Distributed Power Control in Single-Stream MIMO Wiretap Interference Networks With Full-Duplex Jamming Receivers

Peyman Siyari, Marwan Krunz, *Fellow, IEEE*, and Diep N. Nguyen

***Abstract*—We consider a multi-link interference network that is tapped by an external eavesdropper. To conceal information from the eavesdropper, legitimate links are equipped with *transmitter-based friendly jamming* (TxFJ) and *receiver-based friendly jamming* (RxFJ). Each link seeks to maximize its secrecy rate by determining the best power assignment (PA) for the information, TxFJ, and RxFJ signals. Joint optimization of these parameters is a non-convex problem. Hence, we seek sub-optimal solutions. Specifically, we find a lower bound on the allocated power to TxFJ above which positive secrecy is achievable for a given link. Once positive secrecy is achieved, the secrecy rate becomes monotonically increasing in the power at the transmitter (Alice). Therefore, the rest of Alice's power is allocated to the information signal. Despite its sub-optimality, such an approach precludes the possibility of employing successive interference cancellation by the eavesdropper. The RxFJ PA of a link is adjusted using an on-off PA that depends only on the link's local channel state information (CSI). With every link following such a strategy, we model this interaction as a non-cooperative game. 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 eavesdropper's CSI (E-CSI) and propose a framework that is robust to unknown E-CSI. Our results indicate that this robust framework performs close to when E-CSI is fully known to legitimate links. Moreover, empirically it is shown that the secrecy sum-rate scales with the power budget of transmitters.**

Manuscript received March 22, 2018; revised August 31, 2018 and November 12, 2018; accepted November 14, 2018. Date of publication November 23, 2018; date of current version December 18, 2018. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Laura Cottatellucci. This work was supported in part by the NSF under Grants CNS-1409172, CNS-1513649, CNS-1731164, and IIP-1822071, in part by Australian Defense Science and Technology Group, in part by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under Grant number 102.04-2016.23, and in part by the Qatar Foundation under Grant NPRP 8-052-2-029. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the NSF, and QF. This paper was presented in part at the IEEE International Conference Communication 2017, Workshop on Full-duplex Communications for Future Wireless Networks, May 2017. *(Corresponding author: Peyman Siyari.)*

P. Siyari is with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA (e-mail: psiyari@email.arizona.edu).

M. Krunz is with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA, and also with the Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW 2007 Australia (e-mail: krunz@email.arizona.edu).

D. N. Nguyen is with the Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW 2007 Australia, and also with Posts and Telecommunications Institute of Technology, Vietnam (e-mail: diep.nguyen@uts.edu.au).

Digital Object Identifier 10.1109/TSP.2018.2883008

***Index Terms*—Interference network, friendly jamming, full-duplex radios, game theory, distributed design.**

I. Introduction

A. Motivation

PHYSICAL-LAYER (PHY-layer) security has recently gained considerable attention because of its potential to provide secrecy in scenarios where it is either expensive or computationally demanding to use cryptographic methods. The most basic model for information-theoretic PHY-layer security is the so-called *wiretap channel*. The wiretap channel involves communication between a legitimate transmitter (Alice) and a corresponding receiver (Bob); such communication 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 uses multiple antennas and a portion of her transmit power to create a bogus signal –known as *artificial noise* or *transmitter-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. In addition to 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] Despite having a similar effect as the TxFJ method, CJ approaches face several implementation challenges related to mobility, trustworthiness, and synchronization.

To address these challenges, some authors suggested equipping Bob with in-band full-duplex (FD) capabilities, allowing him to generate his own friendly jamming signal while receiving the information signal from Alice [3], [4]. Such an FJ signal is hereafter referred to as *receiver-based friendly jamming* (RxFJ) [3]. Using RxFJ, many of the disadvantages of CJ can be mitigated. Other works study PHY-layer security with FD capability at both Alice and Bob for bidirectional communica-

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

tions, i.e., Bob transmits information signals to Alice rather than generating RxFJ (see [5] and references therein).

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, legitimate links may or may not be interested in listening to the transmissions of their neighboring links. In the former case, 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*.

B. Overview of Proposed Approach

In this paper, we study PHY-layer security in a multi-link wiretap channel. In our network model, legitimate links share the same bandwidth, 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 RxFJ power, and the power assignment (PA) between the information and TxFJ signals. The joint optimization of these parameters is a non-convex, computationally intractable problem. To address it, instead we seek sub-optimal solutions but distributed solutions that can be implemented by individual links.

Our work is motivated by the following simple observation: For a given link, when no secrecy is required, the higher the power budget at Alice, the higher is the information rate at the intended receiver (Rx). However, when secrecy is also a requirement, although the information rate still increases monotonically with Alice's power, the secrecy rate may not necessarily behave as such because more power transmitted from Alice also increases the leakage rate at Eve [2]. Motivated by this observation, we find a lower bound on the TxFJ power above which positive secrecy is achievable for a given link. Once positive secrecy is achieved, the secrecy rate becomes a monotonically increasing function of Alice's power, thus having the same trend as the information rate. Therefore, the rest of Alice's power can be allocated to the information signal. 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. In contrast, when the aim is to maximize the sum of secrecy rates, we cannot ensure that every link achieves a non-zero secrecy rate [6]. 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. By ensuring that every link achieves a non-zero secrecy rate, Eve cannot apply SIC.[2]

We assume that when legitimate nodes set their transmission parameters, there is no centralized authority responsible for computations and optimization. Hence, links have to make distributed decisions. 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 these interactions between legitimate links using the theory of non-cooperative games.

C. Related Work

The works in [9]–[11] studied secure precoding in wiretap interference networks. Moreover, the authors in [12] studied power control in a multi-channel interference network without considering TxFJ and RxFJ. All of these works assumed that Alice has full knowledge of the eavesdropper's channel state information (E-CSI), which may not be a practical assumption. Regarding the power assignment between the information and TxFJ signals, the works in [13] and [14] focused only on a single-link scenario, and their approaches are not extendable to the case of multiple links. The authors of [15] exploited full-duplex capability at 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 tradeoff in minimizing downlink and uplink powers, subject to certain constraints on information and secrecy rates of downlink and uplink users. The work in [16] studied power minimization for the information, TxFJ, and RxFJ signals in a broadcast channel with confidential messages under given guarantees on the secrecy rate for each Bob. Power minimization was done at the BS in *centralized* fashion (the BS must acquire the CSI between itself and all downlink users). We investigate a more challenging scenario (i.e., interference channel) where contrary to [16], distributed computation and 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 for each given link.
- We propose a non-cooperative game to model the power control problem in the interference network under study. Assuming first that Alice-/Bob-Eve channels are fully known, we derive sufficient conditions under which the proposed non-cooperative game admits 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 a 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.

[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 signal-to-interference-plus-noise-ratio (SINR) while snooping on other transmissions with non-zero secrecy rates.

- 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 should emphasize that in this paper, we first propose a distributed design under full knowledge of E-CSI. Although availability of E-CSI at all links is not a practical assumption, we use this case to build foundations for our distributed algorithm and establish important performance metrics. After conducting such analysis, we then relax knowledge of E-CSI and propose a version of our algorithm that is robust to uncertainties in E-CSI knowledge.

Notation: Boldface uppercase/lowercase symbols denote matrices/vectors. $\mathbf{a} \geq \mathbf{b}$ denotes 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 the expected value, complex conjugation, 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 ($Q \geq 2$), $\text{Alice}_1, \ldots, \text{Alice}_Q$, that communicate with their respective receivers, $\text{Bob}_1, \ldots, \text{Bob}_Q$. 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 imperfect SIS.[4] This self-interference model was adopted in several works (see [15], [18]), and practical implementations of it exist in the literature (see e.g., [19]).[5] $\mathbf{m}_r \in \mathbb{C}^{M_r}$, $r \in \mathcal{Q}$ is the RxFJ signal created by Bob_r, which is a zero mean circularly symmetric complex Gaussian random variable (ZMCSCG-RV) with covariance matrix of $E[\mathbf{m}_r\mathbf{m}_r^\dagger] = p'_r\mathbf{I}$ where p'_r is RxFJ power. $\mathrm{Tr}(\mathbf{m}_q\mathbf{m}_q^\dagger) = M_q p'_q \leq P'_q$ where P'_q denotes the power limit at Bob_q for RxFJ. $\mathbf{H}'_{rq} \in \mathbb{C}^{M_q \times M_r}$, $r \neq q$, 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 $\tilde{\mathbf{H}}_{rq} = \bar{\mathbf{H}}_{rq}d_{rq}^{-\eta/2}$, 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. $\mathbf{G}'_q \in \mathbb{C}^{L \times M_q}$ 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 statistical characteristics as $\mathbf{n}_q$. For Alice_q, $q \in \mathcal{Q}$, its transmitted 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 $\mathbf{T}_q \in \mathbb{C}^{N_q}$ is the precoder and $x_q \in \mathbb{C}$ is the information signal. In other words, we use multiple transmit and receive antennas at each link to achieve MIMO diversity gain, and spatial multiplexing gain, i.e., multiple antennas are used for *beamforming*.[6]

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 fraction 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.[7] 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 $\mathbf{V}_q^{(2)}$ denotes 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 $\tilde{\mathbf{H}}_{qq}$.[8] The information signal 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 , achieving the

[3] 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] 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, leading to residual self-interference at the receive chain [17].

[5] We assume that FD receivers are not experiencing dynamic range issues that cause the additive noise at the receive chain to be dependent on the transmit power of the FD device. Relaxing this assumption is a subject for future research.

[6] Later on, we explain the rationale behind this choice.

[7] Notice that the TxFJ power is distributed uniformly between various 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 distribution of TxFJ power among different dimensions of $\mathbf{v}_q$ is optimal (see [2], [13]).

[8] 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.

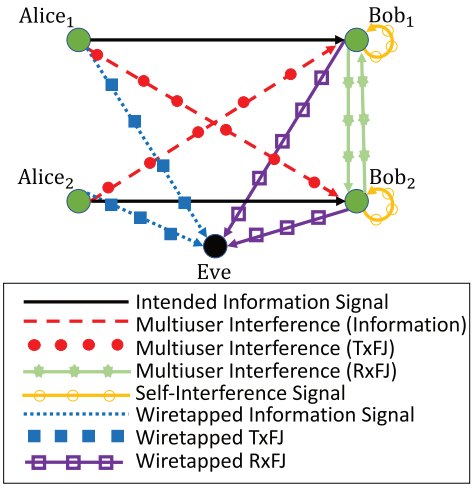

Fig. 1. System model.

maximum transmit-diversity gain [20]. Let $\mathbf{H}_{qq} \triangleq \tilde{\mathbf{H}}_{qq}\mathbf{V}_q^{(1)}$, $\mathbf{H}_{j_{qq}} \triangleq \tilde{\mathbf{H}}_{qq}\mathbf{V}_q^{(2)}$, $\mathbf{H}_{qr} \triangleq \tilde{\mathbf{H}}_{qr}\mathbf{V}_q^{(1)}$, $\mathbf{H}_{j_{qr}} \triangleq \tilde{\mathbf{H}}_{qr}\mathbf{V}_q^{(2)}$, $\mathbf{G}_q \triangleq \tilde{\mathbf{G}}_q\mathbf{V}_q^{(1)}$, and $\mathbf{G}_{j_q} \triangleq \tilde{\mathbf{G}}_q\mathbf{V}_q^{(2)}$. 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 the other link. 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. Assuming that $\mathbf{d}_q^\dagger\mathbf{H}_{j_{qq}}\mathbf{v}_q = 0$,[9] an estimate of x_q is given by:

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

Hence, the information rate for the qth link is expressed as:

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

where

$$a_q \triangleq \tag{6a}$$

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

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

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

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

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

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

where

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

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

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

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

The linear receivers $\mathbf{d}_q$ and $\mathbf{r}_q$, $q \in \mathcal{Q}$, are chosen according to the maximal ratio combining (MRC) [20] method so as to maximize the reception of the 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 $\tilde{\mathbf{H}}_{qq} = \mathbf{U}_q\mathbf{\Sigma}_\mathbf{q}\mathbf{V}_q^\dagger$). Using this linear receiver, the TxFJ signal of Alice$_q$ will be nullified at Bob$_q$. In other words, $\mathbf{d}_q^\dagger\mathbf{H}_{j_{qq}}\mathbf{v}_q = 0$. Let $\tilde{\mathbf{G}}_q = \mathbf{L}_q\mathbf{D}_q\mathbf{R}_q$ be the SVD of $\tilde{\mathbf{G}}_q$ where $\mathbf{L}_q$ and $\mathbf{R}_q$ are matrices of left and right singular vectors, respectively, and $\mathbf{D}_q$ is the diagonal matrix of singular values in descending order. Thus, while eavesdropping on the qth link,

[9]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 so that this assumption holds.

[10]Because none of the links knows whose transmission Eve is interested in, each link tries to protect its own transmission from Eve. Thus, the secrecy rate of each link can be determined by (10) (see [21]).

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 cases where Eve 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 for the TxFJ signal for each link depends only on the channel between the two nodes comprising that link, which is relatively more practical to obtain.

Our choice of the beamforming vector $\mathbf{T}_q$ comes from the fact that the number of antennas at Eve may not be known. 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.

III. Problem Formulation

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

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

Due to the non-concavity of the objective function in (11) w.r.t. the decision variables,[12] the optimization in (11) is non-convex. To find a tractable (and yet suboptimal) solution, we decompose the analysis of RxFJ and power assignment (PA) between information and TxFJ signals into two sub-problems. We first propose a tractable solution for p'_q. Then, we propose a method to find a suboptimal PA between information and TxFJ signals.

A. Computation of RxFJ Power

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

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

One can do a simple one-dimensional search to find the optimal value of p'_q. However, such an approach demands knowledge of multiuser interference (MUI) at Eve (i.e., c_q), which may not be available to Bob_q. In the remainder of this section, we propose a a different method for setting the RxFJ power. While at first it may seem that our method requires knowledge of MUI at Eve, we later show that this method can be relaxed to handle the case when knowledge of Eve's MUI is not available.

We first obtain conditions that result in positive secrecy at link q. Positive secrecy in (10) is achievable if and only if the objective value in (12) is larger than one. It can be easily shown that this is true if and only if the optimal objective value of the following optimization is larger than one:[13]

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

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 a set of conditions/solutions that result in positive secrecy, we can examine these solutions by checking the objective value they yield for (13) instead of (12). The first and second derivatives of $g(p'_q)$ are as follows:

$$\frac{\partial g(p'_q)}{\partial p'_q} = -\frac{b_q c_q - a_q d_q}{(a_q + b_q p'_q)^2} \tag{14a}$$

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

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

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

Simplifying the first condition of (15), a threshold for SIS factor can be established[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), (15) often yields the optimal RxFJ power, signifying that the solution to (13) is very likely the optimal solution to (12) as well.

Considering (16), we can conclude the following: Given c_q and d_q, if the (normalized) MUI at Bob_q (a_q) is not as strong as the (normalized) self-interference channel ($\frac{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}$), i.e., if $\frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 a_q}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$ is small, the power of RxFJ should be very weak to maintain positive secrecy, leading to ${p'_q}^* = 0$. However, if

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

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

[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 lost, one can set a minimum RxFJ power to prevent RxFJ from going to zero.

$\frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 a_q}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$ 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. Specifically, a large d_q/c_q indicates that RxFJ degrades Eve's reception more than the MUI received at Eve (c_q). Hence, smaller SIS suppression (i.e., larger τ_q) is allowed, indicating that $p_q'^* = P_q'$ becomes the favorable solution.

It can be seen in (15) that the optimal RxFJ power that solves (13) depends on two factors: MUI at Bob$_q$ (i.e., a_q) and MUI at Eve while eavesdropping on the qth link (i.e., c_q). It may not be practical for a legitimate node to know the MUI at Eve. Later on, we show that using a specific technique in setting TxFJ can help us to mitigate the dependence on Eve's MUI.

B. PA Between TxFJ and Information Signals

After finding a set of conditions/solutions for RxFJ power (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). This is done through the following formulation:

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

Although the optimal ϕ_q can be found via a simple one-dimensional search, we would like to eventually solve (17) without requiring knowledge of Eve's MUI. In this part of the paper, we propose a solution to (17) in the perfect E-CSI scenario. Later on, we show that our approach is extendable to the case of unknown E-CSI.

Similar to the approach taken in the previous section, 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 the TxFJ power of Alice$_q$ (i.e., σ_q) because according to (9a), c_q is a function of σ_q. Reducing (19) gives us a bound on the portion of power allocated to the information signal (i.e., ϕ_q) shown in (20). For ease of presentation, we do not introduce the new notations in (20) yet; we do so in in the next section. We refer to (19) as *the lower-bound on TxFJ power of link q to guarantee positive secrecy*.

$$\phi_q \le \max\left\{ \min\left\{ 1 - \frac{1}{P_q} \sum_{\substack{r=1 \\ r \ne q}}^{Q} \{ (A_{q,r} - B_{q,r})\, \phi_r P_r + C_{q,r} P_r + D_{q,r} p_r' \} - \frac{p_q'}{P_q} E_q - \frac{F_q}{P_q} \delta, 1 \right\}, 0 \right\} \tag{20}$$

To make use of this lower bound, we first introduce the following result.

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

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

$$c_q = a_q + (b_q - d_q) p_q' + \delta \tag{21}$$

where $\delta > 0$ is a positive real value. Replacing the term c_q in (9a) with the RHS of (21), and taking the derivative of (10) (without the $\max\{\bullet\}$ operator) w.r.t. P_q and ϕ_q, we have

$$\frac{\partial C_q^{sec}}{\partial P_q} = \frac{\phi_q \delta}{(a_q + \phi_q P_q + b_q p_q')(a_q + \phi_q P_q + b_q p_q' + \delta)} \tag{22a}$$

$$\frac{\partial C_q^{sec}}{\partial \phi_q} = \frac{P_q \delta}{(a_q + \phi_q P_q + b_q p_q')(a_q + \phi_q P_q + b_q p_q' + \delta)} \tag{22b}$$

which are both positive, and hence the lemma is proven. ■

Recall that in setting the RxFJ power in (15), we observed that its optimal value $p_q'^*$ depends on Eve's and Bob$_q$ MUI. 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:

$$p_q'^* = \begin{cases} P_q', & \text{if} \quad b_q < d_q \\ 0, & \text{if} \quad b_q > d_q. \end{cases} \tag{23}$$

Using the bound in (19), the following property shows the sufficiency of (23) to conclude (15).

Proposition 1: Provided that the following conditions hold, the conditions on the optimal RxFJ power in (23) imply those of (15):

- c_q satisfies (19) and $a_q + (b_q - d_q) p_q' + \delta > 0$.
- $(b_q - d_q) P_q' + \delta < 0$ when $b_q < d_q$

Proof: Assume that (23) is used to obtain the RxFJ power of link q. Hence, we set $p_q'^* = P_q'$ when $b_q < d_q$. If $a_q + (b_q - d_q) p_q' + \delta > 0$ and c_q satisfies (19) (first condition of Proposition 1), then $c_q = a_q + (b_q - d_q) P_q' + \delta > 0$ when $b_q < d_q$. Assuming that $(b_q - d_q) P_q' + \delta < 0$ (second condition of Proposition 1), one can conclude that $a_q > c_q$, or equivalently $a_q > a_q + (b_q - d_q) P_q' + \delta$. Hence, $b_q < d_q$ is readily sufficient to deduce $b_q < \frac{a_q d_q}{c_q}$ that appears 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 (23). Given (19) and $p_q' = 0$, c_q must

satisfy $c_q = a_q + \delta$, and since $\delta > 0$, $a_q < c_q$. Therefore, $b_q > d_q$ is sufficient to deduce $b_q > \frac{a_q d_q}{c_q}$ that appears in (15). ■

Remark 1: If $b_q < d_q$ 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 schemes in (15) and (23) result in ${p'_q}^* = P'_q$. However, when $b_q < d_q$ (suggesting ${p'}^*_q = P'_q$ in (23)) but $c_q = a_q + (b_q - d_q)P'_q < 0$, we have $b_q > \frac{a_q d_q}{c_q}$ (suggesting ${p'}^*_q = 0$ in (15)). Hence, we have conflicting decisions made by (15) and (23). Condition $(b_q - d_q)P'_q + \delta < 0$ sets an upper bound on δ, i.e., $0 < \delta < (d_q - b_q)P'_q$ if $b_q < d_q$. According to (6) and (9), the terms b_q and d_q are in fact functions of self-interference, Alice-Bob, Bob-Eve, and Alice-Eve channels. Hence, if Proposition 1 holds, Bob_q only has to check whether or not

$$\tau_q < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_q|^2} \tag{24}$$

to decide whether RxFJ is needed or not. In other words, (23) is sufficient to set the RxFJ power of Bob_q.[15] The intuitive interpretation of (24) 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 enough, 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), the RxFJ power assignment in (23) is more desirable, as it does not require real-time tracking of Eve's MUI at Bob_q.

Combining (19) and (23), we have

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

Since the inequalities in (25) are strict, we write the following:

$$\begin{cases} c_q = a_q + (b_q - d_q)P'_q + \delta, & \text{if} \quad b_q < d_q \\ c_q = a_q + \delta, & \text{if} \quad b_q > d_q \end{cases}. \tag{26}$$

Using mathematical manipulations of Equations (18)–(26), we can convert problem (17) to the following problem:

$$\begin{aligned} &\underset{\phi_q,\, \delta}{\text{maximize}} \quad C_q^{sec} \\ &\text{s.t.} \quad c_q = a_q + (b_q - d_q){p'_q}^* + \delta \\ &c_q > 0 \\ &0 < \delta < (d_q - b_q)P'_q + J(1 - t_q) \\ &0 \le \phi_q \le 1 \end{aligned} \tag{27}$$

where ${p'_q}^*$ in the first constraint is set according to (23), J is a sufficiently large positive number, and

$$t_q = \begin{cases} 1 & \text{if} \quad b_q < d_q \\ 0 & \text{if} \quad b_q > d_q \end{cases}. \tag{28}$$

[15]The sufficiency of (23) is examined in [23, Fig. 3] but is skipped in this paper due to space limitation.

The first constraint in (27) is a constraint on ϕ_q, which is needed so that the optimal solution yields positive secrecy.[16] In other words, this constraint replaces the more general constraint in (17), so 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 (27) ensure that setting ${p'_q}^*$ according to (23) is sufficient to satisfy the more general conditions in (15). Note that t_q is not a decision variable of (27), and can be easily computed by knowing b_q and d_q.

Because c_q is a function of ϕ_q, one can simplify the first constraint in (27) to find the value of ϕ_q that yields positive secrecy for the objective of (27). However, we still need to determine the value of δ to ensure that such value found for ϕ_q is the optimal one for problem (27). A simple one-dimensional search in the interval defined by the third constraint in (27) 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 obtain δ. On the one hand, we do not wish to choose δ near its upper bound due to the fact that a higher δ increases the lower bound on TxFJ, which subsequently decreases the amount of power allocated to the information signal. On the other hand, selecting δ close to zero is also not desirable, as in (22b) the growth rate of secrecy rate would be decreased. Hence, we choose $\delta = \frac{1}{2}|d_q - b_q|P'_q$. We show later that this heuristic choice of δ yields a performance close to that of the optimal solution found by a one-dimensional search.

IV. Game Formulation

In this section, using the ideas in Section III, we propose a power control scheme based on non-cooperative games. The first constraint in (27) can be written in a general form, as follows

$$\begin{cases} c_q \ge a_q + (b_q - d_q)P'_q + \delta, & \text{if} \quad b_q < d_q \\ c_q \ge a_q + \delta, & \text{if} \quad b_q > d_q. \end{cases} \tag{29}$$

Simplifying (29) and taking into account the other constraints of (27), an upper bound on ϕ_q can be written as in (20), with $\delta = \frac{1}{2}|d_q - b_q|P'_q$ and the newly introduced notations in (20) are given in (30):

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

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

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

[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 (20). In (27), however, for the sake of simplicity, we present this constraint in a more compact form.

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

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

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

Hence, link q's optimization problem in (27), where $q \in \mathcal{Q}$, can be written as

$$\begin{aligned} \underset{\phi_q}{\text{maximize}} \quad & C_q^{sec} \\ \text{s.t.} \quad & (20). \end{aligned} \tag{31}$$

With every legitimate link following such a strategy, the resulting interaction between them can be modeled as a non-cooperative game, where players are 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. According to Lemma 1, upon achieving positive secrecy for link q (i.e., satisfying the constraint in (31)), the secrecy rate becomes a monotonically increasing function of ϕ_q. Hence, the best-response of the qth link, $q \in \mathcal{Q}$, is when ϕ_q meets its upper bound in (20) 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.

A. Existence and Uniqueness of Nash Equilibrium

The first game-theoretic analysis that we perform is to examine whether the game characterized by (31) admits a NE. 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 [24]. Convexity of each player's strategy set is easy to prove, and thus omitted for brevity. Replacing c_q with $a_q + (b_q - d_q)P'_q + \delta$ in (10) (as the first constraint in (27) suggests) and taking the second derivative of (10) w.r.t. ϕ_q, we have:

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

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.

Theorem 1: The game in (31), for which the best response of each player is when (20) holds with equality, has a unique NE iff:

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

where $\rho(\bullet)$ indicates the spectral radius of a matrix (i.e., largest absolute value of eigenvalues of a matrix), $\mathbf{A}$ is a matrix whose (q,r) element, $\forall (q,r) \in \mathcal{Q}^2$, is given by

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

and $[\mathbf{B}]_{q,r}, \forall (q,r) \in \mathcal{Q}^2$ is defined as:

$$[\mathbf{B}]_{q,r} \triangleq \begin{cases} \dfrac{P_r}{P_q}B_{q,r}\ , & r \neq q \\ 0\ , & r = q \end{cases}. \tag{35}$$

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

Proof: The uniqueness of NE can be proven by leveraging the fixed-point theorem. In fact, if the iterative computation of each player's best-response (i.e., ϕ_q meeting its upper bound in (20) with equality for all q) has a fixed point, the convergence point is the NE of the game [25]. We first analyze the existence of a fixed point for the argument inside $\max\{\min\{\bullet,1\},0\}$ in (20). Then, we extend the analysis to include $\max\{\min\{\bullet,1\},0\}$. Concatenating the best responses of all links, the following fixed-point problem in its $n-$th iteration can be established:

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

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 other terms in (20) for all q. The rest of the proof is presented in [23, Appendix A]. ■

Remark 2: Using the condition in (33), the convergence of the Jacobi iterative algorithm in the sense of [25, 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 [25, Ch. 6]).

B. Algorithm Design

We now design an algorithm to implement the proposed power control game. 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 $\Theta_q^{(n)} = \{\theta_{1,q}^{(n)}, \ldots, \theta_{Q,q}^{(n)}\}$ 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 shown in Algorithm 1. Other termination criteria can be used instead of the maximum iteration number.

Special cases of the asynchronous scheme include Jacobi (or simultaneous) and Gauss-Seidel (or sequential)

Algorithm 1: Asynchronous Iterative Secure Power Allocation (Full E-CSI Version).

1: Set p'_q and δ according to (23) and Proposition 1 (see Section III).
2: **for** n=1 to `maximum iteration` **do**
3: Set $\phi_q^{(n)} = \begin{cases} \text{Equal to RHS of (20),} & \text{if } n \in \mathbb{T}_q \\ \phi_q^{(n-1)} & \text{otherwise} \end{cases}$, $\forall(q) \in \mathcal{Q}$.
4: **end for**

schemes [25]. The Jacobi scheme can be described as follows ($q \in \mathcal{Q}$):

$$\mathbb{T}_q = \{1, 2, \ldots, it_{\max}\}$$

$$\Theta_q^{(n)} = \{n-1, \ldots, n-1\}$$

where $it_{\max}$ is the maximum iteration number. In other words, in the Jacobi scheme, all links simultaneously update their actions at each iteration. The Gauss-Seidel scheme can be described as follows:

$$\mathbb{T}_q = \{q, q+Q, q+2Q, \ldots, q+\left(\frac{it_{\max}}{Q}-1\right)Q\}$$

$$\Theta_j^{(n)} = \begin{cases} \{n-(q-1), \ldots, n-1\} & \text{if} \quad j = 1, \ldots, q-1 \\ \{n, n-(Q-1), \ldots, n-q\} & \text{if} \quad j = q, \ldots, Q \end{cases}$$

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 asynchronously to the unique NE of the proposed game if Theorem 1 holds.

Proof: See [23, Appendix B]. ■

Note that (20) was derived only to proceed with the game-theoretic analysis of the problem. A detailed procedure to find the optimal value of ϕ_q in a node is as follows. At a given iteration of our algorithm, say the nth iteration, after setting the optimal value of RxFJ, in order to determine the optimal PA, Bob$_q$ needs to first measure the interference at his receive chain, i.e., $a_q^{(n-1)} + b_q^{(n-1)} {p'_q}^*$ must be measured, where $a_q^{(n-1)}$ and $b_q^{(n-1)}$ indicate the values of a_q and b_q at the previous iteration. Assuming that full knowledge of E-CSI is available, Bob$_q$ also knows the MUI at Eve in the previous iteration, i.e., $c_q^{(n-1)} + d_q^{(n-1)} {p'_q}^*$ is known.[17] Hence, Bob$_q$ does the following:

1) He subtracts the term $\frac{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|\sigma_q^{(n-1)}}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}$ from $c_q^{(n-1)}$;
2) He adds the result of subtraction to $d_q^{(n-1)} {p'_q}^*$. Denote the result of this addition as g_q;
3) He finds the optimal PA in the nth iteration, which can be described as:

$$\phi_q^* = \max\left\{\min\left\{1 - \frac{\left|\mathbf{r}_q^\dagger \mathbf{G}_q\right|^2}{\left|\mathbf{r}_q^\dagger \mathbf{G}_{jq}\right| P_q} \times (a_q^{(n-1)} + b_q^{(n-1)} p'_q - g_q), 1\right\}, 0\right\}. \tag{37}$$

It can be seen that setting the optimal PA involves simple addition, subtraction and division of scalar values. Moreover, there is no need to know all interference terms at Bob$_q$ and Eve because only the aggregate of these terms (i.e., a_q and c_q) need to be known.

C. Discussion on 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 [25, Proposition A.20] that for any induced matrix norm[18] $||\bullet||$ 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

$$||\mathbf{A}+\mathbf{B}||_\infty = \max_q \sum_{r=1}^{Q} \frac{P_r}{P_q} |A_{q,r} - B_{q,r}| < 1. \tag{38}$$

The physical intuition drawn from the condition in (38) is not straightforward. One way to interpret this condition is to decompose this condition as follows: The term $A_{q,r}$ in (38) is 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 (38) 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.

It can be seen that the uniqueness condition depends on the location of Eve as well because both $A_{q,r}$ and $B_{q,r}$ depend on Eve's channels. Other studies such as [6], [9], [12] 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 mitigate knowledge of E-CSI and set the NE uniqueness (derived in Theorem 1) free of Eve's role. None of the approaches in [6], [9], [10], [12] were shown to be

[17] Notice that throughout the iterations of our algorithm, $b_q^{(n-1)} = b_q^{(n)}$ and $d_q^{(n-1)} = d_q^{(n)}$. However, the values of a_q and c_q can vary across iterations.

[18] 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 in the RHS are vector norms.

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.

A. Computing the Best Response Under E-CSI Uncertainties

As knowledge of E-CSI becomes unknown, each legitimate link needs to ensure that positive secrecy is still preserved. Recalling the inequalities in (29) and (20), positive secrecy happens when $c_q > a_q + (b_q - d_q)p'_q$ or equivalently

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

where

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

Under unknown E-CSI, for a given *probability of positive secrecy*, denoted by ε, the qth link needs to satisfy the following:

$$\Pr\{(1-\phi_q)P_q > \psi_q + \tau_q p'_q E_q\} \geq \varepsilon. \tag{40}$$

Using (23) and the Bayes law of total probability, we have

$$\begin{aligned}
&\Pr\{(1-\phi_q)P_q > \psi_q + \tau_q p'_q E_q\} \\
&\quad = \Pr\{b_q < d_q\}(1 - \Pr\{(1-\phi_q)P_q \leq \psi_q + \tau_q P'_q E_q\}) \\
&\qquad + \Pr\{b_q > d_q\}(1 - \Pr\{(1-\phi_q)P_q \leq \psi_q\}).
\end{aligned} \tag{41}$$

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 (40) 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.[19] Using Markov inequality in (41), the following holds

$$\begin{aligned}
&\Pr\{b_q < d_q\}(1 - \Pr\{(1-\phi_q)P_q < \psi_q + \tau_q P'_q E_q\}) \\
&\qquad + \Pr\{b_q > d_q\}(1 - \Pr\{(1-\phi_q)P_q < \psi_q\}) \\
&\quad > \Pr\{b_q < d_q\}\left(1 - \frac{\mathrm{E}[\psi_q + \tau_q P'_q E_q]}{(1-\phi_q)P_q}\right) \\
&\qquad + \Pr\{b_q > d_q\}\left(1 - \frac{\mathrm{E}[\psi_q]}{(1-\phi_q)P_q}\right).
\end{aligned} \tag{42}$$

Hence, (40) remains true as long as we have

$$\begin{aligned}
&\Pr\{b_q < d_q\}\left(1 - \frac{\mathrm{E}[\psi_q + \tau_q P'_q E_q]}{(1-\phi_q)P_q}\right) \\
&\qquad + \Pr\{b_q > d_q\}\left(1 - \frac{\mathrm{E}[\psi_q]}{(1-\phi_q)P_q}\right) \geq \varepsilon.
\end{aligned} \tag{43}$$

Simplifying this inequality, we end up with (44). For the rest of this section, we explain how different terms in (44) can be computed. We first focus on computing $\Pr\{b_q < d_q\}$.

$$\begin{aligned}
\phi_q \leq \max\Bigg\{ \min\Bigg\{ 1 - \Pr\{b_q < d_q\}\frac{\mathrm{E}[\psi_q + \tau_q P'_q E_q]}{(1-\varepsilon)P_q} \\
- \Pr\{b_q > d_q\}\frac{\mathrm{E}[\psi_q]}{(1-\varepsilon)P_q}, 1 \Bigg\}, 0 \Bigg\}.
\end{aligned} \tag{44}$$

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

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

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

$$\Pr\left\{ \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2} < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2} \right\}. \tag{46}$$

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. The division of a (central) chi-square random variable by another independent (central) chi-square random variable has *F-distribution*. 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* [26]. 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 eavesdroppers' positions in several recent works [27]. 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.[20] In summary, let $\Gamma\gamma \triangleq \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}$ 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. Furthermore, let $\nu \triangleq \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$. Using stochastic geometry and F-distribution, we have the following theorem:[21]

Theorem 3: An analytical solution for (46) that is used in (44) is as follows:

$$\Pr\{\Gamma\gamma < \nu\} = \exp\left(-\lambda \int_0^{d_0} \int_0^{2\pi} \Pr\Big\{ \S_q \gamma > \nu \Big\} \beta \,\mathrm{d}\beta \mathrm{d}\varphi \right) \tag{47}$$

where

$$\S_q \triangleq \left(\frac{\beta}{\sqrt{{d_{qq}}^2 + \beta^2 - 2 d_{qq}\beta \cos\varphi}} \right)^{\eta}$$

and $\Pr\{\S_q \gamma > \nu\} = (1 + \frac{\nu}{\S_q})^{-N_q}$.

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

[20] 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.

[21] In [1], we assumed that the large-scale fading component of eavesdropper's channels were known. However, in Theorem 3, we provided an analytical approach to cover the case of unknown large-scale fading components of E-CSI in our power control game.

Proof: See [23, Appendix C]. ■

We now turn our attention to $\mathrm{E}[\psi_q + \tau_q P'_q E_q]$ and $\mathrm{E}[\psi_q]$ in (44). We propagate the expectation in $\mathrm{E}[\psi_q + \tau_q P'_q E_q]$ to each term inside ψ_q using (30). Because the expectation terms in $\mathrm{E}[\psi_q + \tau_q P'_q E_q]$ contain non-negative RVs we can use the following identity:

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

where $\Pr\{\Gamma\gamma > \nu\}$ can be derived from Theorem 3. Hence, the terms involving expectation in $\mathrm{E}[\psi_q + \tau_q P'_q E_q]$ are computable and can be treated the same as $E[\frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}]$.

Note that we focus on no E-CSI knowledge in only Section V of our paper. However, for the purpose of laying a theoretical foundation, until Section V of the paper, we assumed that E-CSI was available. In the scenario where knowledge of E-CSI is not available, it can be shown that our robust scheme is aimed at maximizing the *ergodic secrecy rate*. The details of describing our robust scheme as an ergodic secrecy rate maximization method can be found in [23, Appendix E.A].

B. Distributed Power Control Under E-CSI Uncertainties

Using (44)–(48), we construct a game with the same structure as in Section IV where each link's best response is computed from (44). Same as what we did in the proof of Theorem 1, we concatenate the solution in (44) for all q to establish the following fixed point problem in its $n-$th iteration

$$\Phi^{(n+1)} = \mathbb{1} + \frac{1}{1-\varepsilon}\Big(E[\mathbf{A}+\mathbf{B}]\Phi^{(n)} + E[\mathbf{f}]\Big) \tag{49}$$

It can be seen that (49) is similar to (36) with the only difference that in (49) we applied expectation w.r.t E-CSI to all terms. To analyze the uniqueness of NE, the fixed point problem in (49) must be in closed form, i.e., the expectation terms in (49) must be computable. The close-form representation of these terms was given in (45)–(48). Hence, all the analysis that we did for the NE in the full-ECSI scenario is applicable in the robust scheme as well.

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

$$\rho\left(\frac{E[\mathbf{A}+\mathbf{B}]}{1-\varepsilon}\right) < 1 \tag{50}$$

where the expected value is element-wise. Note that $E[B_{q,r}] = 0$,[22] so one can see that the analysis of $E[\mathbf{A}+\mathbf{B}]$ is simplified to $E[\mathbf{A}]$. 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 (44), 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 $\mathbf{H}_{jrq}$, H'_{rq}, $\forall r, q \in \mathcal{Q}$, $r \neq q$). Hence, no knowledge of MUI at Eve or E-CSI components is needed. Same as the previous section, an alternative condition to (50) is to replace the spectral radius with the infinity norm (see also (38)). Interestingly, the alternative condition for the robust game has a nice interpretation. Specifically, (50) is deduced if

$$\left\|\frac{E[\mathbf{A}]}{1-\varepsilon}\right\|_\infty = \max_q \sum_{r=1}^{Q} \frac{1}{1-\varepsilon}\,|E[A_{q,r}]| < 1. \tag{51}$$

Intuitively, if the interfering channels are small enough, a unique NE exists. Thus, the uniqueness conditions in the robust schemes are not dependent on E-CSI. Algorithm 2 in the next page implements the robust version of our game:

VI. Numerical Results

In this section, we verify our theoretical analyses.[23] 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. Each Alice has a fixed distance (communication range) with her corresponding Bob denoted as $\mathtt{d_{link}}$.[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 $\mathtt{d_{link}}$. 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, $\eta = 2.5$, $\tau_q = -50$ dB,[26] $\mathtt{d_{link}} = 10$ 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, $q \in \mathcal{Q}$.

For the first numerical result, 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 and count the times when the solution found from one-dimensional search reduces to the solution in (15). 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 when the power budget for RxFJ is high. Also, the size of simulation region has a negligible effect on this result.

Next, we compare the performance of our proposed methods for PA between TxFJ and information signals. Specifically, in one method, we use one-dimensional search to find the best

[22] A full treatment of this derivation is given in [23, pp. 27-29].

[23] We did not include several other numerical results due to space limitation. Please find the more comprehensive version of this section in [23].

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

[25] Using a common communication range is a generic assumption in wireless ad hoc networks [27].

[26] Such SIS factors that reduce self-interference below the noise level were reported in recent practical implementation of full-duplex radios [17].

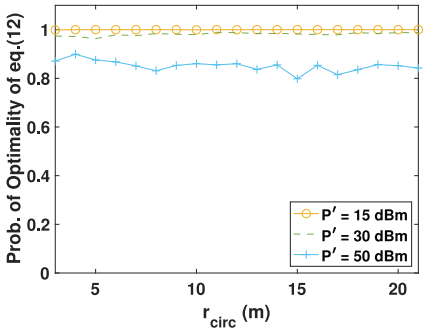

Fig. 2. Probability of having both positive secrecy and the assignment in (15) as the optimal solution for a single-link scenario ($\mathtt{X}_e = \mathtt{Y}_e = 0$, $N_q = 8, M_q = L = 5, P_q = 25$ dBm, $\forall q, Q = 4$).

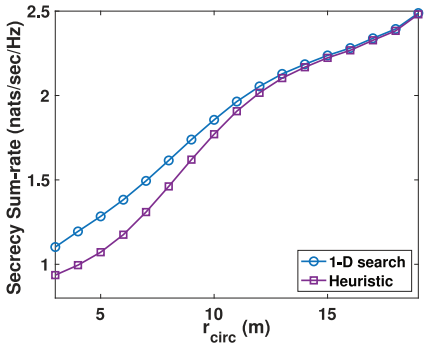

Fig. 3. Comparison of secrecy sum-rate between the one-dimensional search method and the heuristic method for setting δ in (27) ($\mathtt{X}_e = \mathtt{Y}_e = 0$, $N_q = 8, M_q = L = 5, P_q = 25$ dBm, $P'_q = 15$ dBm, $\forall q, Q = 4$).

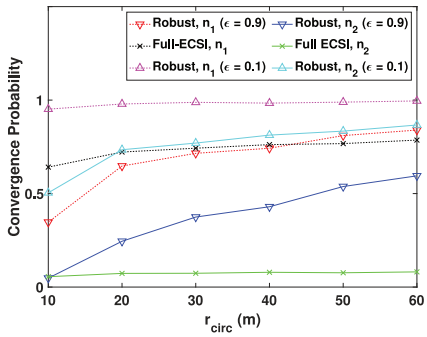

Fig. 4. Probability of convergence vs. $\mathtt{r}_{\mathtt{circ}}$ ($\mathtt{X}_e = \mathtt{Y}_e = 5$, $N_q = 8, M_q = L = 5, \forall q, Q = 4$).

value of δ in (27). In the other method, we use our proposed 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. 3.[27] It can be seen that the proposed 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. 4 shows the variation of convergence (i.e., NE uniqueness) probabilities in robust and full E-CSI methods w.r.t $\mathtt{r}_{\mathtt{circ}}$

[27]Note that the one-dimensional search is in fact the optimal approach in solving (27).

Algorithm 2: Asynchronous Iterative Secure Power Allocation (Robust Version).

1: Given ε, calculate (46) and set $p'_q = P'_q$ if $\Pr\{b_q < c_q\} \geq 0.5$, or $p'_q = 0$ if $\Pr\{b_q < c_q\} < 0.5$.
2: **for** n = 1 to `maximum iteration` **do**
3: Set $\phi_q^{(n)} = \begin{cases} \text{Equal to RHS of (44)}, & \text{if } n \in \mathbb{T}_q \\ \phi_q^{(n-1)} & \text{otherwise} \end{cases}$, $\forall (q) \in \mathcal{Q}$.
4: **end for**

for the four-link case. The convergence probability is calculated as number of times the conditions in (33) and (38) (indicated by "full E-CSI, n_1" and "full E-CSI, n_2", respectively), and their equivalents for the robust game (i.e., (50) indicated by "Robust, n_1" and (51) 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 (38) is very low. However, in the case of unknown E-CSI, since the nodes are indifferent w.r.t. E-CSI, far less restrictive conditions than that of full E-CSI scenario can be achieved. In fact, although the distances between links and Eve become larger as $\mathtt{r}_{\mathtt{circ}}$ grows, the uniqueness of NE in the full E-CSI case still remains unpredictable. On the contrary, in the robust method, by increasing the radius of simulation region, interference at each Bob becomes weaker. So, as the physical interpretation mentioned for (51) 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 (50).

Fig. 5(a)–(c) show the achieved secrecy sum-rate of our proposed power control (under known/unknown E-CSI) vs. the radius of our simulation region. We also plotted the secrecy sum-rate of globally optimal solutions of the secrecy sum-rate maximization. We used Algorithm 1 when the E-CSI is fully known to the legitimate links (indicated by "Full E-CSI" in Fig. 5(c)), and used Algorithm 2 when E-CSI is unknown (indicated by "Robust" in Fig. 5(a)–(b)). Furthermore, Fig. 5(d)–(f) show the resulting sum of information and leaked rates of our methods vs. the radius of our simulation region. Fig. 5(a) and (d) correspond to our robust approach where the probability of positive secrecy is $\varepsilon = 0.9$, while Fig. 5(b) and (e) correspond to $\varepsilon = 0.1$, and Fig. 5(c) and (f) correspond to the case of full E-CSI. We also have two baseline schemes in Fig. 5(a)–(c): the scheme where no RxFJ is used at Bob, and the scheme where no TxFJ is used at Alices. The maximum amount of iterations for Algorithm 1 and 2 is 50. Each approach is examined under two scenarios: 1) when Eve uses MRC decoder, and 2) when Eve uses MMSE decoder.

Although our analysis was limited to the case of using MRC decoder at Eve (see Section II), we still observed the convergence of our algorithm for the case of MMSE decoder. One reason that we did not analyze the case of MMSE receivers at legitimate links or Eve is that MMSE receivers add to the complexity of links' best responses. In fact, in addition to the TxFJ and RxFJ powers being updated at each iteration

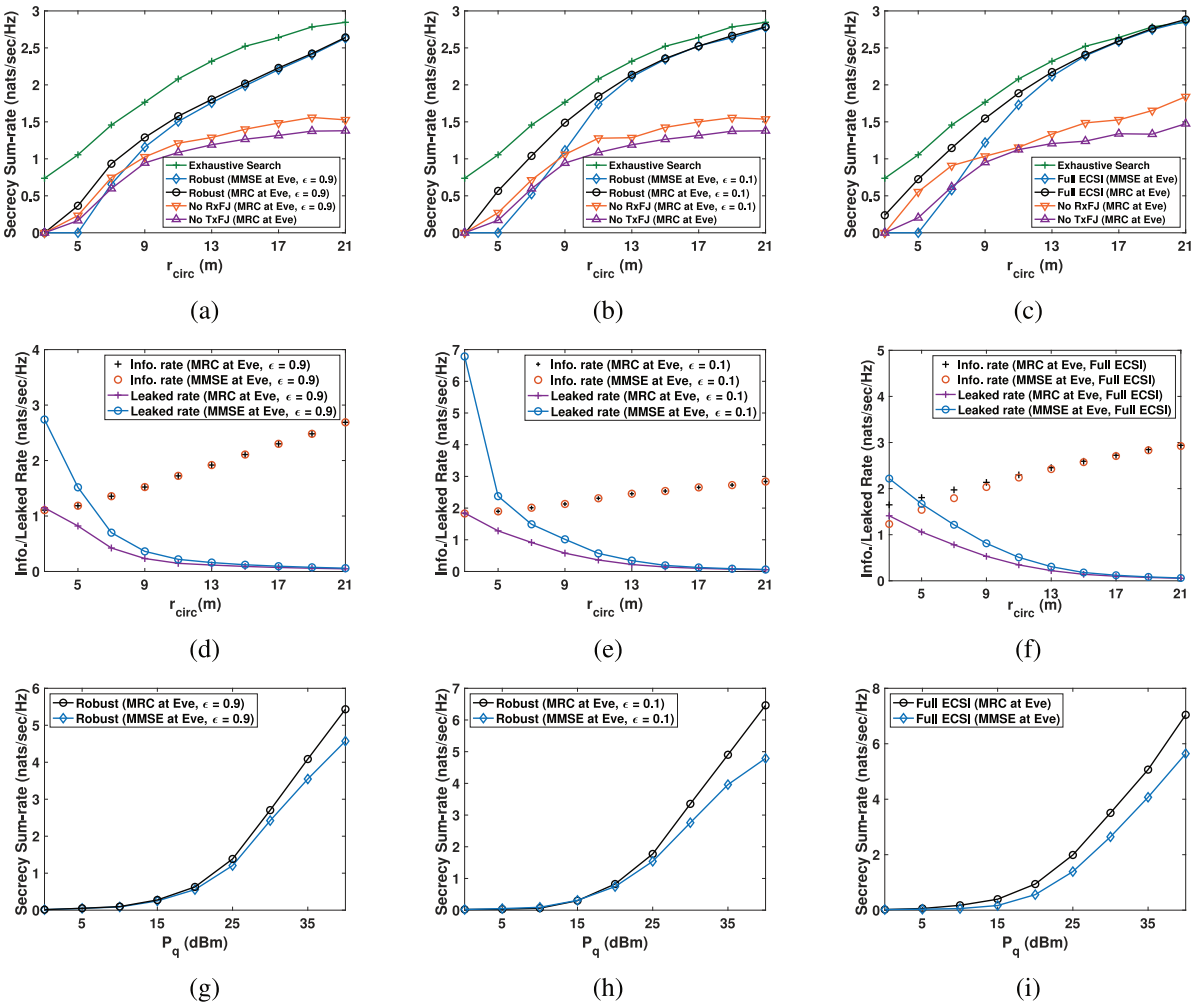

Fig. 5. (a)–(c): Comparison of secrecy sum-rate, (d)–(e): Comparison of information/leaked rate ($\mathrm{X}_e = \mathrm{Y}_e = 5$, $N_q = 8, M_q = L = 5, \forall q, Q = 4$), (g)–(i) Secrecy sum-rate vs. transmit power ($\mathrm{X}_e = \mathrm{Y}_e = 0$, $\mathtt{r_{circ}} = 10$ m, $N_q = 8, M_q = L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

of the game, the MMSE receiver needs to be updated at each iteration of the game as well, thus increasing the complexity of a link's actions. In contrast, using the MRC decoder employed at Eve/Bobs allows us to only focus on TxFJ and RxFJ PA.[28]

From Fig. 5(a)–(c), it can be seen that our approaches have less secrecy compared to globally optimal solutions because the NEs of our proposed game are not necessarily guaranteed to be globally optimum for the secrecy sum-rate. Both cases of the robust method have less secrecy sum-rates than that of the full E-CSI method, although the gap is not large. Furthermore, it can be seen that both no RxFJ and no TxFJ schemes have significantly less secrecy sum-rates compared to our approaches, which signifies the importance of FJ. Lastly, in our particular simulation scenario, it seems that using no TxFJ affects the secrecy sum-rate more than using no RxFJ. Both of these schemes exhibit worse performance when Eve employs MMSE receiver, which is not shown here due to space limitations.

According to Fig. 5(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 have less power remaining for their information signals and thus cannot manage interference between themselves as efficiently as in the full E-CSI case or the case where $\varepsilon = 0.1$. We can see that when $\mathrm{r_{circ}}$ is large (i.e., low SINR at Eve) the performance of MRC and MMSE are very close to each other. This is in fact expected, as the MMSE receiver at Eve theoretically reduces to the MRC receiver for low SINR [28]. For smaller $\mathrm{r_{circ}}$ however, there is a gap between the performance of MMSE and MRC receivers used at Eve.

Fig. 5(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'

[28]Further discussion of the difference in computational complexity between MRC and MMSE receivers is provided in [23, Appenndix D].

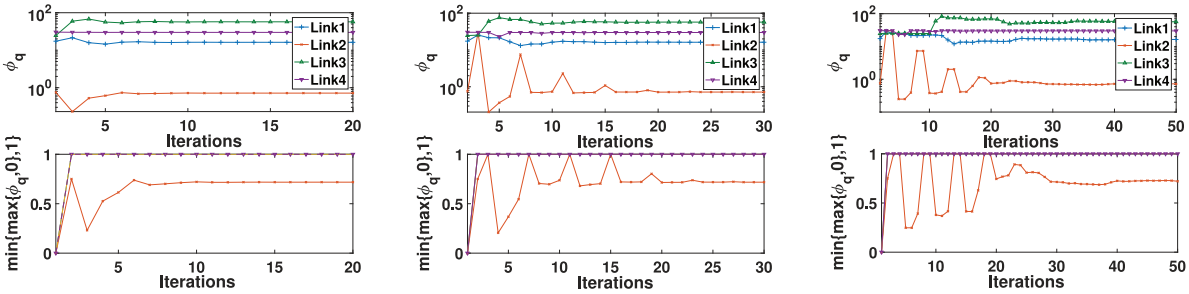

Fig. 6. Convergence of asynchronous algorithm for different update schemes: (a) Jacobi, (b) Gauss-Seidel, (c) Random updates.

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 in previous figures, the secrecy sum-rate achieved for the full E-CSI method (Fig. 5(i)) is larger than that of the robust methods (Fig. 5(g)–(h)). Also, comparing Fig. 5(g) and Fig. 5(h), we conclude that when ε is chosen to be too large, the nodes are not able to do an efficient interference management, thus lower secrecy sum-rate is achieved compared to when ε is small.

Fig. 6 shows the convergence of Algorithm 2 under different update schemes for a settings where the NE is unique. All 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. For the random updates in Fig. 6(c), each link generates a random integer between 2 and 6 that specifies the number of iterations when its action is updated after the current one. As expected, asynchronous actions degrade the convergence speed.[29]

VII. Conclusion

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 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. 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 efficient enough to be considered as best responses for legitimate links. Moreover, the performance of robust schemes are close to the one that assumes knowledge of E-CSI. Lastly, the secrecy sum-rate scales with the power budget at legitimate transmitters, regardless of the knowledge of E-CSI.

[29]We did not include several other numerical results due to space limitation. Please find the more comprehensive version of this section in [23].

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 Int. Conf. Commun. 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. Forensics Secur.*, 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 J. Sel. Areas Commun.*, 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. 35th Annu. IEEE Int. Conf. Comput. Commun.*, 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, "Hierarchical competition as equilibrium program with equilibrium constraints towards security-enhanced wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1564–1578, Jul. 2018.
[12] X. Tang, P. Ren, and Z. Han, "Distributed power optimization for security-aware multi-channel full-duplex communications: A variational inequality framework," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 4065–4079, Sep. 2017.
[13] 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.
[14] 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.
[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] 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.
[17] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proc. ACM SIGCOMM Conf.*, 2013, pp. 375–386.

[18] 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.
[19] D. Bharadia and S. Katti, "Full duplex MIMO radios," in *Proc. 11th USENIX Conf. Netw. Syst. Des. Implementation*, 2014, pp. 359–372.
[20] T. M. Duman and A. Ghrayeb, *Coding for MIMO Communication Systems*. New York, NY, USA: Wiley, 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] P. Siyari, M. Krunz, and D. N. Nguyen, "Secure communications via power control in a MIMO wiretap interference network with jamming transmitters and receivers," Dept. Elect. Comput. Eng., Univ. Arizona, Tucson, AZ, USA, Tech. Rep., TR-UA-ECE-2018-1, 2017. [Online]. Available: http://wireless.ece.arizona.edu/sites/default/files/techrep_peyman_2018_1.pdf
[24] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave N-person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, 1965.
[25] D. P. Bertsekas and J. N. Tsitsiklis, Eds., *Parallel and Distributed Computation: Numerical Methods*. Upper Saddle River, NJ, USA: Prentice-Hall, 1989.
[26] M. Haenggi, *Stochastic Geometry for Wireless Networks*. New York, NY, USA: Cambridge Univ. Press, 2012.
[27] 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.
[28] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York, NY, USA: Cambridge Univ. Press, 2005.

Peyman Siyari received the M.Sc. degree in electrical engineering from AmirKabir University of Technology, Tehran, Iran, in 2013. He is currently working toward the Ph.D. degree at the University of Arizona, Tucson, AZ, USA. His research interests include physical-layer security, convex optimization in signal processing, and game theory.

Marwan Krunz (F'10) is the Kenneth VonBehren Endowed Professor with the Electrical and Computer Engineering Department, University of Arizona Tucson, AZ, USA. He is also an affiliated faculty member of the University of Technology Sydney (UTS). He directs the Broadband Wireless Access and Applications Center, a multi-university industry-focused NSF center that includes affiliates from industry and government labs. He was the UA site Director of Connection One, an NSF IUCRC that focuses on wireless communication circuits and systems. In 2010, he was a Visiting Chair of Excellence with the University of Carlos III de Madrid. He previously held visiting research positions at UTS, INRIASophia Antipolis, HP Labs, University of Paris VI, University of Paris V, University of Jordan, and US West Advanced Technologies. His research interests lie in the areas of wireless communications and networking, with emphasis on resource management, adaptive protocols, and security issues. He has authored or coauthored more than 270 journal articles and peer-reviewed conference papers, and is a co-inventor of several U.S. patents. He is an Arizona Engineering Faculty Fellow (2011–2014), and an IEEE Communications Society Distinguished Lecturer (2013 and 2014). He was the recipient of the 2012 IEEE TCCC Outstanding Service Award, the NSF CAREER award in 1998. He is currently the Editor-in-Chief for the IEEE TRANSACTIONS ON MOBILE COMPUTING (TMC). He was previously on the editorial boards for the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE TMC, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, *Computer Communications Journal*, and IEEE COMMUNICATIONS INTERACTIVE MAGAZINE. He was the General Vice-Chair for WiOpt 2016 and General Co-Chair for WiSec'12. He was the TPC chair for WCNC 2016 (Networking Track), INFOCOM'04, SECON'05, WoWMoM'06, and Hot Interconnects 9. He was and continues to serve on the steering and advisory committees of numerous conferences and on the panels of several funding agencies. He was a keynote speaker, an invited panelist, and a tutorial presenter at numerous international conferences. See www2.engr.arizona.edu/∼krunz for more details.

Diep N. Nguyen received the M.E. and Ph.D. degrees in electrical and computer engineering from the University of California, San Diego, San Diego, CA, USA, and the University of Arizona, Tucson, AZ, USA, respectively. He is a Faculty Member of the School of Computing and Communications, University of Technology Sydney (UTS), Ultimo NSW, Australia. Before joining UTS, he was a DECRA Research Fellow with Macquarie University, and a Member of Technical Staff with Broadcom (California) with ARCON Corporation (Boston), consulting the Federal Administration of Aviation on turning detection of UAVs and aircraft, U.S. Air Force Research Lab on anti-jamming.