{M}) \leq ||\mathbf{M}||$. Using this property, we consider the induced norm $||\bullet||$ to be $||\bullet||_\infty$ which is the infinity norm. Hence, assuming that $\mathbf{M}$ is a $Q\times Q$ matrix, a sufficient condition for $\rho(\mathbf{M}) < 1$ is that whether $||\mathbf{M}||_\infty < 1$. Hence, in our game, we must have

$$||\mathbf{A}+\mathbf{B}||_\infty = \max_q \sum_{r=1}^{Q}\frac{P_r}{P_q}\left|A_{q,r}-B_{q,r}\right| < 1. \tag{31}$$

In other words, every player should check whether

$$\frac{Nq-1}{Nr-1}\Big(\sum_{r=1}^{Q}\left|\frac{|\mathbf{r}_q^\dagger\mathbf{G}_q|^2((N_r-1)|\mathbf{d}_q^\dagger\mathbf{H}_{rq}|^2-|\mathbf{d}_q^\dagger\mathbf{H}_{jr}|^2)}{|\mathbf{r}_q^\dagger\mathbf{G}_{jq}|^2|\mathbf{d}_q^\dagger\mathbf{H}_{qq}|^2}\right.$$
$$\left.-\sum_{r=1}^{Q}\frac{|\mathbf{d}_q^\dagger\mathbf{H}_{qq}|^2((N_r-1)|\mathbf{r}_q^\dagger\mathbf{G}_r|^2-|\mathbf{r}_q^\dagger\mathbf{G}_{jr}|^2)}{|\mathbf{r}_q^\dagger\mathbf{G}_{jq}|^2|\mathbf{d}_q^\dagger\mathbf{H}_{qq}|^2}\right|\Big) < 1,\ \forall q. \tag{32}$$

The physical intuition drawn from the condition in (31) is not straightforward. One can decompose this condition as follows: The first summation is mostly related to the received multi-user interference at each link which should be low enough to guarantee the uniqueness of NE. A sufficient separation between the links can satisfy this condition. The second summation however, does not exhibit any physical intuition related to the channel components, which makes the prediction of a unique NE difficult. We see in the next section that the robust approach makes the iterative procedure independent of the second summation in LHS of (32), thus simplifying the physical intuition to predict the uniqueness of NE.

V. Robust Power Allocation Game

So far, we assumed the full knowledge of Alice-Eve and Bob-Eve channels (i.e., ECSI) in every analysis. However, the knowledge of ECSI is not practical to achieve in several scenarios. In this section, we incorporate the assumption of unknown ECSI in our game. In this analysis we assume that the value of large-scale fading of the Alice-Eve and Bob-Eve channels are known and small-scale fading components are not known. Using the concepts of stochastic geometry, our analysis can be easily extended to the case where the exact knowledge of large-scale fading is also not available.

As the knowledge of ECSI becomes unknown, each link needs to make sure that positive secrecy is still preserved. Recalling the inequalities in (22) and (23), positive secrecy happens when $c_q > a_q + (b_q - d_q)p'_q$ or equivalently

$$(1-\phi_q)P_q > \psi_q + p'_q E_q \tag{33}$$

where

$$\psi_q \triangleq \sum_{\substack{r=1\\r\neq q}}^{Q}\left\{\left(A_{q,r}-B_{q,r}\right)\phi_r P_r + C_{q,r}P_r + D_{q,r}p'_r\right\}.$$

Therefore, for a given probability value ε, the qth link needs to makes sure that the following inequality is satisfied:

$$\Pr\{(1-\phi_q)P_q > \psi_q + p'_q E_q\} \geq \varepsilon. \tag{34}$$

Using (20) and the Bayes law of total probability we have

$$\begin{aligned}&\Pr\{(1-\phi_q)P_q > \psi_q + p'_q E_q\} = \\ &\Pr\{b_q < d_q\}(1-\Pr\{(1-\phi_q)P_q \leq \psi_q + P'_q E_q\})+\\ &\Pr\{b_q > d_q\}(1-\Pr\{(1-\phi_q)P_q \leq \psi_q\}).\end{aligned} \tag{35}$$

Using Markov inequality in (35), the following holds

$$\begin{aligned}&\Pr\{b_q < d_q\}(1-\Pr\{(1-\phi_q)P_q < \psi_q + P'_q E_q\})+\\ &\Pr\{b_q > d_q\}(1-\Pr\{(1-\phi_q)P_q < \psi_q\}) \ >\end{aligned} \tag{36}$$

$$\Pr\{b_q < d_q\}(1-\frac{\mathrm{E}[\psi_q + P'_q E_q]}{(1-\phi_q)P_q}) + \Pr\{b_q > d_q\}(1-\frac{\mathrm{E}[\psi_q]}{(1-\phi_q)P_q}). \tag{37}$$

Simplifying this inequality, we end up with

$$\phi_q \leq \max\{\min\{ \tag{38}$$

$$1-\Pr\{b_q < d_q\}\frac{\mathrm{E}[\psi_q + P'_q E_q\}]}{(1-\varepsilon)P_q} - \Pr\{b_q > d_q\}\frac{\mathrm{E}[\psi_q\}]}{(1-\varepsilon)P_q}, 1\}, 0\}. \tag{39}$$

Using (3) and (6), we simplify $b_q < d_q$, which is as follows

$$b_q < d_q \Rightarrow |\mathbf{r}_q^\dagger\mathbf{G}_q|^2 < \frac{|\mathbf{d}_q^\dagger\mathbf{H}_{qq}|^2}{|\mathbf{d}_q^\dagger\mathbf{H}'_{qq}|^2}|\mathbf{r}_q^\dagger\mathbf{G}'_q|^2. \tag{40}$$

Since the precoder $\mathbf{V}_q^{(1)}$ has orthonomal columns, the small-scale fading component of $\mathbf{G}'_q$ and $\mathbf{G}_q$ remain i.i.d. ZMCSCG with unit variances. The linear receivers $\mathbf{d}_q$, $q = 1,\ldots,Q$, and $\mathbf{r}$ also have orthonormal columns. Hence, $|\mathbf{r}_q^\dagger\mathbf{G}_q|^2$ and $|\mathbf{r}_q^\dagger\mathbf{G}'_q|^2$ both have independent chi-square distributions with two degrees of freedom. The probability $\Pr\{b_q < d_q\}$ can be written as

$$\Pr\{\frac{|\mathbf{r}_q^\dagger\mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger\mathbf{G}'_q|^2} < \frac{|\mathbf{d}_q^\dagger\mathbf{H}_{qq}|^2}{\tau_q|\mathbf{d}_q^\dagger\mathbf{H}'_{qq}|^2}\}. \tag{41}$$

The quantity $X \triangleq \frac{|\mathbf{r}_q^\dagger\mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger\mathbf{G}'_q|^2}$ in (41) is the SINR of a one-branch diversity combiner with one interferer [14]. Hence,

$$\Pr\{b_q < d_q\} = 1 - \frac{1}{1+\frac{|\mathbf{d}_q^\dagger\mathbf{H}_{qq}|^2}{\tau_q|\mathbf{d}_q^\dagger\mathbf{H}'_{qq}|^2}}. \tag{42}$$

We now turn our attention to $\mathrm{E}[\psi_q + P'_q E_q]$, which can be simplified using the following

[8] An matrix norm induced by a vector norm $\mathbf{M}$ is defined as $||\mathbf{M}|| = \max_{||\mathbf{x}||=1}||\mathbf{M}\mathbf{x}||$ where $\mathbf{x}$ is a vector and both norms on the right hand side are vector norms [13].

$$E[A_{q,r}] = \frac{N_q - 1}{(N_r - 1)(N_q - 3)} \frac{(N_r - 1)|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{jr}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}, \tag{43a}$$

$$E[B_{q,r}] = 0, \tag{43b}$$

$$E[C_{q,r}] = \frac{N_q - 1}{(N_r - 1)(N_q - 3)} \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{jr}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \frac{N_q - 1}{(N_q - 3)} \frac{d_{re}^{(-\eta)}}{d_{qe}^{(-\eta)}}, \tag{43c}$$

$$E[D_{q,r}] = \frac{N_q - 1}{(N_q - 3)} \left(\frac{|\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \frac{{d'_{re}}^{(-\eta)}}{d_{qe}^{(-\eta)}} \right), \tag{43d}$$

$$E[E_q] = \frac{N_q - 1}{N_q - 3} \frac{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}. \tag{43e}$$

To derive (43), we examine (24). One can conclude that $|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2$ and $|\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2$ have chi-square distributions with $2(N_q - 1)$ and $2(N_r - 1)$ degrees of freedom, respectively [8, lemma 2]. Furthermore, both $|\mathbf{r}_q^\dagger \mathbf{G}_r|^2$ and $|\mathbf{r}_q^\dagger \mathbf{G}'_r|^2$ have chi-square distributions with two degrees of freedom. The division of a (central) chi-square random variable by another independent (central) chi-square random variable is distributed as *F-distribution*. Hence, the set of equations in (43) can be derived. We choose to use RxFJ whenever $\Pr\{b_q > d_q\} > 0.5$. With the derivations in (38) and (43), we can construct a game with the same structure as in section IV where each link's best response is calculated from (38), and the following must hold to ensure a unique NE:

$$\rho\left(\frac{1}{1-\epsilon} E[\mathbf{A}]\right) < 1, \tag{44}$$

where $\mathbf{A}$ is defined in (28) and the expectation is element-wise. Same as the previous section, an alternative condition to (44) is to replace the spectral radius with infinity norm according to (31). Notice that the absence of $\mathbf{B}$ (defined in (29)) in (44) provides less restrictive NE uniqueness conditions, as we expect that by managing the positioning of the links, a unique NE exists regardless of Eve's channels. The following algorithm summarizes our discussion so far:

Algorithm 1 Iterative Secure Power Allocation

Set p'_q and δ according to (20) (cf. Section III).

1: **for** n=1 to `maximum iteration` **do**
2: **repeat** $\forall(q) \in \{1, ..., Q\}$ Calculate a_q, b_q, c_q, and d_q according to (3) and (6)
3: Set ϕ_q equal to its upper bound according to (23) (full-ECSI version), or (38) (robust version).
4: **until** Convergence
5: **end for**

VI. Numerical Results

In this section, we verify our theoretical analyses. We show the results for the case of four links[9]. We consider a deterministic location for Eve denoted as ($\mathtt{x_e}$, $\mathtt{y_e}$) on a 2-D coordinate system. All Alices are randomly placed on the boundary of a circle, known as simulation region, with radius $\mathtt{r_{circ}}$ whose center is at the origin. Each Alice has a fixed distance (communication range) with her corresponding Bob denoted as $\mathtt{d_{link}}$. Each Bob is placed randomly around his corresponding Alice on the boundary of a circle whose radius is set to $\mathtt{d_{link}}$ with his corresponding Alice at the center of the circle. We set $N_0 = 0$ dBm; $P_q = 25$ dBm, $\forall q$; $P'_q = 15$ dBm; $\eta = 4$; $\tau_q = -100$ dB; and $\mathtt{d_{link}} = 10m$. Jacobi method is used in all simulations[10].

Fig. 1 (a) shows the variation of convergence probabilities of robust and full-ECSI method w.r.t $\mathtt{r_{circ}}$ for the four-link case. The convergence probability is calculated as number of times the conditions in (27) (indicated by n_1 in Fig. 1 (a)) and (32) (indicated by n_2 in Fig. 1 (a)) hold true divided by the number of channel realizations. It can be seen that for the case of full-ECSI, probability of uniqueness of NE using (31) is very low. However, in the case of unknown ECSI, since the nodes are indifferent w.r.t. ECSI, far less restrictive conditions than the case of full-ECSI can be achieved. Moreover, in robust version, as ε becomes larger, the uniqueness conditions become restrictive, which is in line with the derivation in (44).

Fig. 1 (b) shows the achieved secrecy sum-rate of the proposed non-cooperative game and the globally optimal solutions of the secrecy sum-rate maximization for the four-link case. The maximum amount of iterations for Algorithm 1 is set to 50 iterations. It can be seen that in the full-ECSI case, the secrecy sum-rate is less than the globally optimal solutions. Surprisingly, the secrecy sum-rate of robust approach is higher than the full-ECSI case for $r_{circ} > 10$m. This advantage can be seen for both values of ε. The main reason behind this advantage is that in the robust approach, the links set their power allocations in a way to be indifferent w.r.t. ECSI. This provides the links with less restriction, and thus a wider range of candidate solutions may exist, allowing the links to manage the interference between themselves better than the full-ECSI case. Notice that both the NE uniqueness and convergence of Algorithm 1 are affected by ECSI, contributing to more restrictive tradeoff between links. It can be seen in Fig. 1 (c) that although the leaked rate for the robust approach is higher than full-ECSI case –which is the penalty of robust approach– the robust approach is more efficient in managing interference.

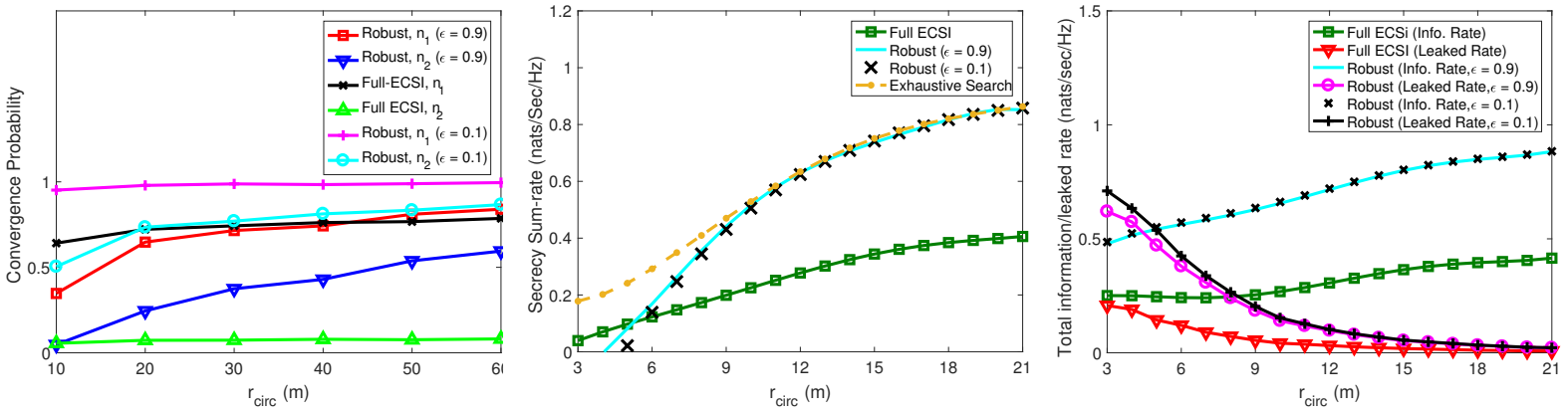
Lastly, one can see in Fig. 1 (c) that even for low values of ε, the performance of robust approach is still superior. We conjecture confidently that this might be due to the fact the *F-distrbution*, which was the distribution involved in best responses in (38), is a positively skewed distribution. Hence, most of the density of the distribution of best response and its mean are concentrated at the left of the median. This means that to ensure that $(1 - \phi_q) > \Pr\{b_q < d_q\} \frac{\mathrm{E}[\psi_q + \tau_q P'_q E_q]}{1-\varepsilon} + \Pr\{b_q > d_q\} \frac{\mathrm{E}[\psi_q]}{1-\varepsilon}$, the density of the values above the mean is relatively low, meaning that the PA factor set by (38) will be most likely providing positive secrecy.

VII. Conclusion

We proposed a joint Tx- and Rx-based friendly jamming mechanism in a MIMO interference network tapped by external eavesdropper(s). Using a game theoretic approach, we proposed a framework under which every link can utilize RxFJ and TxFJ to achieve a positive secrecy rate and relax the knowledge of interference at the external eavesdropper. Sufficient conditions for the uniqueness of the NE were derived. We also proposed a robust version of our game when the eavesdropping

[9] The insights can be generalized to the cases to larger number of links.

[10] We omit proving the convergence of asynchronous method (as a generalization of Jacobi method in the sense of [12]) due to page limitations even though we saw its convergence in our simulations.



(a) (b) (c)

Figure 1: (a) Probability of convergence for full-ECSI and robust version, (b) Comparison of secrecy sum- rate, (c) Comparison of information/leaked rate ($\mathtt{X}_e$= $\mathtt{Y}_e$= 5, $N_q = 8, M_q = L = 5, \forall q, Q = 4$).

channels are unknown. Simulation showed that contrary to intuition, the robust game achieves higher secrecy sum-rate compared to the game with full-ECS, which is mainly due to less restriction in managing multi-user interference for the robust approach. The extension of this framework to the case where MMSE receivers are employed instead of MRC could be an interesting subject of future research.

ACKNOWLEDGEMENTS

This research was supported in part by NSF (grants 1409172 and CNS-1513649), the Army research Office (grant W911NF-13-1-0302), the Qatar National Research Fund (grant NPRP 8-052-2-029), and the 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, QNRF, or ARC.

APPENDIX A
PROOF OF THEOREM 1

Using [14, Proposition 6.1], the fixed point iteration in (30) converges to a point ϕ^* from any initial point iff $\rho(\mathbf{A}+\mathbf{B}) < 1$. We now introduce the following theorem

Theorem 2 (14)**.** *For any square matrix* $\mathbf{M}$ *any* $\epsilon > 0$*, there exists an induced norm,* $||\bullet||$ *such that* $\rho(\mathbf{M}) \leq ||\mathbf{M}|| \leq \rho(\mathbf{M}) + \epsilon$.

Using the above theorem, since $\rho(\mathbf{A}+\mathbf{B}) < 1$, we can choose $\epsilon > 0$ such that $\rho(\mathbf{A}+\mathbf{B})+\epsilon < 1$. Hence, we can find a an induced norm $||\mathbf{A}+\mathbf{B}||$ such that $||\mathbf{A}+\mathbf{B}|| \leq \rho(\mathbf{A}+\mathbf{B})+\epsilon$. So far, we were able to convert the condition $\rho(\mathbf{A}+\mathbf{B})$ to an equivalent condition based on an induced norm, i.e., $||\mathbf{A}+\mathbf{B}||$. We use this result later during this proof. To proceed with further analysis, we need the following definition:

Definition 1 (14)**.** *Consider the following iteration:*

$$\Phi(t+1) = \mathcal{T}\left(\Phi(t)\right), \ k = 1, 2, ..., \tag{45}$$

where $\mathcal{T}$ *is a mapping from a subset* $\mathbb{A}$ *of* $\mathbb{R}$ *to itself, and* t *indicates the index of iterations. If* $\mathcal{T}$ *is continuous and*

$$||\mathcal{T}(\Phi^{(1)}) - \mathcal{T}(\Phi^{(2)})|| \leq \Omega||\Phi^{(1)} - \Phi^{(2)}|| \ , \ \forall(\Phi^{(1)}, \Phi^{(2)}) \in \mathcal{A}^2, \tag{46}$$

where $||.||$ *is a norm in* $\mathcal{A}$ *and* $\Omega \in [0, 1)$*, then the mapping* $\mathcal{T}$ *is a contraction mapping with* Ω *as the contraction modulus, and sequence* $\{\phi(t)\}$ *generated by the iterations in* (45) *converges to the fixed point* ϕ^*.

Using this definition and the result of Theorem 2, we can show the iteration in (30) as a contraction mapping, i.e.,

$$||\mathcal{T}(\phi^{(1)}) - \mathcal{T}(\phi^{(2)})|| \leq ||(\mathbf{A}+\mathbf{B})(\phi^{(1)} - \phi^{(2)})|| \tag{47}$$

$$\leq ||\mathbf{A}+\mathbf{B}||\ ||\phi^{(1)} - \phi^{(2)}|| \tag{48}$$

where $||\mathbf{A}+\mathbf{B}|| < 1$, (48) is due to Cauchy-Schwartz inequality, and the induced norm $||\bullet||$ is chosen such that for some $\epsilon > 0$, we have $||\mathbf{A}+\mathbf{B}|| \leq \rho(\mathbf{A}+\mathbf{B}) + \epsilon < 1$ (c.f. Theorem 2). This result will be used later in this proof.

We now focus on $\min\{\bullet\}$ and $\max\{\bullet\}$ functions. The operator $\max\{\min\{\phi_0, 1\}, 0\}$, for some $\phi_0 > 0$, can be equivalently shown as a Euclidean projection. Specifically, the Euclidean projection of a scalar ϕ_0, denoted as $[\phi_0]^+$, can be written as the following optimization problem

$$\begin{aligned} \underset{\bar{\phi}}{\text{minimize}} \ \ & ||\bar{\phi} - \phi_0||^2 \\ \text{s.t.} \ \ & 0 \leq \bar{\phi} \leq 1. \end{aligned} \tag{49}$$

The KKT conditions of this problem are written as follows:

$$\bar{\phi} - \phi_0 - \nu + \lambda = 0, \tag{50}$$

$$\nu \geq 0, \bar{\phi} \geq 0, \nu\phi = 0 \tag{51}$$

$$\lambda \geq 0, \bar{\phi} \leq 1, \lambda(\phi - 1) = 0; \tag{52}$$

If $\nu \geq 0$, then $\bar{\phi} = 0$. Hence, $\lambda = 0$ and we have $\nu = -\phi_0$, or equivalently $\phi_0 \leq 0$. If $\lambda > 0$, then $\bar{\phi} = 1$. Hence, $\nu = 0$, and we have $1 + \lambda = \phi_0$, or equivalently $\phi_0 \geq 1$. If $\lambda = 0$ and $\nu = 0$, the $0 \leq \bar{\phi} \leq 1$. Hence, $\bar{\phi} = \phi_0$. Summarizing these conditions, we have

$$\bar{\phi}^* = \underset{0\leq\bar{\phi}\leq 1}{\text{argmax}} ||\bar{\phi} - \phi_0||^2 = \begin{cases} 0, & \text{if } \phi_0 \leq 0, \\ 1, & \text{if } \phi_0 \geq 1, \\ \phi_0, & \text{if } 0 \leq \phi_0 \leq 1. \end{cases} \tag{53}$$

The right hand side of (53) is exactly the definition of the operator $\max\{\min\{\bullet, 1\}, 0\}$.

Converting $\max\{\min\{\bullet, 1\}, 0\}$ to Euclidean projection, we use the non-expansive property of Euclidean projection which is as follows [14, Ch. 3, Proposition 3.2]:

$$\left|\left|\left[\mathcal{T}(\phi^{(1)})\right]^+ - \left[\mathcal{T}(\phi^{(2)})\right]^+\right|\right| \leq \left|\left|\mathcal{T}(\phi^{(1)}) - \mathcal{T}(\phi^{(2)})\right|\right| \tag{54}$$

The non-expansive property of Euclidean projectors can be generalized to all vector norms because all vector norms (i.e., norms in $\mathbb{R}^n$) are equivalent, i.e., for any two different norm $||\bullet||^1$ and $||\bullet||^2$ $\exists$ ϕ_1 and ϕ_2 such that $\phi_1||\mathbf{x}||^1 \leq ||\mathbf{x}||^2 \leq \phi_2||\mathbf{x}||^1$, $\forall \mathbf{x} \in \mathbb{R}^n$[16]. Hence,

we have the following chain of inequalities

$$\left|\left|\left[\mathcal{T}(\phi^{(1)})\right]^{+}-\left[\mathcal{T}(\phi^{(2)})\right]^{+}\right|\right| \leq \left|\left|\mathcal{T}(\phi^{(1)})-\mathcal{T}(\phi^{(2)})\right|\right| \quad (55)$$

$$\leq ||(\mathbf{A}+\mathbf{B})(\phi^{(1)}-\phi^{(2)})|| \leq ||\mathbf{A}+\mathbf{B}||\ ||\phi^{(1)}-\phi^{(2)}|| \quad (56)$$

Hence,

$$\left|\left|\left[\mathcal{T}(\phi^{(1)})\right]^{+}-\left[\mathcal{T}(\phi^{(2)})\right]^{+}\right|\right| \leq ||\mathbf{A}+\mathbf{B}||\ \ \left|\left|\phi^{(1)}-\phi^{(2)}\right|\right|. \quad (57)$$

Setting the norm in (57) as the same norm in (48), the best response of each player is a contraction map, and thus has a unique fixed point (NE).

REFERENCES

[1] 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.

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

[3] 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.

[4] D. Bharadia and S. Katti, "Full duplex MIMO radios," in *Proceedings of the 11th USENIX NSDI Conf.*, 2014, pp. 359–372.

[5] Z. Zhang, K. Teh, and K. Li, "Distributed optimization for resilient transmission of confidential information in interference channels," *IEEE Trans. Veh. Technol.*, 2016.

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

[7] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[8] 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.

[9] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, "Large system analysis of artificial noise assisted communication in the multiuser downlink: Ergodic secrecy sum-rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, 2015.

[10] D. A. Schmidt, C. Shi, R. A. Berry, M. L. Honig, and W. Utschick, "Comparison of distributed beamforming algorithms for MIMO interference networks," *IEEE Trans. Signal Process.*, vol. 61, no. 13, pp. 3476–3489, 2013.

[11] T. Basar and G. J. Olsder, Eds., *Dynamic noncooperative game theory*. San Diego, CA, USA: Academic Press, 1995.

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

[13] R. A. Horn and C. R. Johnson, Eds., *Matrix Analysis*. New York, NY, USA: Cambridge University Press, 1986.

[14] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, pp. 666–672, May 1998.