Secure Communications via Power Control in a MIMO Wiretap Interference Network with Jamming Transmitters and Receivers

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

Technical Report
TR-UA-ECE-2018-1
Last Update: Feb. 6, 2018

Abstract

We study secure and distributed power control in a multi-link interference network that is tapped by an external eavesdropper. To conceal information from the eavesdropper, legitimate links are equipped with both *transmit-based friendly jamming* (TxFJ) and *receiver-based friendly jamming* (RxFJ). Each transmitter-receiver (Tx-Rx) pair seeks to maximize its secrecy rate by determining the best power assignment (PA) for the information, TxFJ, and RxFJ signals. The joint optimization of these parameters is a non-convex problem, thus computationally demanding. Hence, each link should seek for suboptimal solutions. To do so, we aim to provide positive secrecy for each link. Despite its suboptimality, such an approach precludes the possibility of employing a strong multiuser detector by the eavesdropper (such as successive interference cancellation). We show that a careful assignment of TxFJ and RxFJ powers of a link can provide it with a positive secrecy rate. The TxFJ PA at a link is done with respect to the observed interference at the corresponding Rx, whereas the RxFJ of that link is adjusted using an on-off PA that depends only on the link's local channel state information (CSI). Hence, the RxFJ adjustment is unaffected by interference fluctuations at the eavesdropper, which facilitates our distributed design. With every link following such a strategy, we model this interaction as a non-cooperative game. Assuming knowledge of eavesdropper's CSI (E-CSI), we derive sufficient conditions for the uniqueness of the resulting Nash equilibrium. We then propose an algorithm to implement the PA game. Lastly, we relax knowledge of E-CSI and propose a framework that is robust to unknown E-CSI at links.

An abridged version of this paper was presented at the IEEE ICC 2017, Workshop on Full-duplex Communications for Future Wireless Networks, May 2017 [1].

Index Terms

Interference network, friendly jamming, full-duplex radios, game theory, distributed design

I. Introduction

Physical-layer (PHY-layer) security has recently gained considerable attention because of its potential to provide secrecy at low computational overhead. This makes such an approach particularly suitable for applications where it is either expensive or computationally demanding to use cryptographic methods. The most common scenario for information-theoretic PHY-layer security is the so-called *wiretap channel*. The wiretap channel involves communications between a legitimate transmitter (Alice) and a corresponding receiver (Bob); such communications is to be secured from an eavesdropper (Eve).

Among proposed methods for PHY-layer security, artificial noise (or friendly jamming) has been noticeably the subject of many research efforts. According to this method [2], Alice can use multiple antennas and a portion of her transmit power to create a bogus signal –known as *artificial noise* or *transmit-based friendly jamming* (TxFJ)– alongside the information signal to confuse a nearby Eve. Assuming that Alice knows Alice-Bob channel, she creates TxFJ via precoding techniques such that the precoded TxFJ signal falls in the null-space of Alice-Bob channel, hence not affecting Bob's reception. Alongside the TxFJ method, secrecy can also be provided with the help of another node (e.g., a relay) that is dedicated to generate friendly jamming (FJ) signals [2]. Such a method is usually referred to as *cooperative jamming (CJ)*[1]. Thus, the secrecy of a legitimate transmission can be further improved by using CJ in addition to the TxFJ. Despite having the same effect as the TxFJ method, the CJ approaches face several implementation issues compared to the TxFJ method such as mobility, trustworthiness and synchronization.

To address this situation, it has been suggested in [3] to equip Bob with in-band full-duplex (FD) capabilities, allowing him to generate his own friendly jamming signal while receiving the information signal from Alice. Such an FJ signal is hereafter referred to as Rx-based friendly jamming (RxFJ) [3]. Another example of using RxFJ is [4], where the authors proposed an optimal power allocation framework to maximize the secrecy rate of a link that is tapped by a single-/multiple-antenna Eve under different configurations (e.g., deterministic/statistical knowledge of channel between Alice and Eve, multi-antenna Bob/Eve with fixed/optimal receiver). Other works consider PHY-layer security when FD capability is used at both Alice and Bob for bidirectional communications, i.e., Bob transmits information signals to Alice rather than generating RxFJ (see [5] and its references). Our focus in this paper is the case where Bob is used to generate RxFJ.

[1] Same as TxFJ, the FJ signals emitted from the helper node in CJ do not affect Bob's reception.

While the single-link scenario is of great importance in developing early observations, secrecy analysis for multi-link settings introduces new challenges not present in the single-link scenario. The definition of secrecy in multi-link settings depends on the specific network under consideration. For instance, links might be interested in transmissions of their neighboring links. Thus, the design must ensure that a given link's transmission is secured from other links. Such a network is referred to as *multi-link channel with confidential messages*. Another possibility is when external Eves exist in the network and the transmissions of legitimate links must be kept secure from these Eves. Such a network is referred to as *multi-link wiretap channel*.

In this paper, we study PHY-layer security in a multi-link wiretap channel. In our network model, legitimate links share the same bandwidth for their transmissions, thus interfering with one another; at the same time, an eavesdropper snoops on ongoing communications, hence the name *wiretap interference channel*. Legitimate links are capable of TxFJ and RxFJ. Our design parameters are the power of RxFJ, and the power assignment (PA) between the information and TxFJ signals. Our work is motivated by the following simple observation: For a given link, when no secrecy is required, the higher the Alice's power budget the higher the information rate at the respective Rx. However, when secrecy is also a requirement, although the information rate still increases monotonically with the power at Alice, the secrecy rate may not be necessarily so because more power transmitted from Alice also increases the leakage rate at Eve.

Our first objective is to find a setting under which the secrecy rate of a link increases monotonically with Alice's power. We find a lower bound on the power allocated to TxFJ above which positive secrecy is achievable for a given link. Once positive secrecy is achieved, the secrecy rate becomes a monotonically increasing function of power at Alice, thus having the same trend as the information rate. Therefore, the rest of Alice's power is allocated to the information signal. Clearly, having a larger power at Alice leads to larger secrecy rates. Although guaranteeing positive secrecy does not offer any sort of optimality in terms of individual or network-wide secrecy, it ensures that no link experiences zero secrecy. On the contrary, when the aim is to maximize the sum of secrecy rates, the issue of having zero secrecy at some links may arise [6]. In fact, by maximizing the sum of secrecy rates, we cannot ensure that every link achieves a non-zero secrecy rate. A zero secrecy scenario can be exploited by Eve, who can perform sophisticated multiuser detection techniques (e.g., successive interference cancellation or SIC) to decode ongoing communications. Such an issue was reported in [7], and it was shown in [8] that an SIC-capable Eve can significantly decrease the network secrecy if some links experience zero secrecy rates. Provided that all links have non-zero secrecy rates, Eve cannot apply SIC[2].

In our framework, the lower bound on the TxFJ power of an Alice (which guarantees positive secrecy) depends on the measured interference at her corresponding Bob. As for the RxFJ power, though its setting generally depends on multiuser interference (MUI), we show that to preserve positive secrecy, it is sufficient for each Bob to set RxFJ based on only his local channels (i.e., Alice-Bob and Bob-Eve channels). This result offers a great simplification to our distributed design, as Bobs do not require to adjust RxFJ w.r.t. MUI which is often varying in time.

We assume that when setting their transmission parameters, there is no centralized authority responsible for computations and optimization. Hence, links have to make decisions in a distributed fashion. Such a design inevitably produces interference at several links. However, because Eve also receives interference from all links, a careful design ensures that interference at legitimate links is properly managed while interference at Eve is kept high as much as possible. We model such an interaction between legitimate links using the theory of non-cooperative games. In our proposed game, legitimate links are the players, the utility of each link (player) is its secrecy rate, and the strategy of each player is to decide on his own RxFJ power as well as the PA between the information and TxFJ signals.

The works in [9], [10] studied secure precoding in wiretap interference networks. Moreover, the authors in [11] studied power control in a multi-channel interference network without considering TxFJ and RxFJ. All of these works assumed full knowledge of the eavesdropper's channel state information (E-CSI) at each Alice, which may not be a practical assumption. In addition, to the best of our knowledge the solutions proposed in those works are not extendable to cover the case of unknown E-CSI. Regarding the PA between the information and TxFJ signals, the works in [12] and [13] focused only on a single-link scenario, and their approaches are not extendable to the case of multiple links. The work in [14] studied power minimization for the information, TxFJ and RxFJ signals in a broadcast channel with confidential messages under given guarantees on the individual secrecy rate for each Bob. The authors of [15] used full-duplex capability in the base station of a broadcast/multiple-access wiretap channel to secure multiple half-duplex downlink and uplink users by generating RxFJ/TxFJ for uplink/downlink communications. They proposed a multi-objective optimization framework to find the best trade-off in minimizing downlink and uplink powers used at the base station, subject to given constraints on information and secrecy rates of downlink and uplink users. In our paper, we investigate a more challenging scenario (i.e., interference channel) where contrary to broadcast channels, distributed computation and

[2] A full description of the effect of a zero secrecy rate on the secrecy of an interference network was given in [8], where we showed that Eve can cancel the interference coming from links with zero secrecy rates, thus increasing the SINR while snooping on other transmissions with non-zero secrecy rates.

limited coordinations are required. Overall, our contributions can be summarized as follows:

- Using TxFJ and RxFJ, we define a lower bound on the power allocated to the TxFJ that guarantees positive secrecy of transmissions at each given link.
- We propose a non-cooperative game to model the power control problem in the interference network under our study. Under the assumption that Alice-/Bob-Eve channels are fully known, we derive sufficient conditions under which the proposed non-cooperative game has a unique Nash equilibrium (NE).
- We propose alternative sufficient conditions for the uniqueness of the NE. Such conditions allow for predicting the existence of a unique NE in distributed fashion.
- We show that our distributed design can be implemented using an asynchronous update algorithm. This algorithm is robust to transmission delays over various links.
- Lastly, we relax the assumption of full knowledge of E-CSI at each Alice and propose a version of our algorithm that is robust to uncertainties in knowledge of E-CSI.

We need to emphasize that in this paper, we first examine our proposed distributed design under full knowledge of E-CSI. Although availability of E-CSI at all links is not a practical assumption, we can build foundations for our distributed algorithm to easily introduce important performance metrics, such as convergence conditions/speed of our algorithm. Once, our analysis is complete, we relax knowledge of E-CSI and propose the version of our algorithm that is robust to uncertainties on E-CSI knowledge.

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

II. System Model

We first describe a model for the network under consideration and introduce the main performance metrics. Consider Q transmitters ($Q \geq 2$), Alice$_1$, $\ldots$, Alice$_Q$ that communicate with their respective receivers, Bob$_1$, $\ldots$, Bob$_Q$. Let $\mathcal{Q} \triangleq \{1, 2, \ldots, Q\}$. Alice$_q$, $q \in \mathcal{Q}$, has N_q transmit antennas, and Bob$_q$ has M_q antennas. A passive Eve with L antennas is also present in the communication range[3]. The received signal at Bob$_q$ is

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

where $\tilde{\mathbf{H}}_{rq} \in \mathbb{C}^{M_q \times N_r}$, $r \in \mathcal{Q}$, is the M_q-by-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 self-interference-suppression (SIS) factor and the self interference channel at Bob$_q$ due to the imperfect SIS at Bob$_q$[4]. Such a model for self-interference was used in several recent works (see [15], [17]), and practical implementations of it exist in the literature (see e.g., [18])[5]. $\mathbf{m}_q \in \mathbb{C}^{M_q}$ is the RxFJ signal created by Bob$_q$, which is a zero mean circularly symmetric complex Gaussian random variable (ZMCSCG-RV) with variance $E[\mathbf{m}_q\mathbf{m}_q^\dagger] = p'_q\mathbf{I}$ where $\text{Tr}(\mathbf{m}_q\mathbf{m}_q^\dagger) = M_q p'_q \leq P'_q$ with P'_q denoting the total power of Bob$_q$ to be used for RxFJ. $H'_{rq} \in \mathbb{C}^{M_q \times M_r}$, $r \neq q$, is the channel from Bob$_r$ to Bob$_q$ because the RxFJ created by other Bobs interfere with Bob$_q$'s reception. $\mathbf{n}_q \in \mathbb{C}^{M_q}$ is the complex additive white Gaussian noise (AWGN) whose covariance matrix is $E[\mathbf{n}_q\mathbf{n}_q^\dagger] = N_0\mathbf{I}$ with $N_0 \in \mathbb{R}^+$. 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 at Eve is

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

where $\tilde{\mathbf{G}}_q \in \mathbb{C}^{L \times N_q}$, $q \in \mathcal{Q}$ denotes the complex channel matrix between Alice$_q$ and Eve. Let $\tilde{\mathbf{G}}_q = \bar{\mathbf{G}}_q d_{qe}^{-\eta/2}$ where $\bar{\mathbf{G}}_q \in \mathbb{C}^{L \times N_q}$ and d_{qe} is the distance between Alice$_q$ and Eve. $\mathbf{G}'_q \in \mathbb{C}^{L \times M_q}$, $q \in \mathcal{Q}$, is the channel between Bob$_q$ and Eve, and $\mathbf{G}'_q = \bar{\mathbf{G}}'_q{d'}_{qe}^{-\eta/2}$ where $\bar{\mathbf{G}}'_q \in \mathbb{C}^{L \times M_q}$ and d'_{qe} is the distance from Bob$_q$ to Eve. 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 TxFJ $\mathbf{w}_q$. 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

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

[4] Recall that enabling in-band full-duplex communications requires suppression of the transmitted signal of the FD-enabled device at its receive chain to allow for simultaneous transmission and reception. However, such suppression may not be perfect, and there is often a residual self-interference captured at the receive chain [16].

[5] We assume that FD receivers are not experiencing dynamic range issues (as pointed out in [19]), which means that the SIS factor τ_q is a constant and independent of the transmit power of the FD device. Incorporating this assumption can be considered as a subject for future research.

$\mathbf{T}_q \in \mathbb{C}^{N_q}$ is the precoder and $x_q \in \mathbb{C}$ is the information signal. In fact, we use multiple transmit and receive antennas at each link to exploit the maximum diversity of the MIMO link, and not exploit the spatial multiplexing, i.e., multiple antennas are used for *beamforming*.

Assume that a Gaussian codebook is used for x_q, i.e., x_q is distributed as a ZMCSCG-RV 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, we write $\mathbf{w}_q \triangleq \mathbf{Z}_q \mathbf{v}_q$, where $\mathbf{Z}_q \in \mathbb{C}^{N_q \times (N_q-1)}$ is the precoder for the TxFJ signal and $\mathbf{v}_q \in \mathbb{C}^{(N_q-1)}$ is the TxFJ signal with i.i.d. ZMCSCG entries and $E[\mathbf{v}_q \mathbf{v}_q^\dagger] = \sigma_q \mathbf{I}$. The scalar value $\sigma_q = \frac{(1-\phi_q)P_q}{N_q-1}$ denotes the TxFJ power[6]. 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 in descending order, 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 $\mathbf{V}_q$ corresponding to the smallest singular values [2]. We assume that Alice$_q$ knows the channel $\tilde{\mathbf{H}}_{qq}$[7]. 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 $\mathbf{V}_q$ corresponding the largest singular value, to execute transmit beamforming [20]. 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 $\mathbf{G}_{j_q}$, $\forall q \in \mathcal{Q}$ denote the E-CSI components. Hence, (1) and (2) can be written as

$$\mathbf{y}_q = \mathbf{H}_{qq}x_q + \mathbf{H}_{j_{qq}}\mathbf{v}_q + \sqrt{\tau_q}\mathbf{H}'_{qq}\mathbf{m}_q + \sum_{\substack{r=1\\r\neq q}}^{Q}(\mathbf{H}_{rq}x_r + \mathbf{H}_{j_{rq}}\mathbf{v}_r + \mathbf{H}'_{rq}\mathbf{m}_r) + \mathbf{n}_q \tag{3a}$$

$$\mathbf{z} = \mathbf{G}_q x_q + \mathbf{G}_{j_q}\mathbf{v}_q + \mathbf{G}'_q\mathbf{m}_q + \sum_{\substack{r=1\\r\neq q}}^{Q}(\mathbf{G}_r x_r + \mathbf{G}_{j_r}\mathbf{v}_r + \mathbf{G}'_r\mathbf{m}_r) + \mathbf{e}. \tag{3b}$$

An illustration of the system model under study is given in Fig. 1 for a two-link network. It can be seen that the interference components at each Bob include his self-interference signal as well as information, TxFJ and RxFJ signals of unintended links. Eve also receives all information, TxFJ and RxFJ signals.

After receiving $\mathbf{y}_q$ at Bob$_q$, a linear receiver $\mathbf{d}_q \in \mathbb{C}^{M_q}$ is applied. Given that $\mathbf{d}_q^\dagger \mathbf{H}_{j_{qq}}\mathbf{v}_q = 0$[8],

[6] Notice that the TxFJ power is distributed uniformly between different dimensions of $\mathbf{v}_q$. In the case of full knowledge of E-CSI, such power division is not optimal. However, when no knowledge of E-CSI is available (which we assume later in this paper), it was shown that uniform division of TxFJ power between different dimensions of $\mathbf{v}_q$ is the optimal approach (see [2], [12]).

[7] Acquiring channel state information (CSI) between Alice$_q$ and its corresponding Bob$_q$ is assumed to be done securely. For example, a two-phase channel estimation can be performed, where in the first/second time-slot, Alice$_q$/Bob$_q$ sends the pilot signals to Bob$_q$/Alice$_q$. This way, we avoid having to send explicit CSI feedback from one communication end to another, thus lowering the probability of eavesdropping on channel estimates.

[8] Note that the choice of the linear receiver (to be discussed near the end of this section) affects this assumption. In this paper, we choose the linear receiver such that this assumption holds.

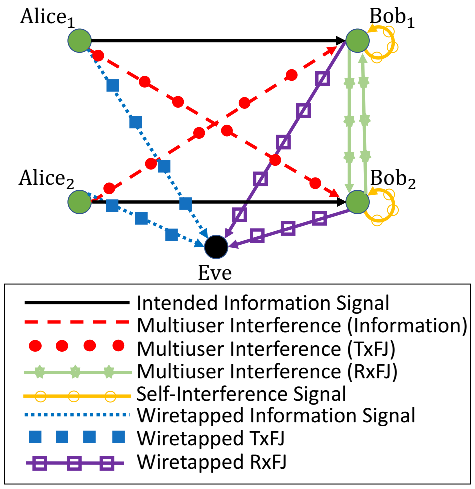

Alice$_1$
Bob$_1$
Alice$_2$
Bob$_2$
Eve
Intended Information Signal
Multiuser Interference (Information)
Multiuser Interference (TxFJ)
Multiuser Interference (RxFJ)
Self-Interference Signal
Wiretapped Information Signal
Wiretapped TxFJ
Wiretapped RxFJ

Fig. 1: System model.

the linear estimate of x_q at Bob$_q$ is

$$\hat{x}_q = \mathbf{d}_q^\dagger(\mathbf{H}_{qq}x_q + \sqrt{\tau_q}\mathbf{H}'_{qq}\mathbf{m}_q + \sum_{\substack{r=1 \\ r\neq q}}^{Q}(\mathbf{H}_{rq}x_r + \mathbf{H}_{jrq}\mathbf{v}_r + \mathbf{H}'_{rq}\mathbf{m}_r) + \mathbf{n}_q). \tag{4}$$

Hence, the information rate for the qth link can be written as[9]

$$C_q = \log(1 + \frac{\phi_q P_q}{a_q + b_q p'_q}) \tag{5}$$

where

$$a_q = \frac{\sum_{\substack{r=1 \\ r\neq q}}^{Q}\left(\left|\mathbf{d}_q^\dagger\mathbf{H}_{rq}\right|^2\phi_r P_r + \left|\mathbf{d}_q^\dagger\mathbf{H}_{jrq}\right|^2\sigma_r + |\mathbf{d}_q^\dagger\mathbf{H}'_{rq}|^2 p'_r\right) + N_0}{\left|\mathbf{d}_q^\dagger\mathbf{H}_{qq}\right|^2} \tag{6a}$$

$$b_q = \tau_q\frac{|\mathbf{d}_q^\dagger\mathbf{H}'_{qq}|^2}{|\mathbf{d}_q^\dagger\mathbf{H}_{qq}|^2}. \tag{6b}$$

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

$$\hat{z}_q = \mathbf{r}_q^\dagger(\mathbf{G}_q x_q + \mathbf{G}_{j_q}\mathbf{v}_q + \mathbf{G}'_q\mathbf{m}_q + \sum_{\substack{r=1 \\ r\neq q}}^{Q}(\mathbf{G}_r x_r + \mathbf{G}_{j_r}\mathbf{v}_r + \mathbf{G}'_r\mathbf{m}_r) + \mathbf{e}). \tag{7}$$

[9] Note that the distribution characteristics of the additive noise do not change after passing through the linear receiver [20].

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

$$C_{eq} = \log(1 + \frac{\phi_q P_q}{c_q + d_q p'_q}) \tag{8}$$

where

$$c_q = \frac{\left|\mathbf{r}_q^\dagger \mathbf{G}_{jq}\right| \sigma_q}{\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2} + \frac{\sum_{\substack{r=1\\ r\neq q}}^{Q} \left(\left|\mathbf{r}_q^\dagger \mathbf{G}_r\right|^2 \phi_r P_r + \left|\mathbf{r}_q^\dagger \mathbf{G}_{j_r}\right|^2 \sigma_r + |\mathbf{r}_q^\dagger \mathbf{G}'_r|^2 p'_r \right) + N_0}{\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2} \tag{9a}$$

$$d_q = \frac{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}. \tag{9b}$$

Finally, the secrecy rate of Alice$_q$ can be written as[10]

$$C_q^{sec} = \max\{C_q - C_{eq}, 0\}. \tag{10}$$

The linear receivers $\mathbf{d}_q$ and $\mathbf{r}_q$, $q \in \mathcal{Q}$, are assumed to be chosen according maximal ratio combining (MRC [20]) method to maximize the reception of signal at Bob$_q$ and Eve, respectively. Hence, $\mathbf{d}_q = \mathbf{U}_q^{(1)}$ where $\mathbf{U}_q^{(1)}$ is the first column of $\mathbf{U}_q$ (recall that $\tilde{\mathbf{H}}_{qq} = \mathbf{U}_q \mathbf{\Sigma_q} \mathbf{V}_q^\dagger$). Using this linear receiver, the TxFJ signal of Alice$_q$ will be nullified at Bob$_q$ as shown in the system model in Fig. 1 (i.e., $\mathbf{d}_q^\dagger \mathbf{H}_{j_q q} \mathbf{v}_q = 0$, $q \in \mathcal{Q}$, see (4)). 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 in descending order. Thus, while eavesdropping on qth link, Eve sets its linear receiver $\mathbf{r}_q = \mathbf{L}_q^{(1)}$ where $\mathbf{L}_q^{(1)}$ is the first column of matrix $\mathbf{L}_q$[11].

We need to emphasize that the choice of precoder (i.e., beamformers) for TxFJ signal in this paper is mainly driven by the fact that acquiring E-CSI knowledge may not be possible in the cases where eavesdropper is a passive node. For a single-link scenario, it was shown in [22] that optimizing the precoders of information and TxFJ signals requires complete knowledge of E-CSI. However, in this paper, the beamforming vector of TxFJ signal for each link depends only on the channel between the two nodes comprising that link, which is relatively more practical to achieve.

[10] Note that in specifying the secrecy rate of a link, because no link has the knowledge on whose transmission Eve is interested, all legitimate links protect their transmissions from Eve. Thus, the secrecy rate of each link can be determined by (10) (see [21]).

[11] Note that other decoders (such as MMSE [20]) can also be employed by Eve. This issue will be discussed later in the simulation section.

Our choice of beamforming vector of information signal for each link comes from the fact that the number of antennas at Eve may not be known in some cases. As pointed out in [2], the main limitation of the TxFJ method is that if Eve has more antennas than Alice, then Eve may be able to nullify the effect of TxFJ on itself by a specific choice of decoder (i.e., linear receiver) at its receive antennas. Looking at (7), the general form of the TxFJ signal from the Alice$_q$ received at Eve can be written as $\mathbf{r}_q^\dagger \mathbf{G}_{j_q} \mathbf{v}_q = \mathbf{r}_q^\dagger \tilde{\mathbf{G}}_q \mathbf{V}'_q \mathbf{v}_q$ where $\mathbf{V}'_q$ is the N rightmost columns of $\mathbf{V}_q$, $0 \leq N \leq N_q - 1$. Let $\tilde{\mathbf{G}}_q \mathbf{V}'_q = \mathbf{L}'_q \mathbf{D}'_q \mathbf{R}'_q$ be the SVD of the $L \times N$ matrix $\tilde{\mathbf{G}}_q \mathbf{V}'_q$, 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. If $L > N$, indicating that $\tilde{\mathbf{G}}_q \mathbf{V}'_q$ is a tall matrix, then Eve has more antennas than the total dimensions considered for the TxFJ signal of Alice$_q$. Hence, if Eve knows $\tilde{\mathbf{G}}_q \mathbf{V}'_q$, she can choose $\mathbf{r}_q$ to be the rightmost $L - N$ columns of the matrix $\mathbf{L}'_q$. This way, Eve can nullify the TxFJ signal, i.e., $\mathbf{r}_q^\dagger \tilde{\mathbf{G}}_q \mathbf{V}'_q \mathbf{v}_q = 0$. Therefore, with sufficiently high number of antennas, Eve can nullify the effect of TxFJ on herself. To prevent this, we need to make sure that $L - N \leq 0$, so $N \geq L$. To ensure that $N \geq L$, Alice$_q$ Tx uses as many dimensions for the TxFJ signal as possible. Hence, we set N to its maximum value, i.e., $N = N_q - 1$, meaning that $\mathbf{V}'_q$ is the $N_q - 1$ rightmost columns of $\mathbf{V}_q$, so $\mathbf{V}'_q = \mathbf{V}_q^{(2)}$ (compare with (3) and the description above it). This way, at least we know that Alice$_q$ cannot do any better to prevent nullification of TxFJ on Eve. Obviously, by choosing, for example, $N = 1$ (i.e., allocating one dimension to the TxFJ precoder), even an Eve with $L = 2$ antennas can nullify the effect of TxFJ on herself.

As mentioned before, the information signal $\mathbf{s}_q$ can be written as $\mathbf{s}_q = \mathbf{T}_q x_q$, where $\mathbf{T}_q$ is the precoding matrix (precoder) and x_q is the information signal. With the aforementioned choice of TxFJ beamformer, the beamformer that can maximize the information rate of the Alice$_q$ would be $\mathbf{T}_q = \mathbf{V}_q^{(1)}$, where $\mathbf{V}_q^{(1)}$ is the $N_q - N = N_q - (N_q - 1) = 1$ leftmost column of $\mathbf{V}_q$, i.e., the first column of $\mathbf{V}_q$. Such a choice of precoders forces x_q to be a scalar value, signifying that only single-stream signals are allowed to be transmitted.

Overall, with these choices of precoders, we first make sure that our precoders do not require knowledge of E-CSI, then we make sure that our TxFJ signal will not be nullified at an Eve that has relatively low number of antennas. Such an approach in assigning precoders was also used in [23], [24]. Notice that with knowledge of number of antennas at Eve, the exact amount of dimensions for the TxFJ beamformer can be chosen to ensure that Eve is not able to nullify the TxFJ at herself. However, in the case of collusion between multiple eavesdroppers, they can form a MIMO receiver with higher number of receive antennas. The precoders we chose in this paper are practical and easy to implement, as they only require CSI of the direct channel from Alice to the intended Bob.

III. Problem Formulation

In this section, we present necessary bounds to achieve positive secrecy and make foundations for our game-theoretic formulation. We form the following optimization problem for $q \in \mathcal{Q}$:

$$\begin{aligned} \underset{\phi_q, p'_q}{\text{maximize}} \quad & C_q^{sec} \\ \text{s.t.} \quad & 0 \leq \phi_q \leq 1 \\ & 0 \leq p'_q \leq P'_q. \end{aligned} \tag{11}$$

Due to the non-concavity of the objective function in (11) w.r.t. decision variables, the optimization in (11) is non-convex[12]. 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 p'_q that results in not only maintaining positive secrecy, but also alleviating the need for knowledge of MUI at Eve and Bob$_q$. Then, we propose a method to find a suboptimal value for the PA between information and TxFJ signals.

A. RxFJ Power Assignment

Removing the $\max\{\bullet\}$ and $\log(\bullet)$ operators from C_q^{sec} in (10), the secrecy maximization w.r.t. p'_q can be written as

$$\begin{aligned} \underset{p'_q}{\text{maximize}} \quad & \frac{1 + \frac{\phi_q P_q}{a_q + b_q p'_q}}{1 + \frac{\phi_q P_q}{c_q + d_q p'_q}} \\ \text{s.t.} \quad & 0 \leq p'_q \leq P'_q. \end{aligned} \tag{12}$$

One can do a simple one-dimensional search to find the optimal value of p'_q. However, such an approach demands knowledge of MUI at Eve to be available, which may be difficult to achieve. In the remainder of this section, we propose a method for setting RxFJ power that can set the RxFJ PA independent of MUI at Eve and Bob$_q$.

We first find conditions that result in having positive secrecy at link q. Positive secrecy in (10) is achievable if and only if the objective value in (12) is larger than one. Furthermore, it can be easily shown that the objective value in (12) is larger than one if and only if the optimal

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

objective value of the following optimization is larger than one[13]:

$$\underset{p'_q}{\text{maximize}} \quad g(p'_q) \triangleq \frac{\frac{\phi_q P_q}{a_q+b_q p'_q}}{\frac{\phi_q P_q}{c_q+d_q p'_q}} = \frac{c_q + d_q p'_q}{a_q + b_q p'_q}$$
$$\text{s.t.} \quad 0 \leq p'_q \leq P'_q. \tag{13}$$

Note that the relationship between the solutions of (12) and (13) (that result in their corresponding objective values being larger than one) is of necessary and sufficient type. Hence, if we are seeking for a set of conditions/solutions that result in positive secrecy, we can do so by analyzing (13) instead of (12). The first and second derivatives of $g(p'_q)$ are as follows

$$\frac{dg(p'_q)}{dp'_q} = -\frac{b_q c_q - a_q d_q}{(a_q + b_q p'_q)^2} \tag{14a}$$
$$\frac{d^2 g(p'_q)}{d{p'_q}^2} = 2b_q \frac{b_q c_q - a_q d_q}{(a + bp'_q)^3}. \tag{14b}$$

Hence, the optimal value of p'_q (i.e., ${p'_q}^*$) that solves (13) is as follows:

$${p'_q}^* = \begin{cases} P'_q & \text{if } b_q < \dfrac{a_q d_q}{c_q} \\ 0 & \text{if } b_q > \dfrac{a_q d_q}{c_q}. \end{cases} \tag{15}$$

Simplifying the first condition of (15), a threshold for SIS factor is as follows[14]

$$\tau_q < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2} \frac{a_q d_q}{c_q}. \tag{16}$$

Later on, we show in simulations that whenever positive secrecy is achievable (i.e., the objective in (12) is larger than one), the rule in (15) also frequently holds, signifying that the solution to (13) is very likely optimal to (12) as well if positive secrecy is achievable (see Fig. 2).

Considering (16), we can conclude the following. Given c_q and d_q, if a_q (the normalized MUI at Bob$_q$) is not as strong as normalized the self-interference channel, i.e., $\frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 a_q}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$ is small, the power of RxFJ should be very weak to maintain positive secrecy, i.e., ${p'_q}^* = 0$. However, if $\frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 a_q}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$ is large, the effect of RxFJ on Bob$_q$ is not as significant as MUI, so less suppression of self-interference can be allowed and still maintain positive secrecy, i.e., ${p'_q}^* = P'_q$ becomes the favorable solution. An equivalent intuition holds for d_q/c_q when $\frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$ and a_q are given,

[13] One can simply set the objective of (12) to be larger than one and end up with $g(p'_q) > 1$ (and vice versa) where $g(p'_q)$ is defined in (13).

[14] Although when $p'_q = 0$ the benefits of RxFJ are not present, one can set a minimum RxFJ power to prevent RxFJ from going to zero.

meaning that a large d_q/c_q indicates that RxFJ significantly degrades Eve's reception compared to the MUI received at Eve (i.e., c_q). Hence, the FD-enabled Bob$_q$ can perform less suppression, i.e., $p_q'^* = P_q'$ becomes the favorable solution.

It can be seen in (15) that the optimal value of RxFJ that solves (13) depends on two factors: MUI at Bob$_q$ (i.e., a_q) and MUI at Eve while eavesdropping the qth link (i.e., c_q). It may not be practical for a legitimate node to have knowledge on MUI at a close-by Eve because Eve could be a passive device, or Eve does not broadcast the MUI she is receiving. In addition, because MUI at Bob is varying (due to the behavior of other links) while the SIS factor is not, changing RxFJ according to MUI variations at Bob (in order to satisfy the rule in (15)) is not desirable. We show in the following that a specific technique in setting TxFJ will help us to mitigate knowledge of MUI at Bob and Eve in setting RxFJ.

B. PA Between TxFJ and Information Signals

After finding a suitable set of conditions/solutions for p_q' (i.e., the rule in (15)), we now focus on finding the optimal PA between TxFJ and information signals of Alice$_q$ (i.e., ϕ_q):

$$\begin{aligned} \underset{\phi_q}{\text{maximize}} \quad & C_q^{sec} \\ \text{s.t.} \quad & 0 \leq \phi_q \leq 1. \end{aligned} \tag{17}$$

Note that although a simple one-dimensional search can find us the optimal value of ϕ_q, we would like to solve (17) by avoiding the required knowledge of MUI at Bob$_q$ and Eve. To do so, same as what we proposed for the RxFJ PA, we approach problem (17) by first finding a bound on ϕ_q that guarantees positive secrecy of link q. Thus, the objective in (17) is assumed to be positive, which reduces to

$$\frac{\phi_q P_q}{a_q + b_q p_q'} > \frac{\phi_q P_q}{c_q + d_q p_q'}. \tag{18}$$

Simplifying this inequality, we end up with the following

$$c_q > a_q + (b_q - d_q) p_q'. \tag{19}$$

The inequality in (19) is a bound on TxFJ power of Alice$_q$ (i.e., σ_q) because according to (9a), c_q includes σ_q. Hence, reducing (19) gives us a bound for ϕ_q as well. However, for ease of presentation, instead of writing ϕ_q at the left hand side of the inequality in (19), we use c_q and refer to (19) as *the bound on TxFJ power of link* q *that provides it with positive secrecy.*

To make use of the lower bound on TxFJ derived from (18), we first introduce a property of the secrecy rate of Alice$_q$

Lemma 1. *If* (19) *is satisfied, the secrecy rate* C_q^{sec} *is a monotonically increasing function of* P_q *and* ϕ_q*, respectively.*

Proof: The inequality in (19) can be written as

$$c_q = a_q + (b_q - d_q)p'_q + \delta \tag{20}$$

where $\delta > 0$ is a positive real value. Replacing the term c_q in (10) with the right hand side (RHS) of (20), and taking the derivative of (10) (without the $\max\{\bullet\}$ operator) w.r.t. P_q and ϕ_q, we have

$$\frac{dC_q^{sec}}{d_q P_q} = \frac{\phi_q \delta}{(a_q + \phi_q P_q + b_q p'_q)(a_q + \phi_q P_q + b_q p'_q + \delta)} \tag{21a}$$

$$\frac{dC_q^{sec}}{d\phi_q} = \frac{P_q \delta}{(a_q + \phi_q P_q + b_q p'_q)(a_q + \phi_q P_q + b_q p'_q + \delta)} \tag{21b}$$

which are both positive and prove the lemma. ■

In order to mitigate knowledge of MUI at Bob$_q$ and Eve in (15) (i.e., a_q and c_q), we examine the following alternative conditions for RxFJ:

$$p_q'^{\,*} = \begin{cases} P'_q, & \text{if} \;\; b_q < d_q \\ 0, & \text{if} \;\; b_q > d_q. \end{cases} \tag{22}$$

The following property shows the sufficiency of (22) to conclude (15).

Proposition 1. *Provided that the following conditions hold, the RxFJ PA scheme in* (22) *are sufficient to satisfy* (15)*:*

- c_q *satisfies* (19) *and* $c_q > 0$.
- $(b_q - d_q)P'_q + \delta < 0$ *when* $b_q < d_q$

Proof: Assume that we use the conditions in (22) to decide on RxFJ power of link q. Hence, according to (20), c_q must satisfy $c_q = a_q + (b_q - d_q)P'_q + \delta > 0$ when $b_q < d_q$. Assuming that $(b_q - d_q)P'_q + \delta < 0$, one can conclude that $a_q > a_q + (b_q - d_q)P'_q + \delta$. Hence, $b_q < d_q$ is readily sufficient to deduce $b_q < \frac{a_q d_q}{c_q}$ that appeared in (15). Similarly, $b_q > d_q$ can be proven to be sufficient to satisfy $b_q > \frac{a_q d_q}{c_q}$. Specifically, we set $p'_q = 0$ according to (22). Hence, according to (20), c_q must satisfy $c_q = a_q + \delta$. Since $\delta > 0$, then $a_q < c_q$. Therefore, $b_q > d_q$ is sufficient to deduce $b_q > \frac{a_q d_q}{c_q}$ that appeared in (15). ■

Remark 1: The key to conclude Proposition 1 are the assumptions $c_q > 0$ and $(b_q - d_q)P'_q + \delta < 0$. Regarding the importance of $c_q > 0$, if we have $b_q < d_q$ and $c_q = a_q + (b_q - d_q)P'_q > 0$, then $b_q < d_q$ is sufficient to satisfy $b_q < \frac{a_q d_q}{c_q}$), so both RxFJ PA schemes in (15) and (22) impose

${p'_q}^* = P'_q$. However, when $b_q < d_q$ (suggesting ${p'}_q^* = P'_q$), but $c_q = a_q + (b_q - d_q)P'_q < 0$, we have $b_q > \frac{a_q d_q}{c_q}$ (suggesting ${p'}_q^* = 0$). Hence, we have conflicting decisions. in Proposition 1. Condition $(b_q - d_q)P'_q + \delta < 0$ sets an upper bound on δ to keep RxFJ PA independent of MUI at Bob$_q$ and Eve, i.e., $0 < \delta < (d_q - b_q)P'_q$ if $b_q < d_q$[15]. According to (6) and (9), the constants b_q and d_q are in fact functions of self-interference channel, Alice-Bob channel, Bob-Eve channel, and Alice-Eve channels. Hence, if Proposition 1 holds, Bob$_q$ only has to check whether or not

$$\tau_q < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_q|^2} \tag{23}$$

to decide on RxFJ. In other words, (22) is sufficient to set the RxFJ power of Bob$_q$. The intuitive interpretation from (23) is that the SIS factor needs to be small if the self-interference channel (i.e., $|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|$) has a large value, but if the Bob-Eve channel (i.e., $|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2$) is large, it can cancel out the effect of self-interference channel. In other words, Bob$_q$ must not use RxFJ if the self interference is not removed well enough. However, if Eve suffers more from the generated RxFJ, then Bob$_q$ can use it. Compared to (15), condition (22) is more desirable, as it does not impose real-time tracking of MUI (at Eve) to Bob$_q$, thus simplifying the design. Combining (19) and (22), we have

$$\begin{cases} c_q > a_q + (b_q - d_q)P'_q, & \text{if} \quad b_q < d_q \\ c_q > a_q, & \text{if} \quad b_q > d_q \end{cases}. \tag{24}$$

Since the inequalities in (24) are strict, we write the following:

$$\begin{cases} c_q = a_q + (b_q - d_q)P'_q + \delta, & \text{if} \quad b_q < d_q \\ c_q = a_q + \delta, & \text{if} \quad b_q > d_q \end{cases}. \tag{25}$$

Overall, by mathematical manipulations done in equations (18)–(25), we convert problem (17) to the following problem:

$$\begin{aligned} \underset{\phi_q,\ \delta}{\text{maximize}} \quad & C_q^{sec} \\ \text{s.t.} \quad & c_q = a_q + (b_q - d_q){p'_q}^* + \delta \\ & c_q > 0 \\ & 0 < \delta < (d_q - b_q)P'_q + J(1 - t_q) \\ & 0 \leq \phi_q \leq 1 \end{aligned} \tag{26}$$

[15] In the simulation section, we also observe the physical interpretation drawn from these conditions.

where ${p'_q}^*$ in the first constraint is set according to (22), J is a sufficiently large number, and

$$t_q = \begin{cases} 1 & \text{if} \quad b_q < d_q \\ 0 & \text{if} \quad b_q > d_q \end{cases}. \tag{27}$$

The first constraint in (26) is a constraint on ϕ_q that imposes the optimal solution to yield positive secrecy[16]. In other words, this constraint replaces the more general constraint in (17), such that we can ignore the $\max\{\bullet\}$ operator in $C_q^{sec} = \max\{C_q - C_{eq}\}$. This constraint together with the second and third constraints in (26) ensure us that setting the RxFJ PA in (22) is sufficient to satisfy the more general conditions in (15) (but without the need to know MUI at Bob$_q$ and Eve). Note that t_q is a binary variable that is not among decision variables of (26), and can be computed offline.

Because c_q is a function of ϕ_q, one can simplify (25) to find the value of ϕ_q that yields positive secrecy to the objective of (26). However, we still need to determine the value of δ to ensure the optimality of the solution in (25) for problem (26). A simple one-dimensional search in the interval defined by the second constraint in (26) can provide us with the best value of δ and subsequently the optimal value of ϕ_q. To avoid additional computation imposed by the one-dimensional search process, we propose the following heuristic technique to set a value for δ. On the one hand, we do not wish to choose δ near its upper bound due to the fact that the increase in δ also increases the lower bound on TxFJ which subsequently decreases the amount of power allocated to the information signal[17]. On the other hand, the choice of δ close to zero is also not desirable, as in (21b) the growth rate of secrecy rate would be decreased. Hence, we choose $\delta = \frac{1}{2}\left|d_q - b_q\right| P'_q$. In simulations, we show that this heuristic choice of δ yields a relatively close performance to that of the the optimal solution found by one-dimensional search. In the next section, we use the derived conditions to model a secure power control game.

IV. Game Formulation

In this section, using the ideas of Section III, we propose a power control scheme based on non-cooperative games.

[16] Note that the term c_q is a function of ϕ_q (see (9)). An equivalent expanded version of this constraint is given in equation (29) later in this paper. In (26), however, for the sake of simplicity, we present this constraint in a more compact form.

[17] This can be seen in (29) where we expand the first constraint in (26) with ϕ_q on the right hand side.

$$\phi_q \leq \max\left\{ \min\left\{1 - \frac{1}{P_q}\sum_{\substack{r=1\\ r\neq q}}^{Q} \Big\{ \left(A_{q,r} - B_{q,r}\right)\phi_r P_r + C_{q,r}P_r + D_{q,r}p'_r \Big\} - \frac{p'_q}{P_q}E_q - \frac{F_q}{P_q}\delta, 1\right\}, 0\right\} \tag{29}$$

$$A_{q,r} = \frac{N_q - 1}{N_r - 1}\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2}{|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2}\left((N_r - 1)|\mathbf{d}_q^{\dagger}\mathbf{H}_{rq}|^2 - |\mathbf{d}_q^{\dagger}\mathbf{H}_{jrq}|^2\right) \tag{30a}$$

$$B_{q,r} = \frac{N_q - 1}{N_r - 1}\frac{(N_r - 1)|\mathbf{r}_q^{\dagger}\mathbf{G}_r|^2 - |\mathbf{r}_q^{\dagger}\mathbf{G}_{jr}|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2} \tag{30b}$$

$$C_{q,r} = \frac{N_q - 1}{N_r - 1}\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2|\mathbf{d}_q^{\dagger}\mathbf{H}_{jrq}|^2 - |\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2|\mathbf{r}_q^{\dagger}\mathbf{G}_{jr}|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2} \tag{30c}$$

$$D_{q,r} = (N_q - 1)\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2|\mathbf{d}_q^{\dagger}\mathbf{H}'_{rq}|^2 - |\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2|\mathbf{r}_q^{\dagger}\mathbf{G}'_r|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2} \tag{30d}$$

$$E_q = (N_q - 1)\frac{\tau_q|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2|\mathbf{d}_q^{\dagger}\mathbf{H}'_{qq}|^2 - |\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2|\mathbf{r}_q^{\dagger}\mathbf{G}'_q|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2} \tag{30e}$$

$$F_q = (N_q - 1)\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2}. \tag{30f}$$

A. Nash Equilibrium: Existence and Uniqueness

The condition in (25) can be written in general form as

$$\begin{cases} c_q \geq a_q + (b_q - d_q)P'_q + \delta, & \text{if} \quad b_q < d_q \\ c_q \geq a_q + \delta, & \text{if} \quad b_q > d_q. \end{cases} \tag{28}$$

Therefore, after setting RxFJ (according to (22)) and allocating a portion of transmit power to TxFJ (according to (25)), using (6) and (9), an upper bound on ϕ_q can be written as (29) where the newly introduced notations in (29) are given in (30). Hence, link q's optimization problem in (26), where $q \in \mathcal{Q}$, can be written as

$$\begin{aligned} \underset{\phi_q,\ \delta}{\text{maximize}} \quad & C_q^{sec} \\ \text{s.t.} \quad & (29) \\ & 0 < \delta < (d_q - b_q)P'_q + J(1 - t_q) \\ & 0 \leq \phi_q \leq 1. \end{aligned} \tag{31}$$

With every legitimate link following such a strategy, the resulting interaction between them can be modeled as non-cooperative game [25] where the players are the links, the strategy set of the qth player is the set of constraints in (31), and the utility of each player is his secrecy rate. The result of Lemma 1 suggests that the best-response of the qth link, $q \in \mathcal{Q}$, is when ϕ_q meets its upper bound in (29) with equality. The Nash equilibrium is a point at which no player is willing to unilaterally change his strategy given the strategies of other players [25].

Before going forward with our analysis, we need to emphasize that so far, all our derivations were based on the assumption that link q, $q \in \mathcal{Q}$, knows the MUI at Eve who eavesdrops on its communications. In fact, although we were able to make RxFJ PA independent of MUI at Eve (by using (22)), setting the PA between TxFJ and information signal of Alice$_q$ as in (29) still requires knowledge of MUI at Eve. Such knowledge is possible if, for example, Eve feeds back the interference she is receiving to link q. However, this is an unrealistic assumption. Another possibility is when Eve is an active node, so link q can acquire $\mathbf{G}_q$ and $\mathbf{G}_{j_q}$ from Eve's activity. Then, the legitimate links can coordinate with each other and exchange these acquired channel gains, as well as their RxFJ powers and their PAs between TxFJ and information signals, so that link q can use the best response in (29). While exchanging power levels can be possible via suitable control signaling schemes[18], knowledge of E-CSI (i.e., $\mathbf{G}_q$ and $\mathbf{G}_{j_q}$, $\forall q \in \mathcal{Q}$) at each link is a restricting assumption, if not impossible, especially when Eve is a passive device. Nevertheless, the analysis under full E-CSI assumption enables us to analyze the game more easily. It also serves us as both a roadmap that leads to our next proposed scheme (designed later in this paper) and a benchmark to our next proposed scheme (designed later in this paper) that is robust to uncertainties in knowledge of E-CSI.

Using the NE existence conditions of concave games, an 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, i.e., C_q^{sec} is concave w.r.t ϕ_q [25]. Convexity of each player's strategy set in our game is easy to prove, thus omitted for the sake of brevity. Replacing the term c_q with the RHS of (20) and plugging it in (10), we take the second derivative of (10) w.r.t. ϕ_q, which can be expressed as

$$\frac{d^2 C_q^{sec}}{d\phi_q^2} = P_q^2 \left(\frac{1}{a_q + \delta + \phi_q P_q + bp'_q} - \frac{1}{a_q + \phi_q P_q + bp'_q} \right) \tag{32}$$

which is always negative indicating that C_q^{sec} is concave w.r.t. ϕ_q. A necessary and sufficient condition for the uniqueness of NE is proven in the following theorem.

[18] Examples of such signaling protocols can be found in [26], [27].

Theorem 1. *The game defined in* (31) *for all $q \in \mathcal{Q}$ for which the best response of each player is set according to* (29) *has a unique NE iff the following condition is satisfied:*

$$\rho(\mathbf{A}+\mathbf{B}) < 1 \tag{33}$$

where $\rho(\bullet)$ indicates the spectral radius of a matrix (i.e., largest absolute value of eigenvalues of a matrix), $\mathbf{A}$ is a Q-by-Q matrix whose entries are written as

$$\mathbf{A} = \begin{cases} -\frac{P_r}{P_q}A_{q,r} \quad , & r \neq q \\ & \quad ,\forall(r,q) \in \mathcal{Q} \\ 0 \quad , & r = q \end{cases} \tag{34}$$

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

$$\mathbf{B} = \begin{cases} \frac{P_r}{P_q}B_{q,r} \quad , & r \neq q \\ & \quad ,\forall(r,q) \in \mathcal{Q}. \\ 0 \quad , & r = q \end{cases} \tag{35}$$

with $A_{q,r}$ and $B_{q,r}$ defined in (30).

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 (29) with equality for all q) has a fixed point, the convergence point is the NE of the game [28]. We first analyze the existence of a fixed point for the argument inside $\max\{\min\{\bullet,1\},0\}$ in (29). Then, we extend the analysis to include $\max\{\min\{\bullet,1\},0\}$. Concatenating the constraint in (29) for all q (without considering $\max\{\min\{\bullet,1\},0\}$), the following fixed-point problem in its $t-$th iteration can be established:

$$\Phi^{(t+1)} = \mathcal{T}(\Phi^{(t)}) = \mathbb{1} + (\mathbf{A}+\mathbf{B})\Phi^{(t)} + \mathbf{f} \tag{36}$$

where $\Phi = [\phi_1, \ldots, \phi_Q]^T$, $\mathbb{1}$ is a vector of appropriate size whose entries are all 1, and $\mathbf{f}$ is a vector constructed by concatenating the other terms in (29) for all q. The rest of the proof is presented in Appendix. ■

Remark 2: Using this condition, the convergence of Jacobi iterative algorithm in the sense of [28, Ch. 2, Proposition 6.8] is guaranteed. In fact, at every iteration, all players simultaneously update their actions. Later on, we prove the convergence of our secure power control game under totally asynchronous updates (in the sense of [28, Ch. 6] defined in the next subsection).

Remark 3: Notice that in (36), the fixed-point iteration is a function of only the power allocation factors of links (i.e., Φ) and not the RxFJs. In fact, results of Lemma 1 and Proposition 1 enable us to use a simpler fixed-point operation, as the RxFJ PA in (22) is not dependent on other links' actions. If we were to use the method in (15) and not use the sufficient conditions in (22), then we had to also include the RXFJs in the fixed-point iteration because the conditions in (15) are functions of MUI, thus requiring to observe the actions of other links. In such cases, we found it almost unlikely to set up a fixed-point operation and a simple distributed design. Later on when we propose our robust approach, we will relax knowledge of E-CSI as well, but for the sake of better understanding of the mechanics of our solution, we assumed knowledge of E-CSI in this section to thoroughly investigate the properties of our secure power control game. The flexibility of our method in covering the case of unknown E-CSI is a feature that we could not observe in previous works (e.g., [11]). We will show that all of previous and subsequent properties of our secure power control game can be easily extended to the case of unknown E-CSI.

B. Algorithm Design

The Jacobi iterative algorithm [28, Ch. 2] requires all links to simultaneously update their actions. Such a requirement may not always be practical due to possible delays in the network. Therefore, it could be the case that the measured interference at some Bobs are not according to the latest changes in the network. Thus, the actions of such links would be based on outdated received interference, thus preventing the possibility of having simultaneous updates at all links. In the following, we show that our proposed iterative framework allows for asynchronous implementation, which makes our game robust to possible delays in the network.

Let $\mathbb{T}_q, \ \forall q \in \mathcal{Q}$, be the set of iteration numbers when the qth link updates its action. For example, $\mathbb{T}_q = \{1, 3, 5\}$ indicates that the qth links performs the update in (31) in first, third and fifth iterations. Furthermore, Let $\Theta_q^{(n)} = \{\theta_{1,q}^{(n)}, \dots, \theta_{Q,q}^{(n)}\}$ denote the set of most recent times that the interference coming from each link is measured at Bob$_q$ in the nth iteration. Hence, $\theta_{r,q}^{(n)}$ is the most recent iteration in which the interference from the rth link, $r \neq q$ is captured/updated, and $\theta_{r,q}^{(n)} \leq n-1$. Therefore, in the nth iteration, the qth link, $q \in \mathcal{Q}$, performs the update in (31) based on $\Theta_q^{(n)}$ if $n \in \mathbb{T}_q$. Using these definitions, we can now present an asynchronous algorithm that implements our proposed game, which is as follows:

Algorithm 1 Asynchronous Iterative Secure Power Allocation (full E-CSI version)

```
Set $p'_q$ and $\delta$ according to (22) and Proposition 1 (see Section III).
for n=1 to maximum iteration do
    Set $\phi_q^{(n)} = \begin{cases} \text{Equal to RHS of (29),} & \text{if } \ n \in \mathbb{T}_q \\ \phi_q^{(n-1)} & \text{otherwise} \end{cases}, \forall (q) \in \mathcal{Q}.$
end for
```

Other suitable termination criteria can be used instead of the maximum iteration number. Special cases of the asynchronous scheme include Jacobi (or simultaneous) scheme and Gauss-Seidel (or sequential) scheme [28]. The Jacobi scheme can be described as follows ($q \in \mathcal{Q}$):

$$\mathbb{T}_q = \{1, 2, ..., it_{max}\}$$
$$\Theta_q^{(n)} = \{n-1, ..., n-1\}$$

where it_{max} is the maximum iteration number. The Gauss-Seidel scheme can be described as follows:

$$\mathbb{T}_q = \{q, q+Q, q+2Q, ..., q + \left(\frac{it_{max}}{Q} - 1\right) Q\}$$
$$\Theta_q^{(n)} = \begin{cases} \{n-(q-1), ..., n-1\} & \text{if } j = 1, \ldots, q-1 \\ \{n, n-(Q-1), ..., n-q\} & \text{if } j = q, \ldots, Q \end{cases}$$

which means that in each iteration, only one link updates its action, while all other links use their previously chosen actions. The following theorem guarantees the feasibility of asynchronous implementation of our proposed game:

Theorem 2. *Algorithm 1 converges to the unique NE of the proposed game if Theorem 1 holds.*

Proof: See Appendix B. ■

C. Alternative Sufficient Conditions for NE Uniqueness

Although (33) is a tight condition, evaluating it requires 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 [28, Proposition A.20] that for any induced matrix norm[19] $|| \bullet ||$ 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-by-Q matrix, a sufficient condition for $\rho(\mathbf{M}) < 1$ is whether $||\mathbf{M}||_\infty < 1$. Using this property in our game, a sufficient condition for our game to have a unique NE is whether

$$||\mathbf{A}+\mathbf{B}||_\infty = \max_q \sum_{r=1}^{Q} \frac{P_r}{P_q} |A_{q,r} - B_{q,r}| < 1. \tag{37}$$

The physical intuition drawn from the condition in (37) is not straightforward. One way to interpret this condition is to decompose this condition as follows: The term $A_{q,r}$ in (37) is

[19] The induced norm of matrix $\mathbf{M}$ is defined as $||\mathbf{M}|| \triangleq \max_{||\mathbf{x}||=1} ||\mathbf{M}\mathbf{x}||$ where $\mathbf{x}$ is a vector and both norms on the RHS are vector norms.

mostly related to the MUI at each Bob which should be low enough, i.e., $|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|,\ \forall q \in \mathcal{Q}$ in $A_{q,r}$ should be large enough to guarantee the uniqueness of NE (see (30)). A sufficient separation between the links can satisfy this condition. The term $B_{q,r}$ in (37) is related to E-CSI components (see (30)). At first, it may seem that this condition requires each link to be the dominant interferer at Eve w.r.t. other links (i.e., $|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|,\ \forall q \in \mathcal{Q}$ in $B_{q,r}$ should be large enough). However, this is physically not possible. Instead, a more reasonable interpretation is that the NE is unique if every link has equal contribution in interfering with Eve's reception. This way, the second summation in (37) would be constant which only depends on the number of interfering links and the analysis of uniqueness is done via only the first summation. Since the nodes are not guaranteed to be positioned in a way that facilitates equal contribution in interfering with Eve, the only possibility is when Eve is far from all links. More discussion on this interpretation is given in the simulations section.

It can be seen that the uniqueness condition depends on the location of Eve because the terms $C_{q,r}$, $D_{q,r}$, E_q and F_q all depend on Eve's channels. Other studies such as [6], [9], [11] have also confirmed the dependency of the unique NE (of non-cooperative secure power control games) on Eve's channels. Such a coupling is neither practical (because E-CSI must be known) nor favorable (because Eve plays a role in the stability of the game). In what follows, we aim to not only mitigate knowledge of E-CSI, but also set both the NE uniqueness and positive secrecy conditions (derived in Theorem 1) free of Eve's role. None of the approaches in [6], [9]–[11] were shown to be extendable to the case of unknown E-CSI. However, we show that our approach can be simply extended to cover the case of unknown E-CSI.

V. Robust Power Allocation Game

In this section, we incorporate the assumption of unknown E-CSI in our game. As knowledge of E-CSI becomes unknown, each legitimate link needs to ensure that positive secrecy is still preserved. Recalling the inequalities in (28) and (29), positive secrecy happens when $c_q > a_q + (b_q - d_q)p'_q$ or equivalently

$$(1-\phi_q)P_q > \psi_q + \tau_q p'_q E_q \tag{38}$$

where

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

Under unknown E-CSI, for a given probability value ε, the qth link needs to satisfy the following:

$$\Pr\{(1-\phi_q)P_q > \psi_q + \tau_q p'_q E_q\} \geq \varepsilon. \tag{39}$$

Using (22) and the Bayes law of total probability we have

$$\begin{aligned}&\Pr\{(1-\phi_q)P_q > \psi_q + \tau_q p'_q E_q\} = \\ &\Pr\{b_q < d_q\}(1 - \Pr\{(1-\phi_q)P_q \leq \psi_q + \tau_q P'_q E_q\}) + \\ &\Pr\{b_q > d_q\}(1 - \Pr\{(1-\phi_q)P_q \leq \psi_q\}).\end{aligned} \tag{40}$$

We assume that $\psi_q + \tau_q p'_q E_q$ is a non-negative number for both values of p'_q, i.e., $\Pr\{\psi_q + \tau_q p'_q E_q > 0\} = 1$, otherwise (39) is always satisfied when $\psi_q + \tau_q p'_q E_q < 0$, and Alice$_q$ can spend all of the transmit power on information signal[20]. Using Markov inequality in (40), the following holds

$$\begin{aligned}&\Pr\{b_q < d_q\}(1 - \Pr\{(1-\phi_q)P_q < \psi_q + \tau_q P'_q E_q\}) + \\ &\Pr\{b_q > d_q\}(1 - \Pr\{(1-\phi_q)P_q < \psi_q\}) \ > \\ &\Pr\{b_q < d_q\}(1 - \frac{\mathrm{E}[\psi_q + \tau_q P'_q E_q]}{(1-\phi_q)P_q}) + \Pr\{b_q > d_q\}(1 - \frac{\mathrm{E}[\psi_q]}{(1-\phi_q)P_q}).\end{aligned} \tag{41}$$

Hence, (39) remains true as long as we have

$$\Pr\{b_q < d_q\}(1 - \frac{\mathrm{E}[\psi_q + \tau_q P'_q E_q]}{(1-\phi_q)P_q}) + \Pr\{b_q > d_q\}(1 - \frac{\mathrm{E}[\psi_q]}{(1-\phi_q)P_q}) \geq \varepsilon. \tag{42}$$

Simplifying this inequality, we end up with

$$\phi_q \leq \max\left\{\min\left\{1 - \Pr\{b_q < d_q\}\frac{\mathrm{E}[\psi_q + \tau_q P'_q E_q]}{(1-\varepsilon)P_q} - \Pr\{b_q > d_q\}\frac{\mathrm{E}[\psi_q]}{(1-\varepsilon)P_q}, 1\right\}, 0\right\}. \tag{43}$$

Using (6) and (9), we simplify $b_q < d_q$, which is as follows

$$b_q < d_q \Rightarrow |\mathbf{r}_q^\dagger \mathbf{G}_q|^2 < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2} |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2. \tag{44}$$

The probability $\Pr\{b_q < d_q\}$ can be written as

$$\Pr\{\frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2} < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}\}. \tag{45}$$

The small-scale fading components of $\mathbf{r}_q^\dagger \mathbf{G}'_q$ and $\mathbf{r}_q^\dagger \mathbf{G}_q$ are ZMCSCG-RVs with unit variances. Hence $|\mathbf{r}_q^\dagger \mathbf{G}_q|^2$ and $|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2$ both have chi-square distributions with 2 and $2N_q$ degrees of freedom, respectively. To tackle the issue of unknown large-scale fading components of $\mathbf{r}_q^\dagger \mathbf{G}'_q$ and $\mathbf{r}_q^\dagger \mathbf{G}_q$ we use *stochastic geometry* [29]. One can model nodes' positions according to a spatial distribution, e.g., a Poisson point process (PPP). For instance, stochastic geometry has been used in modeling

[20] Intuitively, if Eve is not close no power needs to be allocated to TxFJ, hence suggesting that $\psi_q + \tau_q p'_q E_q < 0$.

eavesdroppers' positions in several recent works [30], [31]. We model the location(s) of Eve(s) according to an independent homogenous PPP, namely Ω, with density λ. Such a representation can be used to model single or multiple Eves depending on the choice of λ[21]. Let $\Gamma\gamma \triangleq \frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}'_q|^2}$ and $\nu \triangleq \frac{|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2}{\tau_q|\mathbf{d}_q^{\dagger}\mathbf{H}'_{qq}|^2}$ where Γ and γ are RVs that represent large-scale and small-scale fading components of $\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}'_q|^2}$, respectively.

Theorem 3. *An analytical solution for* (45) *that is used in* (43) *is as follows:*

$$Pr\{\Gamma\gamma < \nu\} = exp\Bigg(- \lambda \int_0^{d_0} \int_0^{2\pi} Pr\Big\{\S_q\gamma > \nu\Big\}\beta \; d\beta d\varphi\Bigg) \tag{46}$$

where $\S_q \triangleq \left(\frac{\beta}{\sqrt{{d_{qq}}^2+\beta^2-2d_{qq}\beta COS\varphi}}\right)^{\eta}$ *and* $Pr\{\S_q\gamma > \nu\} = (1+\frac{\nu}{\S_q})^{-N_q}$.

Proof: See Appendix C. ■

We now turn our attention to $\mathrm{E}[\psi_q + \tau_q P'_q E_q]$ and $\mathrm{E}[\psi_q]$ in (43). We propagate the expectation in $\mathrm{E}[\psi_q + \tau_q P'_q E_q]$ to each term inside ψ_q using (30). Hence, the expectation of the terms in (30) can be written as

$$E[A_{q,r}] = \frac{N_q-1}{N_r-1}\left(\frac{(N_r-1)|\mathbf{d}_q^{\dagger}\mathbf{H}_{rq}|^2 - |\mathbf{d}_q^{\dagger}\mathbf{H}_{jrq}|^2}{|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2}\right) E\left[\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2}\right] \tag{47a}$$

$$E[B_{q,r}] = \frac{N_q-1}{N_r-1}E\left[\frac{(N_r-1)|\mathbf{r}_q^{\dagger}\mathbf{G}_r|^2 - |\mathbf{r}_q^{\dagger}\mathbf{G}_{jr}|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2}\right] \tag{47b}$$

$$E[C_{q,r}] = \frac{N_q-1}{N_r-1}E\left[\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2|\mathbf{d}_q^{\dagger}\mathbf{H}_{jrq}|^2 - |\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2|\mathbf{r}_q^{\dagger}\mathbf{G}_{jr}|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2}\right] \tag{47c}$$

$$E[D_{q,r}] = (N_q-1)E\left[\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2|\mathbf{d}_q^{\dagger}\mathbf{H}'_{rq}|^2 - |\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2|\mathbf{r}_q^{\dagger}\mathbf{G}'_r|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2}\right] \tag{47d}$$

$$E[E_q] = (N_q-1)E\left[\frac{\tau_q|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2|\mathbf{d}_q^{\dagger}\mathbf{H}'_{qq}|^2 - |\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2|\mathbf{r}_q^{\dagger}\mathbf{G}'_q|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}_{jq}|^2|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2}\right] \tag{47e}$$

Because the expectation terms contain non-negative RVs we can use the following identity:

$$E\left[\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}'_q|^2}\right] = \int_0^{\infty} \mathrm{Pr}\{\Gamma\gamma > \nu\}d\nu \tag{48}$$

where $\mathrm{Pr}\{\Gamma\gamma > \nu\}$ can be derived from Theorem 3. Other expectation terms that include E-CSI components can be treated the same as how we treat $E\left[\frac{|\mathbf{r}_q^{\dagger}\mathbf{G}_q|^2}{|\mathbf{r}_q^{\dagger}\mathbf{G}'_q|^2}\right]$.

[21] For example, if Eve is known to be distributed inside a certain region, we can find a suitable λ (that represents the density as λ Eves per unit of the surface area) such that the PPP matches our settings.

While in the simulation section, we focus on the case where no knowledge on E-CSI components is available to links (i.e., both large-scale and small-scale fading parts of E-CSI components are not known), we can interpret the derivations for unknown E-CSI by considering the case where large-scale fading part of E-CSI is available[22]. Hence, we can give a close-form representation to (43). Regarding the calculation of $\Pr\{b_q < d_q\}$ in (43), the quantity $X \triangleq \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_q'|^2}$ in (45) is the SINR of a one-branch diversity combiner with N_q interferers [33, eq. (19)]. Thus,

$$\Pr\{b_q < d_q\} = 1 - \left(1 + \big(\frac{d_{qe}}{d'_{qe}}\big)^{\eta} \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}\right)^{-N_q}. \tag{49}$$

To compute $\mathrm{E}[\psi_q + \tau_q P'_q E_q]$ and $\mathrm{E}[\psi_q]$ in (43), we know that random variables $|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2$, $|\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2$, $|\mathbf{r}_q^\dagger \mathbf{G}_r|^2$, and $|\mathbf{r}_q^\dagger \mathbf{G}'_r|^2$ have chi-square distributions with $2(N_q - 1)$, $2(N_r - 1)$, 2, and N_r degrees of freedom, respectively [13, Lemma 2]. Note that all of the aforementioned RVs are independent from each other because the precoding matrices $\mathbf{V}_q^{(1)}$ and $\mathbf{V}_q^{(2)}, \forall q$ are unitary and orthogonal to each other (see Section II). The division of a (central) chi-square random variable by another independent (central) chi-square random variable has *F-distribution* [34]. Hence,

$$E[A_{q,r}] = \frac{N_q - 1}{(N_r - 1)(N_q - 3)} \frac{(N_r - 1)|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{jrq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} \tag{50a}$$

$$E[B_{q,r}] = 0 \tag{50b}$$

$$E[C_{q,r}] = \frac{N_q - 1}{(N_r - 1)(N_q - 3)} \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{jrq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \frac{N_q - 1}{N_q - 3} \big(\frac{d_{re}}{d_{qe}}\big)^{(-\eta)} \tag{50c}$$

$$E[D_{q,r}] = \frac{N_q - 1}{N_q - 3} \left(\frac{|\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \big(\frac{d'_{re}}{d_{qe}}\big)^{(-\eta)} \right) \tag{50d}$$

$$E[E_q] = \frac{N_q - 1}{N_q - 3} \left(\frac{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \big(\frac{d'_{qe}}{d_{qe}}\big)^{(-\eta)} \right). \tag{50e}$$

The last issue is related to choosing a suitable value of RxFJ. As it was shown in Section III, the choice of RxFJ depends on whether $b_q < d_q$ or $b_q > d_q$. When $b_q < d_q$ becomes a random variable in the case of unknown E-CSI, we choose to use RxFJ whenever $\Pr\{b_q < d_q\} > 0.5$. With the derivations in (43), (49) and (50), we can construct a game with the same structure as in section IV where each link's best response is computed from (43). Using the same logic

[22] Apart from the fact that the assumption of knowledge of large-scale fading components of E-CSI gives us valuable insights on the performance of the robust approach, a justification of such assumption is given in [32, Section V].

behind Theorem 1, the following must hold to ensure a unique NE for the robust game:

$$\rho\left(\frac{E[\mathbf{A}+\mathbf{B}]}{1-\varepsilon}\right) < 1 \tag{51}$$

Note that $E[B_{q,r}] = 0$, so one can see that the analysis of the matrix $E\left[\mathbf{A}+\mathbf{B}\right]$ (see Section IV and Theorem 1), where the expected value is element-wise, is simplified to $E\left[\mathbf{A}\right]$. Therefore, the E-CSI is no longer present in NE uniqueness conditions. Moreover, for the qth link, $q \in \mathcal{Q}$ to perform the PA scheme in (43), it requires the PA's set by other links (i.e., ϕ_r, $\forall r \in \mathcal{Q}$, $r \neq q$), as well as the interfering channels between other legitimate links and Bob$_q$ (i.e., $\mathbf{H}_{rq}$ and $\mathbf{H}_{jrq}$, $\forall r \in \mathcal{Q}$, $r \neq q$). Hence, no knowledge of MUI at Eve or E-CSI components is needed[23]. Same as the previous section, an alternative condition to (51) is to replace the spectral radius with the infinity norm according to (37). Interestingly, the alternative condition for the robust game has a nice interpretation. Specifically, (51) is deduced if

$$||\frac{E[\mathbf{A}]}{1-\varepsilon}||_\infty = \max_q \sum_{r=1}^{Q} \frac{1}{1-\varepsilon}\,|E[A_{q,r}]| < 1. \tag{52}$$

Intuitively, if the interfering channels are small enough (i.e., if $|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2$, $\forall q \in \mathcal{Q}$ are dominant, see (50)), a unique NE exists. The following asynchronous algorithm implements the robust version of our game:

Algorithm 2 Asynchronous Iterative Secure Power Allocation (robust version)

```
Given $\varepsilon$, calculate (45) and set $p'_q = P'_q$ if $\Pr\{b_q < c_q\} \geq 0.5$, or $p'_q = 0$ if $\Pr\{b_q < c_q\} < 0.5$.
for n=1 to maximum iteration do
    Set $\phi_q^{(n)} = \begin{cases} \text{Equal to RHS of (43),} & \text{if } n \in \mathbb{T}_q \\ \phi_q^{(n-1)} & \text{otherwise} \end{cases}, \forall (q) \in \mathcal{Q}.$
end for
```

VI. Numerical Results

In this section, we verify our theoretical analyses. We show our results for a four-link network[24]. Eve is located at ($\mathtt{X_e}$, $\mathtt{Y_e}$) on a 2-D coordinate system. 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 of the coordinate system. Specifically, only the phase of Alices' placements has uniform distribution. Each Alice has a fixed distance (communication range) with her corresponding Bob denoted

[23] Note that the case where large-scale fading part of E-CSI is known was only mentioned to give intuitions on the behavior of the robust scheme. In simulations, we only consider the case where neither the large-scale nor the small-scale fading parts of E-CSI are known.

[24] The results for this case can be generalized to arbitarily larger number of links.

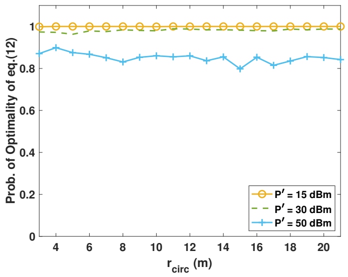


Fig. 2: Probability of having both positive secrecy and the assignment in (15) as the optimal solution for a single-link scenario ($\mathtt{X}_e$= $\mathtt{Y}_e$= 0, $N_q = 8, M_q = L = 5, P_q = 25$ dBm$, \forall q, Q = 4$)

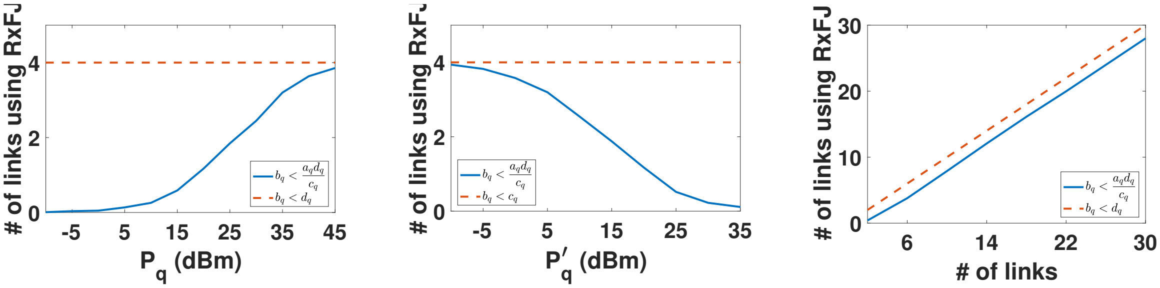
as $\mathtt{d}_{\mathtt{link}}$[25]. Each Bob is placed randomly around his corresponding Alice on the boundary of a circle whose center is the location of Bob's corresponding Alice with radius $\mathtt{d}_{\mathtt{link}}$. Again, only the phase of Bobs' placements has uniform distribution. The noise level is set to 0 dBm. Unless stated otherwise, the power constraint for each legitimate link is set to $P_q = 20$ dBm, $\forall q$, the maximum RxFJ power at each Bob is $P'_q = 15$ dBm, $\eta = 2.5$, $\tau_q = -100$ dB[26], $\mathtt{d}_{\mathtt{link}} = 10$ m, and finally Jacobi algorithm is used in all simulations. Regarding the unknown location for Eve, Bob$_q$ assumes that Eve is distributed in a circle around him with radius $r_0 = 5$ m according to a PPP with $\lambda = \frac{1}{25\pi}$ Eve/m^2, $q \in \mathcal{Q}$.

We set up our system model in the presence of an eavesdropper where the PA between TxFJ and information signal for all links is set to $\phi = 0.5$. We aim to find out if the RxFJ PA scheme in (15) is sufficiently close to an optimal scheme to solve (12). To do so, we perform the optimal assignment of RxFJ power for (12) with a simple one-dimensional search method for several channel realizations. In Fig. 2, we plot the probability of having both positive secrecy and the optimal value of RxFJ power for problem (12) (found from a one-dimensional search) being either the maximum or zero according to the scheme in (15) for all links. Such probability shows how frequent the scheme in (15) gives us the optimal value of RxFJ power. It can be seen in Fig. 2 that this probability is very high even for the cases where the power budget for RxFJ is high. Also, it can be seen the size of simulation region (which affects the distance between the legitimate Tx and the eavesdropper) has a negligible effect on this probability.

Fig. 3 (a)-(c) show the number of links that use RxFJ in the network for the two RxFJ PA schemes derived in (15) and (22) where in (15), c_q is set according to (25). We assumed that all links use $\phi_q = 0.5$ as the PA for information and TxFJ signals. It can be seen from these figures that using the RxFJ PA in (22) has a close performance to (15) whenever Alices' power

[25] Using a common communication range is a generic assumption in wireless ad hoc networks [30], [31].

[26] Such an SIS factor was reported in recent practical implementations of full-duplex radios [16].



(a) (b) (c)

Fig. 3: Number of links using RxFJ using the bound in (15) and the bound (22) vs. (a) transmit powers ($P'_q = 15$ dBm) (b) RxFJ powers ($P_q = 25$ dBm) (c) number of links ($\mathtt{X}_e = \mathtt{Y}_e = 0$, $\mathtt{r}_{\mathtt{circ}} = 20$ m, $N_q = 8, M_q = L = 5, \forall q, Q = 4$).

budgets are high enough or when Bobs' RxFJ power budgets are low enough. Examining c_q in (25), one can easily see that low transmit powers would decrease a_q and high RxFJ powers would increase $(b_q - d_q)P'_q$. Both of these situations are detrimental to the scheme in (22), as they violate the condition $c_q > 0$ which is a requirement for sufficiency of the scheme in (22) (See Proposition 1 and Remark 1). Using high enough power budgets at Alices and low enough RxFJ powers at Bobs for all links can ensure that such a conflict does not occur. As it can be seen in Fig. 3 (c), for a suitable choice of transmit power and RxFJ power, both conditions stay close to each other regardless of number of links in the network. Hence, the sufficient condition (22) was considered in our design, and it allowed us to proceed with our distributed design and game-theoretic implementation. Next, we compare the performance of our proposed methods for PA between TxFJ and information signals in a single-link scenario. Specifically, in one method, we use one-dimensional search to find the best value of δ in (26). In the other method, we use the heuristic method for finding δ, i.e., $\delta = \frac{1}{2}|d_q - b_q|P'_q$. We compare the resulting secrecy sum-rate of these two methods in Fig. 4[27]. It can be seen that the heuristic method has a very close performance to that of the one-dimensional search, suggesting that we can use the heuristic method for assigning δ without imposing the relatively larger computational complexity of the one-dimensional search method.

Fig. 5 shows the probability of satisfying the uniqueness conditions derived in (33) and (37) for a two-link scenario with full knowledge of E-CSI. The vertical axis at the left of each subfigure indicates the probability of satisfying (33), i.e., $\rho(\mathbf{A} + \mathbf{B}) < 1$. Specifically, each point on the curve related to (33) (indicated by n_1) is the result of averaging the number of times (33) holds over 100 network topologies where in each topology 500 channel realizations are simulated and

[27] Note that the one-dimensional search is in fact the optimal approach in PA that results in positive secrecy (see Section III.B)

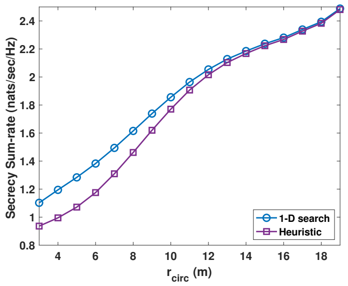
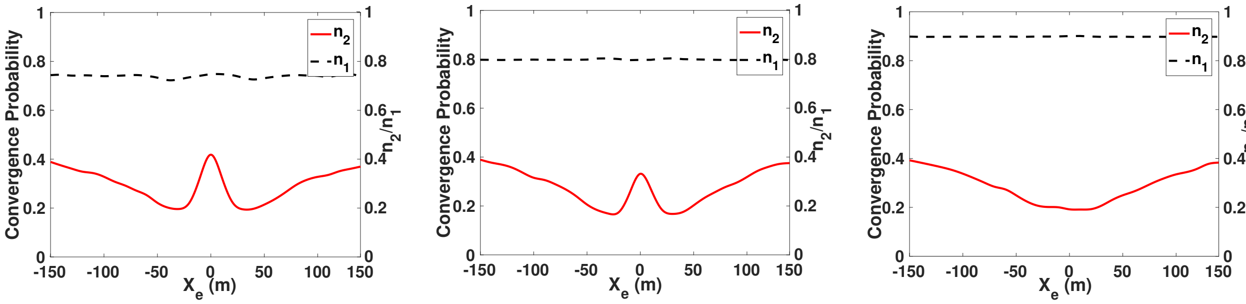


Fig. 4: Comparison of secrecy sum-rate between the one-dimensional search method and the heuristic method for setting δ in (26) ($\mathtt{X}_e$= $\mathtt{Y}_e$= 0, $N_q = 8, M_q = L = 5, P_q = 25$ dBm$, P'_q = 15$ dBm$, \forall q, Q = 4$)

averaged. Thus, the probability of convergence for (33) is $n_1/(100 * 500)$ where n_1 denotes the number of times that (33) is satisfied over all network topologies and channel realizations. Let n_2 denote the number of times that condition (37) is satisfied given that (33) is already satisfied. Hence, the vertical axis at the right of each subfigure indicates the ratio n_2/n_1 for which we have $n_2/n_1 < 1$, since n_2 counts the times (37) is true among the times (33) holds.

The horizontal axis in Fig. 5 indicates the value of $\mathtt{X}_\mathtt{e}$. While the value of $\mathtt{Y}_\mathtt{e}$ is fixed for a subfigure, it is different from one subfigure to another. For the two-link case, condition (33) is highly probable in all scenarios. The practical condition in (37), however, is only good when Eve is relatively far from the network, but as Eve becomes closer to the network this condition is less efficient. Interestingly, as Eve approaches the origin, for $\mathtt{Y}_\mathtt{e} = 0$ in Fig. 5 (a), the probability of satisfying (37) increases. The reason for such a result is because of the simulation model, which verifies the physical interpretation given for (37). In fact, the origin is where the distance of all links to Eve is the same because the simulation model puts all of Alices in the boundary of the simulation region which is a circle. One can see that when the y-coordinate of Eve changes in Fig. 5 (b) and Fig. 5 (c), the location $\mathtt{X}_\mathtt{e} = 0$ becomes more similar to other points inside the simulation region. We did not however, see this phenomenon for higher number of links, which is attributed to the fact that the second summation in (37) becomes too large with high number of links, even though it is a constant for when $(\mathtt{X}_\mathtt{e}, \mathtt{Y}_\mathtt{e}) = (0, 0)$.

Fig. 6 (a) shows the variation of convergence probabilities of robust and full E-CSI method w.r.t $\mathtt{r}_\mathtt{circ}$ for the four-link case. The convergence probability is calculated as number of times the conditions in (33) and (37) (indicated by “full E-CSI, n_1”and “full E-CSI, n_2”, respectively, in Fig. 6 (a)), and their equivalents for the robust game (i.e., (51) indicated by “Robust, n_1”and (52) indicated by “Robust, n_2”) hold true divided by the number of channel realizations. It can be seen that for the case of full E-CSI, probability of uniqueness of NE using (37) is very low. However, in the case of unknown E-CSI, since the nodes are indifferent w.r.t. E-CSI, far less



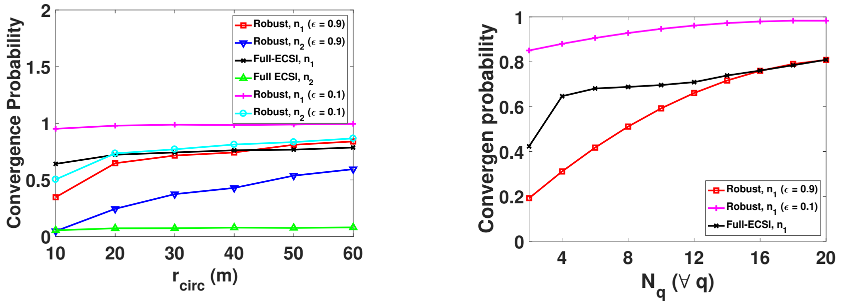
(a) (b) (c)

Fig. 5: Probability of convergence vs. eavesdropper's location for the full E-CSI case: (a) $\mathtt{Y_e{=}0}$, (b) $\mathtt{Y_e{=}10m}$, (c) $\mathtt{Y_e{=}40\ m}$, ($\mathtt{r_{circ}{=}30m}$, $N_q = 8, M_q = L = 1, \forall q, Q = 2$).

restrictive conditions than that of full E-CSI scenario can be achieved. In fact, by increasing the radius of simulation region, interference at each Bob becomes weaker. So, as the physical interpretation mentioned for (52) suggested, the NE uniqueness becomes more often. Moreover, in robust version, as ε becomes larger, the uniqueness conditions become more restrictive, which is in line with the derivation in (51). In other words, by increasing ε, the robust method becomes closer to the full E-CSI method

Fig. 6 (b) shows the convergence probability versus number of transmit antennas at each link. It can be seen that the probability of NE uniqueness becomes higher with more transmit antennas. The reason is that as the number of antennas grows, the communication channels become almost deterministic and only dependent on large-scale fading components. Specifically, looking at (29), (30), (43) and (50), it can be shown that for large number of antennas, the values of $|\mathbf{r}_q^\dagger \mathbf{G}_q|^2$, $|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2$ and $|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2$ would be close to their large-scale fading components multiplied by 2, as their distributions are chi-squares with two degrees of freedom [13, Lemma 3]. Using the same argument, the values of $\frac{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2}{N_q-1}$, $\frac{|\mathbf{d}_q^\dagger \mathbf{H}_{jrq}|^2}{N_r-1}$, and $\frac{|\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2}{N_r-1}$ will be asymptotically close to their large-scale fading component multiplied by certain factors, as $|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2$, $|\mathbf{d}_q^\dagger H_{jrq}|^2$, and $|\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2$ have chi-square distributions with $2(N_q-1)$, $2(N_r-1)$ and $2(N_r-1)$ degrees of freedom, respectively. Hence, the values of $A_{q,r}$ and $B_{q,r}$ are both close to zero which result in small eigenvalues and thus satisfying the convergence condition in (33) more often. The same argument holds for conditions in (37), (52), i.e., they become more probable as the number of transmit antennas grow.

Fig. 7 (a)-(c) show the achieved secrecy sum-rate of robust and full E-CSI methods as well as the globally optimal solutions of the secrecy sum-rate maximization vs. the radius of our simulation region. Furthermore, Fig. 7 (d)-(f) show the resulting sum of information and leaked rates of our methods vs. the radius of our simulation region. The maximum amount of iterations for Algorithm 1 and 2 are set to 50 iterations. We conducted this simulation for two scenarios:



(a) (b)

Fig. 6: (a) Probability of convergence vs. $\mathtt{r_{circ}}$ ($\mathtt{X}_e$= $\mathtt{Y}_e$= 5, $N_q = 8, M_q = L = 5, \forall q, Q = 4$), (b) Probability of convergence vs. N_q ($\mathtt{X_e}$=$\mathtt{Y_e}$= $0, \mathtt{r_{circ}} = 15$ m, $M_q = L = 5, \forall q \in \mathcal{Q}$)

1) when Eve uses MRC decoder, and 2) when Eve uses MMSE decoder[28]. From Fig. 7 (a)-(c), it can be seen that our apporaches have less secrecy compared to globally optimal solutions. The reason is that the NEs of our proposed game are not necessarily guaranteed to be globally optimum for the secrecy sum-rate. NE is a stable point where no link can gain more secrecy given the interference received from other nodes. In other words, the NE of our game is *unilaterally optimum* for each link. Furthermore, both cases of the robust method have less secrecy sum-rates than that of the full E-CSI method.

According to Fig. 7 (d)-(e), for a given ε in the robust method, regardless of the decoder at Eve, the sum of information rates remains the same, which indicates that the interference management between legitimate links in the robust method is completely decoupled from Eve characteristics. In other words, in the robust method, the nodes are indifferent to E-CSI. Moreover, for when $\varepsilon = 0.9$, the leaked rate is significantly reduced compared to when $\varepsilon = 0.1$ because the probability of achieving positive secrecy is set to be higher for when $\varepsilon = 0.9$. However, the penalty for achieving positive secrecy with high probability (in the robust method) is that the nodes cannot manage interference between themselves as efficiently as in the full E-CSI case or the case where $\varepsilon = 0.1$. This leads to having lower sum of information rates when $\varepsilon = 0.9$. Another penalty of choosing ε to be too high is that the uniqueness of NE becomes less often. As it was shown in Fig. 6 (a), by increasing ε, the probability of NE uniqueness in the robust scheme decreases. The issue of not having a unique NE can lead to instability of our power control algorithm, as this algorithm is not guaranteed to converge to any point if the NE uniqueness conditions are violated. Hence, the iterations of our algorithm must be manually terminated with no sign of convergence. It can also be seen in Fig. 7 (a)-(c) that when Eve employs MMSE decoder, the secrecy sum-rate decreases more than when MRC decoder is

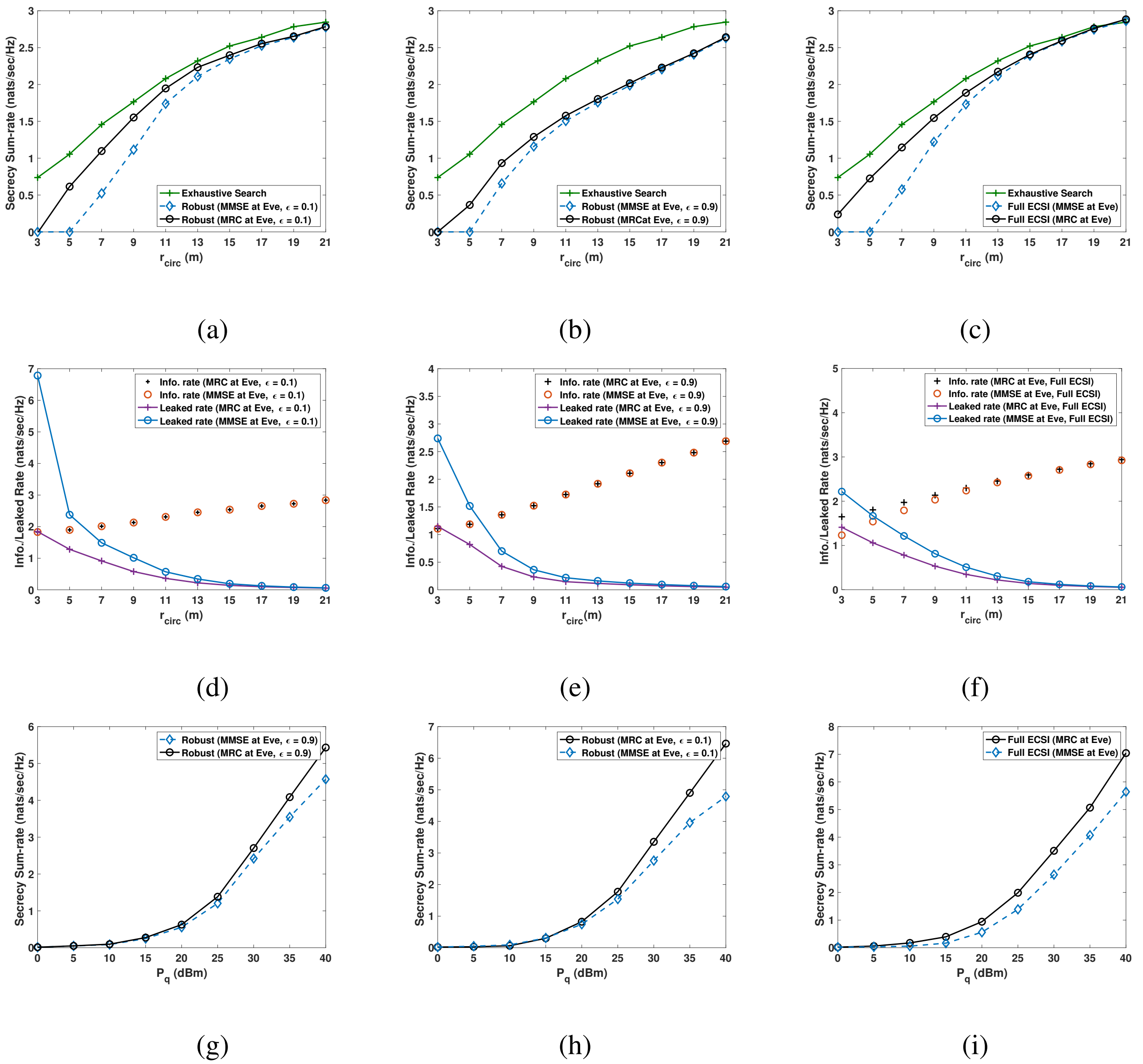
[28] Although our analysis was limited to the case of using MRC decoder at Eve, we still observed the convergence of our algorithm for the case of MMSE decoder.

adopted. The reason is that the MMSE receiver takes into account the effect of interference, so Eve is able to mitigate a part of interference on herself. According to (29), in the full E-CSI case, the action of a link depends on the decoder that Eve uses. Therefore, we can see in Fig. 7 (f) that the sum of information rates for the full E-CSI case is affected when Eve uses MMSE decoder. As the radius of simulation region increases, the SINR at Eve decreases, so it is well-known that for the low SINR regime, the MMSE receiver must reduce to the MRC receiver [20]. This phenomenon can be seen in Fig. 7 (d)-(f) where the leaked rate at Eve is the same for both decoders for a large enough $\mathtt{r}_{\mathtt{circ}}$.

Fig. 7 (g)-(i) show that in all approaches secrecy sum-rate grows as P_q increases. Hence, by using RxFJ and TxFJ, positive secrecy and arbitrary secrecy levels (by changing the links' transmit powers) are achievable, thus extending the same property that existed in the single-user scenario [2]. We also verified such a scaling at the per-link level. Same as what was discussed above, the secrecy sum-rate achieved for the full E-CSI method is larger than that of the robust methods. Also when ε is chosen to be too large, the nodes are not able to do an efficient interference management. This could sound as a counter-intuitive result. In fact, a low value of ε increases the probability of having zero secrecy (see SectionV). However, one can see that the performance of the robust approach is still acceptable for when $\varepsilon = 0.1$. We conjecture that this could be due to the *F-distrbution*, which was the distribution involved in reducing the best responses in (29) to (43). The F-distribution is a positively skewed distribution. Hence, most of the density of the distribution of best response is concentrated at the left of the median, and the mean is most likely at the left of the median. This means that to ensure that $(1-\phi_q) > \Pr\{b_q < d_q\}\frac{\mathrm{E}[\psi_q+\tau_q P_q' E_q\}]}{(1-\varepsilon)P_q} + \Pr\{b_q > d_q\}\frac{\mathrm{E}[\psi_q]}{(1-\varepsilon)P_q}$, the density of the values above the mean is relatively low, suggesting that the PA factor in (43) will be most likely providing positive secrecy[29].

Fig. 8 shows the convergence of the proposed asynchronous algorithm under different update schemes for a sample settings where the NE is unique. All update schemes converge to the same point, indicating the uniqueness of NE. The Jacobi method converges faster due to simultaneous updates for all users at each iteration. Fig. 8 (c) also shows convergence under random updates for each link. Each link generates a random integer in interval $[2, 6]$ that specifies the number of iterations after the current iteration when the link updates his action (i.e., the update pattern denoted by $\mathbb{T}_q$, see Section IV.B). Clearly, introducing asynchronism in the system degrades the convergence speed, but the system will eventually converge to the NE. It can also be seen

[29] In [1] we had a different simulation in which at a given iteration, when the NE uniquness is not achieveable, no link transmits. Because the robust methods enjoy better convergence behavior, we saw in that simulation that the performance of robust methods become superior to the full E-CSI case.



(a) (b) (c)

(d) (e) (f)

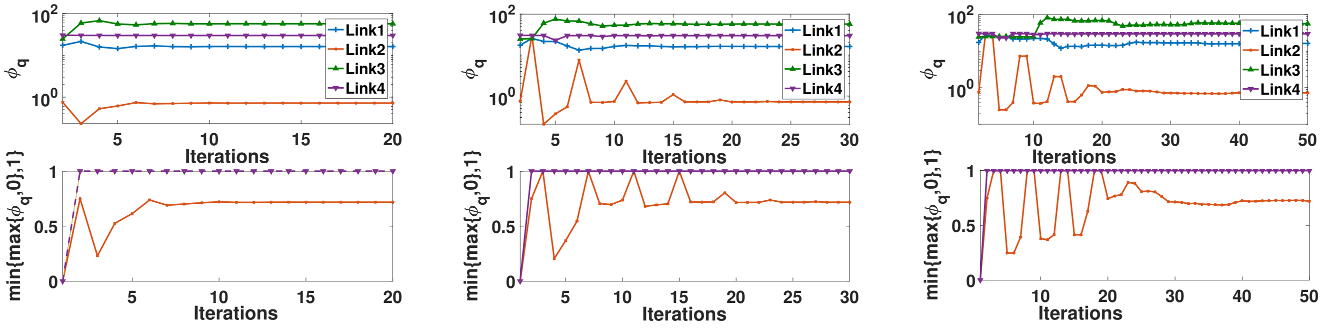
(g) (h) (i)

Fig. 7: (a)-(c): Comparison of secrecy sum-rate, (d)-(e): Comparison of information/leaked rate ($\mathtt{X}_e$= $\mathtt{Y}_e$= 5, $N_q = 8, M_q = L = 5, \forall q, Q = 4$), (g)-(i) Secrecy sum-rate vs. transmit power ($\mathtt{X}_e$= $\mathtt{Y}_e$= 0, $\mathtt{r}_{\mathtt{circ}} = 10$ m, $N_q = 8, M_q = L = 5, \forall q, Q = 4$)

from the figures of the bottom and above rows that the convergence occurs with and without $\min\{\max\{\bullet, 0\}, 1\}$ operator. Clearly, such an operator does not impact the convergence.

VII. Conclusions

In this paper, we proposed a game-theoretic approach for power control in an interference network tapped by an external eavesdropper. We proposed a framework under which every link can utilize both RxFJ and TxFJ to achieve a positive secrecy rate. Next, we modeled the



(a)

(b)

(c)

Fig. 8: Convergence of asynchronous algorithm for different update schemes: (a) Jacobi, (b) Gauss-Seidel, (c) Random updates.

interaction between the players as a game and derived sufficient conditions for the uniqueness of the resulting NE. We also proposed an asynchronous algorithm that can implement the proposed game and is robust to practical issues in the network such as transmission delays. Next, we proposed another version of our game that is robust to when the eavesdropping channels are unknown. We showed in simulation that our proposed approach for achieving positive secrecy using TxFJ and RxFJ are sufficient to be considered as best responses for legitimate links. Analytical characterization of the network model and proposed game when Eve uses MMSE decoder could be an interesting subject of future research.

Appendix A
Proof of Theorem 1

Using [28, Proposition 6.1], the fixed point iteration in (36) converges to a point ϕ^* from any initial point iff $\rho(\mathbf{A}+\mathbf{B}) < 1$. We now introduce the following theorem

Theorem 4. *[28, Ch. 2, Proposition 6.6] For any square matrix* $\mathbf{M}$ *and any* $\epsilon > 0$*, there exists an induced norm,* $||\bullet||$ *such that* $\rho(\mathbf{M}) \leq ||\mathbf{M}|| \leq \rho(\mathbf{M}) + \epsilon$[30]. □

Using the above theorem, since $\rho(\mathbf{A}+\mathbf{B}) < 1$, we can choose $\epsilon > 0$ arbitrarily close to zero such that $\rho(\mathbf{A}+\mathbf{B}) + \epsilon < 1$. Hence, we can find a an induced norm $||\mathbf{A}+\mathbf{B}||$ such that $||\mathbf{A}+\mathbf{B}|| \leq \rho(\mathbf{A}+\mathbf{B}) + \epsilon$. Therefore, we are 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:

[30] For the sake easy presentation, we omitted introducing the weighted norm, while this is the type of norm used in [28, Ch. 2, Proposition 6.6]. Nevertheless, all of our analyses can be extended to the case of weighted norms as well.

Definition 1. *[28] Consider the following iteration:*

$$\Phi^{(t+1)} = \mathcal{T}\left(\Phi^{(t)}\right),\ t = 1, 2, ..., \tag{53}$$

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

$$||\mathcal{T}(\Phi^{(1)}) - \mathcal{T}(\Phi^{(2)})|| \leq \Omega||\Phi^{(1)} - \Phi^{(2)}||\ ,\ \forall\{\Phi^{(1)}, \Phi^{(2)}\} \in \mathbb{A}^2, \tag{54}$$

where $||.||$ is a norm in $\mathbb{A}$ and $\Omega \in [0, 1)$, then the mapping $\mathcal{T}$ is a contraction mapping with Ω as the contraction modulus, and sequence $\left\{\phi^{(t)}\right\}$ generated by iterations in (53) *converges to the fixed point ϕ^*.*

Using this definition and the result of Theorem 4, we can show the iteration in (36) as a contraction mapping, i.e.,

$$||\mathcal{T}(\Phi^{(1)}) - \mathcal{T}(\Phi^{(2)})|| \leq ||(\mathbf{A} + \mathbf{B})(\Phi^{(1)} - \Phi^{(2)})|| \tag{55}$$

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

where $||\mathbf{A} + \mathbf{B}|| < 1$, (56) is due to Cauchy-Schwartz inequality, and the induced norm $||\bullet||$ is chosen such that for some $\epsilon > 0$ we have $||\mathbf{A} + \mathbf{B}|| \leq \rho(\mathbf{A} + \mathbf{B}) + \epsilon < 1$ (cf. Theorem 4). 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

$$\begin{aligned} \underset{\bar{\phi}}{\text{minimize}}\ \ & ||\bar{\phi} - \phi_0||^2 \\ \text{s.t.}\ \ & 0 \leq \bar{\phi} \leq 1. \end{aligned} \tag{57}$$

The KKT conditions of this problem are written as follows:

$$\bar{\phi} - \phi_0 - \nu + \lambda = 0, \tag{58}$$

$$\nu \geq 0, \bar{\phi} \geq 0, \nu\phi = 0 \tag{59}$$

$$\lambda \geq 0, \bar{\phi} \leq 1, \lambda(\phi - 1) = 0; \tag{60}$$

If $\nu > 0$, 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 $\nu = 0$, then $0 \leq \bar{\phi} \leq 1$. Hence, $\bar{\phi} = \phi_0$. Summarizing these conditions, we have

$$\bar{\phi}^* = \underset{0\leq\bar{\phi}\leq 1}{\text{argmax}}||\bar{\phi} - \phi_0||^2 = \begin{cases} 0, & \text{if } \phi_0 \leq 0, \\ 1, & \text{if } \phi_0 \geq 1, \\ \phi_0, & \text{if } 0 \leq \phi_0 \leq 1. \end{cases} \tag{61}$$

The right hand side of (61) 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 [28, Ch. 3, Proposition 3.2]:

$$\left|\left|\left[\mathcal{T}(\Phi^{(1)})\right]^+ - \left[\mathcal{T}(\Phi^{(2)})\right]^+\right|\right| \leq \left|\left|\mathcal{T}(\Phi^{(1)}) - \mathcal{T}(\Phi^{(2)})\right|\right| \tag{62}$$

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 $||\bullet||^2$ $\exists$ $\alpha_1 \in \mathbb{R}$ and $\alpha_2 \in \mathbb{R}$ such that $\alpha_1||\mathbf{x}||^1 \leq ||\mathbf{x}||^2 \leq \alpha_2||\mathbf{x}||^1$, $\forall \mathbf{x} \in \mathbb{R}^n$ [35]. Hence, we have the following chain of inequalities

$$\left|\left|\left[\mathcal{T}(\Phi^{(1)})\right]^+ - \left[\mathcal{T}(\Phi^{(2)})\right]^+\right|\right| \leq \left|\left|\mathcal{T}(\Phi^{(1)}) - \mathcal{T}(\Phi^{(2)})\right|\right| \tag{63}$$

$$\leq ||(\mathbf{A}+\mathbf{B})(\Phi^{(1)} - \Phi^{(2)})|| \leq ||\mathbf{A}+\mathbf{B}||\ ||\Phi^{(1)} - \Phi^{(2)}|| \tag{64}$$

Hence,

$$\left|\left|\left[\mathcal{T}(\Phi^{(1)})\right]^+ - \left[\mathcal{T}(\Phi^{(2)})\right]^+\right|\right| \leq ||\mathbf{A}+\mathbf{B}||\ \ \left|\left|\Phi^{(1)} - \Phi^{(2)}\right|\right|. \tag{65}$$

Setting the norm in (65) as the same norm in (56), the best response of each player is a contraction map, and thus has a unique fixed point (NE).

Appendix B
Proof of Theorem 2

Similar to the proof of Theorem 1, consider the following iteration:

$$\Phi^{(t+1)} = \mathcal{T}\left(\Phi^{(t)}\right),\ t = 1, 2, ..., . \tag{66}$$

We use the asynchronous convergence theorem [28], which is as follows:

Theorem 5. *The iteration in* (66) *converges asynchronously if the following conditions are satisfied:*

1) *There exists a sequence of nonempty sets* $\mathcal{X}(t)$ *such that*

$$\cdots \subset \mathcal{X}(t+1) \subset \mathcal{X}(t) \subset \cdots \subset \mathcal{X}. \tag{67}$$

2) *The iteration $\mathcal{T}(\bullet)$ must satisfy $\mathcal{T}(\Phi^{(t)}) \in (t+1)$. Furthermore, every limit point of $\Phi^{(t)}$ must be a fixed point of $\mathcal{T}(\bullet)$.*
3) *For every t, we must have $\mathcal{X}(t) = \mathcal{X}_1(t) \times \cdots \times \mathcal{X}_Q(t)$ where $\mathcal{X}_q(t) \subset \mathcal{X}_q$, $q \in \mathcal{Q}$.*

□

The first item of Theorem 5 can be proven as follows. let $\Phi^* = [\Phi_1^*, \ldots, \Phi_Q^*]^T$ be the fixed point of the iteration in (66). Consider the following set

$$\mathcal{X}_q(t) = \{\Phi \in \mathbb{A} : ||\Phi - \Phi^*||_{2,\text{block}} \leq \alpha^t ||\Phi^{(0)} - \Phi^*||_{2,\text{block}}\} \subset \mathbb{A} \tag{68}$$

where $\mathbb{A} = \{\Phi \in \mathbb{R}^Q : 0 \leq \Phi \leq 1\}$, $||\mathbf{a}||_{2,\text{block}} = \max_{q\in\mathcal{Q}} ||\mathbf{a}_q||_2$ is the vector block-maximum norm for $\mathbf{a} = [\mathbf{a}_1, \ldots, \mathbf{a}_Q]^T$ with $|| \bullet ||_2$ defined as the Euclidean norm, and $\alpha = ||\mathbf{A} + \mathbf{B}||$ with $\mathbf{A}$ and $\mathbf{B}$ defined in (34) and (35). It can be easily seen that iff $\alpha < 1$ we have

$$\alpha^{t+1} ||\Phi^{(0)} - \Phi^*||_{2,\text{block}} < \alpha^t ||\Phi^{(0)} - \Phi^*||_{2,\text{block}}, \ \forall n = 0, 1, \ldots. \tag{69}$$

Hence, we can conclude that

$$\mathcal{X}(t+1) \subset \mathcal{X}(t) \subset \mathbb{A}, \ t = 1, 2, \ldots. \tag{70}$$

The second item of Theorem 5 can be concluded from Theorem 1. As for the third item of Theorem 5, consider the following. The set $\mathcal{X}(t) = \mathcal{X}_1(t) \times \cdots \times \mathcal{X}_Q(t)$ can be decomposed as follows for all t:

$$\mathcal{X}_q(t) = \{0 \leq \Phi_q \leq 1 : ||\Phi_q - \Phi_q^*|| \leq \alpha^t ||\Phi^{(0)} - \Phi^*||_{2,\text{block}}\}. \tag{71}$$

Hence, all three conditions required for asynchronous convergence of Algorithm 1 can be satisfied provided that Theorem 1 holds.

APPENDIX C
PROOF OF THEOREM 3

Without loss of generality assume that Ω represents a set of multiple independent (fictitious) Eves, whose locations (inside a given area) follows the PPP distribution with density λ. Obviously, these multiple Eves can be simplified to one Eve provided that a certain density and a certain area are given. Denote $e \in \Omega$ as an arbitrary Eve. Using expectation by conditioning, the probability in (45) can be written as

$$\Pr\{\Gamma\gamma < \nu\} = \underset{\Omega}{E}\left[\prod_{e\in\Omega}\Pr\{\Gamma_e\gamma_e < \nu|\Omega\}\right] \tag{72a}$$

$$= \underset{\Omega}{E}\left[\exp\left(\sum_{e\in\Omega}\log\Big(\Pr\{\Gamma_e\gamma_e < \nu|\Omega\}\Big)\right)\right]. \tag{72b}$$

In our scenario, each Bob assumes Eves are distributed according to the PPP Ω in a circle around him with radius d_0. The relation between d_{qe} and d'_{qe} can be written as $d_{qe} = \sqrt{{d_{qq}}^2 + {d'_{qe}}^2 - 2d_{qq}d'_{qe}\cos\varphi}$, where φ is the angle between d'_{qe} and d_{qq} that is uniformly distributed in the range $[0, 2\pi]$. Thus,

$$\Gamma = \Big(\frac{\beta}{\sqrt{{d_{qq}}^2 + \beta^2 - 2d_{qq}\beta\cos\varphi}}\Big)^{\eta}. \tag{73}$$

Let $d'_{qe} = \beta$. The expectation in (72b) is equivalent to *Laplace functional* of a point process, so (72a) can be reduced to [29, Ch. 7]

$$\Pr\{\Gamma\gamma < \nu\} = \exp\Bigg(-\lambda\int_0^{d_0}\int_0^{2\pi}\Pr\Big\{\Big(\frac{\beta}{\sqrt{{d_{qq}}^2 + \beta^2 - 2d_{qq}\beta\cos\varphi}}\Big)^{\eta}\gamma > \nu\Big\}\beta d\beta d\varphi\Bigg). \tag{74}$$

Let $\S_q \triangleq \Big(\frac{\beta}{\sqrt{{d_{qq}}^2+\beta^2-2d_{qq}\beta\cos\varphi}}\Big)^{\eta}$, $q \in \mathcal{Q}$. The quantity γ in (74) is the SINR of a one-branch diversity combiner with N_q interferers whose CDF is [33]

$$F_X(\gamma) = 1 - \frac{1}{1+\gamma}. \tag{75}$$

Using (75) in (74), we end up with

$$\Pr\{\S_q\gamma > \nu\} = \Big(1 + \frac{|\mathbf{d}_q^{\dagger}\mathbf{H}_{qq}|^2}{\S_q\tau_q|\mathbf{d}_q^{\dagger}\mathbf{H}'_{qq}|^2}\Big)^{-N_q}. \tag{76}$$

References

[1] P. Siyari, M. Krunz, and D. N. Nguyen, "Joint transmitter- and receiver-based friendly jamming in a MIMO wiretap interference network," in *Proc. IEEE ICC 2017 Conf. Workshops*, May 2017, pp. 1323–1328.

[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] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[5] Q. Li, Y. Zhang, J. Lin, and S. X. Wu, "Full-duplex bidirectional secure communications under perfect and distributionally ambiguous eavesdropper's CSI," *IEEE Trans. Signal Process.*, vol. 65, no. 17, pp. 4684–4697, Sep. 2017.

[6] P. Siyari, M. Krunz, and D. N. Nguyen, "Friendly jamming in a MIMO wiretap interference network: A nonconvex game approach," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 601–614, Mar. 2017.

[7] 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.

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

[9] Z. Zhang, K. C. Teh, and K. H. Li, “Distributed optimization for resilient transmission of confidential information in interference channels,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 494–501, Jan. 2017.

[10] 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.

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

[12] 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.

[13] 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.

[14] B. Akgun, O. O. Koyluoglu, and M. Krunz, “Exploiting full-duplex receivers for achieving secret communications in multiuser MISO networks,” *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 956–968, Feb. 2017.

[15] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, “Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5511–5526, Aug. 2016.

[16] D. Bharadia, E. McMilin, and S. Katti, “Full duplex radios,” in *Proc. ACM SIGCOMM Conference*, 2013, pp. 375–386.

[17] A. C. Cirik, Y. Rong, and Y. Hua, “Achievable rates of full-duplex MIMO radios in fast fading channels with imperfect channel estimation,” *IEEE Trans. Signal Process.*, vol. 62, no. 15, pp. 3874–3886, Aug. 2014.

[18] D. Bharadia and S. Katti, “Full duplex MIMO radios,” in *Proc. USENIX NSDI 2014 Conf.*, 2014, pp. 359–372.

[19] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, “Full-duplex MIMO relaying: Achievable rates under limited dynamic range,” *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1541–1553, Sep. 2012.

[20] T. M. Duman and A. Ghrayeb, *Coding for MIMO Communication Systems*. New York, NY, USA: John Wiley and Sons, Ltd, 2007.

[21] 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.

[22] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, “Transmit solutions for MIMO wiretap channels using alternating optimization,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

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

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

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

[26] F. Wang, M. Krunz, and S. Cui, “Price-based spectrum management in cognitive radio networks,” *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 74–87, Feb 2008.

[27] A. Muqattash and M. Krunz, “POWMAC: a single-channel power-control protocol for throughput enhancement in wireless ad hoc networks,” *IEEE J.Sel. Areas Commun.*, vol. 23, no. 5, pp. 1067–1084, May 2005.

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

[29] M. Haenggi, *Stochastic Geometry for Wireless Networks*. New York, NY, USA: Cambridge University Press, 2012.

[30] X. Zhang, X. Zhou, and M. R. McKay, “Enhancing secrecy with multi-antenna transmission in wireless Ad Hoc networks,” *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[31] T. X. Zheng, H. M. Wang, J. Yuan, Z. Han, and M. H. Lee, “Physical layer security in wireless Ad Hoc networks under a hybrid full-/half-duplex receiver deployment strategy,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.

[32] P. Siyari, M. Krunz, and D. N. Nguyen, “Secure communications via power control in a mimo wiretap interference network with jamming transmitters and receivers,” University of Arizona Department of ECE, Tech. Rep., 2017. [Online]. Available: http://wireless.ece.arizona.edu/sites/default/files/jsac18_peyman.pdf

[33] 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.

[34] S. Ross, *Introduction to Probability and Statistics for Engineers and Scientists*. Elsevier Science, 2009.

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