Receiver-Based Friendly Jamming With Single-antenna Full-duplex Receivers in a Multiuser Broadcast Channel

Berk Akgun, O. Ozan Koyluoglu, and Marwan Krunz
Department of Electrical and Computer Engineering
University of Arizona
Tucson, AZ 85721
Email: {berkakgun, ozan, krunz}@email.arizona.edu

***Abstract*—This paper considers a broadcast channel with a multi-antenna transmitter (Alice) sending two independent confidential data streams to two legitimate users (Bob and Charlie) in the presence of a passive eavesdropper (Eve). To enhance their secrecy rates, Bob and Charlie are assumed to be capable of self-interference suppression (SIS). Alice, on the other hand, uses MIMO precoding to generate the two confidential information signals along with its own (Tx-based) friendly jamming. The interfering signals at Bob and Charlie are removed by employing the zero-forcing technique. This, however, leaves "vulnerability regions" around Bob and Charlie, which can be exploited by a nearby eavesdropper. We address this problem by augmenting Tx-based friendly jamming with Rx-based friendly jamming, generated by Bob and Charlie. For the resulting broadcast channel, a secrecy encoding scheme is developed to construct the signals intended to Bob and Charlie. The corresponding achievable secrecy sum-rate is characterized, and an optimization problem is formulated. A special case of this problem is investigated. Simulation results show the effectiveness of utilizing (Tx- and/or Rx-based) jamming, and the impact of the degree of SIS on physical-layer security.**

I. Introduction

As wireless mobile systems continue to be widely adopted, confidentiality of their communication 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 rely on computational limitations at the adversaries. Physical (PHY) layer security, on the other hand, can be implemented regardless of the adversary's computational power.

Wyner [1] initiated the concept of *secrecy capacity* by defining 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 and the secrecy region of the Gaussian MIMO broadcast channel was obtained in [3] and [4], respectively. To guarantee secrecy, Goel and Negi [5] introduced the concept of artificial noise, a.k.a. *friendly jamming*. The authors in [6] studied a multiuser broadcast channel where linear precoding and cooperative jamming are jointly designed to enhance PHY security. A full-duplex (FD) receiver that sends artificial noise for secure communication was proposed in [7], [8], and [9] for various scenarios. Remarkably, none of above works includes receivers with "full-duplex antennas", as multi-antenna FD receivers considered therein refer to having some antennas exclusively used for receiving data and others to send FJ signals. Moreover, none of these studies consider a multiuser scenario where receivers transmit friendly jamming signals. In contrast, in this paper, we consider a two-user scenario with single-antenna full-duplex receivers, transmitting friendly jamming signals.

Our work is motivated by recent studies regarding wireless channel correlations. Specifically, the authors in [10] and [11] showed the vulnerability of security schemes that rely on the common "half-wavelength decorrelation" assumption, and suggested enforcing guard zones around receivers up to 19 wavelengths. In particular, when the eavesdropper's channel is highly correlated with that of a legitimate user, the MIMO-based nullification of Alice's FJ signal at Bob extends to Eve as well. This increases the SINR at Eve, significantly reducing the secrecy rate. The goal of our work is to provide message confidentiality independent of Eve's CSI in a scenario where Alice sends two independent confidential messages to two legitimate users (Bob and Charlie). To achieve such a goal, we propose to use receiver-based friendly jamming (RxFJ), along with transmitter-based friendly jamming (TxFJ) as introduced in [5]. This way, Eve's received signal is degraded even if its CSI is highly correlated with that of Bob and Charlie. To remove TxFJ at Bob and Charlie, a zero-forcing technique is employed by Alice. (This technique also provides confidentiality for Bob's message at Charlie, and vice versa.) For the resulting broadcast channel, we develop an information-theoretic secrecy precoding scheme for the information signals, and characterize the corresponding secrecy sum-rate. In our scheme, the required amount of randomization to achieve information theoretic security is shared by the codewords intended to Bob and Charlie (a scheme referred to in [12] as cooperative encoding for secrecy). Furthermore,

This research was supported in part by ARO (Grant W911NF-13-1-0302) and in part by NSF (Grants IIP-1265960 and CNS-1409172). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of ARO or NSF.

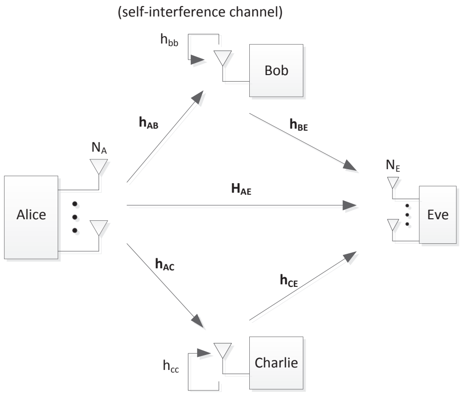

Fig. 1: System model with both TxFJ and RxFJ.

these codewords are designed over multiple fading blocks to overcome the limitations of fading and the absence of Eve's CSI. (This can be considered as a multi-user extension of the scheme in [13].)

We formulate an optimization problem to maximize the secrecy sum-rate. The objective is to optimize the power allocation for the two information messages, the TxFJ signal, and the two RxFJ signals (subject to a total power constraint). To investigate the optimal solution for this problem, we further assume that the legitimate links demand a certain SINR to attain a reliable communication, and they can not communicate if the realized SINR is below this threshold. Simulation results are obtained for two block fading models: a) protocol model, where TxFJ is assumed to be ineffective around the receivers (receiver zone) and RxFJ is assumed to be ineffective outside the receiver zone; b) path-loss model where the signals degrade in proportion to distance (in addition to fading).

Throughout the paper, we denote vectors and matrices by bold lower-case and upper-case letters, respectively. $(\cdot)^\dagger$ represents the complex conjugate transpose of a vector or matrix. 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 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. $[x]^+ = \max(x, 0)$.

II. System Model

As shown in Figure 1, we consider a two-user broadcast channel in which Alice transmits two independent confidential data streams to Bob and Charlie in the presence of Eve. Let the number of antennas at Alice and Eve be N_A and N_E, respectively. The intended receivers, Bob and Charlie, have FD radios, each with a single antenna [14]. We assume that $N_E < N_A$. Let $\mathbf{x}_A \in \mathcal{C}^{N_A\times 1}$ be Alice's transmit signal, which includes two information messages plus TxFJ. Let x_B and x_C denote the RxFJ signals from Bob and Charlie, respectively.

The signals received by Bob, Charlie, and Eve are, respectively, given by:

$$y_B = \mathbf{h}_{AB}\mathbf{x}_A + h_{BB}x_B + h_{CB}x_C + n_B \quad (1)$$

$$y_C = \mathbf{h}_{AC}\mathbf{x}_A + h_{BC}x_B + h_{CC}x_C + n_C \quad (2)$$

$$\mathbf{y}_E = \mathbf{H}_{AE}\mathbf{x}_A + \mathbf{h}_{BE}x_B + \mathbf{h}_{CE}x_C + \mathbf{n}_E \quad (3)$$

where $\mathbf{h}_{AB} \in \mathcal{C}^{1\times N_A}$, $\mathbf{h}_{AC} \in \mathcal{C}^{1\times N_A}$, $\mathbf{h}_{BE} \in \mathcal{C}^{N_E\times 1}$, and $\mathbf{h}_{CE} \in \mathcal{C}^{N_E\times 1}$ are the channel vectors between Alice and Bob, Alice and Charlie, Bob and Eve, and Charlie and Eve, respectively. h_{BB} and h_{CC} are the self-interference channel gains, whereas h_{CB} and h_{BC} are the channel gains between Charlie and Bob, and between Bob and Charlie, respectively. $\mathbf{H}_{AE} \in \mathcal{C}^{N_E\times N_A}$ is the channel matrix between Alice and Eve. $n_B \sim \mathcal{CN}(0, \sigma_B^2)$, $n_C \sim \mathcal{CN}(0, \sigma_C^2)$ and $\mathbf{n}_E \sim \mathcal{CN}(0, \mathbf{I}_{N_E}\sigma_E^2)$ represent AWGN at Bob, Charlie and Eve, respectively. We assume block fading (the indices representing fading blocks and time instants are suppressed to improve readability). Furthermore, we assume that Eve's instantaneous CSI is not known to Alice, Bob, or Charlie (only the statistical CSI is assumed). However, Eve may know her own channels and other channels by overhearing exchanged control packets between Alice and Bob/Charlie.

We impose the following instantaneous power constraints:

$$\mathbb{E}[\mathbf{x}_A^\dagger \mathbf{x}_A] \leq P_A \quad (4)$$

$$\mathbb{E}[\,|x_i|^2] \leq P_i, \quad i \in \{B, C\} \quad (5)$$

where P_A, P_B, and P_C are given constants.

III. Rx-based FJ with Zero-forcing

A. Communication Scheme

The transmit signal at Alice can be expressed as:

$$\mathbf{x}_A = \mathbf{v}_B s_B + \mathbf{v}_C s_C + \mathbf{z}_A w_A \quad (6)$$

where $s_B \sim \mathcal{CN}(0, \sigma_{S_B}^2)$ and $s_C \sim \mathcal{CN}(0, \sigma_{S_C}^2)$ are the information signals, $\mathbf{v}_B \in \mathcal{C}^{N_A\times 1}$ and $\mathbf{v}_C \in \mathcal{C}^{N_A\times 1}$ are normalized precoding vectors for Bob and Charlie, respectively, such that $\mathbf{v}_B^\dagger \mathbf{v}_B = 1$ and $\mathbf{v}_C^\dagger \mathbf{v}_C = 1$, $w_A \sim \mathcal{CN}(0, \sigma_{J_A}^2)$ is the TxFJ signal, and $\mathbf{z}_A \in \mathcal{C}^{N_A\times 1}$ is its precoding vector. We let $\mathbf{z}_A^\dagger \mathbf{z}_A = 1$. The RxFJ signals transmitted by Bob and Charlie are given by $x_i = w_i$, $i \in \{B, C\}$, where $w_i \sim \mathcal{CN}(0, \sigma_{J_i}^2)$.

Given the above, the received signals at Eve, Bob, and Charlie reduce to:

$$\begin{aligned} \mathbf{y}_E &= \mathbf{H}_{AE}\mathbf{v}_B s_B + \mathbf{H}_{AE}\mathbf{v}_C s_C + \mathbf{H}_{AE}\mathbf{z}_A w_A \\ &\quad + \mathbf{h}_{BE} w_B + \mathbf{h}_{CE} w_C + \mathbf{n}_E \quad (7) \\ y_i &= \mathbf{h}_{Ai}\mathbf{v}_i s_i + \mathbf{h}_{Ai}\mathbf{v}_j s_j + \mathbf{h}_{Ai}\mathbf{z}_A w_A \\ &\quad + h_{ii} w_i + h_{ji} w_j + n_i \quad (8) \end{aligned}$$

where in (8) $\{i, j\} \in \{B, C\}$ and $i \neq j$.

To provide confidentiality for Bob's message at Charlie, we consider zero-forcing precoding for the information signal intended to Bob such that it is cancelled out at Charlie, and vice versa. Accordingly, we consider the following zero-forcing constraints.

$$\mathbf{h}_{Ai}\mathbf{v}_j = 0, \quad \{i, j\} \in \{B, C\},\ i \neq j \quad (9)$$

We note that $\mathbf{h}_{AB}$ and $\mathbf{h}_{AC}$ should be linearly independent (otherwise, the cancellation will occur at the intended receivers as well), and the independence occurs with probability 1 due to fading. Constraint (9) reduces the degrees of freedom for the selection of the precoder $\mathbf{v}_C$ ($\mathbf{v}_B$) by one, leaving $N_A - 1$ degrees of freedom. In Subsection III-C, we discuss how to uniquely determine the "optimal" $\mathbf{v}_C$ ($\mathbf{v}_B$) that maximizes the information rate at Charlie (Bob).

The TxFJ signal coming from Alice to Bob is designed to be orthogonal to the channel between them in order to improve the SINR at Bob. A similar constraint is also imposed on the TxFJ signal observed by Charlie. In other words, we require

$$\mathbf{h}_{Ai}\mathbf{z}_A \quad = \quad 0 \quad i \in \{B, C\} \tag{10}$$

It follows that $\mathbf{z}_A \in [\mathrm{span}(\mathbf{h}_{AB}, \mathbf{h}_{AC})]^{\perp}$.

We consider a full-duplex radio design as introduced in [14] to eliminate the self-interference arising from the transmission of RxFJ signal w_B at Bob (w_C at Charlie). In particular, we incorporate into the model a residual self-interference term using SIS ratio, defined as the portion of self-interference left after suppression. This residual term is denoted with the scale factor $\alpha \in [0, 1]$. Accordingly, (8) becomes:

$$y_i \quad = \quad \mathbf{h}_{Ai}\mathbf{v}_i s_i + \alpha h_{ii} w_i + h_{ji} w_j + n_i. \tag{11}$$

With this communication scheme, by controlling the RxFJ powers at Bob and Charlie, we can manage the interference they impose on each other.

B. Achievable Secrecy Sum-Rate

Let $\mathcal{I}(X;Y)$ refer to the mutual information between any two signals X and Y. Given the communication scheme described in the previous section, the Alice→Bob and Alice→Charlie links can support the following instantaneous mutual information expressions:

$$R_B \overset{\text{def}}{=} \mathcal{I}(S_B; Y_B) = \log(1 + \mathrm{SINR_B}) \tag{12}$$

$$R_C \overset{\text{def}}{=} \mathcal{I}(S_C; Y_C) = \log(1 + \mathrm{SINR_C}) \tag{13}$$

where for $i \in \{B, C\}$,

$$\mathrm{SINR}_i = \frac{\sigma_{S_i}^2 |\mathbf{h}_{Ai}\mathbf{v}_i|^2}{\alpha |h_{ii}|^2 \sigma_{J_i}^2 + |h_{ji}|^2 \sigma_{J_j}^2 + \sigma_i^2}.$$

Remark 1: Later on, we incorporate the constraint $\mathrm{SINR}_i \geq T$, where T is a required minimum SINR at Bob/Charlie. In that case, we assume $R_i = \log(1 + T)$, if $\mathrm{SINR_i} \geq T$, and zero otherwise, for $i \in \{B, C\}$.

Regarding the received signal at Eve given in (7), we utilize the following mutual information expressions:

$$\begin{aligned} R_{E,B} &\overset{\text{def}}{=} \mathcal{I}(S_B; Y_E) \\ &= \log(1 + \sigma_{S_B}^2 \mathbf{h}_{AE_B}^{\dagger} (\sigma_{S_C}^2 \mathbf{h}_{AE_C} \mathbf{h}_{AE_C}^{\dagger} \\ &\quad + K)^{-1} \mathbf{h}_{AE_B}) \end{aligned} \tag{14}$$

$$\begin{aligned} R_{E,C} &\overset{\text{def}}{=} \mathcal{I}(S_C; Y_E | S_B) \\ &= \log(1 + \sigma_{S_C}^2 \mathbf{h}_{AE_C}^{\dagger} K^{-1} \mathbf{h}_{AE_C}) \end{aligned} \tag{15}$$

where $\mathbf{h}_{AE_B} \overset{\text{def}}{=} \mathbf{H}_{AE}\mathbf{v}_B$, $\mathbf{h}_{AE_C} \overset{\text{def}}{=} \mathbf{H}_{AE}\mathbf{v}_C$ and $K \overset{\text{def}}{=} \sigma_{J_A}^2 \mathbf{H}_{AE}\mathbf{z}_A\mathbf{z}_A^{\dagger}\mathbf{H}_{AE}^{\dagger} + \sigma_{J_B}^2 \mathbf{h}_{BE}\mathbf{h}_{BE}^{\dagger} + \sigma_{J_C}^2 \mathbf{h}_{CE}\mathbf{h}_{CE}^{\dagger} + \sigma_E^2 \mathbf{I}_{N_E}$, $\{i, j\} \in \{B, C\}$ and $i \neq j$. These expressions correspond to employing an MMSE-SIC decoder at Eve (a sum-rate optimal receiver strategy), and are utilized in the proof of secrecy. In particular, secrecy precoding for the signals intended to Bob and Charlie are designed according to the leakage seen by the eavesdropper over the fading channels, i.e., the required amount of randomization. The following theorem provides the resulting sum-rate.

Theorem 1: An achievable secrecy sum-rate is given by

$$R_{\text{sum}} = \mathbb{E}\left[[R_B - R_{E,B}]^+ + [R_C - R_{E,C}]^+ \right] \tag{16}$$

where the expectation is defined over fading blocks.

Proof: Please refer to Appendix. ■

We note that in the proposed coding scheme, the achievable secrecy rates at Bob and Charlie are given by $R_B^{(s)} \overset{\text{def}}{=} \mathbb{E}\left[[R_B - R_{E,B}]^+\right]$ and $R_C^{(s)} \overset{\text{def}}{=} \mathbb{E}\left[[R_C - R_{E,C}]^+\right]$, respectively. Signal rate seen by Eve, on the other hand, is bounded by the designed rate. For instance, for fading blocks where Eve's signal rate on Bob's signal ($R_{E,B}$) is higher than the signal rate R_B, the amount of information flow regarding s_B to Eve is bounded by R_B. This mechanism occurs on the fly, i.e., without the instantaneous CSI of Eve. Furthermore, if the network includes multiple eavesdroppers (say, with different channel fading distributions), the achieved sum-rate can be written by:

$$R_{\text{sum}} = \min_{E \in \mathcal{E}} \left\{ \mathbb{E}\left[[R_B - R_{E,B}]^+ + [R_C - R_{E,C}]^+ \right] \right\}$$

where $\mathcal{E}$ denotes the set of eavesdroppers.

C. Optimization Formulation

Given the achievable secrecy rate defined in Theorem 1, our objective is to maximize this rate by optimizing the power allocation to data and jamming signals, and designing the best possible beamforming vectors. The corresponding optimization formulation is given by:

$$\underset{\{\sigma_{S_B}^2 + \sigma_{S_C}^2 + \sigma_{J_A}^2 \leq P_A, \sigma_{J_B}^2 \leq P_B, \sigma_{J_C}^2 \leq P_C\}}{\text{maximize}} \qquad R_{\text{sum}} \tag{17}$$

and subject to constraints (9), (10), and $\mathbf{v}_B^{\dagger}\mathbf{v}_B = \mathbf{v}_C^{\dagger}\mathbf{v}_C = \mathbf{z}_A^{\dagger}\mathbf{z}_A = 1$. At this point, we consider a practical assumption, which enables us to solve the above optimization problem. We assume that the SINR at Bob/Charlie must be greater than or equal to T; otherwise, R_B and R_C will be equal to zero. As a result, we should allocate just enough power for the information signals to satisfy this SINR threshold. The rest of the power budget at Alice is used for TxFJ in order to decrease the SINR level at Eve as much as possible. Therefore, we set $\mathrm{SINR}_i = T$ for $i \in \{B, C\}$.

We note that there is more than one possible linear precoding vectors that satisfy the constraint $\mathbf{h}_{Ai}\mathbf{v}_j = 0$, for $\{i, j\} \in \{B, C\}$ and $i \neq j$. In this case, $\mathbf{v}_j$ should be chosen such that $|\mathbf{h}_{Aj}\mathbf{v}_j|$ takes its maximum value. With this maximization (and the norm constraints on the beamforming vectors), we can write $\sigma_{J_B}^2$ and $\sigma_{J_C}^2$ as functions of $\sigma_{S_B}^2$ and $\sigma_{S_C}^2$ for a given T and α. Then, $\sigma_{J_A}^2$ is given by:

$$\sigma_{J_A}^2 = P_A - \sigma_{S_B}^2 - \sigma_{S_C}^2. \tag{18}$$

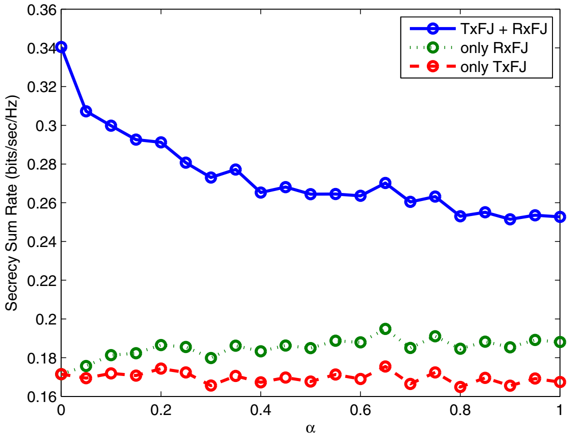

Fig. 2: Effect of self-interference suppression on the secrecy sum-rate (bits/second/Hz).

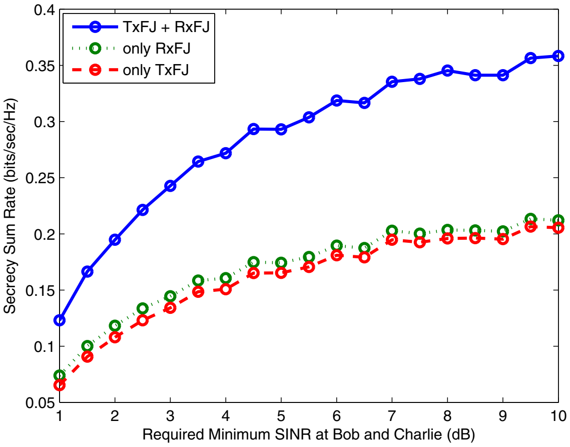

Fig. 3: Effect of the minimum required SINR of the users, T, on the secrecy sum-rate (bits/second/Hz).

Now, the question is which beamforming vector for TxFJ should be chosen. If Alice has 3 antennas ($N_A = 3$), then there will be only one possible dimension such that $\mathbf{z}_A \in [\text{span}(\mathbf{h}_{AB}, \mathbf{h}_{AC})]^{\perp}$. If $N_A > 3$, we end up with a multi-dimensional solution space for $\mathbf{z}_A$. In this case, $\sigma^2_{J_A}$ can be evenly distributed among randomly chosen normalized vectors that are orthogonal to each other and that fully represent this space. This way, we increase the effective region of TxFJ.

Given the above setup, we can derive the optimal R_{sum} in terms of $\sigma^2_{S_B}$ and $\sigma^2_{S_C}$ for a given T and α. Note that, all the necessary parameters to run this algorithm are the channel state information of the receivers and the channel statistics of the eavesdropper as well as the receivers' power constraint. In the literature, there are many algorithms and wireless system designs that perfectly provide these parameters for the transmitter. Alice can calculate the optimal power allocation and precoding design to maximize R_{sum} as described above. Thus, the only overhead of this TxFJ & RxFJ system (as compared to TxFJ) is to transmit the information of power allocations to the RxFJ from Alice to the receivers.

IV. Simulation Results

To demonstrate the efficacy of our design, we provide simulation results using $N_A = 3$ and $N_E = 4$. The carrier frequency is set 2.4 GHz. Alice, Bob, and Charlie are located at points (3,5), (7,7), and (7,3), respectively, in a 10 meter × 10 meter area. The transmit power budgets at Alice, Bob, and Charlie, normalized to the noise power, are taken as $P_A = 100$ dB and $P_B = P_C = 10$ dB, respectively. Unless stated otherwise, we set $\text{SINR}_B = \text{SINR}_C = 5$ dB and $\alpha = 0.1$ (partial SIS). Two interference models are considered: Protocol model and SINR model.

A. Protocol Model

In the protocol model, Eve's location is not known; however, if she is located inside a "vulnerability zone" of the legitimate receivers, she is immune to TxFJ. Since Alice employs zero-forcing to cancel the TxFJ signal at both Bob and Charlie, this signal will be weak in that area. The authors in [15] showed that a guard (vulnerability) zone of 19 wavelengths around a legitimate receiver is required to prevent eavesdropping. In our simulations, the guard zone is set to 10 wavelengths. We further assume that RxFJ has no effect outside this guard zone since the power of the RxFJ signal has to be small by design (especially, when SIS is imperfect). Rayleigh fading is assumed, so all channel entries are i.i.d. Circularly Symmetric Gaussian random variables $\mathcal{CN}(0, 1)$. When we only use TxFJ, Alice's normalized power budget is taken as 120 dB to make a fair comparison.

With the above setting, the simulation run is repeated 10000 times, each time with a different channel entries. Figure 2 shows the secrecy sum-rate (R_{sum}) versus α for three different scenarios. The highest secrecy rate is achieved when both RxFJ and TxFJ are used. R_{sum} decreases with α since RxFJ affects the legitimate receivers' SINR. Interestingly, a slightly higher secrecy rate is achieved with the RxFJ-only scheme (RxFJ-only) compared to the TxFJ-only scheme (TxFJ-only). The reason is that regardless of how much power is allocated to TxFJ, R_{sum} is only determined by the power of the information signals, which is constant due to SINR threshold constraint, in the TxFJ-only. On the other hand, when the power of RxFJ changes, the power of the information signal should also change so that the desired SINR at the receivers is kept constant in the RxFJ-only. Thus, RxFJ-only can operate at a better point than TxFJ-only. We will later see a different behavior under the SINR model. Secondly, we investigated the effect of the minimum required SINR T. As seen from Figure 3, increasing T results in higher R_{sum} for the three FJ schemes. Again, the combined Tx/Rx FJ scheme achieves the highest rate. The RxFJ-only achieves a slightly better rate than that of the TxFJ-only, due to the same reasons mentioned before. We remark that if the range of T is extended here, an optimal T value in terms of secrecy sum rate can be found.

B. SINR Model

In this section, we consider the so-called SINR interference model, where the channel gain from each transmit antenna to each receive antenna is given by:

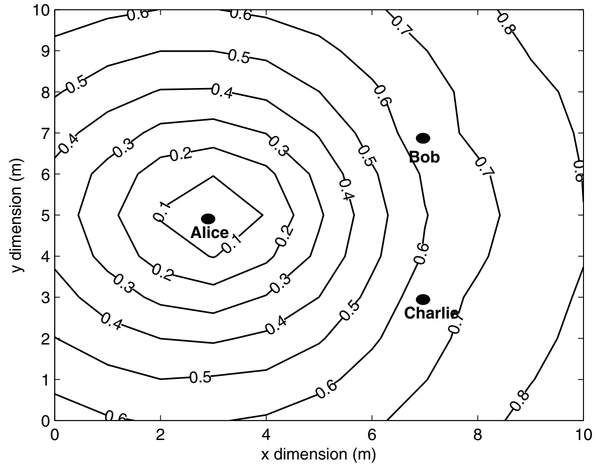

Fig. 4: Contours of secrecy sum-rate in (bits/second/Hz) for various locations of Eve (RxFJ + TxFJ).

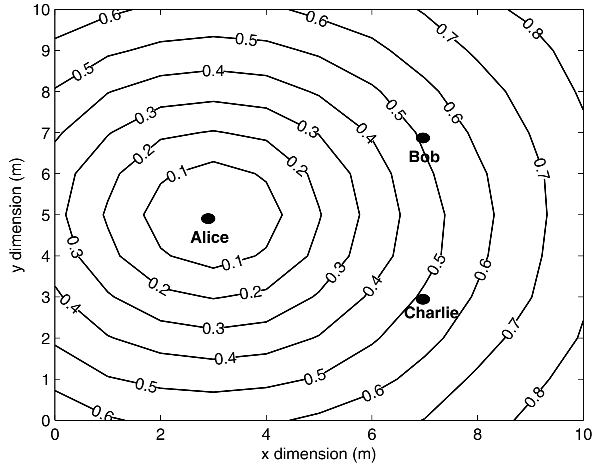

Fig. 5: Contours of secrecy sum-rate in (bits/second/Hz) for various locations of Eve (TxFJ).

$$H = \left(\sqrt{10^{\frac{SL_{dB} + PL_{dB}}{10}}} \right) G \qquad (19)$$

where the quantity between the parenthesis represents the large-scale fading effects, with SL_{dB} and PL_{dB} representing the loss in dB due to shadowing and the path loss, respectively. The second term, $G \sim \mathcal{CN}(0, 1)$, represents small-scale fading effects. Shadowing is assumed to be log-normal with 8 dB standard deviation, $SL_{dB} \sim 8N(0, 1)$; on the other hand, the path loss is modeled as $PL_{dB} = -20 \log_{10}(d)$ where d is the distance between the transmit and receive antennas. We consider full self-interference suppression. In TxFJ-only, the receivers have no power, and P_A is set to 120 dB to maintain the total power budget in the network. Figures 4, 5, and 6 show the contours of the achievable secrecy sum-rate according to Eve's location under three different FJ schemes. In each figure, the locations of Alice, Bob and Charlie are specified. We make a few observations. First, in Figure 5, the contour lines have a circular shape around Alice, as expected, since only TxFJ is used. On the other hand, in Figure 4, the contour lines are not symmetric around Alice. Rather, they are ellipsoid-like, since RxFJ pushes the contour lines towards Alice. As a result, *the performance of RxFJ+TxFJ is always better than the others even if the total power budget is kept constant.* In Figure 6, the contours have a circular shape around Alice except for when they are near to Bob and Charlie. When Eve is between Alice and Bob/Charlie or farther from Bob/Charlie, the TxFJ-only achieves a higher secrecy sum-rate than the RxFJ-only. However, if Eve is around the receivers, the performance of both schemes is similar since RxFJ degrades the SINR of Eve.

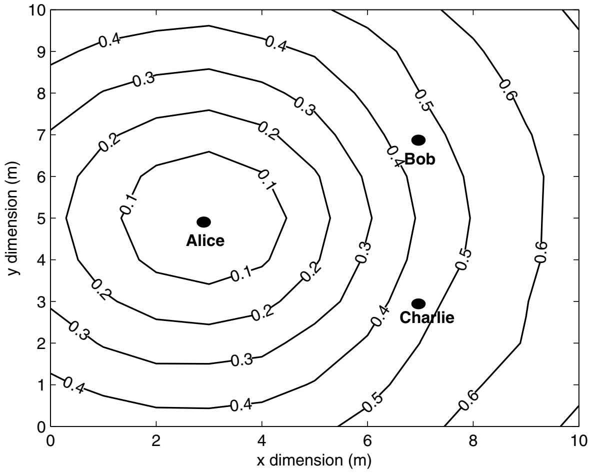

Fig. 6: Contours of secrecy sum-rate in (bits/second/Hz) for various locations of Eve (RxFJ).

V. Conclusions

In this paper, we considered the scenario where a transmitter sends two independent confidential data streams, intended to two legitimate users, in presence of an eavesdropper at an unknown location. With the knowledge of that the security applications require guard zones around receivers up to 19 wavelengths, we proposed using receiver-based friendly jamming (RxFJ) along with transmitter-based friendly jamming (TxFJ). This 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 providing confidentiality for the information messages. We used zero-forcing technique not only to remove the TxFJ interference at intended receivers but also to hide the information messages from the unintended receivers. An optimization problem was formulated for the power allocations of the two information signals, the TxFJ signal, and the two RxFJ signals to maximize the secrecy sum-rate. Assuming that the legitimate links demand a certain SINR such that their achieved data rates remain constant, and they achieve no data rate below this SINR threshold, we provided the optimal solution for this problem.

Our future work will focus on studying more complicated scenarios with more than 2 receivers having multiple antennas.

Appendix

Encoder: Here, we design the codewords s_B^N and s_C^N carrying the secure messages to Bob and Charlie (M_B and M_C), respectively. The encoding is designed such that $P_{e,i} = \Pr\{\hat{M}_i \neq M_i\} \to 0$, where $\hat{M}_i$ is the estimate of M_i at receiver i, and

$$\frac{1}{N}\,\mathcal{I}(M_B, M_C; Y_E^N|\mathbf{H}) \to 0, \tag{20}$$

as $N \to \infty$ (here, $\mathbf{H}$ refers to channel states). The channels given in (7) and (11) are summarized as

$$\begin{aligned} y_i^{(j,t)} &= h_i^{(j,t)} s_i^{(j,t)} + n_i^{(j,t)}, \quad i \in \{B, C\} && (21)\\ \mathbf{y}_E^{(j,t)} &= \mathbf{h}_1^{(j,t)} s_B^{(j,t)} + \mathbf{h}_2^{(j,t)} s_C^{(j,t)} + n_E^{(j,t)} && (22)\end{aligned}$$

where (j,t) indicates channel coherence interval (fading block) $j \in \{1, ..., J\}$ and t-th symbol time $t \in \{1, ..., T\}$ so that total number of channel uses is $N = JT$. This is a block fading interference channel where interference links are removed, and we'll use techniques in [13] and [12] to build encoder. In particular, the signals s_B and s_C share the randomness needed to confuse the eavesdropper as in [12] and designed as in [13] to overcome fading limitations and absence of eavesdropper CSI.

Let $R_B = \mathcal{I}(S_B; Y_B|\mathbf{H}) = \mathbb{E}[\log(1+SINR_B)]$. All binary sequences of length NR_B are generated. Then, they are randomly and uniformly distributed into $2^{NR_B^S}$ bins. Each secret message is assigned to a bin. Then, to transmit any secret message $M_B \in \{1, ..., 2^{NR_B^s}\}$, the transmitter selects the corresponding bin index, and a sequence inside that bin is chosen according to the uniform distribution. This sequence is further divided into J independent blocks $\mathbf{v}_B = [\mathbf{v}_B^{(1)}, \cdots, \mathbf{v}_B^{(J)}]$ where each block $\mathbf{v}_B^{(j)}$ has $T\log(1+\mathrm{SINR}_B^{(j)})$ bits, and transmitted in j-th fading block. To transmit these bits in block j, the transmitter uses i.i.d. Gaussian codebook consisting of $2^{T\log(1+\mathrm{SINR}_B^{(j)})}$ codewords $s_B^{(j)}$ each of length T. Hence, the transmitted signal is given by $s_B^N = (s_B^{(1)}, \cdots, s_B^{(J)})$. A similar scheme is used to construct the signal s_C^N.

Decoder: Bob can decode each message for j-th fading block (as the rate supports channel capacity), and jointly-typical decoding will succeed with high probability as $T \to \infty$. Then, union bound will imply that all messages can be recovered, from which $\mathbf{v}_B$ can be reconstructed and the bin index M_B can be declared as the decoded message. Charlie will use the same scheme to reliably decode M_C.

Security: (Proof Sketch) Consider the following $\mathcal{I}(M_B, M_C; Y_E^N|\mathbf{H})$

$$\begin{aligned}
&= H(M_B, M_C|\mathbf{H}) - H(M_B, M_C|Y_E^N, \mathbf{H})\\
&\overset{(a)}{\leq} H(M_B, M_C|\mathbf{H}) - \mathcal{I}(M_B, M_C; X_S^N|Y_E^N, \mathbf{H})\\
&= H(M_B, M_C) - H(X_S^N|Y_E^N, \mathbf{H})\\
&\quad + H(X_S^N|Y_E^N, M_B, M_C, \mathbf{H})\\
&\overset{(b)}{=} H(M_B, M_C) - \sum_{j=1}^{J} H(X_S^{(j,1:T)}|Y_E^{(j,1:T)}, \mathbf{H})\\
&\quad + H(X_S^N|Y_E^N, M_B, M_C, \mathbf{H})\\
&= H(M_B, M_C) - \sum_{j=1}^{J} [H(X_S^j|\mathbf{H}) - \mathcal{I}(X_S^j; Y_E^j|\mathbf{H})]\\
&\quad + H(X_S^N|Y_E^N, M_B, M_C, \mathbf{H})\\
&\leq H(M_B, M_C) - \sum_{j=1}^{J} (T([R_B^j - R_{E,B}^j]^+)\\
&\quad + T([R_C^j - R_{E,C}^j]^+)) + H(X_S^N|Y_E^N, M_B, M_C, \mathbf{H})\\
&\overset{(c)}{=} H(X_S^N|Y_E^N, M_B, M_C, \mathbf{H})\\
&\overset{(d)}{\leq} N\epsilon,
\end{aligned} \tag{23}$$

where (a) follows as $H(M_B, M_C|X_{S^N}, Y_E^N, \mathbf{H}) \geq 0$, where $X_S^N \triangleq \mathbf{v}_B^N s_B^N + \mathbf{v}_C^N s_C^N$. (b) follows due to memoryless channel and independence of signals. (c) follows by choosing secrecy rates $H(M_B) = JT\mathbb{E}[R_B^j - R_{E,B}^j]^+$ and $H(M_C) = JT\mathbb{E}[R_C^j - R_{E,C}^j]^+$ and, by taking $J \to \infty$ and $T \to \infty$, as time average converges to expected value due to ergodicity of the channel. (d) follows by Fano's inequality as the eavesdropper can decode signals s_B and s_C by employing a list decoding (similar to [12]). Then, (23) shows that the secrecy constraint is satisfied for arbitrarily small ϵ as $N \to \infty$.

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. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 24, no. 3, 1978.

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

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

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

[6] 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.

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

[8] 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.

[9] F. Zhu, F. Gao, M. Yao, and J. Li, "Joint information-and jamming-beamforming for full duplex secure communication," in *Proc. of GLOBECOM'14 Conf.*, 2014, pp. 1614–1618.

[10] 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 CNS'14 Conf.*, pp. 103–108.

[11] 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.

[12] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 5682–5694, 2011.

[13] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

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

[15] 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.*