

# Joint Transmitter- and Receiver-based Friendly Jamming in a MIMO Wiretap Interference Network

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 to 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, the use of artificial noise (or friendly jamming) is shown to be the closest to a practical implementation. In this method (proposed in [1]), 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 [2]. Note that the latest attempt in realizing full-duplex radios [3] 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 [4] and [5] 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 [6] and [7] focused only on the single-link scenario, making their approaches not extendable to the case of multiple links. Furthermore, the authors in [8] 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 ( $Q \geq 2$ ), Alice<sub>1</sub>, ..., Alice<sub>Q</sub> that communicate with their respective receivers, Bob<sub>1</sub>, ..., Bob<sub>Q</sub>. Alice<sub>q</sub>,  $q = 1, \dots, Q$ , has  $N_q$  transmit antennas, and Bob<sub>q</sub>,  $q = 1, \dots, Q$ , has  $M_q$  antennas. A passive Eve with  $L$  antennas also exists in the range of legitimate links' communications. The received signal at Bob<sub>q</sub>,  $\mathbf{y}_q$  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  $\tilde{\mathbf{H}}_{rq} \in \mathbb{C}^{M_q \times N_r}$ ,  $r = 1, \dots, Q$ , is the  $M_q \times N_r$  complex channel matrix between Alice<sub>r</sub> and Bob<sub>q</sub>,  $\mathbf{u}_q \in \mathbb{C}^{N_q}$  is the transmitted signal from Alice<sub>q</sub>.  $\tau_q \in \mathbb{R}^+$  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<sub>q</sub> due to the imperfect SIS at Bob<sub>q</sub>.  $\mathbf{m}_q \in \mathbb{C}^{M_q}$  is the RxFJ signal created by Bob<sub>q</sub>, 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<sub>q</sub> 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<sub>r</sub> to Bob<sub>q</sub> because the jamming signals created by other Bobs interfere with Bob<sub>q</sub>'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<sub>r</sub> and Bob<sub>q</sub> in meters and  $\eta$  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<sub>r</sub> to Bob<sub>q</sub>. The received signal by Eve is

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

where  $\tilde{\mathbf{G}}_q \in \mathbb{C}^{L \times N_q}$ ,  $q = 1, \dots, Q$  denotes the complex channel matrix between Alice<sub>q</sub> and Eve, and  $\tilde{\mathbf{G}}_q = \mathbf{G}_q d_{qe}^{-\eta/2}$  where  $\mathbf{G}_q \in \mathbb{C}^{L \times N_q}$  and  $d_{qe}$  is the distance between Alice<sub>q</sub> and Eve;  $\mathbf{G}'_q \in \mathbb{C}^{L \times M_q}$ ,  $q = 1, \dots, Q$ , is the channel between Bob<sub>q</sub> 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<sub>q</sub> 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 [9], 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  $x_q$  is distributed as a ZMCSCG random variable (i.e., Gaussian codebook) with  $E[x_q x_q^\dagger] = \phi_q P_q$  where  $P_q$  is the total transmit power of Alice<sub>q</sub> 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<sub>q</sub> knows the channel  $\tilde{\mathbf{H}}_{qq}$ . The precoder  $\mathbf{T}_q$  is set to  $\mathbf{T}_q = \mathbf{V}_q^{(1)}$ , where  $\mathbf{V}_q^{(1)}$  is the first column of  $\mathbf{V}_q$ , to set up transmit beamforming. Let  $\mathbf{H}_{qq} \triangleq \tilde{\mathbf{H}}_{qq} \mathbf{V}_q^{(1)}$ ,  $\mathbf{H}_{jq} \triangleq \tilde{\mathbf{H}}_{jq} \mathbf{V}_q^{(2)}$ ,  $\mathbf{H}_{qr} \triangleq \tilde{\mathbf{H}}_{qr} \mathbf{V}_q^{(1)}$ ,  $\mathbf{H}_{jqr} \triangleq \tilde{\mathbf{H}}_{jqr} \mathbf{V}_q^{(2)}$ ,  $\mathbf{G}_q \triangleq \bar{\mathbf{G}}_q \mathbf{V}_q^{(1)}$ ,  $\mathbf{G}_{jq} \triangleq \bar{\mathbf{G}}_{jq} \mathbf{V}_q^{(2)}$ . The terms  $\mathbf{G}_q$  and  $\mathbf{G}_{jq}$  denote the eavesdropping channel components. Hence,

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

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

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

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

Hence, the information rate for the  $q$ th link can be written as

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

where

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

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

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

$$\hat{\mathbf{z}}_q = \mathbf{r}_q^\dagger (\mathbf{G}_q x_q + \mathbf{G}_{jq} \mathbf{v}_q + \mathbf{G}'_q \mathbf{m}_q + \sum_{r=1, r \neq q}^Q (\mathbf{G}_r x_r + \mathbf{G}_{jr} \mathbf{v}_r + \mathbf{G}'_r \mathbf{m}_r) + \mathbf{e}). \quad (4)$$

Thus, the rate at Eve while eavesdropping on Alice<sub>q</sub> (i.e., leaked rate of Alice<sub>q</sub>) is

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

where

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

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

Finally, the secrecy rate of Alice<sub>q</sub> can be written as

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

The linear receivers  $\mathbf{d}_q$  and  $\mathbf{r}_q$ ,  $q = 1, \dots, Q$ , 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  $q$ th link,  $\mathbf{r}_q = \mathbf{L}_q^{(1)}$  where  $\mathbf{L}_q^{(1)}$  is the first

column of matrix  $\mathbf{L}_q$ .

### 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

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

Due to the non-concavity of the objective function in (8) w.r.t. decision variables, the optimization in (8) is non-convex. 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 the knowledge of interference at Eve. The secrecy maximization w.r.t. only  $p'_q$  can be written as

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

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:

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

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

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

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

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

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

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

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

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  $q$ th 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

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

Simplifying this inequality, we end up with the following

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

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

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

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

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

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  $(1 - \phi_q) P_q$ . 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  $C_q^{\text{sec}}$  is a monotonically increasing function of  $P_q$  and  $\phi_q$ , respectively.*

*Proof:* See [10]. ■

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 term  $c_q$ :

$$\begin{cases} c_q = a_q + (b_q - d_q) P'_q + \delta, & \text{if } b_q < d_q, \\ c_q = a_q + \delta, & \text{if } b_q > d_q. \end{cases} \quad (18)$$

The following property shows the sufficiency of (18) for concluding (17).

**Lemma 2.** *Provided that  $(b_q - d_q) P'_q + \delta < 0$  and  $\delta > 0$ , the condition in (18) is sufficient for satisfying (17).*

*Proof:* See [10]. ■

Using Lemma 2, one can conclude that in calculating the value of RxFJ in (18), 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

$$\tau_q < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_q|^2}. \quad (19)$$

The assumption  $(b_q - d_q)P'_q + \delta < 0$  sets an upper bound on  $\delta$ , 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  $b_q > d_q$ . In the next section, we use the derived conditions to model a power control game.

#### IV. GAME FORMULATION

The condition in (18) can be written in general form as

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

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

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

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

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

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

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

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

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

Notice that in establishing (25), the value of  $c_q$  (or equivalently power of TxFJ) is already set according to (18). Hence, in (25), only those  $\phi_q$ 's that exist in the numerators of  $C_q$  and  $C_{eq}$  are treated as variables. The condition in (18) guarantees the secrecy rate being a monotonically increasing function of  $\phi_q$  (cf. Lemma 1). Hence, the best-response of the  $q$ th link,  $q = 1, \dots, Q$ , is when  $\phi_q$  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]. 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 (18),  $C_q^{sec}$  becomes concave w.r.t  $\phi_q$ . Specifically,

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

which is always negative indicating that  $C_q^{sec}$  is concave w.r.t.  $\phi_q$ . 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  $q = 1, \dots, Q$  has a unique NE iff the following condition is satisfied:*

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

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

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

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

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

*Proof:* See [10].  $\blacksquare$

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  $\|\bullet\|$  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

$$\|\mathbf{A} + \mathbf{B}\|_\infty = \max_q \sum_{r=1}^Q \frac{P_r}{P_q} |A_{q,r} - B_{q,r}| < 1. \quad (30)$$

In other words, every player should check whether

$$\begin{aligned} & \frac{N_q - 1}{N_r - 1} \left( \sum_{r=1}^Q \left| \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 ((N_r - 1) |\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{jr}|^2)}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} \right. \right. \\ & \left. \left. - \sum_{r=1}^Q \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 ((N_r - 1) |\mathbf{r}_q^\dagger \mathbf{G}_r|^2 - |\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2)}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} \right) \right) < 1, \quad \forall q. \end{aligned} \quad (31)$$

The physical intuition drawn from the condition in (30) is not straightforward. However, we see in the next section that the robust approach introduces simpler and more applicable physical interpretations to predict a unique 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

$$(1 - \phi_q)P_q > \psi_q + p'_q E_q \quad (32)$$

where

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

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

Therefore, for a given probability value  $\varepsilon$ , the  $q$ th link needs to make sure that the following inequality is satisfied:

$$\Pr\{(1 - \phi_q)P_q > \psi_q + p'_q E_q\} \geq \varepsilon. \quad (33)$$

Using (18) and the Bayes law of total probability we have

$$\begin{aligned} \Pr\{(1 - \phi_q)P_q > \psi_q + p'_q E_q\} = & \quad (34) \\ \Pr\{b_q < d_q\}(1 - \Pr\{(1 - \phi_q)P_q \leq \psi_q + P'_q E_q\}) + & \\ \Pr\{b_q > d_q\}(1 - \Pr\{(1 - \phi_q)P_q \leq \psi_q\}). & \end{aligned}$$

Using Markov inequality in (34), the following holds

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

$$\Pr\{b_q < d_q\}(1 - \frac{E[\psi_q + P'_q E_q]}{(1 - \phi_q)P_q}) + \Pr\{b_q > d_q\}(1 - \frac{E[\psi_q]}{(1 - \phi_q)P_q}). \quad (36)$$

Simplifying this inequality, we end up with

$$\begin{aligned} \phi_q \leq \max\{\min\{ & \quad (37) \\ 1 - \Pr\{b_q < d_q\} \frac{E[\psi_q + P'_q E_q]}{(1 - \varepsilon)P_q} - \Pr\{b_q > d_q\} \frac{E[\psi_q]}{(1 - \varepsilon)P_q}, 1\}, 0\}. & \quad (38) \end{aligned}$$

The details of deriving  $E[\psi_q]$  and  $P(b_q < d_q)$  are given in [10], thus skipped here for brevity. It turns out that [10]

$$\Pr\{b_q < d_q\} = 1 - \frac{1}{1 + \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}}. \quad (39)$$

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

$$E[A_{q,r}] = \frac{N_q - 1}{(N_r - 1)(N_q - 3)} \frac{(N_r - 1)|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{jr}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}, \quad (40a)$$

$$E[B_{q,r}] = 0, \quad (40b)$$

$$E[C_{q,r}] = \frac{N_q - 1}{(N_r - 1)(N_q - 3)} \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{jr}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \frac{N_q - 1}{(N_q - 3)} \frac{d_{re}^{(-n)}}{d_{qe}^{(-n)}}, \quad (40c)$$

$$E[D_{q,r}] = \frac{N_q - 1}{(N_q - 3)} \left( \frac{|\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \frac{d_{re}^{(-n)}}{d_{qe}^{(-n)}} \right), \quad (40d)$$

$$E[E_q] = \frac{N_q - 1}{N_q - 3} \frac{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}. \quad (40e)$$

We choose to use RxFJ whenever  $\Pr\{b_q > d_q\} > 0.5$ . With the derivations in (37) and (40), we can construct a game with the same structure as in section IV where each link's best response is calculated from (37), and the following must hold to ensure a unique NE:

$$\rho \left( \frac{1}{1 - \varepsilon} E[\mathbf{A}] \right) < 1, \quad (41)$$

where  $\mathbf{A}$  is defined in (28) and the expectation is element-wise. An alternative condition to (41) is to replace the spectral radius with infinity norm according to (30). Notice that the absence of  $\mathbf{B}$  (defined in (29)) in (41) provides less restrictive NE uniqueness conditions, as we expect that by placing the legitimate links far enough from each other, 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  $\delta$  according to (18) (cf. Section III).

- 1: **for**  $n=1$  to maximum iteration **do**
  - 2:   **repeat**  $\forall (q) \in \{1, \dots, Q\}$  Calculate  $a_q, b_q, c_q,$  and  $d_q$  according to (3) and (6)
  - 3:    Set  $\phi_q$  equal to its upper bound according to (23) (full-ECSI version), or (37) (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. We consider a deterministic location for Eve denoted as  $(X_e, Y_e)$ . All Alices are randomly placed on the boundary of a circle, known as simulation region, with radius  $r_{\text{circ}}$  whose center is at the origin. Each Alice has a fixed distance (communication range) with her corresponding Bob denoted as  $d_{\text{link}}$ . Each Bob is placed randomly around his corresponding Alice on the boundary of a circle whose radius is set to  $d_{\text{link}}$  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  $d_{\text{link}} = 10$  m. Jacobi method is used in all simulations.

Fig. 1 (a) shows the variation of convergence probabilities of robust and full-ECSI method w.r.t  $r_{\text{circ}}$  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)), (31) (indicated by  $n_2$  in Fig. 1 (a)) and their equivalents for the robust version 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 that of full-ECSI scenario can be achieved. Moreover, in robust version, as  $\varepsilon$  becomes larger, the uniqueness conditions become more restrictive, which is in line with the derivation in (41).

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. 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  $r_{\text{circ}} > 10$ m. This advantage can be seen for both values of  $\varepsilon$ . 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 when it is known, contributing to more restrictive

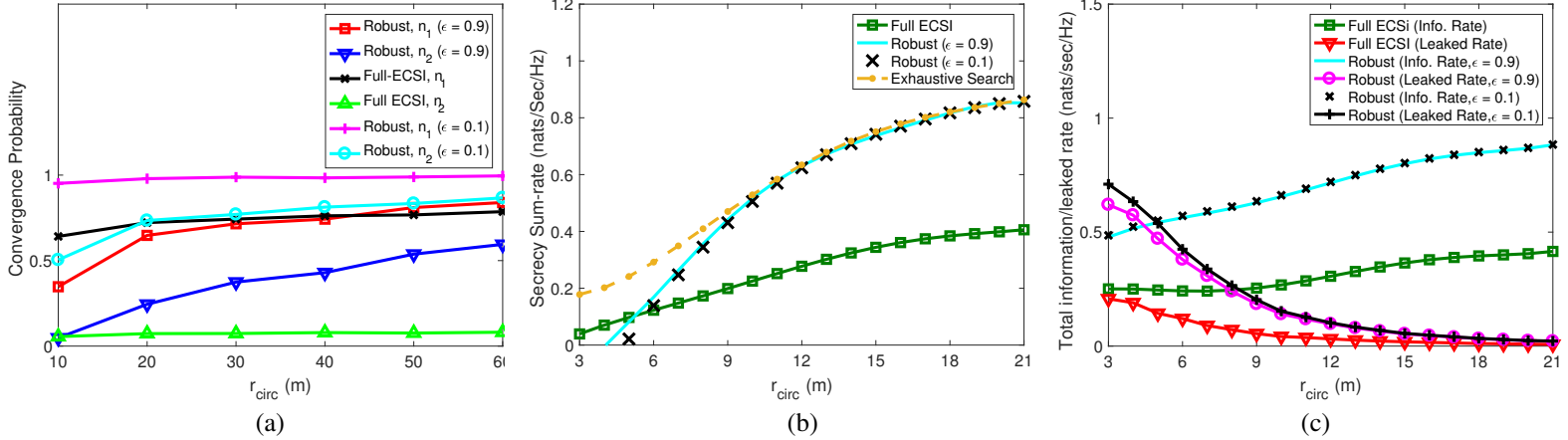


Figure 1: (a) Probability of convergence for full-ECSI and robust version, (b) Comparison of secrecy sum-rate, (c) Comparison of information/leaked rate ( $X_e = Y_e = 5$ ,  $N_q = 8$ ,  $M_q = L = 5$ ,  $\forall q$ ,  $Q = 4$ ).

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.

It can be seen in Fig. 1 (c) that even for low values of  $\epsilon$ , the performance of robust approach is still superior. We conjecture that this might be due to the fact the  $F$ -distribution, which was the distribution involved in best responses in (37) (see [10]), 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. Thus, to ensure that  $(1 - \phi_q) > \Pr\{b_q < d_q\} \frac{E[\psi_q + \tau_q P_q' E_q]}{1 - \epsilon} + \Pr\{b_q > d_q\} \frac{E[\psi_q]}{1 - \epsilon}$ , the density of the values above the mean is relatively low.

## 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 Rx-FJ and Tx-FJ 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 channels are unknown. Simulation showed that contrary to intuition, the robust game achieves higher secrecy sum-rate compared to the game with full-ECSI, 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.

## REFERENCES

- [1] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [2] 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.
- [3] D. Bharadia and S. Katti, "Full duplex MIMO radios," in *Proceedings of the 11th USENIX NSDI Conf.*, 2014, pp. 359–372.
- [4] Z. Zhang, K. Teh, and K. Li, "Distributed optimization for resilient transmission of confidential information in interference channels," *IEEE Trans. Veh. Technol.*, 2016.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] P. Siyari, M. Krunz, and D. N. Nguyen, "Secure communications in a MIMO wiretap interference channel with full-duplex receivers." [Online]. Available: [http://wireless.ece.arizona.edu/sites/default/files/icc17\\_peyman.pdf](http://wireless.ece.arizona.edu/sites/default/files/icc17_peyman.pdf)
- [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.