Interference Channels with Confidential Messages: Scaling up the Secure Degrees of Freedom with No CSIT

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

***Abstract*—We consider the K-user interference channel with confidential messages (IC-CM) with intersymbol interference (ISI). The main contribution of this paper is to show that sum-secure degrees of freedom (SDoF) can be made to linearly increase with the number of users K with no channel state information at the transmitters (CSIT). We demonstrate that this is true whenever the channel impulse response (CIR) lengths from the legitimate transmitters towards their respectively intended receivers are larger than those from the interfering transmitters towards the unintended receivers. To design this scheme, we use: a) the simple channel matrix structures of the received signal space to eliminate interference and allow decodability at the intended receivers. b) an injection of artificial noise into the transmitted signal from a strategically chosen small number of transmitters that act as cooperative jammers in order to preserve confidentiality of messages at unintended receivers. This is the first work showing that the SDoF of the K-user IC-CM with ISI can linearly increase with K, the number of users.**

I. Introduction

Efficient communication using wireless channel resources seeks to maximize reliable communication rates at a minimum cost of transmission power. Research on physical (PHY) layer security seeks to maximize the secure rates of communication between the legitimate users while at the same time making sure that any eavesdroppers in the vicinity are not able to decode any information. A vast majority of the proposed solutions on PHY layer security so far rely on the assumption that channel state information (CSI) is available the transmitters (CSIT). A detailed survey on PHY layer security can be found in [1]. However, this assumption of CSIT availability is not a feasible one as the eavesdropping nodes cannot voluntarily cooperate in collecting CSI and feeding it back to the transmitters. In this paper, we aim to show that the sum-secure degrees of freedom (SDoF) for the K-user single-input single-output (SISO) interference channel with intersymbol interference (ISI) can scale linearly with the number of users. Perhaps the most interesting aspect of the proposed scheme is that it does not require CSIT. We leverage the inherent heterogeneity present in different ISI links (across transmitters and receivers) along with artificial noise to achieve secrecy. The considered model is the secure version of the non-secure model that was investigated in [2],

This work was supported by NSF grants CAREER-1651492 and CNS-1715947.

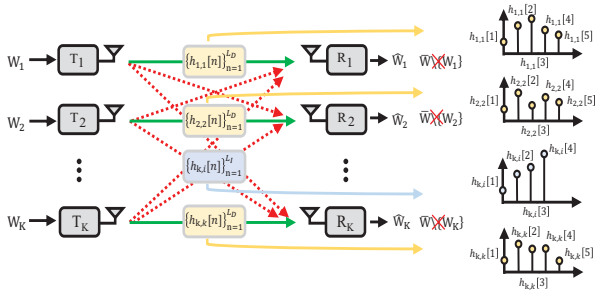

Fig. 1: K-user interference channel with confidential messages with intersymbol interference. L_D and L_I denote the effective number of channel taps from kth transmitter to the intended receiver k and from the interfering ith transmitter to the unintended receiver k, respectively.

where it was shown that exploitation of ISI heterogeneity due to the inherent randomness of the wireless channel can lead to significant gains in spectral efficiency. Under full CSI availability assumption, the sum-DoF of the K-user IC without ISI was investigated in [3] and its secure version in [4]. The concept of achieving secrecy [1] by exploitation of ISI heterogeneity originates from our previous work [5], [6].

II. System Model

We consider the K-user interference channel with confidential messages (IC-CM) with symmetric ISI where each transmitter $k \in \{1, 2, \ldots, K\}$ is interested in sending an independent message W_k, where $k \in \{1, 2, \ldots, K\}$, to the kth receiver (see Fig. 1). The message transmission must preserve the confidentiality constraint, i.e., each receiver must not be able to learn any information about the other $K-1$ unintended messages. The channel from the kth transmitter to the kth receiver is represented by the channel impulse response (CIR) denoted by $\{h_{k,k}[n]\}_{n=1}^{L_{k,k}}$ and $L_{k,k}$ denotes the effective number of channel taps or CIR length of the desired (i.e., direct) link, i.e., from the kth transmitter to the intended receiver k. Similarly, $\{h_{k,i}[n]\}_{n=1}^{L_{k,i}}$ denotes the CIR between the ith transmitter and the kth receiver and $L_{k,i}$ denotes the effective number of channel taps or CIR length of the interfering (i.e., indirect) link, i.e., from the ith transmitter to the unintended receiver k. In this paper, we focus on symmetric ISI, i.e., we assume that $L_{k,k} = L_D$ for all $k \in \{1, 2, \ldots, K\}$ and $L_{k,i} = L_I$ for $i \neq k \in \{1, 2, \ldots, K\}$.

The channel is assumed to be linear time invariant (LTI) over the transmission blocklength. All the CIR coefficients are assumed to be independent and identically distributed (i.i.d.) random variables drawn from a continuous distribution. Furthermore, the transmitters have no knowledge of channel state information (i.e., no CSIT). They only know the effective CIR lengths L_D and L_I towards the intended and unintended receivers, respectively. For coherent decoding, each receiver k is assumed to know its local channel coefficients, i.e. channel state information at the receiver (CSIR).

Let $x[n]$ be the symbol transmitted by transmitter k at time n. The signal $y_k[n]$ received at time n by receiver k is

$$y_k[n] = \sum_{i=1}^{K} \sum_{\ell=1}^{L_{k,i}} h_{k,i}[\ell] x[n-\ell+1] + z_k[n], \tag{1}$$

where $z_k[n]$ is the channel noise seen by receiver k at time n. The channel noise is assumed to be circularly symmetric and Gaussian with zero mean and unit variance. Each transmitted signal $x_k[n]$ must satisfy the average power constraint, $E[x_k^2[n]] \leq P$.

Let W_k, for $k \in \{1, 2, \ldots, K\}$, be the message from the kth transmitter to the kth receiver. A secure rate of communication $R_k = \frac{\log(|W_k|)}{n}$ is achievable if there exists an n-length code such that, for $n \to \infty$ and $\epsilon \to 0$, the following reliability and confidentiality constraints are satisfied:

$$Pr[W_k \neq \hat{W}_k] \leq \epsilon \tag{2}$$

$$\frac{1}{n} I(\overline{W}_{\{k\}}; y_k^{(n)} | W_k) \leq \epsilon, \tag{3}$$

where $\overline{W}_{\{k\}} = \overline{W} \backslash \{W_k\}$ and $\overline{W} = \{W_1, W_2, \ldots, W_K\}$.

The sum secrecy capacity C_s is defined as the supremum of all achievable secure sum rates $R_s = \sum_{k=1}^{K} R_k$. We define sum secure degrees of freedom (SDoF) as the pre-log of the sum secrecy capacity as follows

$$\mathsf{SDoF} = \lim_{P \to \infty} \frac{C_s}{\log(P)}. \tag{4}$$

III. Main Result and Illustrative Example

We state the main contribution of this paper in the following Theorem. It shows that with no CSIT, we can make SDoF linearly scale up with the number of users K.

Theorem 1. *For the K-user IC-CM with symmetric ISI where L_D and L_I denote the ISI length parameters for $L_D > L_I$, the following SDoF is achievable without any CSIT*

$$\mathsf{SDoF} = \begin{cases} \frac{(K-(L_I-1))^+}{L_D}, & L_D \geq L_I \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

where $(x)^+ \triangleq \max(x, 0)$.

Fig. 2 shows the achievable rate of the current result versus its non-secure version in [2] for $L_D = 3$ and $L_I = 2$.

We introduce the following example in order to illustrate the main idea behind the proposed transmission scheme.

Example 1. Consider a K-user IC-CM with symmetric ISI where $L_D = 3$ and $L_I = 2$. This means that any symbol sent by the kth (dedicated) transmitter during a given time slot will be seen over $L_D = 3$ time slots at the (indented) receiver k. Similarly, any signal sent by the ith (interfering) transmitter, $i \neq k$, will be seen over $L_I = 2$ time slots at the receiver k. Our goal is to show that $\mathsf{SDoF} = (K-3)/3$ is achievable.

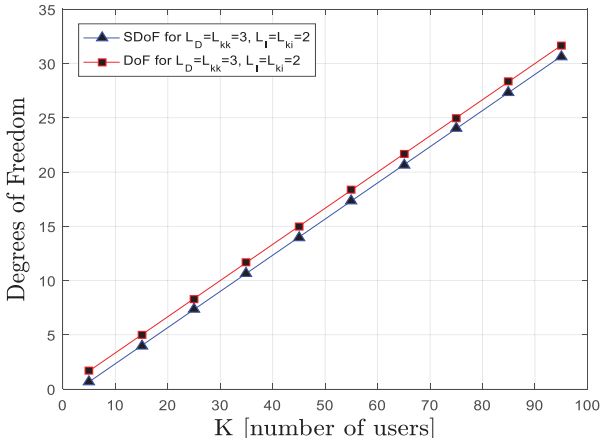

Fig. 2: Comparison of the achievable rate of the (current) secure K-user IC-CM with ISI model (triangles) versus its non-secure version (squares) in [2] for ISI link length parameters $L_D = 3$ and $L_I = 2$.

Transmission phase: For secrecy, we use the following transmission strategy:

- Let the first $J = L_I + 1 = 3$ transmitters, each send an independent artificial noise symbol in the first time slot. That is, the first transmitter sends $x_1[1] = n_1$, the second transmitter sends $x_2[1] = n_2$, and the third transmitter sends $x_3[1] = n_3$.
- Let all of the remaining $K - J = K - 3$ transmitters only send an information symbol over the first time slot, each. That is, the fourth transmitter sends $x_4[1] = s_4$, the fifth transmitter sends $x_5[1] = s_5$, $\ldots$, and the Kth transmitter sends $x_K[1] = s_K$.
- All the transmitters then remain silent over the last $L_D - 1 = 2$ time slots, i.e., over the second and third time slots. This can also be thought of as zero-padding.

Decodability at the k^{th} receiver: Note that all the receivers, i.e., 1 through K observe the signals with the same structure. Furthermore, since the channel coefficients are i.i.d. random variables drawn from a continuous distribution, for the above L_D and L_I values, the kth receiver observes a total of L_D linear combinations respectively over L_D time slots:

- $L_k[1]\,(x_1[1], \ldots, x_J[1], x_{J+1}[1], \ldots, x_K[1])$ is received over the first time slot.
- $L_k[2](x_1[1], \ldots, x_J[1], x_{J+1}[1], \ldots, x_K[1])$ is received over the second time slot.
- $L_k[3](x_k[1])$ is received over the third time slot.

Therefore, the first receiver (for example) observes $L_D = 3$ independent linear combinations respectively over the first 3 times slots: $L_1[1](n_1, n_2, n_3, s_4, s_5, \ldots, s_k)$, $L_1[2](n_1, n_2, n_3, s_4, s_5, \ldots, s_K)$, $L_1[3](n_1)$.

Note that, because $L_D > L_I$, the kth receiver always gets its dedicated symbol $x_k[1]$ from the linear combination received in the last time slot, i.e. the L_Dth time slot. For example, the first receiver is directly able to decode $x_1[1] = n_1$ from $L_1[3](n_1)$ alone. Therefore, we have a total of K dedicated communication links where each receiver $k \in \{1, 2, \ldots, K\}$ is able to decode its dedicated symbol. Furthermore, since J out of the K decoded symbols are the artificial noises sent from the J cooperative jammers, this scheme thus transmits a total of $K - J = K - 3$ information symbols over the transmission block of length $L_D = 3$ time slots.

Secrecy at the k^{th} receiver: This transmission scheme achieves secrecy as follows: After decoding its dedicated symbol from $L_k[L_D](x_k[1])$, each receiver k remains only with $L_I = 2$ independent linear combinations (i.e., observed in the first L_I time slots) with $K - 1$ interfering symbols. Furthermore, the rank of the matrix formed by the L_I independent linear combination is $L_I = J - 1 = 2$, i.e., equal to the number of the interfering noises from $J - 1$ cooperative jammers. Thus, since the interfering artificial noise symbols occupy the same space as the interfering (i.e., unintended) information symbols, the kth receiver is not able to solve for any of the unintended symbols. Therefore, our scheme securely achieves the transmission of $K - 3$ information symbols over 3 time slots, i.e., achieving $\mathsf{SDoF} = (K - 3)/3$.

IV. Proof of Theorem 1

The proof of Theorem 1 is divided into three sections. In Section IV-A, we describe the general transmission scheme. In Section IV-B, we describe the received signal and the corresponding channel matrix structures. In Section IV-C, we leverage the channel structure to analyze SDoF of the scheme.

A. General Transmission Scheme

We now consider the general transmission scheme for the K-user IC-CM with symmetric ISI for any $L_{k,k}$ and $L_{k,i}$ (where $L_{k,k} = L_D$, $L_{k,i} = L_I$ for $i \neq k \in \{1, 2, \ldots, K\}$, and $L_D > L_I$). This scheme works over a transmission block of total duration $T = L_D$ time slots. The order of information and artificial noise symbols transmission is described next. To preserve security, we let any $J = L_I + 1$ transmitters out of K serve as cooperative jammers. For ease of presentation (and without loss of generality), we consider the first J transmitters to be the cooperative jammers.

Transmission phase:

- Let the first J transmitters send an artificial noise symbol, each, over the first time slot. That is, they send $x_1[1] = n_1$, $x_2[1] = n_2$, …, $x_J[1] = n_J$.
- Let all the remaining $K - J$ transmitters send an information symbol, each, over the first time slot. That is, they send $x_{J+1}[1] = s_{J+1}$, $x_{J+2}[1] = s_{J+2}$, …, $x_K[1] = s_K$.
- In the last $L_D - 1$ time slots, let all transmitters remain silent. This can also be thought of as zero-padding.

Decodability at the k^{th} receiver: We enforce the kth receiver to decode its dedicated symbol, i.e., from the kth transmitter. Note that this symbol can either be an artificial noise or information symbol depending on whether or not the corresponding transmitter k is a cooperative jammer or not. This decoding is feasible whenever the desired (i.e. direct) ISI link length L_D is greater than the interfering (i.e. indirect) ISI link length L_I. This is because the kth receiver observes L_D equations (out of which $L_I + 1$ are independent) where the equation $L_k[L_D](\ .\ )$ observed in the last time slot, (i.e., the L_Dth time slot) contains its dedicated symbol only. Hence, this directly allows receiver k to decode $x_k[1]$. We further note that a similar signal structure is observed at all of the K receivers.

Secrecy at the k^{th} receiver: The described above transmission scheme preserves confidentiality because it adheres to the following signal spaces conditions:
We noted above that each receiver $k \in \{1, 2, \ldots, K\}$ observes L_D linear combinations. However, due to the interference link length L_I, only the first L_I linear combinations out of L_D contain the interfering symbols from the other $K - 1$ transmitters. This implies that after decoding its dedicated symbol $x_k[1]$, the receiver k remains with only L_I independent linear combinations with $K-1$ unknowns. Therefore, to preserve confidentiality of the interfering symbols, all we need to do is to ensure that the number of (interfering) artificial noise symbols (sent from the cooperative jammers) is equal to the number of the remaining linear combinations, i.e., L_I. Furthermore, to ensure that security is also preserved at all of the J receivers that form direct J links to their respective J cooperative jamming transmitters, we have to impose that the condition $J - 1 \geq L_I$ be satisfied.

B. Received Signal and Channel Matrix Structures

Let X_K be the composite signal vector of size $K \times 1$ sent from all K transmitters. The $L_D \times 1$ signal vector Y_k seen at the kth receiver over the transmission blocklength $T = L_D$ can thus be written as follows

$$Y_k = \mathbf{H_k} X_K + Z_k \tag{6}$$

$$= \mathbf{H_{kk}} x_k + \sum_{i \neq k}^{K} \mathbf{H_{ki}} x_i + Z_k \tag{7}$$

$$= \mathbf{H_{kk}} x_k + \mathbf{H_k^{(-k)}} X_K^{(-k)} + Z_k \tag{8}$$

where $\mathbf{H_k}$ is the composite channel matrix seen at the kth receiver, $\mathbf{H_{kk}} = \begin{bmatrix} h_{kk}[1] & h_{kk}[2] & \ldots & h_{kk}[L_D] \end{bmatrix}^\top$,
$\mathbf{H_{ki}} = \begin{bmatrix} h_{ki}[1] & h_{ki}[2] & \ldots & h_{ki}[L_I] & 0 & \ldots & 0 \end{bmatrix}^\top$, $i \neq k$,

$$\mathbf{H_k^{(-k)}} = \begin{bmatrix} h_{k,1}[1] & \ldots & h_{k,k-1}[1] & h_{k,k+1}[1] & \ldots & h_{k,K}[1] \\ h_{k,1}[2] & \ldots & h_{k,k-1}[2] & h_{k,k+1}[2] & \ldots & h_{k,K}[2] \\ \vdots & \vdots & \ddots & \vdots & & \\ h_{k,1}[L_I] & \ldots & h_{k,k-1}[L_I] & h_{k,k+1}[L_I] & \ldots & h_{k,K}[L_I] \\ 0 & 0 & \ldots & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \ldots & 0 \end{bmatrix} \tag{9}$$

$$X_K = \begin{bmatrix} x_1[1] & \dots & x_K[1] \end{bmatrix}^\top$$
$$X_K^{(-k)} = \begin{bmatrix} x_1[1] & \dots & x_{k-1}[1] & x_{k+1}[1] & \dots & x_K[1] \end{bmatrix}^\top,$$
and Z_k is an $L_D \times 1$ noise vector whose elements are complex circularly independent zero-mean unit-variance.

In the next Section, we do the SDoF calculation using the signal and matrix structures that we described above. Furthermore, we will introduce Lemma 1 and Lemma 2 which respectively show that the rank of the matrix $\mathbf{H_k}$ is $L_I + 1$ and the rank of the matrix $\mathbf{H_k^{(-k)}}$ is L_I. The consequence of these channel matrix structures and their rank properties is that they lead to decodability and confidentiality.

In particular, we show that although the receiver k is able to decode intended message $x_k[1]$, it is not able to decode any symbols sent from the remaining $K-1$ interfering transmitters. This is because after decoding its dedicated symbol, the dedicated receiver remains only with a signal portion $Y_k^{(-k)} = \mathbf{H_k^{(-k)}} X_K^{(-k)} + Z_k$ where $X_K^{(-k)} = X_i$ for $i \neq k \in \{1, 2, \dots, K\}$. However, this remaining (interfering) signal occupies a space that is completely immersed in artificial noise symbols. To prove this fact, we show that the rank of the matrix $\mathbf{H_k^{(-k)}}$ is $J - 1 = L_I$, i.e., equivalent to the number of artificial noise symbols sent from $J-1$ cooperative jammers. This in turn implies that any message from transmitter k will not be decoded by any other unintended receiver i, for $i \neq k \in \{1, 2, \dots, K\}$. From here on, for simplicity of notation, we adopt the notation x_k to represent $x_k[1]$ since all the K transmitters send their symbols only during the first time slot.

C. SDoF Calculation

For a blocklength T, the following secure rate is achievable for receiver k, for $k = J+1, \dots, K$
$$R_k = \frac{I(x_k; Y_k) - \max_{i \neq k} I(x_k; Y_i)}{T}, \tag{10}$$
Furthermore, since all the channel coefficients are i.i.d, then from here on, we will use the fact that $\max_{i \neq k} I(x_k; Y_i) = I(x_k; Y_i)$ for any $i \neq k$.

Using differential entropy, we expand numerator of (10) as
$$I(x_k; Y_k) = h(Y_k) - h(Y_k|x_k) \tag{11}$$
$$I(x_k; Y_i) = h(Y_i) - h(Y_i|x_k). \tag{12}$$
Furthermore, the first term of (11) can be expanded as
$$h(Y_k) = h(\mathbf{H_k} X_K + Z_k) \tag{13}$$
$$= \log(\pi e)^{L_D} \det(\mathbf{I_{L_D}} + P \mathbf{H_k} \mathbf{H_k}^{\mathsf{H}}), \tag{14}$$
where $\mathbf{A}^{\mathsf{H}}$ denotes the complex conjugate of $\mathbf{A}$ and P is the symbol transmission power. $\mathbf{H_k}$ is the composite channel matrix seen at the kth receiver obtained by concatenation of $\mathbf{H_{kk}}$ and $\mathbf{H_k^{(-k)}}$. In Lemma 1, we show that the matrix $\mathbf{H_k}$ has rank $L_I + 1$ almost surely.

Lemma 1. *Let $\mathbf{H_k}$ be an $L_D \times K$ composite channel matrix seen at the kth receiver from all of the K transmitters. Furthermore, let the first column $\mathbf{H_{kk}}$ of $\mathbf{H_k}$ be the vector whose elements are the i.i.d. channel coefficients randomly picked from a continuous distribution such that $\mathbf{H_{kk}} = \begin{bmatrix} h_{kk}[1] & h_{kk}[2] & \dots & h_{kk}[L_D] \end{bmatrix}^\top$. Let the remaining $K-1$ columns of $\mathbf{H_k}$ be of the form $\mathbf{H_{ki}} = \begin{bmatrix} h_{ki}[1] & h_{ki}[2] & \dots & h_{ki}[L_I] & 0 & \dots & 0 \end{bmatrix}^\top$, for $i \neq k \in \{1, 2, \dots, K\}$ and $L_D > L_I$. Then, $\mathbf{H_k}$ is of rank $L_I + 1$ almost surely.*

Proof. The proof of Lemma 1 follows similar arguments as those of Lemma 1 in [5] and is thus omitted here. □

Similarly, the second term of (11) can be expanded as
$$h(Y_k|x_k) = h(\mathbf{H_{kk}} x_k + \mathbf{H_k^{(-k)}} X_K^{(-k)} + Z_k | x_k) \tag{15}$$
$$= h(\mathbf{H_k^{(-k)}} X_K^{(-k)} + Z_k) \tag{16}$$
$$= \log(\pi e)^{L_D} \det(\mathbf{I_{L_D}} + P \mathbf{H_k^{(-k)}} \mathbf{H_k^{(-k)}}^{\mathsf{H}}), \tag{17}$$
where $\mathbf{H_k^{(-k)}}$ is the $L_D \times (K-1)$ matrix carrying the interfering symbols vector $X_K^{(-k)} = X_i$, $i \neq k \in \{1, 2, \dots, K\}$ as shown by equation (8) and (16) follows from the independence of x_k and $(X_K^{(-k)}, Z_k)$. In Lemma 2, we show that the matrix $\mathbf{H_k^{(-k)}}$ has rank L_I almost surely.

Lemma 2. *Let $\mathbf{H_k^{(-k)}}$ be an $L_D \times (K-1)$ composite channel matrix seen at the kth receiver from all of the $K-1$ interfering transmitters as shown in equation* (8)*. Then, $\mathbf{H_k^{(-k)}}$ is of rank L_I almost surely.*

Proof. The proof of Lemma 2 follows similar arguments as those of Lemma 1 in [5] and is thus omitted here. □

The first term of (12) can be expanded as
$$h(Y_i) = \mathbf{H_i} X_K + Z_i \tag{18}$$
$$= \log(\pi e)^{L_D} \det(\mathbf{I_{L_D}} + P \mathbf{H_i} \mathbf{H_i}^{\mathsf{H}}), \tag{19}$$
where $\mathbf{H_i}$ is the composite channel matrix seen at the ith receiver. Here the matrix $\mathbf{H_i}$ has the same structure as $\mathbf{H_k}$ in (6). In turn, implies that (by Lemma 1) $\mathbf{H_i}$ is also of rank $L_I + 1$ almost surely.

The second term of (12) can be expanded as
$$h(Y_i|x_k) = h(\mathbf{H_{ii}} x_i + \mathbf{H_i^{(-i)}} X_K^{(-i)} + Z_i | x_k) \tag{20}$$
$$= h(\mathbf{H_i^{(-k)}} X_K^{(-k)} + Z_i) \tag{21}$$
$$= \log(\pi e)^{L_D} \det(\mathbf{I_{L_D}} + P \mathbf{H_i^{(-k)}} \mathbf{H_i^{(-k)}}^{\mathsf{H}}), \tag{22}$$
where $\mathbf{H_i^{(-k)}}$ is the $L_D \times 1$ channel matrix carrying the symbol vector $X_K^{(-k)}$ to receiver $i \neq k \in \{1, 2, \dots, K\}$. The equation (21) is due to the independence of x_k from $(X_K^{(-k)}, Z_k)$. Note here that the matrix $\mathbf{H_i^{(-k)}}$ has a different structure from $\mathbf{H_k^{(-k)}}$ and is of rank $L_I + 1$. See Lemma 3.

Lemma 3. *Let $\mathbf{H_i^{(-k)}}$ be an $L_D \times (K-1)$ matrix whose first column is identical to that of $\mathbf{H_i}$ and whose subsequent $K-2$ columns are randomly picked from those of the last $K-1$ of $\mathbf{H_i}$ without repetition. Then, the matrix $\mathbf{H_i^{(-k)}}$ is of rank $L_I + 1$ almost surely.*

Proof. The proof of Lemma 3 directly follows from the fact that $\mathbf{H_i^{(-k)}}$ is a truncation of the full row rank matrix $\mathbf{H_i}$ by one random column. Furthermore, since $\mathbf{H_i}$ has similar structure as $\mathbf{H_k}$, removing one of its last $K-1$ columns does not alter its rank. Therefore, $\mathsf{rank}(\mathbf{H_i^{(-k)}}) = L_I + 1$. □

We rewrite equation (11) using (14) and (17) as follows

$$I(x_k;Y_K) = \log \frac{\det(\mathbf{I_{L_D}} + P\mathbf{H_k}\mathbf{H_k}^{\mathsf{H}})}{\det(\mathbf{I_{L_D}} + P\mathbf{H_k^{(-k)}}\mathbf{H_k^{(-k)}}^{\mathsf{H}})} \quad (23)$$

$$= \log \frac{\det(\mathbf{I_{L_D}} + P\Psi_\mathbf{k}\Lambda_\mathbf{k}\Lambda_\mathbf{k}^{\mathsf{H}}\Psi_\mathbf{k}^{\mathsf{H}})}{\det(\mathbf{I_{L_D}} + P\Psi_\mathbf{k}^{(-\mathbf{k})}\Lambda_\mathbf{k}^{(-\mathbf{k})}\Lambda_\mathbf{k}^{(-\mathbf{k})^{\mathsf{H}}}\Psi_\mathbf{k}^{(-\mathbf{k})^{\mathsf{H}}}} \quad (24)$$

$$= \sum_{\ell=1}^{\mathsf{rank}(\mathbf{H_k})} \log(1+P\lambda_{k\ell}^2) - \sum_{\ell=1}^{\mathsf{rank}(\mathbf{H_k^{(-k)}})} \log(1+P\lambda_{k\ell}^{(-k)^2}), \quad (25)$$

where the numerator of equation (24) comes from the singular value decomposition (SVD) of the composite channel matrix $\mathbf{H_k}$ into $\Psi_\mathbf{k}\Lambda_\mathbf{k}\mathbf{V_k}^{\mathsf{H}}$ [7]. Similarly, the denominator of equation (24) comes from the SVD of the interfering channel matrix $\mathbf{H_k^{(-k)}}$ into $\Psi_\mathbf{k}^{(-\mathbf{k})}\Lambda_\mathbf{k}^{(-\mathbf{k})}\mathbf{V_k^{(-k)}}^{\mathsf{H}}$. The first term of (25) comes from Sylvester's identity $\det(\mathbf{I}+\mathbf{AB}) = \det(\mathbf{AB}+\mathbf{I})$ and the fact that $\Psi_\mathbf{k}$ and $\mathbf{V_k}$ are unitary matrices whose product forms an identity matrix [7]. Furthermore, since by Lemma 1, $\mathbf{H_k}$ is of rank L_I+1, then the nonzero portion of matrix $\Lambda_\mathbf{k}$ is a square diagonal matrix whose elements are L_I+1 ordered squares of the singular values (SVs) of $\mathbf{H_k}$ [8]. Similarly, the second term of (25) comes from Sylvester's identity and the fact that $\Psi_\mathbf{k}^{(-\mathbf{k})}$ and $\mathbf{V_k^{(-k)}}$ are unitary matrices whose product forms an identity matrix. Furthermore, since by Lemma 2, $\mathbf{H_k^{(-k)}}$ is of rank L_I, then the nonzero portion of matrix $\Lambda_\mathbf{k}^{(-\mathbf{k})}$ is a square diagonal matrix whose elements are L_I ordered squares of SVs of $\mathbf{H_k^{(-k)}}$.

We also rewrite (12) using (19) and (22) as follows

$$I(x_k;Y_i) = \log \frac{\det(\mathbf{I_{L_D}} + P\mathbf{H_i}\mathbf{H_i}^{\mathsf{H}})}{\det(\mathbf{I_{L_D}} + P\mathbf{H_i^{(-k)}}\mathbf{H_i^{(-k)}}^{\mathsf{H}})} \quad (26)$$

$$= \sum_{\ell=1}^{\mathsf{rank}(\mathbf{H_i})} \log(1+P\lambda_{i\ell}^2) - \sum_{\ell=1}^{\mathsf{rank}(\mathbf{H_i^{(-k)}})} \log(1+P\lambda_{i\ell}^{(-k)^2}), \quad (27)$$

where equations (26)-(27) follow analogous arguments as those of (23)-(25).

Combining the definition of SDoF in (4), secure rate in (10) and the expansions of its terms in (25) and (27) plus the fact that only $K-J$ transmitters transmit information symbols, we obtain

$$\mathsf{SDoF} = \lim_{P\to\infty} \frac{\sum_{k=J+1}^{K} R_k}{T\log(P)} = \lim_{P\to\infty} \sum_{k=J+1}^{K} \frac{R_k}{T\log(P)}$$

$$= \lim_{P\to\infty} \sum_{k=J+1}^{K} \frac{(I(x_k;Y_k) - \max_{i\neq k} I(x_k;Y_i))}{T\log(P)} \quad (28)$$

$$= \sum_{k=J+1}^{K} \frac{\left(\mathsf{rank}(\mathbf{H_k}) - \mathsf{rank}(\mathbf{H_k^{(-k)}})\right)}{T}$$

$$- \sum_{k=J+1}^{K} \frac{\left(\mathsf{rank}(\mathbf{H_i}) - \mathsf{rank}(\mathbf{H_i^{(-k)}})\right)}{T} \quad (29)$$

$$= \sum_{k=J+1}^{K} \frac{1}{L_D} = \frac{(K-J)}{L_D} = \frac{K-(L_I+1)}{L_D}, \quad (30)$$

where (29) follows from Lemma 1, Lemma 2, and Lemma 3. The last equation follows from the secrecy enforcement that J be at least of value L_I+1 and $T = L_D$. This completes the proof of Theorem 1. □

V. Conclusion

We introduced a scheme showing that SDoF for the K-user IC-CM with ISI can linearly increase with K through ISI heterogeneity exploitation even without CSIT. Specifically, strategically chosen J out of K transmitters send artificial noise symbols. This aligns interfering symbols in a separate subspace from each respectively desired symbol at the intended receiver k while ensuring that these interfering symbols are completely masked by artificial noise. There are several interesting future research directions such as the extension to the IC-CM with non-symmetric ISI and derivation of upper bound on SDoF of IC-CM with ISI.

References

[1] 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.

[2] N. Lee, "A blind interference management technique for the K-user interference channel with ISI: Interference-free OFDM," in *Proc. IEEE International Conference on Communications (ICC)*, 2017.

[3] 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.

[4] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2647–2661, 2015.

[5] J. d. D. Mutangana, R. Tandon, and N. Lee, "Blind cooperative jamming: Exploiting ISI heterogeneity to achieve positive secure DoF," in *Proc. IEEE Global Communications Conference on Communications*, 2017.

[6] J. d. D. Mutangana, D. Kumar, and R. Tandon, "MIMO wiretap channel with ISI heterogeneity achieving secure DoF with no CSI," in *Proc. Asilomar Conference on Signals, Systems, and Computers*, 2017.

[7] S. Friedberg, A. Insel, and L. Spence, *Linear Algebra*. Pearson Education, 2003.

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