MIMO Wiretap Channel with ISI Heterogeneity– Achieving Secure DoF with no CSI

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

***Abstract*—We consider the multiple-input multiple-output (MIMO) wiretap channel with intersymbol interference (ISI) in which a transmitter (Alice) wishes to securely communicate with a receiver (Bob) in presence of an eavesdropper (Eve). We focus on the practically relevant setting in which there is no channel state information (CSI) at Alice about either of the channels to Bob or Eve, except statistical information about the ISI channels (i.e., Alice only knows the effective number of ISI taps). The key contribution of this work is to show that even with no CSI at Alice, positive secure degrees of freedom (SDoF) are achievable by carefully exploiting a) the heterogeneity of the ISI links to Bob and Eve, and b) the relative number of antennas at all the three terminals. To this end, we propose a novel achievable scheme that carefully mixes information and artificial noise symbols in order to exploit ISI heterogeneity to achieve positive SDoF. To the best of our knowledge, this is the first work to explore the idea of exploiting ISI channel length heterogeneity to achieve positive SDoF for the MIMO wiretap channel with no CSI at the legitimate transmitter.**

I. Introduction

The key idea behind physical (PHY) layer security is to exploit the inherent randomness in the wireless channel such as fading or noise. While these characteristics have always been seen as impairments, the paradigm of physical-layer security takes advantage of these characteristics in order to improve security. The majority of research developments on PHY layer security have been made under the assumptions of availability of the knowledge of wireless channel–be it instantaneous [1]–[3], delayed [4], [5], or alternating [6]. Another approach to chieve security uses cooperative jammers to purposefully send artificial noise in a manner that aligns the interference in the signal space at the adversary's node while keeping this interference discardable at the legitimate receiver's node [7], [8]. The problem of secrecy capacity of MIMO wiretap channels with ISI under full CSI availability was recently solved by [9]. We refer the reader to [10], [11] for an excellent recent surveys on this topic.

Assumptions on the availability of channel knowledge from adversaries are by far the most critical and unrealistic as it is not practically feasible to fetch CSI from eavesdropping nodes. Thus the need for schemes that achieve security in the absence of CSIT. For channels without ISI, recent work [12] has explored SDoF for the MIMO wiretap channel with a helper and showed that, in the absence of CSI, positive SDoF can be achieved whenever the number of antennas at the eavesdropper is less than the number of antennas at the legitimate receiver. In this paper, we will show that, for channels with ISI, positive SDoF can be achieved in the absence of CSI at the transmitters, even when the legitimate receiver has a smaller number of antennas than the eavesdropper.

This work was supported by NSF grants CCF-1559758 and CNS-1715947.

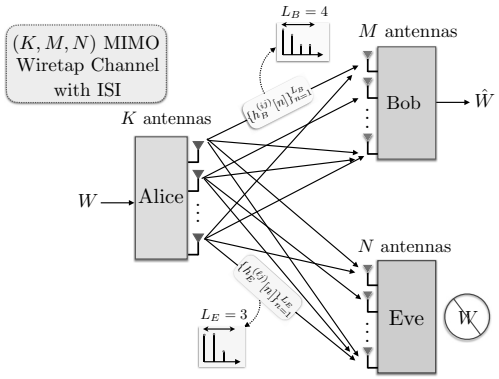

Fig. 1: The (K, M, N) MIMO Wiretap channel with ISI. L_B and L_E denote the effective channel taps for the channels between Alice and Bob and Alice and Eve, respectively.

One of the positive aspects of the wireless medium is that it not only possesses randomness, but it can also offer abundant statistical heterogeneity. That is, channels to the legitimate users and adversaries can be statistically dissimilar, based on their relative multi-path propagation environment and fading [13], [14]. In this work, we focus on the MIMO wiretap channel with inter symbol interference (ISI), where the channels to Bob and Eve are MIMO ISI Channels. The main novel aspect of this paper is to show that in the presence of statistical heterogeneity in ISI, channel statistical knowledge alone is in fact sufficient enough to achieve positive secure degrees of freedom (SDoF). This exploitation of ISI heterogeneity (the difference in channel impulse response (CIR) lengths towards Bob and Eve) is particularly practical for Ultra-wideband (UWB) systems that tend to have several hundreds of channel taps [13].

More specifically, we consider the MIMO wiretap channel with ISI. Taking into account the ISI link lengths towards both the legitimate receiver and the eavesdropper, the transmitter instead uses varying portions of its number of antennas over the course of the transmission duration to methodically transmit both information and artificial noise symbols in a manner that allows the decodability of information symbol at the legitimate receiver while keeping these information

symbols fully immersed in artificial noise symbols at the eavesdropper. A general scheme is obtained as a function of the number of antennas at the terminals and the characteristics of the ISI channels, thereby leading to a lower bound on the SDoF.

II. System Model

In this paper, we focus on the MIMO wiretap channel with ISI as shown in Fig. 1, where Alice (A) (with K antennas), wants to securely communicate with Bob (B) (with M antennas), in the presence of an eavesdropper, Eve (E) (equipped with N antennas). The channels from Alice to Bob and Eve are assumed to be ISI channels, where $\left\{h_B^{(ij)}[q]\right\}_{q=1}^{L_B}$ denotes the channel impulse response (CIR) between the jth antenna of Alice and the ith antenna at Bob, where $i = 1,\dots M$ and $j = 1,\dots,K$. Similarly, $\left\{h_E^{(\ell j)}[q]\right\}_{q=1}^{L_E}$ denotes the CIR between the jth antenna at Alice and the ℓth antenna at Eve, where $j = 1,\dots K$ and $\ell = 1,\dots,N$. All CIR coefficients are assumed to be independent and identically distributed (i.i.d.) from a continuous distribution. L_B and L_E are channel tap length parameters, i.e., the maximum number of effective channel taps between Alice and Bob and between Alice and Eve, respectively. The CSI availability assumptions are:

- Alice does not have any instantaneous CSI and she only knows the ISI link lengths L_B and L_E.
- Bob only knows his local channel coefficients $\left\{h_B^{(ij)}[q]\right\}_{q=1}^{L_B}$, $i = 1,\dots M$ and $j = 1,\dots,K$, which are necessary for coherent decoding at his end.
- Eve has access to all coefficients (i.e. can access all CIRs).

Let $\mathbf{X_A}[k]$ be a $K \times 1$ symbol vector transmitted by Alice at time k, then the respective signal vectors seen at Bob and Eve at are

$$\mathbf{Y_B}[k] = \sum_{n=1}^{L_B} \mathbf{H_B}[n]\mathbf{X_A}[k-n+1] + \mathbf{Z_B}[k] \tag{1}$$

$$\mathbf{Y_E}[k] = \sum_{n=1}^{L_E} \mathbf{H_E}[n]\mathbf{X_A}[k-n+1] + \mathbf{Z_E}[k] \tag{2}$$

where $(\mathbf{H_B}[n])_{(i,j)} = h_B^{(ij)}[n]$ and $(\mathbf{H_E}[n])_{(i,j)} = h_E^{(\ell j)}[n]$. $\mathbf{Z_B}[k]$ and $\mathbf{Z_E}[k]$ are channel noise vectors respectively received at Bob and Eve at time k and whose elements are complex circularly independent zero-mean unit-variance. Each symbol vector $\mathbf{X_A}[k]$ is transmitted with power P satisfying the constraint

$$\mathbf{E}\left[{\mathbf{X_A}}^2[k]\right] \le P. \tag{3}$$

A secure rate of communication $R_s = \frac{\log(|W|)}{n}$ is achievable, if there exists an n-length code that, for any $\epsilon \to 0$ and $n \to \infty$, satisfies both the reliability and secrecy constraints:

$$Pr[W \neq \hat{W}] \le \epsilon \tag{4}$$

$$\frac{1}{n} H(W|{\mathbf{Y_E}}^{(n)}) \ge R_s - \epsilon, \tag{5}$$

where (4) represents the decoding error probability, and (5) represents the uncertainty about the transmitted message W given ${\mathbf{Y_E}}^{(n)} = \{\mathbf{Y_E}[k]\}_{k=1}^n$, the signal observed at Eve. $\hat{W} = g({\mathbf{Y_B}}^{(n)})$, where ${\mathbf{Y_B}}^{(n)} = \{\mathbf{Y_B}[k]\}_{k=1}^n$ is the signal observed at Bob and $g(\,.\,)$ represents a decoding operation.

The secrecy capacity C_s is defined as the supremum of all securely achievable rates R_s. We next define the secure degrees of freedom (SDoF) as the pre-log of secrecy capacity.

$$\mathsf{SDoF} \triangleq \lim_{P\to\infty} \frac{C_S}{\log(P)}. \tag{6}$$

The main contribution of this paper is stated in the following theorem which shows that positive SDoF is achievable under the CSI assumptions stated above.

III. Main Result

Theorem 1. *For the (K, M, N) MIMO wiretap channel without any CSIT and with effective ISI channels of CIR lengths L_B and L_E for Bob and Eve, the following SDoF is achievable*

$$\mathsf{SDoF} \ge \frac{\left((K-N)\left(\left\lceil\frac{M(L_B-1)}{K-M}\right\rceil - \frac{N(L_E-1)}{K-N}\right)\right)^+}{\left\lceil\frac{M(L_B-1)}{K-M}\right\rceil + (\max(L_B,L_E)-1)}, \tag{7}$$

where $(x)^+ \triangleq \max(x,0)$ and $\lceil x\rceil = \min\{n \in \mathbb{Z} | n \ge x\}$.

The following illustrative example shows the key idea of exploiting ISI heterogeneity to transmit a mix of information and artificial noise symbols in order to achieve positive SDoF.

Example 1: Consider the $(K, M, N) = (3, 1, 2)$ MIMO wiretap channel with ISI and $(L_B, L_E) = (3, 1)$, i.e., any symbol sent by Alice will be seen over $L_B = 3$ time slots at each of Bob's $M = 1$ antenna and over $L_E = 1$ time slot at each of Eve's $N = 2$ antennas. Our goal is to show that we can achieve $\mathsf{SDoF} = \frac{1}{3}$. Our scheme works over 3 time slots as shown in Fig. 2.

Transmission by Alice: In the first time slot, Alice sends an information symbol S and two artificial noise symbols (N_1, N_2) (all distributed as i.i.d. Gaussian with power P) on its $K = 3$ antennas, i.e., a vector $\mathbf{X}_A[1] = [S\ N_1\ N_2]^\top$, where $\mathbf{X}^\top$ denotes the transpose of $\mathbf{X}$. For the remaining two time-slots, Alice remains silent, which can be viewed as zero-padding (i.e., $\mathbf{X}_A[2] = \mathbf{X}_A[3] = [0\ 0\ 0]^\top$).

Decodability at Bob: Since the channel coefficients are distributed i.i.d., Bob (with $M = 1$ antenna) observes three independent linear equations over three time slots because $L_B = 3$; in other words, Bob observes $L_{1B}(S, N_1, N_2), L_{2B}(S, N_1, N_2), L_{3B}(S, N_1, N_2)$, from which he is able to solve for information symbol S and discard the artificial noises.

Secrecy at Eve: Since Eve's ISI channel has effective tap length of $L_E = 1$, she will only observe two equations on her $N = 2$ antennas in the first time slot; in other words, Eve observes $L_{1E}(S, N_1, N_2), L_{2E}(S, N_1, N_2)$, which means her observations are fully immersed in the artificial noises (N_1, N_2). For this scheme, the achievable secure rate can be obtained as $R_s = \frac{I(S;\mathbf{Y}_B) - I(S;\mathbf{Y}_E)}{3} = \frac{\log(P)}{3} + o(\log(P))$, which can be shown to achieve $\mathsf{SDoF} = \frac{1}{3}$, matching the expression stated in Theorem 1.

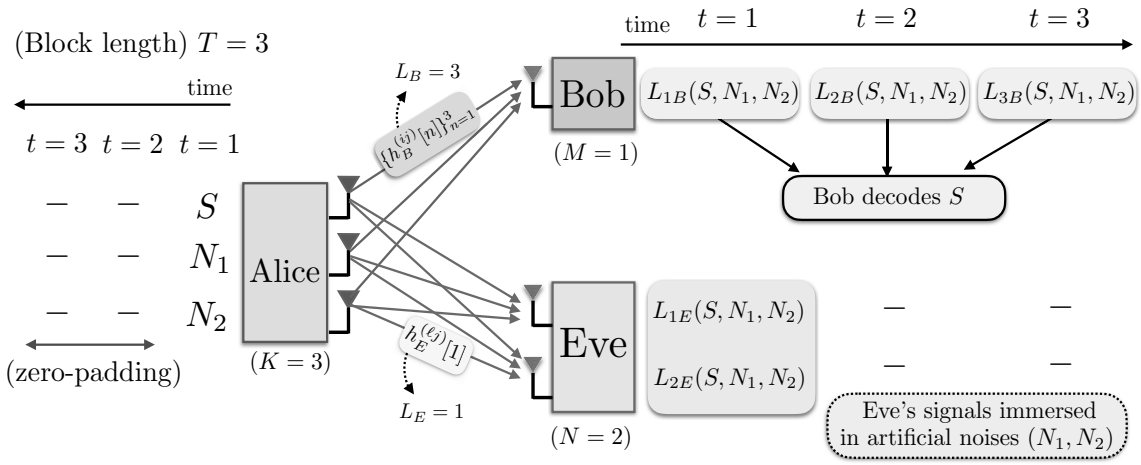

Fig. 2: Illustrative example for the MIMO Wiretap channel with ISI heterogeneity where $(K, M, N) = (3, 1, 2)$ and $(L_B, L_E) = (3, 1)$. For this example, we can achieve a secure degrees of freedom (SDoF) of $1/3$ by sending one symbol securely to Bob in 3 time slots.

IV. Proof of Theorem 1

The proof is divided into three parts. In the first part, we describe the transmission scheme strategy. In the second part, we describe the transmitted signal, the ISI channel matrices, and the received signal vectors. In the third part, we characterize the secrecy rate, and calculate the SDoF of the proposed scheme.

A. Transmission Scheme

We now consider the general setting of arbitrary (K, M, N) antenna configurations and arbitrary (L_B, L_E), the ISI tap length parameters. The general scheme works over a transmission block of duration T. Alice transmits a combination of information symbols along with artificial noises during the first r time slots, and remains silent during the last $(\max(L_B, L_E) - 1)$ time slots. Thus, the total transmission block duration is

$$T = r + (\max(L_B, L_E) - 1). \tag{8}$$

• *Transmission by Alice*: In each of the first r time slots, Alice sends α_i information symbols, for $i = 1, 2, \ldots, r$, and $(K - \alpha_i) = \beta_i$ artificial noise symbols on her K antennas. Hence, Alice transmits a total of $\sum_{i=1}^{r} \alpha_i$ information symbols (IS) and a total of $rK - \sum_{i=1}^{r} \alpha_i = \sum_{i=1}^{r} \beta_i$ artificial noise (AN) symbols over r time slots. Due to ISI heterogeneity, transmissions sent during each such time slot will be observed over L_B time slots at Bob and over L_E time slots at Eve.

• *Decodability at Bob*: We enforce Bob to decode both information symbols as well as artificial noise symbols, and this is feasible as long as the total number of (ISs + ANs), i.e., rK is no larger than the number of linearly independent equations seen at Bob. That is

$$rK \leq M(r + L_B - 1). \tag{9}$$

Hence, r must satisfy

$$r \leq \left\lceil \frac{M(L_B - 1)}{K - M} \right\rceil, \tag{10}$$

where the right hand side of the inequality (10) is ceiled because the number of symbol transmission time slots is a positive integer. From (8) and (10), we thus obtain the following inequality for the transmission block duration

$$T \leq \left\lceil \frac{M(L_B - 1)}{K - M} \right\rceil + (\max(L_B, L_E) - 1). \tag{11}$$

• *Secrecy at Eve*: In order to achieve secrecy, we ensure that the signal space at Eve is completely immersed in artificial noise. In particular, the total number of ANs, i.e., $rK - \sum_{i=1}^{r} \alpha_i = \sum_{i=1}^{r} \beta_i$ must be at least as large as the number of independent equations seen at Eve. This leads to the constraint

$$rK - \sum_{i=1}^{r} \alpha_i \geq N(r + L_E - 1), \tag{12}$$

where the right hand side of the inequality (12) represents the number of equations seen at Eve. This equation (12) is later used in the equivocation analysis and the secrecy rate calculation.

B. Matrix Representation of Input and Output Signals

Let $\mathbf{X_A}$ be a composite signal vector of size $rK \times 1$, consisting of both the information and artificial noise symbols transmitted from Alice, whose components are the $K \times 1$ vectors $\mathbf{X_A}[i]$ transmitted during the ith time slot, for $i = 1, 2, \ldots, r$, satisfy the power constraint in (3). Over the duration of a whole transmission block of length T, the received signal vectors at Bob and Eve can be written by means of two equivalent matrix representation forms as shown next. These representations will be useful in the analysis of the secrecy rate and the SDoF calculations in subsection 4.3. The outputs at Bob and Eve over the transmission block can be written as follows. Starting from equations (1) and (2), we can write the composite signals $\mathbf{Y_B} = [\mathbf{Y_B}[1], \mathbf{Y_B}[2], \ldots, \mathbf{Y_B}[r + L_B - 1]]$ and $\mathbf{Y_E} = [\mathbf{Y_E}[1], \mathbf{Y_E}[2], \ldots, \mathbf{Y_E}[r + L_E - 1]]$ as follows:

$$\mathbf{Y_B} = \mathbf{H_B}\mathbf{X_A} + \mathbf{Z_B} \tag{13}$$

$$\mathbf{Y_E} = \mathbf{H_E}\mathbf{X_A} + \mathbf{Z_E}. \tag{14}$$

where $\mathbf{X_A} = [\mathbf{X_A}[1], \mathbf{X_A}[2], \ldots, \mathbf{X_A}[r]]^\top = [\mathbf{S}_{\alpha_1}, \mathbf{N}_{\beta_1}, \mathbf{S}_{\alpha_2}, \mathbf{N}_{\beta_2}, \ldots, \mathbf{S}_{\alpha_r}, \mathbf{N}_{\beta_r}]^\top$, $\mathbf{S}_{\alpha_i}$ is an $\alpha_i \times 1$ vector consisting of all the information symbols transmitted

by Alice over α_i antennas in the ith time slot, for $i = 1, 2, \ldots, r$, and $\mathbf{N}_{\beta_i}$ is a $(K - \alpha_i) \times 1$ vector consisting of all the artificial noise symbols transmitted by Alice over $\beta_i = K - \alpha_i$ antennas in the ith time slot. $\mathbf{Y_B}$ is the $M(r + L_B - 1) \times 1$ composite signal vector seen at Bob. Here $(\mathbf{H_B}[n])_{(i,j)} = h_B^{(ij)}[n]$ and $\mathbf{H_B}[n]$ is an $M \times K$ matrix. $\mathbf{H_B}$ is the composite $M(r + L_B - 1) \times rK$ channel matrix seen at Bob, $\mathbf{X_A}$ is the $rk \times 1$ composite symbols vector transmitted by Alice over the whole transmission block, whereas $\mathbf{Z_B}$ is the $M(r + L_B - 1) \times 1$ composite channel noise vector seen at Bob.

Similarly, $\mathbf{Y_E}$ is the $N(r + L_E - 1) \times 1$ composite signal vector seen at Eve. $\mathbf{H_E}$ is the composite $N(r+L_E-1)\times rK$ channel matrix seen at Eve. Here $(\mathbf{H_E}[n])_{(i,j)} = h_E^{(\ell j)}[n]$ and $\mathbf{H_E}[n]$ is an $N \times K$ matrix. Whereas $\mathbf{Z_E}$ is the $N(r + L_E - 1) \times 1$ composite channel noise vector seen at Eve. Due to space limitations, the explicit channel matrix structures are provided in the full version of the paper [15].

Using properties of the system model equations (1)-(2) and their matrix form representation in (13)-(14), we can further rewrite $\mathbf{Y_B}$ and $\mathbf{Y_E}$ by splitting the channel matrices into the information symbol and artificial noise carrying matrices as

$$\mathbf{Y_B} = \mathbf{H_B^S S} + \mathbf{H_B^N N} + \mathbf{Z_B} \tag{15}$$

$$\mathbf{Y_E} = \mathbf{H_E^S S} + \mathbf{H_E^N N} + \mathbf{Z_E}, \tag{16}$$

where $[\mathbf{H_B^S}\ \ \mathbf{H_B^N}] = \mathbf{H_B}$. Here $\mathbf{H_B^S}$ is the information symbol carrying submatrix of size $M(r+L_B-1)\times\sum_{i=1}^{r}\alpha_i$ whereas $\mathbf{H_B^N}$ is the artificial noise carrying submatrix of size $M(r + L_B - 1) \times \sum_{i=1}^{r}\beta_i$. Similarly, $[\mathbf{H_E^S}\ \mathbf{H_E^N}] = \mathbf{H_E}$. And $\mathbf{H_E^S}$ is the information symbol carrying submatrix of size $N(r + L_E - 1) \times \sum_{i=1}^{r}\alpha_i$ whereas $\mathbf{H_E^N}$ is the artificial noise carrying submatrix of size $N(r + L_E - 1) \times \sum_{i=1}^{r}\beta_i$. $\mathbf{S} = [\mathbf{S}_{\alpha_1}\ \mathbf{S}_{\alpha_2}\ \ldots\ \mathbf{S}_{\alpha_r}]^\top$ is the information symbols subvector of $\mathbf{X_A}$ whereas $\mathbf{N} = [\mathbf{N}_{\beta_1}\ \mathbf{N}_{\beta_2}\ \ldots\ \mathbf{N}_{\beta_r}]^\top$ is the artificial noise symbols subvector of $\mathbf{X_A}$. The explicit channel matrix structures are provided in the full version of the paper [15].

C. Secrecy Rate and SDoF Calculation

The secrecy rate R_s over a transmission block of duration T is given by

$$R_S = \frac{I(\mathbf{S};\mathbf{Y_B}) - I(\mathbf{S};\mathbf{Y_E})}{T}, \tag{17}$$

where $I(\mathbf{S};\mathbf{Y_B})$ is the mutual information between transmitted composite information symbols vector $\mathbf{S}$ and $\mathbf{Y_B}$, the received composite signal vector at Bob. $I(\mathbf{S};\mathbf{Y_E})$ is the mutual information between $\mathbf{S}$ and $\mathbf{Y_E}$, the received composite signal vector at Eve. In terms of differential entropy, we can write,

$$I(\mathbf{S};\mathbf{Y_B}) = h(\mathbf{Y_B}) - h(\mathbf{Y_B}|\mathbf{S}) \tag{18}$$

$$I(\mathbf{S};\mathbf{Y_E}) = h(\mathbf{Y_E}) - h(\mathbf{Y_E}|\mathbf{S}). \tag{19}$$

We can now use equation (13) to write $h(\mathbf{Y_B})$ as

$$h(\mathbf{Y_B}) = h(\mathbf{H_B X_A} + \mathbf{Z_B}) \tag{20}$$

$$= \log(\pi e)^{M(r+L_B-1)} \det(\mathbf{I_B} + P\mathbf{H_B}{\mathbf{H_B}}^H), \tag{21}$$

where (21) follows from [16] and $\mathbf{I_B} + P\mathbf{H_B}{\mathbf{H_B}}^H$ is the covariance matrix of $\mathbf{Y_B}$. $\mathbf{I_B}$ is an $M(r+L_B-1)\times M(r+L_B-1)$ covariance matrix of the channel noise vector $\mathbf{Z_B}$. P is the symbol transmission power. Lemma 1 (stated below) shows that the matrix $\mathbf{H_B}$ is of rank $M(r+L_B-1)$, almost surely. Using equation (15), we can write $h(\mathbf{Y_B}|\mathbf{S})$ as follows

$$h(\mathbf{Y_B}|\mathbf{S}) = h(\mathbf{H_B^S S} + \mathbf{H_B^N N} + \mathbf{Z_B}|\mathbf{S}) \tag{22}$$

$$= h(\mathbf{H_B^N N} + \mathbf{Z_B}) \tag{23}$$

$$= \log(\pi e)^{M(r+L_B-1)} \det(\mathbf{I_B} + P\mathbf{H_B^N}{\mathbf{H_B^N}}^H), \tag{24}$$

where (23) follows from the independence of $\mathbf{S}$ from $(\mathbf{N}, \mathbf{Z_B})$. $\mathbf{I_B}$ is the channel noise covariance matrix identical to the one in (21).

From substitution of (21) and (24) into (18), we obtain

$$I(\mathbf{S};\mathbf{Y_B}) = \log \frac{\det(\mathbf{I_B} + P\mathbf{H_B}{\mathbf{H_B}}^H)}{\det(\mathbf{I_B} + P\mathbf{H_B^N}{\mathbf{H_B^N}}^H)} \tag{25}$$

$$= \log \frac{\det(\mathbf{I_B} + P\mathbf{\Psi_B}\mathbf{\Lambda_B}{\mathbf{\Lambda_B}}^H{\mathbf{\Psi_B}}^H)}{\det(\mathbf{I_B} + P\mathbf{\Psi_B^N}\mathbf{\Lambda_B^N}{\mathbf{\Lambda_B^N}}^H{\mathbf{\Psi_B^N}}^H)} \tag{26}$$

$$= \log \frac{\det(\mathbf{I_B} + P\hat{\mathbf{\Lambda}}_\mathbf{B})}{\det(\mathbf{I_{B_N}} + P\hat{\mathbf{\Lambda}}_\mathbf{B}^\mathbf{N})} \tag{27}$$

$$= \sum_{i=1}^{rK} \log\,(1 + P|\lambda_{B_i}|^2) - \sum_{i=1}^{\sum_{i=1}^{r}\beta_i} \log\,(1 + P|\lambda_{B_i}^N|^2), \tag{28}$$

where the numerator of (26) stems from the singular value decomposition (SVD) of $\mathbf{H_B}$ into $\mathbf{\Psi_B}\mathbf{\Lambda_B}{\mathbf{V_B}}^H$ whereas the denominator follows from the SVD of $\mathbf{H_B^N}$ into $\mathbf{\Psi_B^N}\mathbf{\Lambda_{B_N}}{\mathbf{V_B^N}}^H$. The numerator of (27) follows from the well-known Sylvester's determinant identity $\det(\mathbf{I} + \mathbf{AB}) = \det(\mathbf{I} + \mathbf{BA})$, matrix scalar multiplication, associativity, and commutativity properties, and the fact that $\mathbf{\Psi_B}$ and ${\mathbf{V_B}}^H$ are unitary matrices whose product is an identity matrix. Similarly, 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 $\mathbf{\Psi_B^N}$ and ${\mathbf{V_B^N}}^H$ are unitary matrices whose product is an identity matrix. It should now be noted that $\mathbf{H_B}$ is of rank $rK \leq M(r+L_B-1)$, almost surely. See Lemma 1. The first term of (28) stems from the fact that $\hat{\mathbf{\Lambda}}_\mathbf{B}$ is a square diagonal matrix whose nonzero elements are the $rK \leq M(r+L_B-1)$ ordered squares of random singular values of the matrix $\mathbf{H_B}$ [13]. The second term follows from the fact that $\hat{\mathbf{\Lambda}}_\mathbf{B}^\mathbf{N}$ is a square diagonal matrix whose nonzero elements are the $N(r+L_E-1) \leq (rK-\sum_{i=1}^{r}\alpha_i) = \sum_{i=1}^{r}\beta_i$ ordered squares of random singular values of the full column rank matrix $\mathbf{H_B^N}$ (also see Lemma 1 and Lemma 2).

Lemma 1. *Let $\mathbf{H_{B_i}}$ be a channel matrix of size $(r + L_B - 1) \times rK$ whose nonzero elements in the first K columns $\mathbf{C_{1B}}, \mathbf{C_{2B}}, \ldots, \mathbf{C_{KB}}$ are the i.i.d. continuous random channel coefficients from the jth antenna at Alice, for $j = 1, 2, \ldots, K$, to the ith antenna at Bob, for $i = 1, 2, \ldots, M$, such that $\mathbf{C_{iB}} = \left[h_B^{ij}[1]\ \ h_B^{ij}[2]\ \ \ldots\ \ h_B^{ij}[L_B]\ \ 0\ \ \ldots\ \ 0\right]^\top$. And let the remaining $rK - K$ columns of $\mathbf{H_{B_i}}$ be $r - 1$ simultaneous vertically circular permutations of the first K columns, respectively. Then, the matrix $\mathbf{H_B} = [\mathbf{H_{B_1}}\ \mathbf{H_{B_2}}\ \ldots\ \mathbf{H_{B_M}}]^\top$*

is of rank $rK \leq M(r + L_B - 1)$.

Proof. The proof of Lemma 1 is presented in [15]. □

Using equation (14), we expand the first term of (19) as

$$h(\mathbf{Y_E}) = h(\mathbf{H_E X_A} + \mathbf{Z_E}) \tag{29}$$

$$= \log(\pi e)^{N(r+L_E-1)} \det(\mathbf{I_E} + P\mathbf{H_E}\mathbf{H_E}^H), \tag{30}$$

where $\mathbf{I_E} + P\mathbf{H_E}\mathbf{H_E}^H$ is the covariance matrix of $\mathbf{Y_E}$. $\mathbf{I_E}$ is an $N(r + L_E - 1) \times N(r + L_E - 1)$ covariance matrix of the channel noise vector $\mathbf{Z_E}$.

Similarly, using equation (16), we can write the second term of (19) as follows

$$h(\mathbf{Y_E}|\mathbf{S}) = h(\mathbf{H_E^S S} + \mathbf{H_E^N N} + \mathbf{Z_E}|\mathbf{S}) \tag{31}$$

$$= h(\mathbf{H_E^N N} + \mathbf{Z_E}) \tag{32}$$

$$= \log(\pi e)^{N(r+L_E-1)} \det(\mathbf{I_E} + P\mathbf{H_E^N}\mathbf{H_E}\mathbf{N}^H), \tag{33}$$

where (32) follows from the independence of $\mathbf{S}$ from $(\mathbf{N}, \mathbf{Z_E})$. $\mathbf{I_E}$ is the channel noise covariance matrix similar to (30).

From substitution of (30) and (33) into (19), we obtain

$$I(\mathbf{S}; \mathbf{Y_E}) = \log \frac{\det(\mathbf{I_E} + P\mathbf{H_E}\mathbf{H_E}^H)}{\det(\mathbf{I_E} + P\mathbf{H_E^N}\mathbf{H_E^N}^H)} \tag{34}$$

$$= \sum_{i=1}^{N(r+L_E-1)} \log(1 + P|\lambda_{E_i}|^2) - \sum_{i=1}^{\sum_{i=1}^{r}\beta_i} \log(1 + P|\lambda_{E_i}^N|^2), \tag{35}$$

where (34)-(35) follow similar arguments as (25)-(28). Lemma 2 shows that the matrix $\mathbf{H_E}$ is of rank $N(r + L_E - 1) \leq (rK - \sum_{i=1}^{r} \alpha_i) = \sum_{i=1}^{r} \beta_i$, almost surely.

Lemma 2. *Let* $\mathbf{H}_{\mathbf{E}_\ell}$ *be a channel matrix of size* $(r + L_E - 1) \times rK$ *whose nonzero elements in the first* K *columns* $\mathbf{C_{1E}}, \mathbf{C_{2E}}, \ldots, \mathbf{C_{KE}}$ *are the i.i.d. continuous random channel coefficients from the* j*th antenna at Alice, for* $j = 1, 2, \ldots, K$*, to the* l*th antenna at Eve, for* $\ell = 1, 2, \ldots, N$*, such that* $\mathbf{C_{iE}} = \begin{bmatrix} h_E^{\ell j}[1] & h_E^{\ell j}[2] & \ldots & h_E^{\ell j}[L_E] & 0 & \ldots & 0 \end{bmatrix}^\top$*. And let the remaining* $rK - K$ *columns of* $\mathbf{H}_{\mathbf{E}_\ell}$ *be* $r - 1$ *simultaneous vertically circular permutations of the first* K *columns, respectively. Then, the matrix* $\mathbf{H_E} = [\mathbf{H_{E_1}}\ \mathbf{H_{E_2}}\ \ldots\ \mathbf{H_{E_N}}]^\top$ *is of rank* $N(r + L_E - 1) \leq (rK - \sum_{i=1}^{r} \alpha_i)$.

Proof. The proof of Lemma 2 is presented in [15]. □

From the definition of SDoF in (6), the definition of secrecy rate in (17), and the expansion of the individual terms of equations (18) and (19) into (28) and (35), respectively, we obtain the expression of Theorem 1. See [15] for details. ■

V. Conclusions

We have presented a novel approach to exploit ISI heterogeneity to achieve positive SDoF for the MIMO wiretap channel even without any CSIT. In particular, we showed that the transmitter can use the ISI link lengths towards the legitimate receiver and the eavesdropper to carry out a transmission that mixes both the information and artificial noise symbols and, in the end, be able to achieve secure communication. We showed this to be true even when the number of antennas at the eavesdropper is larger than the number of antennas at the legitimate receiver. There are several interesting directions for future work: a) this idea can be applied to various other multi-user networks to achieve robust secrecy without any instantaneous CSIT; b) another open problem is to obtain information-theoretic upper bounds on the SDoF in presence of ISI heterogeneity.

References

[1] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas–Part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[2] 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.

[3] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.

[4] R. Tandon, P. Piantanida, and S. Shamai, "On multi-user MISO wiretap channels with delayed CSIT," in *IEEE International Symposium on Information Theory*, 2014, pp. 211–215.

[5] S. Lashgari and A. S. Avestimehr, "Secrecy DoF of blind MIMOME wiretap channel with delayed CSIT," *IEEE Transactions on Information Forensics and Security*, vol. PP, no. 99, pp. 1–1, 2017.

[6] P. Mukherjee, R. Tandon, and S. Ulukus, "Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT," *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 3823–3853, 2017.

[7] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3425–3441, 2008.

[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] N. Shlezinger, D. Zahavi, Y. Murin, and R. Dabora, "The secrecy capacity of Gaussian MIMO channels with finite memory," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1874–1897, 2017.

[10] A. Yener and S. Ulukus, "Wireless physical layer security: Lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.

[11] J. Xie and S. Ulukus, "Secure degrees of freedom of multiuser networks: One-time-pads in the air via alignment," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1857–1873, 2015.

[12] T. Y. Liu, P. Mukherjee, S. Ulukus, S. C. Lin, and Y. W. P. Hong, "Secure degrees of freedom of MIMO rayleigh block fading wiretap channels with no CSI anywhere," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2655–2669, 2015.

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

[14] 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

[15] J. Mutangana, D. Kumar, and R. Tandon, "MIMO wiretap channel with ISI heterogeneity– Achieving secure DoF with no CSI," 2016. [Online]. Available: http://www2.engr.arizona.edu/~tandonr/conference-papers/Asilomar-secrecy-2017-full.pdf

[16] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2006.