Blind Cooperative Jamming: Exploiting ISI Heterogeneity to Achieve Positive Secure DoF

Jean de Dieu Mutangana Ravi Tandon
Department of Electrical and Computer Engineering
University of Arizona, Tucson, AZ 85721
E-mail: {*mutangana, tandonr*}@email.arizona.edu

Namyoon Lee
Department of Electrical Engineering
POSTECH, Pohang, Gyeongbuk, Korea 37673
E-mail: {*nylee*}@postech.ac.kr

***Abstract*—We investigate secure degrees of freedom (SDoF) of a single-input single-output (SISO) wiretap channel with a single helper without channel state information at the transmitters (CSIT). Wireless communication systems inherently suffer from intersymbol interference (ISI) due to channel dispersion. In this paper, we propose a novel blind cooperative jamming scheme that exploits the ISI heterogeneity to achieve positive SDoF, even without any CSIT. In order to achieve positive SDoF, the proposed approach only requires statistical properties of the ISI channel. In particular, we show that if L_B is the effective ISI channel multipath link length towards the legitimate receiver (Bob) and L_E is the link length towards the eavesdropper (Eve), a positive SDoF of $\frac{L_B-L_E}{2(L_B-1)}$ is achievable. To the best of our knowledge, this is the first work that exploits ISI link length heterogeneity to achieve positive secure degrees of freedom.**

I. Introduction

Achieving high secure communication rates in the presence of eavesdroppers remains a challenging problem in wireless communication systems due to their broadcast nature. Extensive studies have been conducted exploiting channel differences between transmitters, legitimate receivers, and eavesdroppers in order to achieve physical layer security. Achievable information theoretic secrecy regions have been characterized for a variety of eavesdropped communication channels (e.g. [1], [2], and [3]). Because of difficulty in characterizing the exact secrecy capacity regions, research on secure degrees of freedom (SDoF) for different types of channels in the presence of channel state information (CSI) has been of growing interest (e.g. [4] and [5]). Using number theory based approximations, [6] and [7] characterized achievable SDoF for the Gaussian wiretap channel with multiple helpers. SDoF of a MIMO wiretap channel in the presence of a helper with multiple antennas is investigated in [8].

In this paper, we focus on a single-input single-output (SISO) wiretap channel with a single helper without channel state information at the transmitters (CSIT) and with intersymbol interference (ISI) links between terminals. This work differs from blind interference alignment in [9] because it does not impose any requirements on channel coherence patterns. It only requires statistical knowledge of ISI link lengths towards the receivers. Previous research has largely assumed availability of CSIT to achieve positive SDoF. On the contrary, removing CSIT assumptions is advantageous, since in reality it may be hard to fully obtain perfect channel characterization and it may not be possible to acquire CSI from eavesdropping nodes. It, therefore, remains of great importance to explore the following problem: *Can we achieve any positive SDoF while completely removing the need for channel state information at the same time?*

This work was supported by the U.S. National Science Foundation grants CCF-1559758 and CNS-1715947.

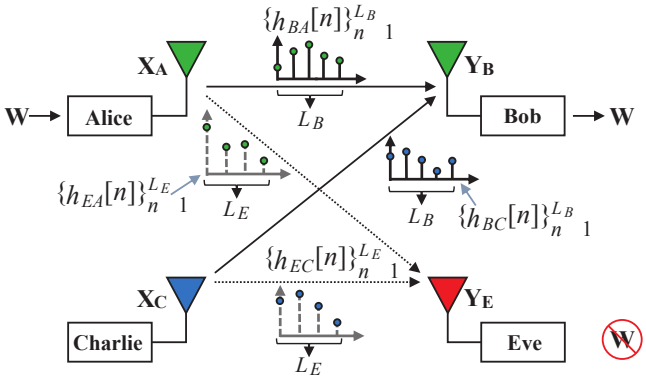

Fig. 1: Wiretap channel with a Helper and Intersymbol Interference.

The main contribution of this paper is to show that for heterogeneous ISI channels (i.e. channels with different ISI link lengths in terms of the number of channel taps towards different receivers), positive SDoF can be achieved even without any CSI at the transmitters.

In particular, this heterogeneity in ISI link lengths can be exploited to mix transmission of information and artificial noise symbols in a manner that allows the legitimate receiver to decode the transmitted information symbols and keeps the information symbols completely submersed in artificial noise symbols at the eavesdropper's node. We devise a scheme that takes advantage of the difference in ISI link lengths towards the legitimate receiver and the eavesdropper in order to achieve positive SDoF without CSIT (i.e. no knowledge of the channel coefficients at the transmitters). This work is inspired by recent work [10], which explored how ISI heterogeneity can be exploited to achieve significant gains in spectral efficiency for multi-user interference channels, even without CSIT.

II. System Model Description

We consider a wiretap model with intersymbol interference (ISI) where Alice (A) wants to securely communicate with Bob (B) in the presence of an eavesdropper Eve (E). Secure communication here is facilitated by the presence of an interfering "Helper" that we denote as Charlie (C). See Fig. 1. Each node is equipped with a single antenna. The channels

978-1-5090-5019-2/17/$31.00 ©2017 IEEE

from Alice and Charlie to Bob and Eve are assumed to be ISI channels, where $\{h_{BA}[n]\}_{n=1}^{L_B}$, $\{h_{BC}[n]\}_{n=1}^{L_B}$, $\{h_{EA}[n]\}_{n=1}^{L_E}$, and $\{h_{EC}[n]\}_{n=1}^{L_E}$ denote the channel impulse responses (CIRs) from Alice and Charlie to Bob and from Alice and Charlie to Eve, respectively. All CIR coefficients are assumed to be independently and identically distributed continuous random variables. L_B and L_E are channel tap length parameters and they are described as follows. We consider L_B to be the maximum number of effective channel taps between Alice and Bob (as well as the maximum number of effective channel taps between Charlie and Bob). L_E is the maximum number of effective channel taps between Charlie and Eve (as well as the maximum number of effective channel taps between Alice and Eve). The CSI availability assumptions are:

- Alice and Charlie do not have any CSI (i.e. no knowledge of the channel coefficients (CIRs)). They only know the ISI link lengths L_B and L_E.
- Bob only knows local channel coefficients $\{h_{BA}[n]\}_{n=1}^{L_B}$ and $\{h_{BC}[n]\}_{n=1}^{L_B}$. This is necessary for decoding at Bob.
- Eve has access to all coefficients (i.e. can access all CIRs).

Let $X_A[k]$ and $X_C[k]$ be the respective symbols transmitted by Alice and Charlie at time k, then the respective signals seen at receivers Bob and Eve are given by

$$Y_B[k] = \sum_{n=1}^{L_B} X_A[k-n]h_{BA}[n] + \sum_{n=1}^{L_B} X_C[k-n]h_{BC}[n] + Z_B[k] \quad (1)$$

$$Y_E[k] = \sum_{n=1}^{L_E} X_A[k-n]h_{EA}[n] + \sum_{n=1}^{L_E} X_C[k-n]h_{EC}[n] + Z_E[k], \quad (2)$$

where $Z_B[k]$ and $Z_E[k]$ are complex circularly independent zero mean unit variance channel noises respectively received at Bob and Eve at time k. All symbols $X_A[k]$ and $X_C[k]$ are transmitted with a power P, each satisfying the constraints:

$$\mathbf{E}[X_A^2[k]] \leq P \quad (3)$$

$$\mathbf{E}[X_C^2[k]] \leq P. \quad (4)$$

For a randomly transmitted message W and its received estimate $\hat{W}$, a secure rate of communication R_S is achievable, if there exists an n-length code that, for any $\epsilon \to 0$ and $n \to \infty$, satisfies both the decodability and security constraints:

$$Pr[W \neq \hat{W}] \leq \epsilon \quad (5)$$

$$\frac{1}{n} H(W|Y_E^{(n)}) \geq R_s - \epsilon, \quad (6)$$

where $Y_E^{(n)}$ is the signal observed at the eavesdropper Eve.

The secrecy capacity C_S is defined as the maximum of R_S. We define the secure degrees of freedom (SDoF) as

$$SDoF = \lim_{P \to \infty} \frac{C_S}{\log(P)}, \quad (7)$$

which is the prelog of secrecy capacity.

III. Main Result: Achievable SDoF Scheme

Theorem 1. *For a heterogeneous ISI wiretap channel in the presence of a single helper without any CSIT and with effective channel interference links of lengths L_B and L_E, the following SDoF is achievable*

$$SDoF \geq \frac{(L_B - L_E)^+}{2(L_B - 1)}, \quad (8)$$

where $(x)^+ \triangleq \max(x, 0)$ and $L_B > 1$.

Before presenting the proof of Theorem 1, we first present some representative examples that highlight the key ideas behind the general scheme and show the feasibility of positive secure degrees of freedom with no CSI at Alice or the Helper.

Example 1: Consider $L_B = 2$ and $L_E = 1$. This means that, for the given values of L_B and L_E, any symbol sent by Alice or Charlie will be seen over two time slots (channel instants) at Bob and over one time slot at Eve. Our goal is to show that the achievable SDoF is $\frac{L_B - L_E}{2(L_B-1)} = \frac{1}{2}$. In the first time slot, Alice transmits an information symbol S_1 and Charlie transmits an artificial noise symbol N_1. Then, Alice and Charlie remain silent over the next time slot, which can also be viewed as zero-padding (see Fig. 2). Since the channel coefficients are independently and identically distributed continuous random variables, Bob observes two independent linear equations $L_{1B}(S_1, N_1)$ and $L_{2B}(S_1, N_1)$, from which he can solve for S_1 and N_1 and, therefore, be able to extract the information symbol S_1. Eve, on the other hand, will only observe one linear equation $L_{1E}(S_1, N_1)$, from which she can neither solve for S_1 nor N_1. Here $L_{iB}(\,.\,)$ and $L_{iE}(\,.\,)$ respectively denote the linear combinations received at Bob and Eve in the ith time slot. Therefore, we can securely transmit $L_B - L_E = 1$ information symbol using $2(L_B - 1) = 2$ time slots, i.e., this scheme achieves $SDoF = \frac{L_B - L_E}{2(L_B-1)} = \frac{1}{2}$.

The following example demonstrates the scenario where Alice (in addition to Charlie) also transmits artificial noise symbols in addition to information symbols to achieve the secure degrees of freedom stated in Theorem 1.

Example 2: Consider $L_B = 3$ and $L_E = 2$. This means that any symbol sent by Alice or Charlie will be seen over three time slots at Bob and over two time slots at Eve. This scheme is composed of a total of $2(L_B - 1) = 4$ time slots and is able to securely deliver $L_B - L_E = 1$ information symbol to Bob. In the first time slot, Alice transmits $L_B - L_E = 1$ information symbol denoted by S_1. In the second time slot, Alice transmits $L_E - 1 = 1$ artificial noise symbol denoted by U_1. In the third and fourth time slots (i.e. over the last $L_B - 1$ time slots), Alice remains silent (which can also be viewed as zero-padding). Charlie consecutively transmits artificial noise symbols N_1 and N_2 over the first and the second time slots (i.e. Charlie sends $L_B - 1$ artificial noise symbols). Charlie remains silent in the third and fourth time slots (see Fig. 3). Since the channel coefficients are independently and identically distributed continuous random variables, Bob observes four independent linear equations $L_{1B}(S_1, N_1)$, $L_{2B}(S_1, N_1, U_1, N_2)$,

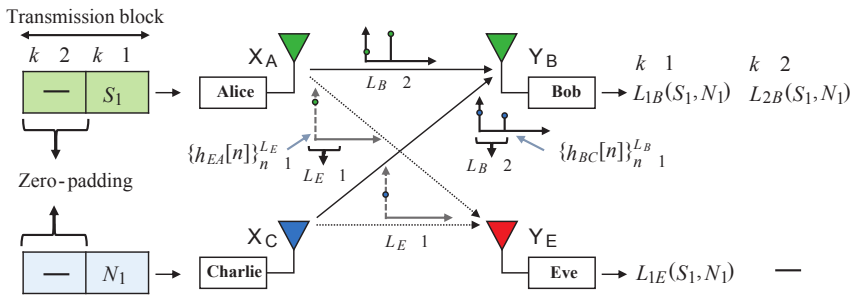

Fig. 2: Wiretap channel with ISI example with $L_B = 2$ and $L_E = 1$ where Charlie sends artificial noise (N_1).

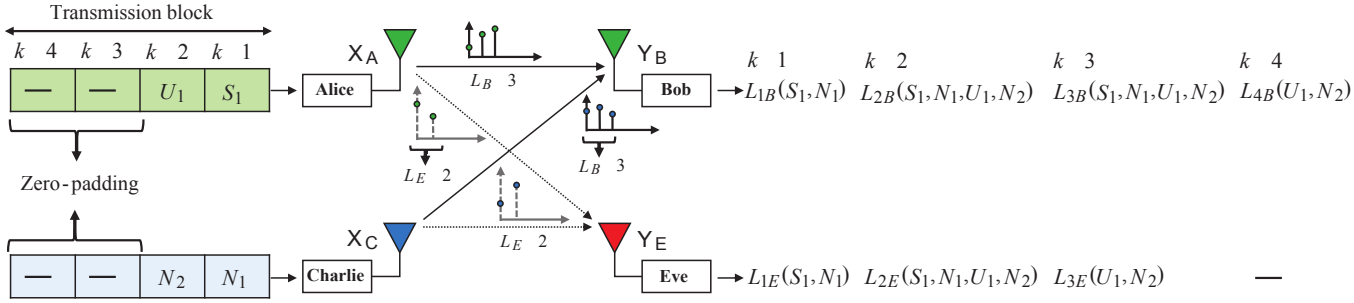

Fig. 3: Wiretap channel with ISI example with $L_B = 3$ and $L_E = 2$ where Alice and Charlie send artificial noise (U_1) and (N_1, N_2).

$L_{3B}(S_1, N_1, U_1, N_2)$, and $L_{4B}(U_1, N_2)$, from which he can solve for S_1, N_1, U_1, and N_2. Bob is, hence, able to extract the information symbol S_1 and discard the artificial noise symbols. Eve, on the other hand, will observe three linear combinations $L_{1E}(S_1, N_1)$, $L_{2E}(S_1, N_1, U_1, N_2)$, $L_{3E}(U_1, N_2)$, where all the $L_B - L_E$ information symbols are fully immersed in the artificial noise symbols (N_1, U_1, N_2). Therefore, we can securely transmit $L_B - L_E = 1$ information symbol to Bob using $2(L_B - 1) = 4$ time slots. Thus, this scheme achieves $SDoF = \frac{L_B - L_E}{2(L_B - 1)} = \frac{1}{4}$.

IV. Proof of Theorem 1

We consider a transmission channel block with length $2(L_B - 1)$ in order to securely transmit $L_B - L_E$ information symbols to Bob. The order of information and artificial noise symbols transmission is described next:

Transmission by Alice

- In the first $L_B - L_E$ time slots, Alice transmits information symbols (i.e. a vector $S = \begin{bmatrix} S_1 & S_1 & \dots & S_{L_B - L_E} \end{bmatrix}$).
- In the next $L_E - 1$ time slots, Alice transmits artificial noise symbols (i.e. a noise vector $U = \begin{bmatrix} U_1 & U_2 & \dots & U_{L_E - 1} \end{bmatrix}$).
- In the last $L_B - 1$ time slots, Alice remains silent.

Transmission by Charlie (helper)

- In the first $L_B - 1$ time slots, Charlie transmits independently and identically distributed Gaussian artificial noise symbols, each with zero mean and variance P (i.e. a noise vector $N = \begin{bmatrix} N_1 & N_2 & \dots & N_{L_B - 1} \end{bmatrix}$).
- In the last $L_B - 1$ time slots, Charlie remains silent.

The received signals at Bob and Eve in a particular block, respectively, can be expressed as follows:

$$Y_B = \mathbf{H_{BA}} X_A + \mathbf{H_{BC}} X_C + Z_B \tag{9}$$

$$Y_E = \mathbf{H_{EA}} X_A + \mathbf{H_{EC}} X_C + Z_E, \tag{10}$$

where Y_B is of size $2(L_B - 1) \times 1$ and Y_E is of size $(L_B + L_E - 2) \times 1$. $\mathbf{H_{BA}}$ is the $2(L_B - 1) \times (L_B - 1)$ channel matrix portion carrying the signal vector X_A of size $(L_B - 1) \times 1$ from Alice to Bob. $\mathbf{H_{BC}}$ is the $2(L_B - 1) \times (L_B - 1)$ portion carrying the signal vector X_C of size $(L_B - 1) \times 1$ from Charlie to Bob. $\mathbf{H_{EA}}$ is the $(L_B + L_E - 2) \times (L_B - 1)$ portion carrying X_A from Alice to Eve and $\mathbf{H_{EC}}$ is the $(L_B + L_E - 2) \times (L_B - 1)$ portion carrying X_C from Charlie to Eve. Note that $X_A = [S\ U]^T$ and $X_C = [N]^T$. Thus, $\mathbf{H_{BA}} X_A$ has structure

$$\mathbf{H_{BA}} X_A = \begin{bmatrix} h_{BA}[1] & 0 & \cdots & 0 \\ h_{BA}[2] & h_{BA}[1] & \ddots & \vdots \\ \vdots & h_{BA}[2] & \ddots & 0 \\ h_{BA}[L_B] & \vdots & \ddots & h_{BA}[1] \\ 0 & h_{BA}[L_B] & \ddots & h_{BA}[2] \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & h_{BA}[L_B] \end{bmatrix} \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_{L_B - L_E} \\ U_1 \\ U_2 \\ \vdots \\ U_{L_E - 1} \end{bmatrix},$$

and $\mathbf{H_{BC}} X_C$ is given by

$$\mathbf{H_{BC}} X_C = \begin{bmatrix} h_{BC}[1] & 0 & \cdots & 0 \\ h_{BC}[2] & h_{BC}[1] & \ddots & \vdots \\ \vdots & h_{BC}[2] & \ddots & 0 \\ h_{BC}[L_B] & \vdots & \ddots & h_{BC}[1] \\ 0 & h_{BC}[L_B] & \ddots & h_{BC}[2] \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & h_{BC}[L_B] \end{bmatrix} \begin{bmatrix} N_1 \\ N_2 \\ \vdots \\ N_{L_B - 1} \end{bmatrix}.$$

Similarly, $\mathbf{H_{EA}}X_A$ is given by

$$\mathbf{H_{EA}}X_A = \begin{bmatrix} h_{EA}[1] & 0 & \cdots & 0 \\ h_{EA}[2] & h_{EA}[1] & \ddots & \vdots \\ \vdots & h_{EA}[2] & \ddots & 0 \\ h_{EA}[L_E] & \vdots & \ddots & h_{EA}[1] \\ 0 & h_{EA}[L_E] & \ddots & h_{EA}[2] \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & h_{EA}[L_E] \end{bmatrix} \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_{L_B-L_E} \\ U_1 \\ U_2 \\ \vdots \\ U_{L_E-1} \end{bmatrix}$$

and $\mathbf{H_{EC}}X_C$ is given by

$$\mathbf{H_{EC}}X_C = \begin{bmatrix} h_{EC}[1] & 0 & \cdots & 0 \\ h_{EC}[2] & h_{EC}[1] & \ddots & \vdots \\ \vdots & h_{EC}[2] & \ddots & 0 \\ h_{EC}[L_E] & \vdots & \ddots & h_{EC}[1] \\ 0 & h_{EC}[L_E] & \ddots & h_{EC}[2] \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & h_{EC}[L_E] \end{bmatrix} \begin{bmatrix} N_1 \\ N_2 \\ \vdots \\ N_{L_B-1} \end{bmatrix}.$$

Z_B and Z_E are channel noise vectors received at Bob and Eve, respectively. The signals Y_B and Y_E can be rewritten as

$$Y_B = \mathbf{H_{BS}}S + \mathbf{H_{BU}}U + \mathbf{H_{BN}}N + Z_B \quad (11)$$

$$Y_E = \mathbf{H_{ES}}S + \mathbf{H_{EU}}U + \mathbf{H_{EN}}N + Z_E, \quad (12)$$

where $\mathbf{H_{BS}}$ is the $2(L_B-1)\times(L_B-L_E)$ channel matrix portion of $\mathbf{H_{BA}}$ over which the information symbol vector S is received from Alice to Bob, $\mathbf{H_{BU}}$ is the $2(L_B-1)\times(L_E-1)$ channel matrix portion of $\mathbf{H_{BA}}$ over which the artificial noise symbol vector U is received from Alice to Bob, whereas $\mathbf{H_{BN}}$ is the $2(L_B-1)\times(L_B-1)$ channel matrix equivalent to $\mathbf{H_{BC}}$ over which the artificial noise symbol vector N is received from Charlie to Bob. $\mathbf{H_{ES}}$ is the $(L_B+L_E-2)\times(L_B-L_E)$ portion of $\mathbf{H_{EA}}$ over which S is received from Alice to Eve, $\mathbf{H_{EU}}$ is the $(L_B+L_E-2)\times(L_E-1)$ portion of $\mathbf{H_{EA}}$ over which U is received from Alice to Eve, whereas $\mathbf{H_{EN}}$ is the $(L_B+L_E-2)\times(L_B-1)$ matrix equivalent to $\mathbf{H_{EC}}$ over which N is received from Charlie to Eve.

To facilitate the proof of Theorem 1 using matrix properties, a simplified view of the proposed system of equations (11) and (12) is to think of a combined input signal vector X of size $2(L_B-1)\times 1$ created from the concatenation of the vectors S and U from Alice and N from Charlie such that $X = \begin{bmatrix} S & U & N \end{bmatrix}^T$. Each entry in the vector X, be it an information symbol or an artificial noise symbol, is assumed to be transmitted with a power P satisfying the power constrains in equations (3) and (4). Moreover, a horizontal concatenation can be done to matrices $\mathbf{H_{BS}}$, $\mathbf{H_{BU}}$, and $\mathbf{H_{BN}}$ to form a composite matrix $\mathbf{H_B}$, whereas a horizontal concatenation of matrices $\mathbf{H_{ES}}$, $\mathbf{H_{EU}}$, and $\mathbf{H_{EN}}$ leads to a composite matrix $\mathbf{H_E}$. Equations (11) and (12) can, hence, be simplified into

$$Y_B = \mathbf{H_B}X + Z_B \quad (13)$$

$$Y_E = \mathbf{H_E}X + Z_E, \quad (14)$$

where $\mathbf{H_B}$ is the complete $2(L_B-1)\times 2(L_B-1)$ channel matrix seen at Bob and $\mathbf{H_E}$ is the complete $(L_B+L_E-2)\times 2(L_B-1)$ channel matrix seen at Eve.

Information theoretically, for a transmission block of length $2(L_B-1)$, the achievable secrecy rate R_S is defined as

$$R_S = \frac{I(S;Y_B) - I(S;Y_E)}{2(L_B-1)}, \quad (15)$$

where $I(S;Y_B)$ is the mutual information between the information symbol vector S transmitted by Alice and Y_B, the signal received at Bob. $I(S;Y_E)$ is the mutual information between S and the vector Y_E received at Eve. These terms can be written as

$$I(S;Y_B) = h(Y_B) - h(Y_B|S) \quad (16)$$

$$I(S;Y_E) = h(Y_E) - h(Y_E|S). \quad (17)$$

Next, the terms of equation (16) are expanded as follows:

$$h(Y_B) = h(\mathbf{H_{BS}}S + \mathbf{H_{BU}}U + \mathbf{H_{BN}}N + Z_B) \quad (18)$$

$$= \log(\pi e)^{2(L_B-1)}\det(\mathbf{K_{B_{SUN}}}) \quad (19)$$

$$= \log(\pi e)^{2(L_B-1)}\det(\mathbf{I_{B_{SUN}}} + P\mathbf{H_{B_{SUN}}}\mathbf{H^H_{B_{SUN}}}), \quad (20)$$

where (19) follows from [11], $\mathbf{K_{B_{SUN}}} = \mathbf{I_{B_{SUN}}} + P\mathbf{H_{B_{SUN}}}\mathbf{H^H_{B_{SUN}}}$ is the covariance matrix of Y_B, $\mathbf{M^H}$ denotes the complex conjugate of $\mathbf{M}$, and $\mathbf{I_{B_{SUN}}}$ is the $2(L_B-1)\times 2(L_B-1)$ covariance of Z_B. $\mathbf{H_{B_{SUN}}}$ is identical to the channel matrix $\mathbf{H_B}$, and P is the symbol transmission power.

$$h(Y_B|S) = h(\mathbf{H_{BS}}S + \mathbf{H_{BU}}U + \mathbf{H_{BN}}N + Z_B|S) \quad (21)$$

$$= h(\mathbf{H_{BU}}U + \mathbf{H_{BN}}N + Z_B) \quad (22)$$

$$= h(\mathbf{H_{B_{UN}}}[UN]^T + Z_B) \quad (23)$$

$$= \log(\pi e)^{2(L_B-1)}\det(\mathbf{I_{B_{UN}}} + P\mathbf{H_{B_{UN}}}\mathbf{H^H_{B_{UN}}}), \quad (24)$$

where (22) follows from the independence of S from (U, N, Z_B). $\mathbf{I_{B_{UN}}}$ is equivalent to $\mathbf{I_{B_{SUN}}}$ from (20) and $\mathbf{H_{B_{UN}}}$ is the concatenation of $\mathbf{H_{BU}}$ and $\mathbf{H_{BN}}$. $\mathbf{I_{B_{UN}}} + P\mathbf{H_{B_{UN}}}\mathbf{H^H_{B_{UN}}}$ is the covariance matrix of $\mathbf{H_{B_{UN}}}[UN]^T + Z_B$.

Substituting (20) and (24) into (16), we have

$$I(S;Y_B) = \log\frac{\det(\mathbf{I_{B_{SUN}}} + P\mathbf{H_{B_{SUN}}}\mathbf{H^H_{B_{SUN}}})}{\det(\mathbf{I_{B_{UN}}} + P\mathbf{H_{B_{UN}}}\mathbf{H^H_{B_{UN}}})} \quad (25)$$

$$= \log\frac{\det(\mathbf{I_{B_{SUN}}} + P\mathbf{\Psi_{B_{SUN}}}\mathbf{\Lambda_{B_{SUN}}}\mathbf{\Lambda^H_{B_{SUN}}}\mathbf{\Psi^H_{B_{SUN}}})}{\det(\mathbf{I_{B_{UN}}} + P\mathbf{\Psi_{B_{UN}}}\mathbf{\Lambda_{B_{UN}}}\mathbf{\Lambda^H_{B_{UN}}}\mathbf{\Psi^H_{B_{UN}}})} \quad (26)$$

$$= \log\frac{\det(\mathbf{I_{B_{SUN}}} + P\mathbf{\hat{\Lambda}_{B_{SUN}}})}{\det(\mathbf{I_{B_{UN}}} + P\mathbf{\hat{\Lambda}_{B_{UN}}})} \quad (27)$$

$$= \sum_{i=1}^{2(L_B-1)} \log(1 + P|\lambda_{B_{SUN_i}}|^2) - \sum_{i=1}^{L_B+L_E-2} \log(1 + P|\lambda_{B_{UN_i}}|^2), \quad (28)$$

where the numerator of (26) follows from the singular value decomposition (SVD) of $\mathbf{H_{B_{SUN}}} = \mathbf{H_B}$ into $\mathbf{\Psi_{B_{SUN}}\Lambda_{B_{SUN}}V^H_{B_{SUN}}}$ and the denominator follows from the SVD of $\mathbf{H_{B_{UN}}}$ into $\mathbf{\Psi_{B_{UN}}\Lambda_{B_{UN}}V^H_{B_{UN}}}$. The numerator of (27) follows from the determinant identity $\det(\mathbf{I}+\mathbf{AB}) = \det(\mathbf{I}+\mathbf{BA})$ also known as Sylvester's Identity, matrix scalar multiplication associativity and commutativity properties, and the fact that $\mathbf{\Psi_{B_{SUN}}}$ and $\mathbf{V^H_{B_{SUN}}}$ are unitary matrices whose product is an identity matrix. The denominator of (27) follows from the identity det($\mathbf{I}+\mathbf{AB}$) = det($\mathbf{I}+\mathbf{BA}$), matrix scalar multiplication associativity and commutativity properties, and the fact that $\mathbf{\Psi_{B_{UN}}}$ and $\mathbf{V^H_{B_{UN}}}$ are unitary matrices whose product is an identity matrix. As shown by Lemma 1, $\mathbf{H_B} = \mathbf{H_{B_{SUN}}}$ is full rank, almost surely (see Appendix). Therefore, the first term of (28) follows from the fact that $\mathbf{\hat{\Lambda}_{B_{SUN}}}$ is a square diagonal matrix whose elements are $2(L_B-1)$ ordered squares of random singular values of the matrix $\mathbf{H_{B_{SUN}}}$ [12]. The second term of (28) follows from the fact that $\mathbf{\hat{\Lambda}_{B_{UN}}}$ is a square diagonal matrix whose elements are (L_B+L_E-2) ordered squares of random singular values of the full column rank matrix $\mathbf{H_{B_{UN}}}$ [12]. $\mathbf{H_{B_{UN}}}$ is full rank since it is a full column submatrix of the full rank matrix $\mathbf{H_B}$. See Lemma 1.

The first term of equation (17) can be expanded as

$$h(Y_E) = h(\mathbf{H_{ES}}S + \mathbf{H_{EU}}U + \mathbf{H_{EN}}N + Z_E) \quad (29)$$

$$= \log(\pi e)^{(L_B+L_E-2)} \det(\mathbf{K_{E_{SUN}}}), \quad (30)$$

where $\mathbf{K_{E_{SUN}}} = \mathbf{I_{E_{SUN}}} + P\mathbf{H_{E_{SUN}}}\mathbf{H^H_{E_{SUN}}}$ is the covariance of Y_E. $\mathbf{I_{E_{SUN}}}$ is the covariance of Z_E and $\mathbf{H_{E_{SUN}}}$ is identical to $\mathbf{H_E}$. In Lemma 2 (see Appendix), it is shown that $\mathbf{H_E}$ is of rank $L_B + L_E - 2$, almost surely.

Similarly, we expand the second term of equation (17) as

$$h(Y_E|S) = h(\mathbf{H_{ES}}S + \mathbf{H_{EU}}U + \mathbf{H_{EN}}N + Z_E|S) \quad (31)$$

$$= h(\mathbf{H_{EU}}U + \mathbf{H_{EN}}N + Z_E) \quad (32)$$

$$= h(\mathbf{H_{E_{UN}}}[UN]^T + Z_E) \quad (33)$$

$$= \log(\pi e)^{(L_B+L_E-2)} \det(\mathbf{I_{E_{UN}}} + P\mathbf{H_{E_{UN}}}\mathbf{H^H_{E_{UN}}}), \quad (34)$$

where (32) is from the independence of S from (U, N, Z_E). $\mathbf{H_{E_{UN}}}$ is the concatenation of $\mathbf{H_{EU}}$ and $\mathbf{H_{EN}}$. $\mathbf{I_{E_{UN}}} + P\mathbf{H_{E_{UN}}}\mathbf{H^H_{E_{UN}}}$ is the covariance of $\mathbf{H_{E_{UN}}}[UN]^T + Z_E$.

Equation (17) can, therefore, be rewritten as

$$I(S;Y_E) = \log \frac{\det(\mathbf{I_{E_{SUN}}} + P\mathbf{H_{E_{SUN}}}\mathbf{H^H_{E_{SUN}}})}{\det(\mathbf{I_{E_{UN}}} + P\mathbf{H_{E_{UN}}}\mathbf{H^H_{E_{UN}}})} \quad (35)$$

$$= \sum_{i=1}^{(L_B+L_E-2)} \log(1+P|\lambda_{E_{SUN_i}}|^2) - \sum_{i=1}^{L_B+L_E-2} \log(1+P|\lambda_{E_{UN_i}}|^2), \quad (36)$$

where (35)-(36) follow the same arguments as (25)-(28)

From the definition of SDoF in (7), the definition of secrecy rate in (15), and the expansion of the individual terms of equations (16) and (17) into (28) and (36), respectively, we obtain the following SDoF.

$$SDoF \geq \lim_{P\to\infty} \frac{R_S}{\log(P)} = \lim_{P\to\infty} \frac{I(S;Y_B) - I(S;Y_E)}{2(L_B-1)\log(P)} \quad (37)$$

$$= \lim_{P\to\infty} \Big(\frac{\sum_{i=1}^{2(L_B-1)} \log(1+P|\lambda_{B_{SUN_i}}|^2)}{2(L_B-1)\log(P)} - \frac{\sum_{i=1}^{L_B+L_E-2} \log(1+P|\lambda_{B_{UN_i}}|^2)}{2(L_B-1)\log(P)} \Big) \quad (38)$$

$$- \lim_{P\to\infty} \Big(\frac{\sum_{i=1}^{L_B+L_E-2} \log(1+P|\lambda_{E_{SUN_i}}|^2)}{2(L_B-1)\log(P)} - \frac{\sum_{i=1}^{L_B+L_E-2} \log(1+P|\lambda_{E_{UN_i}}|^2)}{2(L_B-1)\log(P)} \Big) \quad (39)$$

$$= \Big(\frac{2(L_B-1) - (L_B+L_E-2)}{2(L_B-1)} \Big) - \Big(\frac{(L_B+L_E-2) - (L_B+L_E-2)}{2(L_B-1)} \Big) \quad (40)$$

$$= \frac{L_B - L_E}{2(L_B-1)}. \quad (41)$$

Hence, this completes the proof of Theorem 1.

V. Conclusion and Further Research

We investigated the SISO wiretap channel with ISI in the presence of a helper and characterized its achievable SDoF without any CSIT. We showed how strategic transmission of information and artificial noise symbols achieves positive SDoF by taking the advantage of the heterogeneity in the ISI link lengths towards the legitimate receiver and the eavesdropper. There are several interesting directions for future work stemming from the exploitation of ISI heterogeneity. We are currently investigating the generalization of this scheme to the case of arbitrary ISI link lengths, obtaining an upper bound on SDoF in the ISI heterogeneity, and the use of multiple antennas to further exploit ISI heterogeneity to achieve higher SDoF than the SISO setting.

Appendix

We now provide proofs of ranks of the channel matrices $\mathbf{H_B}$ and $\mathbf{H_E}$ that were essential in the proof of Theorem 1.

Lemma 1. *Let $\mathbf{H_B}$ be a square channel matrix with size $2(L_B-1) \times 2(L_B-1)$ whose nonzero elements in the first column C_{1B} and in second column C_{2B} are the independently and identically distributed continuous random channel coefficients from Alice to Bob and from Charlie to Bob, respectively, such that $C_{1B} = \begin{bmatrix} h_{BA}[1] & h_{BA}[2] & \dots & h_{BA}[L_B] & 0 & \dots & 0 \end{bmatrix}^T$ and $C_{2B} = \begin{bmatrix} h_{BC}[1] & h_{BC}[2] & \dots & h_{BC}[L_B] & 0 & \dots & 0 \end{bmatrix}^T$. And let the rest of columns of $\mathbf{H_B}$ be L_B-2 simultaneous vertically circular permutations of the first and the second columns, respectively. Then, the matrix $\mathbf{H_B}$ is full rank.*

Proof: Consider the received square channel matrix $\mathbf{H_B}$ at Bob. To prove that it is full rank, it suffices to show that

$$\mathbf{H_B}\vec{\alpha}^T = \vec{0} \quad (42)$$

has only the trivial solution $\vec{\alpha} = \vec{0}$, for some vector $\vec{\alpha} = \begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{r_B=2(L_B-1)} \end{bmatrix}$. Since permutations of columns of a matrix do not alter its rank, we can write $\mathbf{H_B}$ with columns permuted into a specific positions and,

$$\begin{bmatrix} h_{BA}^{[1]} & h_{BC}^{[1]} & 0 & 0 & \dots & 0 & 0 \\ h_{BA}^{[2]} & h_{BC}^{[2]} & h_{BA}^{[1]} & h_{BC}^{[1]} & \ddots & \vdots & \vdots \\ h_{BA}^{[3]} & h_{BC}^{[3]} & h_{BA}^{[2]} & h_{BC}^{[2]} & \ddots & 0 & 0 \\ \vdots & \vdots & h_{BA}^{[3]} & h_{BC}^{[3]} & \ddots & h_{BA}^{[1]} & h_{BC}^{[1]} \\ h_{BA}^{[L_B]} & h_{BC}^{[L_B]} & \vdots & \vdots & \vdots & h_{BA}^{[2]} & h_{BC}^{[2]} \\ 0 & 0 & h_{BA}^{[L_B]} & h_{BC}^{[L_B]} & \ddots & h_{BA}^{[3]} & h_{BC}^{[3]} \\ \vdots & \vdots & 0 & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & h_{BA}^{[L_B]} & h_{BC}^{[L_B]} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \vdots \\ \alpha_{r_B} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix} \tag{43}$$

therefore, be able to explicitly write the system in (42) as shown in (43).

From the first row of the system of equations (43), we have $\alpha_1 h_{BA}^{[1]} + \alpha_2 h_{BC}^{[1]} = 0$. This is not possible, since $h_{BA}[1]$ and $h_{BC}[1]$ are independently and identically distributed continuous random channel coefficients respectively selected from two independent channel vectors $H_{BA} = \begin{bmatrix} h_{BA}[1] & h_{BA}[2] & \dots & h_{BA}[L_B] \end{bmatrix}^T$ and $H_{BC} = \begin{bmatrix} h_{BC}[1] & h_{BC}[2] & \dots & h_{BC}[L_B] \end{bmatrix}^T$, unless $\alpha_1 = \alpha_2 = 0$. Now, let $\alpha_1 = \alpha_2 = 0$. From the second row, we get $\alpha_1 h_{BA}^{[2]} + \alpha_2 h_{BC}^{[2]} + \alpha_3 h_{BA}^{[1]} + \alpha_4 h_{BC}^{[1]} = \alpha_3 h_{BA}^{[1]} + \alpha_4 h_{BC}^{[1]} = 0$, which is also not possible unless $\alpha_3 = \alpha_4 = 0$. Continuing recursively through all the equations in (43) in a similar order as above, using the same argument of contradiction, leads to the conclusion that the system in (42) has only the trivial solution $\vec{\alpha} = \vec{0}$. This proves that $\mathbf{H_B}$ is of full rank $2(L_B - 1)$.

Lemma 2. *Let $\mathbf{H_E}$ be a rectangular channel matrix of size $(L_B + L_E - 2) \times 2(L_B - 1)$, where $(L_B + L_E - 2) < 2(L_B - 1)$, whose nonzero elements in the first column C_{1E} and in second column C_{2E} are the independently and identically distributed continuous random channel coefficients from Alice to Eve and from Charlie to Eve, respectively, such that $C_{1E} = \begin{bmatrix} h_{EA}[1] & h_{EA}[2] & \dots & h_{EA}[L_E] & 0 & \dots & 0 \end{bmatrix}^T$ and $C_{2E} = \begin{bmatrix} h_{EC}[1] & h_{EC}[2] & \dots & h_{EC}[L_E] & 0 & \dots & 0 \end{bmatrix}^T$. And let the rest of columns of $\mathbf{H_E}$ be $L_B - 2$ simultaneous vertically circular permutations of the first and the second columns, respectively. Then, $\mathbf{H_E}$ is of rank $(L_B + L_E - 2)$.*

Proof: Consider the received rectangular channel matrix $\mathbf{H_E}$ (of similar construct to $\mathbf{H_B}$ in (43) albeit rectangular) at Eve. To prove that its rank is $(L_B + L_E - 2)$, it suffices to show that its submatrix $\mathbf{H_{E_{UN}}}$ of size $(L_B + L_E - 2) \times (L_B + L_E - 2)$ that carries all the artificial noise symbols (from both Charlie and Alice) is full rank. Therefore, it suffices to show that

$$\mathbf{H_{E_{UN}}} \vec{\beta}^{\,T} = \vec{0} \tag{44}$$

has only the trivial solution $\vec{\beta} = \vec{0}$ for some vector $\vec{\beta} = \begin{bmatrix} \beta_1 & \beta_2 & \dots & \beta_{r_E = L_B + L_E - 2} \end{bmatrix}$. Since permutations of columns of a matrix do not alter its rank, we can write $\mathbf{H_{E_{UN}}}$ with columns permuted into specific positions as in (45).

$$\begin{bmatrix} h_{EC}^{[1]} & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ h_{EC}^{[2]} & h_{EC}^{[1]} & \dots & \vdots & \vdots & \ddots & 0 & 0 \\ h_{EC}^{[3]} & h_{EC}^{[2]} & \dots & 0 & 0 & \vdots & 0 & 0 \\ \vdots & h_{EC}^{[3]} & \ddots & \vdots & h_{EA}^{[1]} & \ddots & \vdots & \vdots \\ h_{EC}^{[L_E]} & \vdots & \ddots & 0 & \vdots & \vdots & 0 & \vdots \\ 0 & h_{EC}^{[L_E]} & \ddots & h_{EC}^{[1]} & \vdots & \vdots & h_{EA}^{[1]} & 0 \\ \vdots & 0 & \ddots & h_{EC}^{[2]} & h_{EA}^{[L_E]} & \vdots & \vdots & h_{EA}^{[1]} \\ \vdots & \vdots & \ddots & h_{EC}^{[3]} & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & h_{EA}^{[L_E]} & \vdots \\ 0 & 0 & \dots & h_{EC}^{[L_E]} & 0 & \dots & 0 & h_{EA}^{[L_E]} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \vdots \\ \beta_{r_E} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix} \tag{45}$$

From the first equation of system (45), we have $\beta_1 h_{EC}^{[1]} = 0$. This is only possible if $\beta_1 = 0$ because $h_{EC}[1]$ is a nonzero channel coefficient selected from the channel vector $H_{EC} = \begin{bmatrix} h_{EC}[1] & h_{EC}[2] & \dots & h_{EC}[L_E] \end{bmatrix}^T$. Now, let $\beta_1 = 0$. From the second row, we have $\beta_1 h_{EC}^{[2]} + \beta_2 h_{EC}^{[1]} = \beta_2 h_{EC}^{[1]} = 0$. This condition is not possible unless $\beta_2 = 0$. Continuing recursively through system (45) with the same logical argument of contradiction shows that the system (44) has only the trivial solution $\vec{\beta} = \vec{0}$. This proves that $\mathbf{H_{E_{UN}}}$ is full rank.

REFERENCES

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

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

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[4] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the K-user Gaussian interference channel," in *Proc. IEEE International Symposium on Information Theory*, pp. 384–388, 2008.

[5] P. Mukherjee, R. Tandon, and S. Ulukus, "Secrecy for MISO broadcast channels via alternating CSIT," in *Proc. IEEE International Conference on Communications*, pp. 4157–4162, 2015.

[6] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," in *Proc. Annual Allerton Conference on Communication, Control, and Computing*, pp. 193–200, 2012.

[7] ——, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Proc. Conference on Information Sciences and Systems*, 2013.

[8] M. Nafea and A. Yener, "Secure degrees of freedom of N×N×M wiretap channel with a K-antenna cooperative jammer," in *Proc. IEEE International Conference on Communications*, pp. 4169–4174, 2015.

[9] S. A. Jafar, "Blind interference alignment," *IEEE Journal of Selected Topics in Signal Processing*, vol. 6, no. 3, pp. 216–227, 2012.

[10] N. Lee, "Interference-free OFDM: rethinking OFDM for interference networks with inter-symbol interference," *CoRR*, vol. abs/1609.02517, 2016. [Online]. Available: http://arxiv.org/abs/1609.02517

[11] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[12] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge University Press, 2005.