Exploiting Full-duplex Receivers for Achieving Secret Communications in Multiuser MISO Networks

Berk Akgun, O. Ozan Koyluoglu, and Marwan Krunz

Abstract

We consider a broadcast channel, in which a multi-antenna transmitter (Alice) sends K confidential information signals to K legitimate users (Bobs) in the presence of L passive eavesdroppers. Alice uses MIMO precoding to generate the information signals along with its own (Tx-based) friendly jamming. Interference at each Bob is removed by MIMO zero-forcing. This, however, leaves a "vulnerability region" around each Bob, which can be exploited by a nearby eavesdropper. We address this problem by augmenting Tx-based friendly jamming (TxFJ) with Rx-based friendly jamming (RxFJ), generated by each Bob. Specifically, each Bob uses self-interference suppression (SIS) to transmit a friendly jamming signal while simultaneously receiving an information signal over the same channel. We minimize the powers allocated to the information, TxFJ, and RxFJ signals under given guarantees on the individual secrecy rate for each Bob. The problem is solved for the cases when the eavesdropper's channel state information is known/unknown. Simulations show the effectiveness of the proposed solution. Furthermore, we discuss how to schedule transmissions when the rate requirements need to be satisfied on average rather than instantaneously. Under special cases, a scheduling algorithm that serves only the strongest receivers is shown to outperform the one that schedules all receivers.

Index terms

Broadcast channel, channel correlation, friendly jamming, full-duplex, physical layer security

I. Introduction

As wireless systems continue to proliferate, confidentiality of their communications becomes one of the main concerns due to the broadcast nature of the wireless medium. Cryptographic techniques can be utilized to address these concerns, but such techniques often assume adversaries with limited computational capabilities. Physical-layer (PHY) security, on the other hand, can be implemented regardless of the adversary's computational power. It also takes advantage of the characteristics of the wireless medium.

The authours are with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, 85721.
E-mail: {berkakgun, ozan, krunz}@email.arizona.edu

An abridged version of this paper was presented at the IEEE Globecom 2015 Conference, San Diego, December 6-10, 2015.

The origins of PHY security dates back to the pioneering work of Wyner [1] that studied the concept of *secrecy capacity* for the degraded wiretap channel. The authors in [2] extended Wyner's work to non-degraded discrete memoryless broadcast channels. Later on, the secrecy capacity of MIMO wiretap channel was obtained in [3]. The secrecy region of the Gaussian MIMO broadcast channel was studied in [4], [5], and [6]. The authors in [7] and [8] studied the problem of secure communications over broadcast channels under individual secrecy constraint, which guarantees that the information leakage to the eavesdroppers from each information message is made vanishing. Even though the joint secrecy constraint, which ensures that the information leakage to the eavesdroppers from all information messages vanishes, is stronger than the individual one, it is not always possible to satisfy. Moreover, the individual secrecy constraint still offers an acceptable secrecy level, while increasing transmission rates [7]. To facilitate secrecy, Goel and Negi [9] introduced the concept of artificial noise, a.k.a. *friendly jamming* (FJ), for Gaussian channels. The idea is to artificially generate Gaussian noise over the channel in order to degrade eavesdropping. This is a special case of the channel prefixing technique proposed in [2], which randomizes the codewords before sending them over the channel. The authors in [10] studied a multiuser broadcast channel, where a sender transmits K independent streams to K receivers. A linear precoding and friendly jamming technique was proposed to enhance PHY security. The authors in [11] studied an outage probability based power allocation problem for data and artificial noise so as to satisfy certain quality of service (QoS) requirements. A full-duplex (FD) receiver that sends artificial noise to secure the communication was proposed in [12] and [13]. This work was later extended to allow both transmitter and receiver to generate artificial noise in [14]. In that model, at least two antennas are needed at the receiver, one for sending the FJ signal and the other to receive the information message. A similar system model was used in [15] but with bipolar-beamforming optimization. The authors in [16] showed that the PHY secrecy can be enhanced using FD jamming receivers without assuming perfect self-interference suppression (SIS). Another system model with one FD base station (BS), one transmitter, one receiver, and one eavesdropper was considered in [17]. In this model, the BS receives a message from the transmitter while sending an information message to the receiver together with an FJ signal. It was assumed that the transmitter's signal does not interfere at the receiver, and the problem of maximizing the secret transmission rate was investigated. None of these works considers a multiuser scenario where multiple receivers generate FJ signals. In contrast, here, we consider a K-user scenario with single-antenna FD receivers, generating FJ signals. Multiuser broadcast channels even without any FJ signal lead to non-convex problem formulations due to interference from unintended information signals. When FJ signals are incorporated to the system to provide secure communications against eavesdroppers, the problem becomes harder to deal with. In addition, we specifically focus on a problem which arises from eavesdroppers having correlated channels with that of legitimate receivers' in this paper.

A. Motivation and Contributions

Our work is motivated by recent studies regarding wireless channel correlations. Specifically, the authors in [18] and [19] showed the vulnerability of the intended receiver to adversaries in the proximity. In particular, when the eavesdropper's channel is highly correlated with that of a legitimate receiver, the MIMO-based nullification

of Alice's FJ signal at that receiver, a.k.a. zero-forcing beamforming (ZFBF), extends to nearby eavesdroppers. This increases the SINR at the eavesdroppers, significantly reducing the secrecy rate. The goal of our work is to provide message confidentiality, independent of the eavesdropper's capability of observing highly correlated signals. We consider a scenario where the transmitter (Alice) sends K independent confidential messages to K legitimate receivers (Bobs). To achieve such a goal in this setup, we propose to use receiver-based friendly jamming (RxFJ), along with transmitter-based friendly jamming (TxFJ). This way, Eve's received signal is degraded even if its channel state is highly correlated with that of Bobs'. To remove TxFJ at each Bob, ZFBF is employed by Alice. This technique also provides confidentiality for the information messages (information signals are zero-forced at unintended receivers). Even though ZFBF technique is a suboptimal solution for broadcast channels, it significantly reduces the implementation complexity [20], [21]. In fact for multiuser MIMO channels, ZFBF becomes optimal in high SNR and some low SNR regimes [20]. Moreover, as the number of users tends to infinity, sum-rate performance of ZFBF is close to the optimal one, as shown in [21]. This technique only requires knowledge of the channel state information (CSI) between Alice and each Bob and works under certain configurations.

First, we formulate an optimization problem to minimize the total network power allocated to the information, TxFJ, and RxFJ signals subject to specific QoS requirements. The goal of this optimization is to guarantee a certain individual secrecy rate for each Bob, with/without eavesdropper's CSI (ECSI). (In unknown ECSI case, it is assumed that the first- and the second-order statistics of ECSI are still known). We exploit the conditions, where using TxFJ and RxFJ has better system performance than using ZFBF to prevent information leakage to the eavesdroppers.

The contributions of this paper can be summarized as follows:

- It is shown that full-duplex capabilities can be exploited in MISO (multiple input single output) broadcast channels to provide confidential communications using RxFJ against the eavesdroppers, whose channels are correlated with that of legitimate receivers.
- Joint power allocation problem to the information, TxFJ, and RxFJ signals to satisfy certain quality of service requirements is investigated, and the optimal solutions are analyzed for practical systems.
- We show how to find the optimal randomization rates for wiretap coding to confuse the eavesdroppers based on the given requirements (individual secrecy rate requirement if ECSI is known, and secrecy outage probability requirement if only the statistics of ECSI is known).
- The effect of different scheduling approaches on the performance of the proposed scheme is analyzed.

The rest of the paper is organized as follows. Section II describes the system model. In Sections III and IV, we present different beamforming techniques with known/unknown ECSI cases. Optimization problem is formulated and analyzed in Section V. We provide simulation results and discussions in Section VI. The paper is concluded in Section VII.

Throughout the paper, we adopt the following notation. Vectors and matrices are denoted by bold lower-case and upper-case letters, respectively. We use column and row vectors notations interchangeably. $(\cdot)^*$ and $(\cdot)^T$ represent the complex conjugate transpose and the transpose of a vector or matrix, respectively. Frobenius norm and the absolute value of a real or complex number are denoted by $\|\cdot\|$ and $|\cdot|$, respectively. $\mathbb{E}[\cdot]$ indicates the expectation

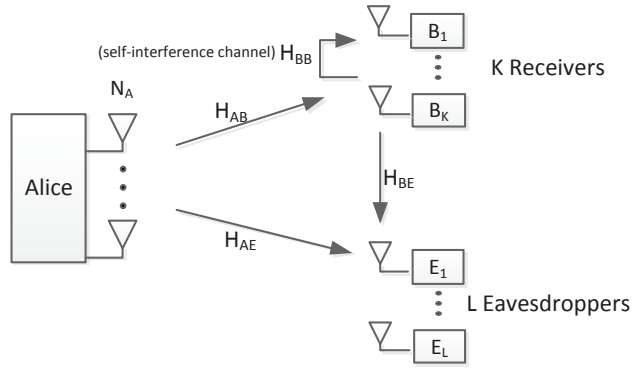


Fig. 1: MU-MISO system model with both TxFJ and RxFJ.

of a random variable. $\mathbf{A} \in \mathcal{C}^{M\times N}$ means that $\mathbf{A}$ is an $M \times N$ complex matrix. $\mathcal{CN}(\mu, \sigma^2)$ denotes a complex Gaussian random variable with mean μ and variance σ^2. $\mathbf{I}_N$ represents an $N \times N$ identity matrix. $[x]^+ = \max(x, 0)$. $\mathbf{A} \succeq 0$ means that matrix $\mathbf{A}$ is positive semi-definite. $\mathrm{rank}(\mathbf{A})$ indicates the rank of matrix $\mathbf{A}$. $I(X;Y)$ refers to the mutual information between random variables X and Y. Let $\mathcal{A}$ and $\mathcal{B}$ be two sets. Then, $\{\mathcal{A} \setminus \mathcal{B}\}$ indicates the set of all elements of $\mathcal{A}$ that are not in $\mathcal{B}$.

II. System Model

As shown in Figure 1, we consider a MU-MISO system, in which Alice transmits K independent confidential data streams to K receivers in the presence of L eavesdroppers. $\mathcal{B} = \{B_1, B_2, \cdots, B_K\}$ is the set of legitimate receivers, each has a single antenna FD radio [22]. $\mathcal{E} = \{E_1, E_2, \cdots, E_L\}$ is the set of eavesdroppers having single-antenna. Legitimate receivers and eavesdroppers are referred to as Bobs and Eves in the rest of the paper, respectively. Let the number of antennas at Alice be N_A. Let $\mathbf{x}_A \in \mathcal{C}^{N_A\times 1}$ be Alice's transmit signal, whereas x_b denote the transmit signal from each Bob for $\forall b \in \mathcal{B}$.

The signals received by each Bob and Eve at time $t \in \{1, \cdots, n\}$ are, respectively, given by:

$$y_b^t = \mathbf{h}_{Ab}\mathbf{x}_A^t + \sqrt{\alpha} h_{bb} x_b^t + \sum_{c\in\{\mathcal{B}\setminus b\}} h_{cb} x_c^t + n_b^t,\ \forall b \in \mathcal{B}$$

$$z_e^t = \mathbf{h}_{Ae}\mathbf{x}_A^t + \sum_{b\in\mathcal{B}} h_{be} x_b^t + n_e^t,\ \forall e \in \mathcal{E}$$

where $\mathbf{h}_{Ab} \in \mathcal{C}^{1\times N_A}$ is the channel vector between Alice and Bob $b \in \mathcal{B}$, while $\mathbf{h}_{Ae} \in C^{1\times N_A}$ is the channel vector between Alice and Eve $e \in \mathcal{E}$. h_{be} denotes the channel between Bob $b \in \mathcal{B}$ and Eve $e \in \mathcal{E}$. h_{bb} and h_{cb} represent the self-interference channel at each Bob and the channel between $c, b \in \mathcal{B}$, where $b \neq c$, respectively. Since the full-duplex radio design is considered at the receivers, a residual self-interference term is incorporated into the model. This residual term defines the portion of the self-interference left after suppression, and is denoted

with the scale factor $\alpha \in [0,1]$, e.g. $\alpha = 0$ means full-suppression (ideal case). $n_b \sim \mathcal{CN}(0,1)$ and $n_e \sim \mathcal{CN}(0,1)$ represent AWGN (Additive White Gaussian Noise) at Bobs and Eves, respectively.

We impose the following instantaneous power constraints:

$$\begin{aligned} \mathbb{E}[\mathbf{x}_A^* \mathbf{x}_A] &\leq \bar{P}_A \\ \mathbb{E}[\,|x_b|^2] &\leq \bar{P}_b,\ \forall b \in \mathcal{B} \end{aligned} \tag{1}$$

where $\bar{P}_A$ and $\bar{P}_b$'s are given constants.

An achievable individual secrecy rate tuple is defined as $\mathcal{R} = (R_1, R_2, \cdots, R_K)$ if there exists codebooks $(2^{nR_k}, n)$ which satisfy both the reliability and security constraints. Let W_k define the secure message from Alice to Bob B_k, where $W_k \in \mathcal{W}_k = [1 : 2^{nR_k}]$. The reliability of the transmission is given as:

$$Pr(\hat{W}_k \neq W_k) \leq \epsilon_0 \tag{2}$$

where $\epsilon_0 \to 0$ as $n \to \infty$, and $\hat{W}_k$ is the estimated message at Bob B_k. The individual secrecy constraints at Bobs and Eves are given by:

$$I(W_k; \mathrm{Y}_{B_l}^n) \leq \epsilon_1,\ \forall (k,l) \in (\mathcal{K} \times \{\mathcal{K} \setminus k\}) \tag{3}$$

$$I(W_k; \mathrm{Z}_e^n) \leq \epsilon_2,\ \forall (k,e) \in (\mathcal{K} \times \mathcal{E}) \tag{4}$$

where $\epsilon_1 \to 0$ and $\epsilon_2 \to 0$ as $n \to \infty$, and $\mathcal{K} = \{1, \cdots, K\}$. Note that the individual secrecy constraints are considered throughout this paper rather than the joint secrecy constraints. Let s_k^n represents the codeword in the codebook to be transmitted in n channel uses. This signal has to contain enough randomness such that the mutual information leakage to Eves will vanish to satisfy (4). Therefore, the secret codebook is generated as follows. $2^{n(R_k + R_k^x)}$ sequences are independently generated according to a certain probability distribution, where R_k^x defines the randomization rate. Then, these sequences are distributed into 2^{nR_k} bins, where the bin index is defined by W_k. As a result, each bin has $2^{nR_k^x}$ codewords, and each codeword is represented by two indices. i.e., $s_k^n(W_k, W_k^x)$. In the rest of the paper, we will require $I(S_k; Y_{B_k}) \geq R_k + R_k^x$ to reliably decode secure message and randomization at B_k, and $I(S_k, Z_e) \leq R_k^x\ \forall k \in \mathcal{K}$ and $\forall e \in \mathcal{E}$ to achieve message security in the sense of individual secrecy. (Note that randomization decoding is necessary to remove ambiguity in the codewords to reveal secret message at Bob. In addition, this adequate amount of randomization implies the security of the message. This is the well-known Wyner's wiretap code [1], specialized to the individual secrecy notion studied in this paper.) The secrecy constraint (3), on the other hand, will be satisfied via ZFBF technique employed at Alice.

The general signaling scheme that we consider in this paper is given by:

$$\mathbf{x}_A^t = \sum_{k \in \mathcal{K}} \mathbf{v}_k s_k^t(W_k, W_k^x) + \sum_{m \in \mathcal{M}} \mathbf{v}_m^{(j)} j_m^t, \quad t = 1, 2, \cdots, n \tag{5}$$

where $\mathcal{K} = \{1, \cdots, K\}$, $\mathcal{M} = \{1, \cdots, M\}$. $s_k^t \sim \mathcal{CN}(0, P_{S_k})$ is the information signal for Bob k at time t, and $\mathbf{v}_k \in \mathcal{C}^{N_A \times 1}$ is its normalized beamforming vector such that $\mathbf{v}_k^* \mathbf{v}_k = 1$. $j_m^t \sim \mathcal{CN}(0, P_m^{(j)})$ and $\mathbf{v}_m^{(j)} \in \mathcal{C}^{N_A \times 1}$ are the m-th TxFJ signal at time t and its beamforming vector, respectively. M is the number of independent TxFJ

signals, and it will be explained later in detail. $\mathbf{v}_m^{(j)}$ is a unit vector as well. The RxFJ signal transmitted by Bobs is given by $x_b = j_b$, where $j_b \sim \mathcal{CN}(0, P_b),\ \forall b \in \mathcal{B}$. In this work, we only consider the linear beamforming. Even though it is a suboptimal technique for broadcast channels, it significantly reduces the implementation complexity. In addition, the authors in [20] and [21] show that sum-rate performance of zero-forcing beamforming is close to the optimal solution asymptotically. In Section III, $\mathbf{v}_k$ is designed such that only the intended receiver gets the information signal $s_k^n(W_k, W_k^x)$, and no TxFJ/RxFJ signal is utilized. On the other hand, Section IV considers how to design the beamforming vectors of TxFJ signals in addition to the beamforming vectors of the information signals with and without the knowledge of ECSI.

III. Beamforming Techniques with Known ECSI

In this section, it is assumed that the channel state information of eavesdroppers (ECSI) is known to Alice and Bobs. Thus, without any friendly jamming signal, it can be ensured that Eves don't receive any information regarding messages. To do that, a well-known zero-forcing beamforming (ZFBF) technique is employed. This technique basically allows to cancel out any signal at any Bob given its CSI. As a result, all of the information signals are canceled out at Eves and unintended Bobs. Therefore, security constraints given in (3) and (4) are satisfied, where R_k^x is assigned as 0 (no need to use randomization rate since Eves don't receive any information signals). Correspondingly, the transmit signal at Alice is given by:

$$\mathbf{x}_A^t = \sum_{k\in\mathcal{K}} \mathbf{v}_k s_k^t(W_k, W_k^x), \quad \mathcal{K} = \{1, \cdots, K\}. \tag{6}$$

To implement ZFBF technique, precoding vector, $\mathbf{v}_k$, is set such that Eves and Bobs except B_k don't receive the information signal, s_k. Let's define the joint channel matrix from Alice to these receivers as

$$\hat{\mathbf{H}}_{B_k} = [\mathbf{h}_{AB_1}^T \cdots \mathbf{h}_{AB_{k-1}}^T \mathbf{h}_{AB_{k+1}}^T \cdots \mathbf{h}_{AB_K}^T \mathbf{h}_{AE_1}^T \cdots \mathbf{h}_{AE_L}^T]^T.$$

Let the singular value decomposition (SVD) of this matrix be $\hat{\mathbf{H}}_{B_k} = \hat{\mathbf{U}}_{B_k}\hat{\mathbf{\Sigma}}_{B_k}\hat{\mathbf{V}}_{B_k}^*$. We assume that each row of $\hat{\mathbf{H}}_{B_k}$ is independent of each other (this is a valid assumption since the antenna configuration at transmitters are designed in this way), and $N_A > (L+K-1)$. (This means that the row length of this matrix is larger than its column length.) Thus, $\mathrm{rank}(\hat{\mathbf{H}}_{B_k}) = (L+K-1)$. Let $\hat{\mathbf{V}}_{B_k}^{(2)}$ correspond to the last $(N_A - L - K + 1)$ columns of $\hat{\mathbf{V}}_{B_k}$. Then, $\hat{\mathbf{V}}_{B_k}^{(2)}$ forms an orthogonal basis for the null space of $\hat{\mathbf{H}}_{B_k}$. Using this decomposition, we set the precoder as $\mathbf{v}_k = \hat{\mathbf{V}}_{B_k}^{(2)}\mathbf{v}_k^{(2)}$. This way, Eves and the unintended Bobs will not be able to receive s_k, since it will be nullified at them. On the other hand, the new channel seen by the receiver B_k becomes $(\mathbf{h}_{AB_k}\hat{\mathbf{V}}_{B_k}^{(2)}) \in \mathcal{C}^{1\times(N_A-L-K+1)}$. Note that this reduces to an interference free channel. To maximize the received signal power over this channel, the second part of the precoder (i.e., $\mathbf{v}_k^{(2)}$) should be designed as follows. Let the SVD of the new channel vector be $(\mathbf{h}_{AB_k}\hat{\mathbf{V}}_{B_k}^{(2)}) = \mathbf{U}_{new}\mathbf{\Sigma}_{new}\mathbf{V}_{new}^*$. The first column of $\mathbf{V}_{new}$ forms an orthogonal basis for the range space of the new channel. Consequently, the second part of the precoder can be chosen in this range space. Indeed, this vector can be given as the following equation:

$$\mathbf{v}_k^{(2)} = \frac{(\mathbf{h}_{AB_k}\hat{\mathbf{V}}_{B_k}^{(2)})^*}{\|\mathbf{h}_{AB_k}\hat{\mathbf{V}}_{B_k}^{(2)}\|} \tag{7}$$

Overall, the precoding vector is designed as:

$$\mathbf{v}_k = \hat{\mathbf{V}}_{B_k}^{(2)} \frac{(\mathbf{h}_{AB_k} \hat{\mathbf{V}}_{B_k}^{(2)})^*}{\|\mathbf{h}_{AB_k} \hat{\mathbf{V}}_{B_k}^{(2)}\|} \tag{8}$$

Based on this scheme, the received signals at B_k and Eves reduce to:

$$y_{B_k}^n = \mathbf{h}_{AB_k} \mathbf{v}_k s_k^n(W_k, W_k^x) + n_{B_k}^n, \quad \forall k \in \mathcal{K} \tag{9}$$

$$z_e^n = n_e^n, \quad \forall e \in \mathcal{E} \tag{10}$$

where $\mathcal{K} = \{1, \cdots, K\}$.

IV. Cooperative FJ

A. Known ECSI

Using the proposed scheme detailed in the previous section, communication rates of Bobs are maximized after imposing the zero-forcing constraints to cancel out the information signals at Eves and unintended Bobs. However, the constraint, $N_A > L + K - 1$, required by the previous strategy may not always satisfied. For example, the number of Eves might be very large so that $L + K - 1 > N_A$. Moreover, even if this constraint is satisfied, having a large number of Eves might cause a very poor system performance (secrecy sum-rate or minimum transmit power). The reason is that having more Eves results in more constraints, and the number of available dimensions to beamform the information signals to the intended Bobs (diversity gain) decreases. Thus, not all dimensions at the intended Bobs are utilized. Furthermore, for the environments where Line-of-Sight (LOS) propagation model is more suitable to use, channels between the transmitter and the receivers are more likely to be correlated, especially if the receivers are close to each other, e.g., distances between them are shorter than 19 wavelength [23]. Let's consider a scenario, where an eavesdropper is near one of the legitimate receivers. When the information signal intended to that receiver is canceled out at the eavesdropper using ZFBF, this signal may become very weak or even canceled out at that receiver as well.

In this section, we propose a strategy that requires zero-forcing constraints only for unintended Bobs. Thus, the security constraint given in (3) is satisfied as previously explained. To satisfy (4), Alice sends TxFJ signals such that they are canceled out at the legitimate receivers by ZFBF, and their signal strength at Eves is maximized. This way, Bobs will not be affected from the TxFJ signals, and the channels of Eves will become weaker. Note that the proposed scheme only requires the constraint, $N_A > K$ rather than $N_A > (L + K - 1)$. Consequently, precoder design for the information signals will have more freedom, as the zero-forcing constraint, which nullifies the information signals at Eves, is no longer active. It means that better precoders can be chosen to increase the signal strength at the intended receivers. For scenarios in which LOS propogation is dominant, like the previous scenario, let's assume that one of the eavesdroppers and one of the legitimate receivers are close to each other so that their channels are highly correlated. Then, since the TxFJ signals is zero-forced at the receiver, their effect may be weak or even vanished at the eavesdropper as well. To overcome this problem, we utilize full-duplex communications. In our model, Bobs are capable of transmitting and receiving signals over the same frequency

band at the same time. As a result, we propose sending RxFJ signals from Bobs. That is, while TxFJ ensures that Eves, whose channels are uncorrelated with Bobs, will be jammed, RxFJ will aim to keep the vicinity of Bobs secure. Besides, whenever a new receiver is served by Alice, one TxFJ dimension is sacrificed. Thus, new Bob coming to the system pays for its service by injecting RxFJ signal into the system, so the total number of dimensions occupied by TxFJ and RxFJ is kept constant. This is important as more dimensions allow to design more effective friendly jamming signals.

Based on the proposed scheme, the transmitted signal at Alice is given by (5). The precoders of the information signals are designed as follows. Let's define

$$\hat{\mathbf{H}}_{B_k} = [\mathbf{h}_{AB_1}^T \cdots \mathbf{h}_{AB_{k-1}}^T \mathbf{h}_{AB_{k+1}}^T \cdots \mathbf{h}_{AB_K}^T]^T \tag{11}$$

Let SVD of this matrix be $\hat{\mathbf{H}}_{B_k} = \hat{\mathbf{U}}_{B_k} \hat{\mathbf{\Sigma}}_{B_k} \hat{\mathbf{V}}_{B_k}^*$. We assume that each row of $\hat{\mathbf{H}}_{B_k}$ is independent of each other, and $N_A > (K-1)$, so $\mathrm{rank}(\hat{\mathbf{H}}_{B_k}) = (K-1)$. Let $\hat{\mathbf{V}}_{B_k}^{(2)}$ correspond to the last $(N_A - K + 1)$ columns of $\hat{\mathbf{V}}_{B_k}$. Then, $\hat{\mathbf{V}}_{B_k}^{(2)}$ forms an orthogonal basis for the null space of $\hat{\mathbf{H}}_{B_k}$. By following the same steps as we did in the previous section, the precoders of the information signals are given as:

$$\mathbf{v}_k = \hat{\mathbf{V}}_{B_k}^{(2)} \frac{(\mathbf{h}_{AB_k} \hat{\mathbf{V}}_{B_k}^{(2)})^*}{\|\mathbf{h}_{AB_k} \hat{\mathbf{V}}_{B_k}^{(2)}\|} \tag{12}$$

Note that, we have more freedom to select the best possible precoders for the information signals using this strategy as compared to the previous one, since the null space of $\hat{\mathbf{H}}_{B_k}$ gets larger.

Our precoding design for TxFJ signals is as follows. First, let's define

$$\mathbf{H}_{AB} = [\mathbf{h}_{AB_1}^T \cdots \mathbf{h}_{AB_K}^T]^T \tag{13}$$

Let SVD of this matrix be $\mathbf{H}_{AB} = \mathbf{U}_{AB} \mathbf{\Sigma}_{AB} \mathbf{V}_{AB}^*$. We assume that each row of $\mathbf{H}_{AB}$ is independent and $N_A > K$, so $\mathrm{rank}(\mathbf{H}_{AB}) = K$. Let $\mathbf{V}_{AB}^{(2)}$ correspond to the last $(N_A - K)$ columns of $\mathbf{V}_{AB}$. Then, $\mathbf{V}_{AB}^{(2)}$ forms an orthogonal basis for the null space of $\mathbf{H}_{AB}$. As a result, each column of $\mathbf{V}_{AB}^{(2)}$ corresponds to the precoder of an independent TxFJ signal so that the null space of the channel matrix between Alice and Bobs can be fully covered by friendly jamming signals. This also implies that $M = N_A - K$. If $\mathbf{V}_{AB}^{(2)}(m)$ represents the m-th column of that matrix, TxFJ signal precoders are given as:

$$\mathbf{v}_m^{(j)} = \mathbf{V}_{AB}^{(2)}(m), \quad \forall m \in \{1, \cdots, N_A - K\} \tag{14}$$

B. Unknown ECSI

In this section, we assume that Alice doesn't know ECSI. However, she knows some properties of eavesdropper's channels such as its first- and second-order statistics. We utilize a strategy very similar to the previous one. Here, the precoding vectors of the information messages are determined following exactly the same steps as in the previous section, since ECSI is not used in their design process. Designing the precoders of the TxFJ signals also follows the same procedure as explained in the previous section.

V. Secure Quality of Service

A. Known ECSI

In this section, we consider a problem that aims to minimize the total power allocated to the information signals, the TxFJ signals, and the RxFJ signals while maintaining *Secure Quality of Service* (SQoS) requirements. These requirements ensure that the mutual information between the information signal, s_k, and the received signal at the intended receiver, y_b, is above a certain threshold, $R_k + R_k^x$ (sum of the individual secrecy rate and the randomization rate of s_k), and the mutual information between the information signal, s_k, and the received signal at the eavesdropper, z_e, is below a certain threshold, R_k^x (the randomization rate of s_k). Furthermore, we assume that the power constraints given in (1) still need to be satisfied. Here, we assume that Alice knows the channels between herself and all the receivers including the eavesdroppers, and the channels between each receiver pair (including the channels between the legitimate receivers and the eavesdroppers). This assumption will hold, e.g., when Bobs send their channel information to Alice. This information exchange will cause an overhead on the system performance. However, the control bits can be used to perform such a task, and its effect will be negligible compared to data transmission. Consequently, the problem formulation is given as:

$$\underset{\substack{P_{S_k}\ \forall k\in\mathcal{K}\\ P_m^{(j)}\ \forall m\in\mathcal{M}\\ P_b\ \forall b\in\mathcal{B}}}{\text{minimize}} \sum_{k\in\mathcal{K}} P_{S_k} + \sum_{m\in\mathcal{M}} P_m^{(j)} + \sum_{b\in\mathcal{B}} P_b$$

$$s.t. \quad \sum_{k\in\mathcal{K}} P_{S_k} + \sum_{m\in\mathcal{M}} P_m^{(j)} \leq \bar{P}_A$$

$$P_b \leq \bar{P}_b,\ \forall b\in\mathcal{B}$$

$$I(S_k;Y_{B_k}) \geq R_k + R_k^x,\ \forall k\in\mathcal{K} \tag{15a}$$

$$I(S_k;Z_e) \leq R_k^x,\ \forall k\in\mathcal{K},\ \forall e\in\mathcal{E} \tag{15b}$$

where $\mathcal{K} = \{1,\cdots,K\}$, $\mathcal{M} = \{1,\cdots,N_A - K\}$, $\mathcal{B} = \{1,\cdots,B_K\}$, and $\mathcal{E} = \{E_1,\cdots,E_L\}$. Given the communication scheme described in the previous section, the mutual information between S_k and Y_b is given by:

$$I(S_k;Y_{B_k}) = \log(1+\text{SINR}_{B_k}),\ \forall k\in\mathcal{K} \tag{16}$$

where

$$\text{SINR}_{B_k} = \frac{P_{S_k}|\mathbf{h}_{AB_k}\mathbf{v}_k|^2}{\alpha P_{B_k}|h_{B_kB_k}|^2 + \sum_{l\in\{\mathcal{K}\setminus k\}} P_{B_l}|h_{B_lB_k}|^2 + 1}.$$

Similarly, the mutual information between S_k and Z_e is given by:

$$I(S_k;Z_e) = \log(1+\frac{P_{S_k}|\mathbf{h}_{Ae}\mathbf{v}_k|^2}{A+B+C+1}) \tag{17}$$

$\forall k\in\mathcal{K}$ and $\forall e\in\mathcal{E}$. $A = \sum_{l\in\{\mathcal{K}\setminus k\}} P_{S_l}|\mathbf{h}_{Ae}\mathbf{v}_l|^2$, $B = \sum_{m\in\mathcal{M}} P_m^{(j)}|\mathbf{h}_{Ae}\mathbf{v}_m^{(j)}|^2$, and $C = \sum_{b\in\mathcal{B}} P_b|h_{be}|^2$. A, B, and C are the interference terms due to other information signals, TxFJ signals, and RxFJ signals, respectively. Note that, since we consider the individual secrecy rates, the interfering information signals help each other by

decreasing the signal strength at each eavesdropper. Based on (16) and (17), the constraints in (15a) and (15b) are, then, given by:

$$P_{S_k}|\mathbf{h}_{AB_k}\mathbf{v}_k|^2 \geq (2^{R_k+R_k^x}-1)(\alpha P_{B_k}|h_{B_kB_k}|^2 + \sum_{l\in\{\mathcal{K}\setminus k\}} P_{B_l}|h_{B_lB_k}|^2+1),\ \forall k\in\mathcal{K}$$

$$P_{S_k}|\mathbf{h}_{Ae}\mathbf{v}_k|^2 \leq (2^{R_k^x}-1)(\sum_{l\in\{\mathcal{K}\setminus k\}} P_{S_l}|\mathbf{h}_{Ae}\mathbf{v}_l|^2 + \sum_{m\in\mathcal{M}} P_m^{(j)}|\mathbf{h}_{Ae}\mathbf{v}_m^{(j)}|^2 + \sum_{b\in\mathcal{B}} P_b|h_{be}|^2+1),\ \forall k\in\mathcal{K},\ \forall e\in\mathcal{E}$$

As a result, we have a linear programming problem, since all of the constraints and the objective function are linear. The achievable individual secrecy rate for B_k satisfies the following inequality.

$$R_k \leq [I(S_k;Y_{B_k}) - I(S_k;Z_e)]^+, \quad \forall e\in\mathcal{E}$$

Therefore, instead of separate SQoS requirements as in (15a) and (15b), the users may request a certain individual secrecy rate. In particular, the constraints in (15a) and (15b) can be replaced as follows:

$$\begin{aligned}
\underset{\substack{P_{S_k}\ \forall k\in\mathcal{K}\\ P_m^{(j)}\ \forall m\in\mathcal{M}\\ P_b\ \forall b\in\mathcal{B}}}{\text{minimize}} \quad & \sum_{k\in\mathcal{K}} P_{S_k} + \sum_{m\in\mathcal{M}} P_m^{(j)} + \sum_{b\in\mathcal{B}} P_b \\
s.t. \quad & \sum_{k\in\mathcal{K}} P_{S_k} + \sum_{m\in\mathcal{M}} P_m^{(j)} \leq \bar{P}_A \\
& P_b \leq \bar{P}_b,\ \forall b\in\mathcal{B} \\
& I(S_k;Y_{B_k}) - I(S_k;Z_e) \geq R_k,\ \forall k\in\mathcal{K}, \forall e\in\mathcal{E}
\end{aligned}$$

where R_k is a non-negative individual secrecy rate. However, this makes the problem non-convex. Here, the same problem formulation in (15) can be used for a given set of randomization rate values R_k^x. Note that, R_k^x is "designed randomization rate" that confuses the eavesdropper, and the problem reduces to choosing the optimal amount of randomization to minimize the total power cost that satisfies the individual secrecy rate requirements. It can be found by a line search method.

B. Unknown ECSI

In this section, we assume that the first and the second order statistics of ECSI are known. In practice, based on the current and the previous channel feedback from the legitimate receivers, Alice may obtain some knowledge about ECSI. We assume that Alice knows

$$\mathbf{K}_{Ae} = \mathbb{E}[\mathbf{h}_{Ae}^*\mathbf{h}_{Ae}] \tag{18}$$

$$\mu_{be} = \mathbb{E}[h_{be}^* h_{be}] \tag{19}$$

$\forall e = \mathcal{E} = \{E_1,\cdots,E_L\}$ and $\forall b\in\mathcal{B} = \{B_1,\cdots,B_K\}$. As the channels are random, we consider replacing the randomization rate constraint in (15b) with an outage constraint, i.e., the probability that the mutual information between the received signal at an Eve, Z_e, and each information signal, S_k, is greater than or equal to the designed randomization rate, R_k^x, is smaller than ϵ_k. Particularly,

$$\Pr\{I(S_k;Z_e) \geq R_k^x\} \leq \epsilon_k,\ \forall k\in\mathcal{K}$$

$$\begin{aligned}\Pr\{I(S_k;Z_e)\geq R_k^x\} &= \Pr\{\log(1+\frac{P_{S_k}\mathbf{v}_k^*\mathbf{h}_{Ae}^*\mathbf{h}_{Ae}\mathbf{v}_k}{D+F+G+1})\geq R_k^x\}\\ &= \Pr\{P_{S_k}\mathbf{v}_k^*\mathbf{h}_{Ae}^*\mathbf{h}_{Ae}\mathbf{v}_k-(2^{R_k^x}-1)(D+F+G)\geq 2^{R_k^x}-1\}\\ &\leq \frac{\mathbb{E}[P_{S_k}\mathbf{v}_k^*\mathbf{h}_{Ae}^*\mathbf{h}_{Ae}\mathbf{v}_k-(2^{R_k^x}-1)(D+F+G)]}{2^{R_k^x}-1}\\ &= \frac{P_{S_k}\mathbf{v}_k^*\mathbf{K}_{Ae}\mathbf{v}_k-(2^{R_k^x}-1)(\bar{D}+\bar{F}+\bar{G})}{2^{R_k^x}-1}\end{aligned}$$

$$\frac{P_{S_k}\mathbf{v}_k^*\mathbf{K}_{Ae}\mathbf{v}_k-(2^{R_k^x}-1)(\bar{D}+\bar{F}+\bar{G})}{2^{R_k^x}-1}\leq 1-\sqrt[L]{1-\epsilon_k} \tag{21}$$

In a scenario, where there is only one eavesdropper, this expression can be used. Nevertheless, if there are L eavesdroppers, this outage probability should be modified as follows:

$$\begin{aligned}1-(1-\Pr\{I(S_k;Z_e)\geq R_k^x\})^L &\leq \epsilon_k,\ \forall k\in\mathcal{K}\\ \Pr\{I(S_k;Z_e)\geq R_k^x\} &\leq 1-\sqrt[L]{1-\epsilon_k},\ \forall k\in\mathcal{K}\end{aligned} \tag{20}$$

Note that we assume all Eves have the same channel properties. By integrating the equation in (17) into this outage probability expression, we obtain the first and the second equalities in (21), where $D=\sum_{l\in\{\mathcal{K}\setminus k\}}P_{S_l}\mathbf{v}_l^*\mathbf{h}_{Ae}^*\mathbf{h}_{Ae}\mathbf{v}_l$, $F=\sum_{m\in\mathcal{M}}P_m^{(j)}(\mathbf{v}_m^{(j)})^*\mathbf{h}_{Ae}^*\mathbf{h}_{Ae}\mathbf{v}_m^{(j)}$, and $G=\sum_{b\in\mathcal{B}}P_b h_{be}^* h_{be}$. Nevertheless, it is not possible to obtain a tractable problem by using this outage constraint. Thus, we exploit Markov's inequality, which states the following:

$$\Pr\{X\geq a\}\leq\frac{\mathbb{E}[X]}{a}$$

where $a>\mathbb{E}[X]$. Therefore, the outage expression can be upper-bounded using Markov's inequality as in the third expression in (21). By assuming the channels are zero mean, this can be modified as in the forth expression, where $\bar{D}=\sum_{l\in\{\mathcal{K}\setminus k\}}P_{S_l}\mathbf{v}_l^*\mathbf{K}_{Ae}\mathbf{v}_l$, $\bar{F}=\sum_{m\in\mathcal{M}}P_m^{(j)}(\mathbf{v}_m^{(j)})^*\mathbf{K}_{Ae}\mathbf{v}_m^{(j)}$, and $\bar{G}=\sum_{b\in\mathcal{B}}P_b\mu_{be}$). Note that we can still write a similar inequality for non-zero mean channel case. As a result, the constraint (20) is converted to the constraint seen in the last equation of (21) for all $k\in\mathcal{K}$.

VI. Simulation Results and Discussions

The channel gain from each transmit antenna to each receive antenna is modeled as:

$$h=\sqrt{Pd^{-2}}G \tag{22}$$

where P and d are the product of the receive and transmit antenna gains and the distance between the corresponding antennas, respectively. $G\sim\mathcal{CN}(0,1)$ represents fading effects of the channel. We assume that the power budgets at Alice, $\bar{P}_A$, and each receiver, $\bar{P}_b$ $\forall b\in\mathcal{B}$, are 200 dB and 20 dB, respectively. We set $P=100$ dB throughout the simulations. We assume that we have an area with dimensions 20×20 meters, and Alice is located in the middle.

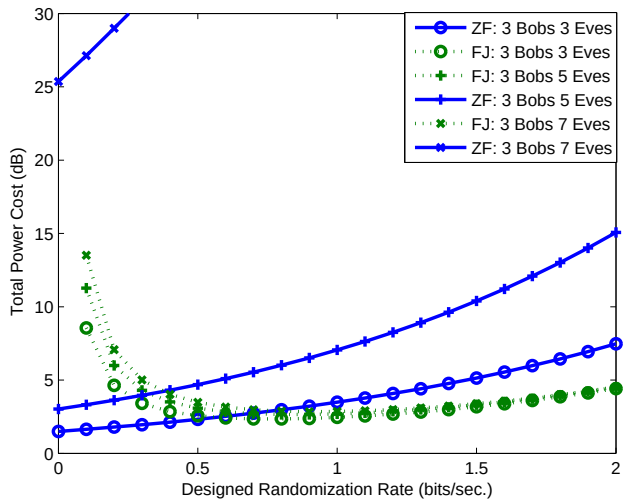


Fig. 2: Total power cost vs. designed randomization rate, R_k^x, with different number of Bobs and Eves.

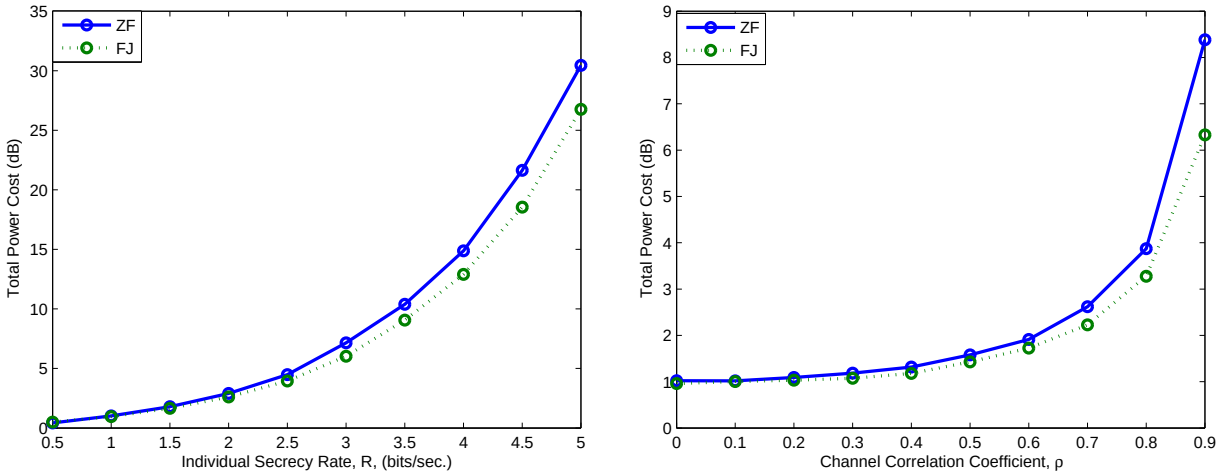
In all simulation results, we show the average values of 2500 different events, where Bobs and Eves are located independently unless otherwise specified. The number of antennas at Alice, N_A, is set to 10.

A. Comparison between ZF and FJ

Zero-forcing (ZF) and friendly jamming (FJ) techniques are introduced in Section III and IV, respectively, for the scenarios where ECSI is known. Here, the performances of these techniques are compared with each other in terms of power cost. We solve the problem (15) where $\alpha = 0$ and $R_k = 2$ bits/sec. $\forall k \in K$. Fig. 2 shows the effect of designed randomization rate, R_k^x, on the total power cost for different number of Bobs and Eves. R_k^x is assumed to be the same $\forall k \in \mathcal{K}$. Since Eves don't receive any signal other than AWGN in ZF case, no randomization rate is required. The optimal randomization rate for ZF is zero as confirmed by the numerical results. We observe that if the number of Eves increases, the performance gain of using FJ over ZF also increases. The main reason is the decrease in multiplexing and power gain of ZF. Also, the total power cost function seems like convex over the designed randomization rate, even though it is not the case in general. The reason is that more power is needed to satisfy (15b) for small values of R_k^x. On the other hand, for large values of R_k^x, even though it becomes easier to satisfy (15b), (15a) needs more power to be satisfied. The reason is that SINR depends on $2^{R_k+R_k^x}$.

Next, using the same setup with 3 Bobs and 5 Eavesdroppers, we evaluated the effect of the individual secrecy rate, R_k. We obtain Fig. 3(a) assuming $R_k = R \ \forall k \in \mathcal{K}$. Power costs are derived for each randomization rate, and the optimal randomization rates are found by line search method. In all the cases, FJ is more effective than ZF, but the performance gain of ZF decreases while R decreases. We also note that the power cost exponentially increases with the individual secrecy rates.

So far, all of the channel entries are generated independently. Here, we consider the scenario where one of the



(a) $R_k = R$ bits/sec. $\forall k \in \mathcal{K}$

(b) $R_k = 1$ bits/sec. $\forall k \in \mathcal{K}$

Fig. 3: Total power cost vs. (a) individual secrecy rate, R, (b) channel correlation coefficient, ρ, with 3 Bobs and 5 Eves.

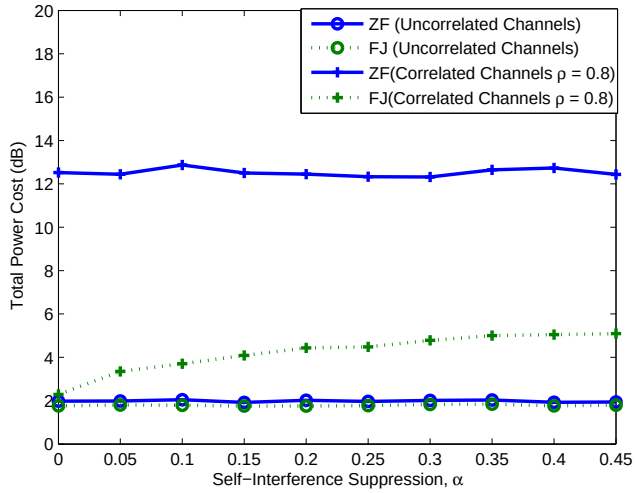


Fig. 4: Total power cost vs. self-interference suppression ratio, α, in correlated and uncorrelated channel cases with 2 Bobs, 6 Eves, and $R_k = 2$ bits/sec. $\forall k \in \mathcal{K}$.

legitimate receiver's channel is correlated with that of an eavesdropper. We randomly associate each Eve with a Bob assuming the correlation between their channels is ρ. As seen from Fig. 3(b), when the correlation between the channels increases, FJ starts outperforming ZF. Since Eves get stronger when the channels are more correlated, much more power have to be allocated to satisfy SQoS requirements. Here, we set $K = 3$, $L = 5$, and $R_k = 1$ bits/sec. $\forall k \in \mathcal{K}$.

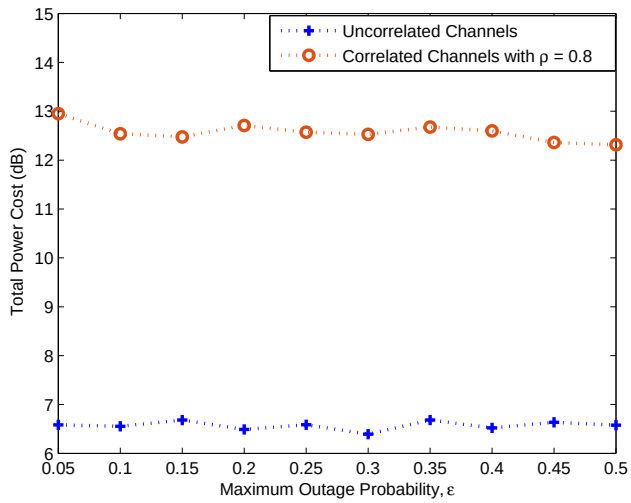


Fig. 5: Total power cost vs. maximum outage probability, ϵ, with unknown ECSI, where $\alpha = 0$, $K = 4$, $L = 4$, and $R_k = 3$ bits/sec. $\forall k \in K$.

The effect of self-interference suppression ratio, α, is investigated in Fig. 4. We set $K = 2$, $L = 6$, and $R_k = 2$ bits/sec. $\forall k \in \mathcal{K}$. Note that, there is no difference in the performance for different values of α in the uncorrelated channel case. This shows that RxFJ is not used in this case. On the other hand, we assume Eves are located near Bobs in the correlated channel case, while the correlation coefficient of the channels, ρ, is equal to 0.8. Unlike the previous case, as α increases (corresponding to less SIS), the power consumption of FJ also increases. As a result, if there is an eavesdropper near the legitimate receiver, and its channel is correlated with that of the receiver, the receiver should use RxFJ to secure its vicinity. Otherwise, since Bob has single antenna (no diversity gain), it is not efficient to use RxFJ.

B. Unknown ECSI

In this section, we show the performance of using cooperative FJ in the scenarios where ECSI is unknown. The objective is to satisfy an individual secrecy outage probability being less than or equal to a certain threshold, ϵ. (Throughout these simulations, it is assumed that all of the users request the same ϵ.) The simulation parameters in Fig. 5 are given by: $\alpha = 0$, $K = 4$, $L = 4$, and $R_k = 3$ bits/sec. $\forall k \in K$. We investigate the effect of ϵ on the objective function when the channels are correlated/uncorrelated. We further assume that there is one eavesdropper near each Bob in the correlated channel case, and the channel coefficient is equal to 0.8 between them. First, it is observed that ϵ has no effect on the system performance in the uncorrelated channel case. On the other hand, the total power cost slightly decreases with ϵ in the correlated channel case, and it requires more power than the uncorrelated channel case as expected. However, one would expect to observe more reduction on the objective function as ϵ gets higher in both cases. The reason why this is not observed is that small amount of power allocation

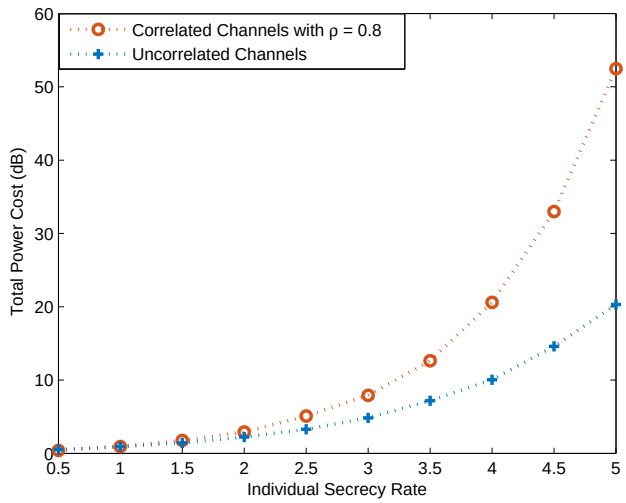


Fig. 6: Total power cost vs. individual secrecy rate with unknown ECSI, where $\alpha = 0$, $K = 3$, $L = 3$, and $\epsilon = 0.1$.

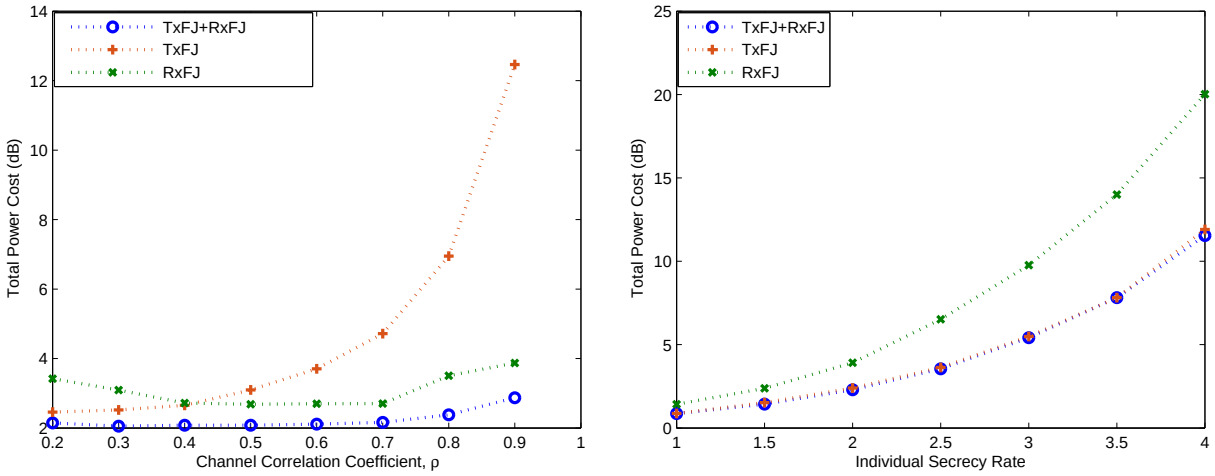
to FJ is enough to satisfy SQoS constraints due to the statistics of ECSI (the interference of the information signals at Eves is enough to provide the individual secrecy).

Next, the effect of individual secrecy rate is observed in Fig. 6, where Bobs request the same amount of individual secrecy rate. Some of the simulation parameters are changed such that $K = 3$, $L = 3$, and $\epsilon = 0.1$. Again, $\rho = 0.8$ in the correlated channel case. As expected, the correlated channel case demands more power to satisfy the SQoS requirements than the uncorrelated channel case.

C. Comparison of Different Jamming Strategies

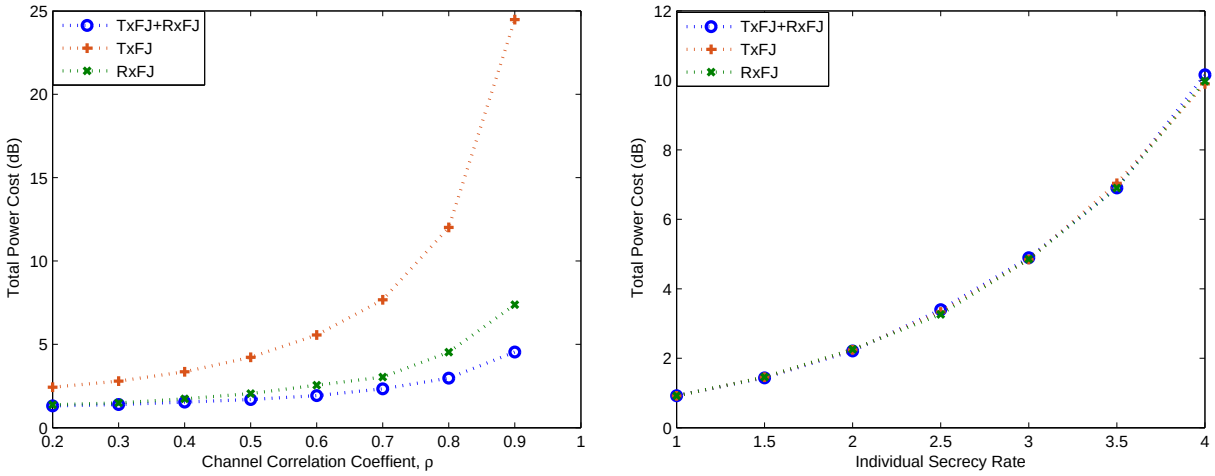
We show the performances of 3 different FJ strategies, namely, only RxFJ, only TxFJ, and cooperative FJ (TxFJ+RxFJ). The following simulation parameters are used in Fig. 7(a): $\alpha = 0$, $K = 3$, $L = 3$, and $\gamma = 2$ bits/sec. $\forall k \in K$. First, we compare the results with respect to channel correlation coefficient by assuming Eves are located near Bobs. TxFJ+RxFJ has the best performance among the others. In addition, TxFJ outperforms RxFJ until $\rho = 0.4$. After that, the performance of RxFJ becomes better than TxFJ, since the beamforming vectors make TxFJ signals weak at the eavesdroppers as the channel correlation increases. On the other hand, Fig. 7(b) compares these three strategies when there is no correlation between channels. As mentioned before, TxFJ and TxFJ+RxFJ almost have the same performance, whereas RxFJ requires more power than the others.

The simulation is repeated for unknown ECSI case in Fig. 8(a) with the same parameters assuming that each Bob requires the outage probability constraint for only its nearest Eve. When the channel correlation coefficient increases, the required power for TxFJ strategy increases more than the other cases. In Fig. 8(b), uncorrelated channels are assumed. The result shows that all of the strategies have the same performance, since the interfering signals at Eves is enough to satisfy SQoS as mentioned before. Overall, considering all of different cases, where



(a) $R_k = 2$ bits/sec. $\forall k \in K$ (b) $\rho = 0$

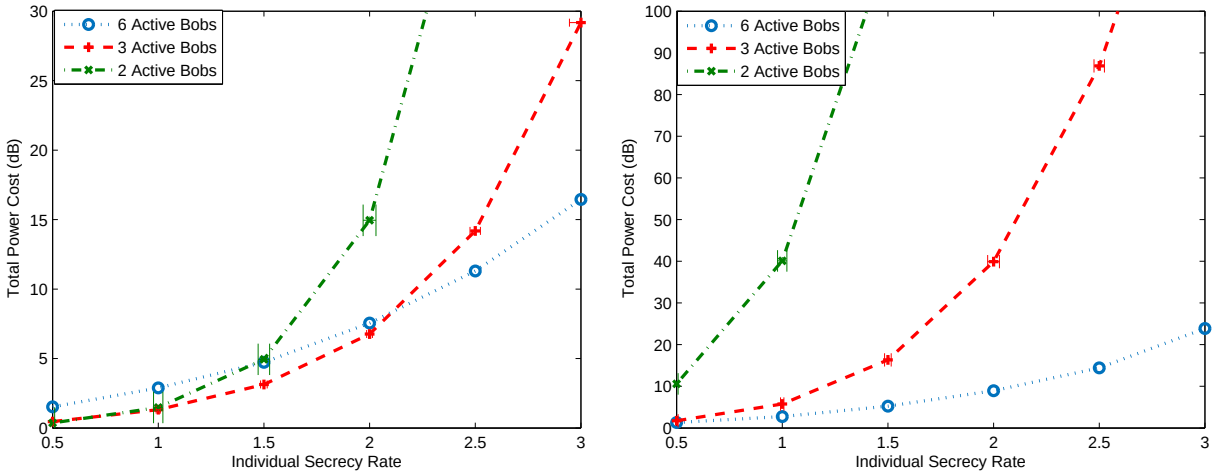
Fig. 7: Total power cost vs. (a) channel correlation coefficient, (b) individual secrecy rate, where ECSI is known, $\alpha = 0$, $K = 3$, and $L = 3$.



(a) $R_k = 2$ bits/sec. $\forall k \in K$ (b) $\rho = 0$

Fig. 8: Total power cost vs. (a) channel correlation coefficient, (b) individual secrecy rate, where ECSI is unknown, $\epsilon = 0.1$, $\alpha = 0$, $K = 3$, and $L = 3$.

ECSI is known/unknown or the channels are correlated/uncorrelated, TxFJ+RxFJ strategy is the best one among other jamming strategies to provide confidentiality for the information messages.



(a) $\rho = 0$ (b) $\rho = 0.9$

Fig. 9: Total power cost vs. individual secrecy rate, where ECSI is known, $\alpha = 0$, $K = 6$, and $L = 5$.

D. Comparison of Different Scheduling Schemes

We average over locations of the users (locations are constant for a block of transmission times and randomly chosen between blocks). Moreover, to obtain the previous numerical results, all of these users are served so that they could achieve the given individual secrecy rate constraints at each time. Here, we investigate whether the total power cost can be reduced further by serving only some of the users. To achieve the same individual secrecy sum-rate, the served users should require a higher individual secrecy rate. Furthermore, the scheduling criteria should make sure that all of the users achieve the same average individual secrecy rate in the long term. For example, let us assume that there are 6 Bobs and 5 Eves, and the individual secrecy rate constraint of each Bob, R_k, is given as r. In this case, the instantaneous individual secrecy sum-rate would be equal to $6r$. However, instead of serving all of them, consider scheduling the closest 3 Bobs (to Alice) for each block. Then, the individual secrecy rate requirement of each of these selected Bobs would be equal to $2r$. If two of them were selected, this requirement would be equal to $3r$, and so on. We compare the results of such a scheduling scheme in Figs. 9(a) and 9(b). Different Bobs are selected for each communication block, since a different topology is created each time. We didn't incorporate a mobility scheme which models a more realistic network model, as this is not the scope of this paper. However, it can be thought as Bobs are moving very fast so that the topology completely changes at each block. Fig. 9(a) is obtained for the case of known ECSI, $\rho = 0$, $\alpha = 0$, $K = 6$, $L = 5$. Number of scheduled Bobs at a given time is showed in the legend. Note that the x-axis represents the average individual secrecy rate over 6 Bobs. (Horizontal bars indicate standard deviation of the achieved rates. We note that the number of repetitions, which is 5000, is enough to have almost equal rates in the long term.) At the low power regime, the proposed scheduling scheme outperforms the regular one, which allows all Bobs to achieve a higher average rate. However, after some

threshold point, the proposed scheme consumes much more power than the regular one. This shows that satisfying 6 individual secrecy rate constraints with rate r is low costly than, for instance, satisfying 3 such constraints with rate $2r$. The reason is that the power is exponentially increases with the required rate due to the log function. On the other hand, Fig. 9(b) shows that the regular scheme always has a better performance, where Eves are located around Bobs, and the channel correlation coefficient between Bobs and corresponding Eves is equal to 0.9. In this case, selecting the closest Bobs to Alice makes the performance worse because Eves are also close to Alice due to the previous statement (they are in the vicinity of Bobs). The effect of number of Eves is also studied, and the results show that performance of the proposed scheme slightly increases relative to the proposed one. Moreover, similar results are obtained for unknown ECSI case.

VII. Conclusion

In this paper, we considered the scenario where a transmitter sends K independent confidential data streams, intended to K legitimate receivers in the presence of L eavesdroppers. With the knowledge that the security applications require guard zones around receivers up to 19 wavelengths, we proposed using RxFJ along with TxFJ. That way, even if an eavesdropper has a highly correlated channel with that of any legitimate receiver and is able to cancel out TxFJ, RxFJ keeps facilitating confidentiality for the information signals. To be able to send RxFJ from the receivers, we considered full-duplex receivers. These receivers are capable of partial/complete self-interference suppression. We used zero-forcing beamforming technique not only to remove the TxFJ interference at intended receivers but also to hide the information signals from the unintended receivers. We showed how to design practical precoders for information signals and TxFJ signals. We formulated a minimum power allocation problem to the information signals, TxFJ signals, and RxFJ signals under certain Secure Quality of Service requirements. We solved this problem with/without the knowledge of eavesdropper's CSI. We obtained the optimal amount of randomness to confuse the eavesdroppers via numerical analyses. The results showed that using RxFJ together with TxFJ increases the system performance in multiuser MISO systems especially when the eavesdropper channels are correlated with that of the legitimate receiver.

Throughout this paper, only Bobs are assumed to have full-duplex capabilities. We note that when Eves have such full-duplex capabilities as well, they would be able to send jamming signals to decrease the signal strength at Bobs, while simultaneously eavesdropping the information messages over the same frequency. Problems that can arise from this model is left for future studies. We also initialized a study of scheduling schemes (here, based on the distance between Alice and Bobs) to further decrease the power cost. The results showed that under certain conditions, different scheduling methods can increase the performance. Therefore, the effect of other scheduling strategies in the context of secret communications will be reported elsewhere.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[4] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2673–2682, 2013.

[5] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Transactions on Information Theory*, vol. 58, no. 9, pp. 5669–5680, 2012.

[6] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," in *IEEE International Symposium on Information Theory Proceedings (ISIT'10)*. IEEE, pp. 2578–2582.

[7] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "Individual secrecy for the broadcast channel," *arXiv preprint arXiv:1511.09070*, 2015.

[8] ——, "Individual secrecy for broadcast channels with receiver side information," *arXiv preprint arXiv:1501.07547*, 2015.

[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[10] J. Yang, I.-M. Kim, and D. I. Kim, "Joint Design of Optimal Cooperative Jamming and Power Allocation for Linear Precoding," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3285–3298, 2014.

[11] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, 2012.

[12] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, 2012.

[13] N. Romero-Zurita, M. Ghogho, D. McLernon, and A. Swami, "Can Bob enhance the security of the multiple antenna wiretap channel?" in *IEEE International Conference on Communication Workshop (ICCW'15)*. IEEE, pp. 447–452.

[14] W. Li, Y. Tang, M. Ghogho, J. Wei, and C. Xiong, "Secure communications via sending artificial noise by both transmitter and receiver: optimum power allocation to minimise the insecure region," *IET Communications*, vol. 8, no. 16, pp. 2858–2862, 2014.

[15] Y. Zhou, Y. Zhu, F. Li, Z. Imm, X. Yin, and Z. Xue, "Securing communication via transmission of artificial noise by both sides: bipolar-beamforming optimization," *Mathematical Problems in Engineering*, 2013.

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

[17] F. Zhu, F. Gao, M. Yao, and J. Li, "Joint information-and jamming-beamforming for full duplex secure communication," in *Proc. of the IEEE Global Communications Conference (GLOBECOM'14)*, 2014, pp. 1614–1618.

[18] X. He, H. Dai, Y. Huang, D. Wang, W. Shen, and P. Ning, "The security of link signature: A view from channel models," in *Proc. of the IEEE Conference on Communications and Network Security (CNS'14)*, pp. 103–108.

[19] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security," in *Proc. of IEEE INFOCOM'13 Conf.*, pp. 200–204.

[20] Q. H. Spencer, M. Haardt *et al.*, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Transactions on Signal Processing*, vol. 52, no. 2, pp. 461–471, 2004.

[21] T. Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 528–541, 2006.

[22] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proc. of the ACM SIGCOMM'13 Conf.*, Hong Kong, China, Aug. 2013, pp. 375 – 386.

[23] X. He, H. Dai, W. Shen, and P. Ning, "Channel correlation modeling for link signature security assessment," in *Proc. of the ACM HotSoS'14 Conf.*