Interference Channels with Confidential Messages: Leveraging OFDM Transmission to Scale up 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 problem of 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 in the absence of channel state information at the transmitters (CSIT). The proposed scheme entails three main ingredients : a) leveraging the simple channel matrix structures resulting from the orthogonal frequency division multiplexing (OFDM) type transmission technique in order to eliminate interference and allow coherent decoding of each message at its respectively intended receiver. b) exploiting the inherent heterogeneity in channel impulse response (CIR) lengths between the transmitters and the receivers (which results from the wireless multipath propagation), and c) injection of artificial noise into the transmitted signal from a strategically chosen small number of transmitters J that act as cooperative jammers in order to preserve full confidentiality of the messages at the unintended receivers. This is the first work showing that the SDoF of the K-user IC-CM with ISI can linearly increase with the number of users without CSIT.**

I. Introduction

Secure communication over the physical (PHY) layer is impacted by the availability of channel state information at the transmitters (CSIT). Unfortunately, the vast majority of PHY layer security solutions that have been proposed thus far rely on the assumption that CSIT is available. We refer the reader to [1] and [2] for recent surveys on PHY layer security. This assumption of CSIT availability is not a practical one because the eavesdropping nodes cannot be expected to reliably cooperate in gathering CSI and feeding it back to the transmitters. In this paper, we 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 linearly increase with the number of users. Perhaps what is even more appealing about the proposed scheme is the fact that it does not require CSIT.

The problem considered in this work is the one studied in [3], with the addition of confidentiality constraints. In [3], it was shown that for the K-user IC, even with no CSIT, heterogeneity of ISI links can be leveraged to obtain significant gain in spectral efficiency. Under full CSI availability at all terminals, the sum-DoF of the K-user IC without ISI was investigated in [4] and its secure version in [5]. The concept of achieving secrecy [1], [2] by leveraging the ISI heterogeneity in the wireless medium originates from our prior works [6], [7].

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

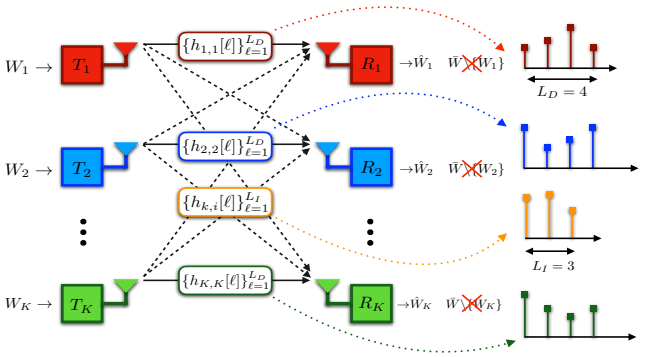

Fig. 1: K-user interference channel with confidential messages with ISI and no CSIT.

The main contribution of this paper lies in showing that SDoF for the K-user IC-CM with ISI linearly increases with the number of users. The main ideas behind the proposed scheme are as follows: **a)** We leverage the simple channel matrix structures resulting from the ODFM transmission techniques in order to eliminate interference and allow coherent decoding of each message at its respectively intended receiver. This is done using the circulant properties of inverse discrete Fourier transform (IDFT) matrices. **b)** We exploit the inherent heterogeneity in channel impulse response (CIR) lengths between the transmitters and the receivers (be they the intended or the unintended receivers) as a result of the wireless multipath propation, and **c)** We strategically designate a small number of transmitters J to act as cooperative jammers, i.e., sending artificial noise, in order to preserve full confidentiality of the messages at the unintended receivers.

II. System Model

We consider the K-user interference channel with confidential messages (IC-CM) with ISI where each transmitter 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 transmission must satisfy confidentiality constraints, i.e., each receiver must not be able to decode any information about the other $K-1$ unintended messages. The channel from the kth transmitter to the intended receiver k is denoted by the channel impulse response (CIR) as $\{h_{k,k}[\ell]\}_{\ell=1}^{L_D}$. L_D denotes the effective number of channel taps or CIR length of the direct

(i.e., desired) link, i.e., from the kth transmitter to the kth receiver. Similarly, the channel from the ith transmitter to the unintended receiver k is denoted by $\{h_{k,i}[\ell]\}_{\ell=1}^{L_I}$, where $k \neq i$. L_I denotes the effective number of channel taps or CIR length of the indirect (i.e., undesired) link, i.e., from the ith transmitter to the kth receiver. In this paper, we focus on symmetric ISI. That is, we assume that the CIR length equals L_D for all $k \in \{1, 2, \ldots, K\}$ and L_I for all $i \neq k \in \{1, 2, \ldots, K\}$. The channel is assumed to be linear time invariant (LTI) over the transmission block length duration. All the channel (CIR) coefficients are assumed to be independent and identically distributed (i.i.d.) random variables drawn from a continuous distribution. Moreover, the transmitters have no knowledge of channel state information. That is, there is no instantaneous CSIT. The transmitters only know the effective CIR lengths L_D and L_I towards the intended and unintended receivers, respectively. To guarantee coherent decoding of the intended message, each receiver k is assumed to know its local channel coefficients.

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

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

where $i, k \in \{1, 2, \ldots, K\}$, $L_{k,i}$ is the CIR length from transmitter i to receiver k, and $z_k[n]$ 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 signal $x_i[n]$ is transmitted with power P satisfying the average power constraint $\mathbb{E}[x_i^2[n]] \leq P$.

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

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

III. Main Result and Illustrative Remarks

We state the main result of this paper in the following Theorem 1. It shows that in the absence of 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 with effective CIR length parameters L_D and L_I, the following SDoF is achievable with no CSIT:*

$$\mathsf{SDoF} = \frac{(K - J)^+ (L_D - L_I)^+}{(N + L_I - 1)}, \tag{5}$$

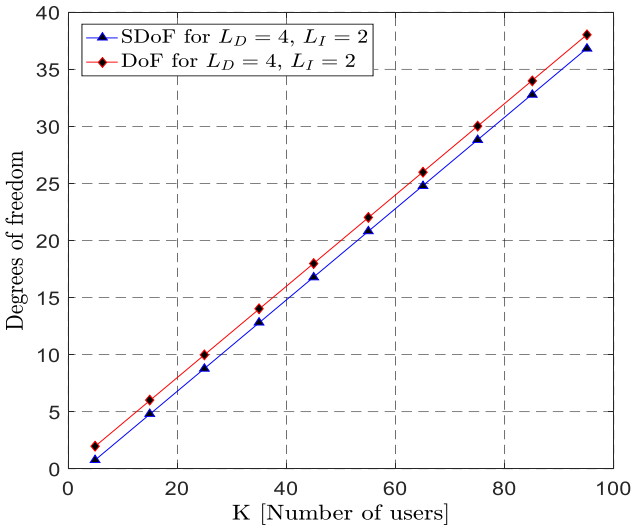

Fig. 2: Comparison of the achievable sum secure rate of the K-user IC-CM with symmetric ISI model (triangles) versus its non-secure version (squares) in [3] for the ISI parameters $L_D = 4$ and $L_I = 2$.

where $J \geq \left\lceil \frac{2(L_I - 1)}{N} \right\rceil + 2$, $N = \max\{L_I, 2(L_D - L_I)\}$, $(x)^+ \triangleq \max\{x, 0\}$, *and* $\lceil x \rceil \triangleq \min\{n \in \mathbb{Z} | n \geq x\}$.

Remark 1. *Comparison with non-secure model [3]*: For symmetric ISI (i.e., where $L_D = L_{k,k}$ and $L_I = L_{k,i \neq k}$), we note that the K-user IC model with ISI in [3] leads to the following DoF:

$$\mathsf{DoF} = \frac{\sum_{k=1}^{K} (L_D - L_I)^+}{(N + L_I - 1)}. \tag{6}$$

Fig. 2 shows the comparison of the achievable rate of the current result versus the non-secure result in [3] for ISI length parameters $L_D = 4$ and $L_I = 2$.

Remark 2. *Linear scaling of SDoF*: 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 (unintended) receiver k. Therefore, under our transmission scheme, we can achieve $\mathsf{SDoF} = \frac{K-3}{3}$, which increases linearly with K.

Due to space limitations, the full proof of the Theorem 1 along with detailed illustrative examples are provided in the full version of the paper [8]. In the next Section, we present a proof sketch and detail the key ideas behind the scheme.

IV. Proof of Theorem 1

The proof of Theorem 1 is subdivided into two Sections. In Section IV-A, we describe the general transmission scheme, the signal matrix structures, and show how decodability and secrecy arise from the designed signal structures. In Section IV-B, we do the calculation of the SDoF of Theorem 1. For

this proof, we use OFDM cyclic prefix and DFT-IDFT based techniques because they lead to systematic signal structures.

A. General Transmission and Channel Matrix Structures

We now consider the general transmission scheme for the K-user IC-CM with symmetric ISI for any CIR length parameters L_D and L_I. This scheme works over a transmission block of total duration T time slots. The block is divided into B OFDM sub-blocks. During each OFDM sub-block $b \in \{1, 2, \ldots, B\}$, the transmitter uses $\bar{N} = N + L_I - 1$ time slots to send an $N = \max\{L_I, 2(L_D - L_I)\}$-length signal vector along with an $(L_I - 1)$-length cyclic prefix. Furthermore, to avoid inter-block interference, we append a guard interval of $L_D - 1$ time slots at the tail end of each transmission block. This leads to a transmission block of total length

$$T = B\bar{N} + L_D - 1. \tag{7}$$

Since all the channel coefficients are i.i.d., and the ISI is symmetric, all receivers observe channel matrices of similar structures. Out of K transmitters, J transmitters act as cooperative jammers and send artificial noises, whereas the remaining $(K - J)$ transmitters send information bearing symbols. The essence of this proof lies in showing that, using the proposed signaling scheme, each one of the $(K-J)$ information bearing transmitters achieves the secure DoF of $\frac{B(L_D-L_I)}{B(N+L_I-1)+L_D-1}$. Thus, the total sum SDoF achieved by our scheme is given by $\mathsf{SDoF} = \sum_{K-J} \frac{B(L_D-L_I)}{B(N+L_I-1)+L_D-1}$. Upon taking the limit as B goes infinity, we then arrive at the expression given in Theorem 1. We next present the details of the transmission scheme.

• **Transmission by the k^{th} transmitter:** Let X_k be the composite signal vector sent by transmitter k during the whole transmission block duration T. Using the above transmission block description leading up to (7), this can thus be written as

$$X_k = \left[X_k^{1\top} \; X_k^{2\top} \; \ldots \; X_k^{B\top} \; \underbrace{0 \ldots 0}_{L_D-1} \right]^\top, \tag{8}$$

where $X_k^b, b \in \{1, 2, \ldots, B\}$ is a vector of length $\bar{N}$ transmitted during the bth sub-block and is of structure

$$X_k^b = \left[\bar{X}_k^{b,cp} \; \bar{X}_k^b \right]^\top, \tag{9}$$

The component vectors of X_k^b have the following structures:

$$\bar{X}_k^b = \left[x_k[(b-1)\bar{N} + 1] \; \ldots \; x_k[(b-1)\bar{N} + N] \right]^\top, \tag{10}$$

which represents the signal of the bth sub-block prior to adding the cyclic prefix, is of length N, whereas

$$\bar{X}_k^{b,cp} = \left[x_k[\bar{b}\bar{N} + N - L_I + 2] \; \ldots \; x_k[\bar{b}\bar{N} + N] \right]^\top \tag{11}$$

is the cyclic prefix of length $L_I - 1$ (i.e., it is a copy of the last $L_I - 1$ symbols of the vector $\bar{X}_k^b$) and $\bar{b} = b - 1$.

In order to exploit the systematic structure of OFDM and DFT matrix properties, the N length vector $\bar{X}_k^b$ is considered to be the frequency domain form precoded vector of the $L_D - L_I$ symbols $s_{k,n}^b, n \in \{1, 2, \ldots, L_D - L_I\}$ from the kth information bearing transmitter (or $n_{k,n}^b, n \in \{1, 2, \ldots, L_D - L_I\}$ from the artificial noise bearing transmitter). This information (or artificial noise) symbols spreading vector can thus be rewritten further as follows using precoding vectors

$$\begin{aligned} \bar{X}_k^b &= \sum_{n=1}^{L_D-L_I} F_n s_{k,n}^b, \text{ for information transmitters,} \\ \bar{X}_k^b &= \sum_{n=1}^{L_D-L_I} F_n n_{k,n}^b, \text{ for artificial noise transmitters,} \end{aligned} \tag{12}$$

where each precoding vector F_n, for $n \in \{1, 2, \ldots, L_D - L_I\}$, is an IDFT vector satisfying the following Lemma 1.

Lemma 1. *Let $\mathbf{H}$ be an $n \times n$ complex circulant matrix. Then $\mathbf{H}$ can be factored as $\mathbf{H} = \mathbf{F}\Lambda\mathbf{F}^{\mathsf{H}}$, where $\mathbf{F} = [F_1, F_2, \ldots, F_n]$ is the n-point IDFT matrix whose column vectors $F_k, k \in \{0, 1, 2, \ldots, n-1\}$ are each given by $F_k = \left[1 \; w_k^1 \; w_k^2 \; \ldots \; w_k^{n-1}\right]$, where $w_k = e^{\frac{j2\pi k}{n}}$ and Λ is the $n \times n$ diagonal matrix whose non-zero elements are the eigenvalues respectively associated with the columns of $\mathbf{F}$.*

Proof. See [9], [10] for the proof of Lemma 1. □

• **Decodability at the k^{th} receiver:** From the above input signal structure description and the input-output relationship in (1), we can now write the received signal for the bth sub-block in the following vector form after removing the cyclic prefix

$$\bar{Y}_k^b = \bar{\mathbf{H}}_{\mathbf{k},\mathbf{k}}^b \bar{X}_k^b + \sum_{i=1, i\neq k}^{K} \bar{\mathbf{H}}_{\mathbf{k},\mathbf{i}}^b X_i^b + \bar{Z}_k^b, \tag{13}$$

where $\bar{\mathbf{H}}_{\mathbf{k},\mathbf{k}}^b$ is an $N \times N$ non-circulant channel matrix carrying the intended symbols from the kth transmitter and $\bar{\mathbf{H}}_{\mathbf{k},\mathbf{i}}^b$ is an $N \times N$ circulant channel matrix carrying the interference from the ith transmitter to the kth receiver. Due to space limitations, we refer the reader to the full version paper [8] for explicit structures of both the interfering and direct link channel matrices. The key aspect is that the channel matrices for interfering links have a circulant structure, whereas the channel matrices for direct links have a non-circulant structure.

The circulant property of $\bar{\mathbf{H}}_{\mathbf{k},\mathbf{i}}^b$ is due to the fact that we appended the cyclic prefix vector of length $L_I - 1$ to the beginning of the transmitted signal in the bth sub-block. Moreover, note that the effective channel matrix $\bar{\mathbf{H}}_{\mathbf{k},\mathbf{k}}^b$ carrying symbols from the kth transmitter to the intended receiver k is non-circulant because the cyclic prefix vector length was chosen to be of length $L_I - 1 < L_D - 1$.

Using the input symbols spreading vector form in (12) and the circulant matrix decomposition property of Lemma 1, we can now rewrite equation (13) as

$$\begin{aligned} \bar{Y}_k^b =& \bar{\mathbf{H}}_{\mathbf{k},\mathbf{k}}^b \sum_{n=1}^{L_D-L_I} F_n s_{k,n}^b + \sum_{i=1, i\neq k}^{K} \bar{\mathbf{H}}_{\mathbf{k},\mathbf{i}}^b \sum_{n=1}^{L_D-L_I} F_n s_{i,n}^b + \bar{Z}_k^b \\ =& \bar{\mathbf{H}}_{\mathbf{k},\mathbf{k}}^b \sum_{n=1}^{L_D-L_I} F_n s_{k,n}^b + \sum_{i=1, i\neq k}^{K} \sum_{n=1}^{L_D-L_I} \lambda_{k,i}^{n,b} F_n s_{i,n}^b + \bar{Z}_k^b, \end{aligned} \tag{14}$$

where (14) comes from the eigenvalue equivalence $\bar{\mathbf{H}}_{\mathbf{k},\mathbf{i}}^b F_n = \lambda_{k,i}^{n,b} F_n$ (or more generally from the linear algebra eigenvalue equivalence notation $\mathbf{A}X = \lambda X$. See [11]). Recall from (12)

that the bth sub-block's transmitted signal $\bar{X}_k^b$ vector was designed from symbols $s_{k,n}^b$, $n \in \{1, 2, \ldots, L_D - L_I\}$, using the IDFT spreading vectors matrix $\mathbf{F} = [F_1\ F_2\ \ldots\ F_{L_D-L_I}]$. Furthermore, the design of the transmission scheme is such that the interference that is seen at the kth receiver from the $K-1$ transmitters can be confined in a space that is (in addition the circulant matrix property that it can be diagonalized by an IDFT matrix obeying Lemma 1) orthogonal to its IDFT matrix complementary vectors matrix $\mathbf{F}_c^{\mathsf{H}} = [F_{L_D-L_I+1}\ F_{L_D-L_I+2}\ \ldots F_{L_D+L_D-2L_I}]^{\mathsf{H}}$. To eliminate the inter-user-interference (IUI), the receiver can thus multiply the received signal $\bar{Y}_k^b$ by the matrix $\mathbf{F}_c^{\mathsf{H}}$ in order to obtain the desired signal component as

$$\tilde{Y}_k^b = \mathbf{F}_c^{\mathsf{H}} \bar{Y}_k^b = \mathbf{F}_c^{\mathsf{H}} \bar{\mathbf{H}}_{\mathbf{k},\mathbf{k}}^b \mathbf{F} S_k^b + \tilde{Z}_k^b, \tag{15}$$

where $\mathbf{F}_c^{\mathsf{H}} \bar{\mathbf{H}}_{\mathbf{k},\mathbf{k}}^b \mathbf{F}$ is of rank $L_D - L_I$. See [3] for the proof of the rank. Each of the $K-J$ receivers out of K is thus able to solve for all of the symbols of the bth sub-block vector $S_k^b = \left[s_{k,1}^b\ s_{k,2}^b\ \ldots\ s_{k,L_D-L_I}^b\right]$.

Secrecy at the k^{th} receiver: This transmission scheme achieves secrecy because it adheres to the following received signal structure at each receiver with respect to the ISI link length parameters L_D and L_I. We have demonstrated above how each receiver can decode its dedicated symbol with regards to the received signal structure. We now look at the complete received signal structure and why any unintended message (i.e., from the ith transmitter) is securely hidden from each unintended receiver k, where $k \neq i$.

We know that each transmitter $k \in \{1, 2, \ldots, K\}$ sends the non-trivial input signal vectors X_k^1, X_k^2, ..., X_k^B respectively over B OFDM sub-blocks as indicated in the input description (8)-(9). Without loss of generality (and for ease of presentation), we prove that confidentiality is achievable for any given vector X_k^b. We note that the complete output signal structure $Y_k^{b'}$ which is observed at receiver k as a result of the transmission of the vector X_k^b before removing the cyclic prefix (i.e., which includes the spillover of the inter-sub-block-interference (IBI) into the next sub-block) can be written as follows

$$Y_k^{b'} = \mathbf{H}_{\mathbf{k},\mathbf{k}}^{\mathbf{b}'} X_k^b + \sum_{i \neq k}^{K} \mathbf{H}_{\mathbf{k},\mathbf{i}}^{\mathbf{b}'} X_i^b + Z_k^{b'}, \tag{16}$$

where $Y_k^{b'}$ and $Z_k^{b'}$ are vectors of length $\hat{N} = \bar{N} + L_D - 1 = (N + L_I - 1) + L_D - 1$. $\mathbf{H}_{\mathbf{k},\mathbf{k}}^{\mathbf{b}'}$ is a $\hat{N} \times \bar{N}$ direct channel matrix carrying the intended (i.e., direct) signal vector $X_k^b = [\bar{X}_k^{b,cp}, \bar{X}_k^b]^\top$ of size $N + L_I - 1 \times 1$. Similarly, $\mathbf{H}_{\mathbf{k},\mathbf{i}}^{\mathbf{b}'}$ is a $\hat{N} \times \bar{N}$ interfering channel matrix carrying the unintended (i.e., interfering) signal vector $X_i^b = [X_i^{b,cp}, \bar{X}_i^b]^\top$ of size $N + L_I - 1 \times 1$ for $i \neq k \in \{1, 2, \ldots, K\}$. More signal structure details are in the full version paper [8]. Note that the last $L_D - L_I$ rows of $\mathbf{H}_{\mathbf{k},\mathbf{i}}^{\mathbf{b}'}$ are all zeros. We further note that, as a result of our precoding strategy in (12), X_i^b can be further expanded as follows

$$X_i^b = \left[\bar{X}_i^{b,cp}, \bar{X}_i^b\right]^\top$$

$$= \underbrace{\begin{bmatrix} \mathbf{0}_{(L_I-1)\times(N-(L_I-1))}\ \mathbf{I}_{(L_I-1)\times(L_I-1)} \\ \mathbf{I}_{N\times N} \end{bmatrix}}_{\mathbf{I_{cp}}} \mathbf{F} S_i^b, \tag{17}$$

where $\mathbf{F} = [F_1\ F_2 \ldots F_{L_D-L_I}]$ is the the composite matrix of precoding vectors, each of size $N \times 1$, the matrix $\mathbf{I_{cp}}$ of size $N + L_I - 1 \times N$ is the combiner that appends the cyclic prefix $\bar{X}_i^{b,cp}$ in front of the precoded signal vector $\bar{X}_i^b = \mathbf{F} S_i^b$ to form the vector X_i^b. $S_i^b = \left[s_{i,1}^b, s_{i,2}^b, \ldots, s_{i,L_D-L_I}^b\right]^\top$ is the vector of $L_D - L_I$ symbols sent by the interfering transmitter $i \neq k \in \{1, 2, \ldots, K\}$ during the bth transmission sub-block. Therefore, from (16), we are now able create a composite interfering channel matrix of the following structure

$$\mathbf{H}_{\mathbf{i}}^{\mathbf{b}'} = \mathbf{H}_{\mathbf{k},\mathbf{i}}^{\mathbf{b}'} \mathbf{I_{cp}} \mathbf{F} = \hat{\mathbf{H}}_{\mathbf{k},\mathbf{i}}^{\mathbf{b}'} \mathbf{F} \tag{18}$$

The detailed structure of the matrix $\hat{\mathbf{H}}_{\mathbf{k},\mathbf{i}}^{\mathbf{b}'}$ is given in the full version paper [8]. We next show that the key to achieving secrecy lies in the structure of the matrix $\hat{\mathbf{H}}_{\mathbf{k},\mathbf{i}}^{\mathbf{b}'}$. Given the above matrix structures, we can rewrite the received signal at the kth receiver as follows

$$Y_k^{b'} = \mathbf{H}_{\mathbf{k}}^{\mathbf{b},\mathbf{K}} X_k^{b,K} + Z_k^{b'} \tag{19}$$

$$= \mathbf{H}_{\mathbf{k},\mathbf{k}}^{\mathbf{b}'} \mathbf{I_{cp}} \mathbf{F} S_k^b + \sum_{i \neq k}^{K} \hat{\mathbf{H}}_{\mathbf{k},\mathbf{i}}^{\mathbf{b}'} \mathbf{F} S_i^b + Z_k^{b'} \tag{20}$$

$$= \hat{\mathbf{H}}_{\mathbf{k},\mathbf{k}}^{\mathbf{b}'} X_k^b + \mathbf{H}_{\mathbf{k}}^{\mathbf{b},\mathbf{K},(-\mathbf{k})} X_K^{b,K,(-k)} + Z_k', \tag{21}$$

where $\mathbf{H}_{\mathbf{k}}^{\mathbf{b},\mathbf{K}}$ is the composite channel matrix seen at the kth receiver, $X_k^{b,K} = \left[X_1^{b\top}\ X_2^{b\top} \ldots X_K^{b\top}\right]^\top$ is the composite input vector sent to receiver k from all K transmitters during the bth sub-block. $\hat{\mathbf{H}}_{\mathbf{k},\mathbf{k}}^{\mathbf{b}'}$ is the channel matrix between the kth transmitter and kth receiver carrying the symbols vector X_k^b from the kth transmitter. $X_K^{b,K,(-k)} = \left[X_1^{b\top} \ldots X_{k-1}^{b\top}\ X_{k+1}^{b\top} \ldots X_K^{b\top}\right]^\top$ is the composite interfering signal vector sent from all transmitters $i \neq k \in \{1, 2, \ldots, K\}$ during the bth sub-block. The composite interfering signals carrying matrix $\mathbf{H}_{\mathbf{k}}^{\mathbf{b},\mathbf{K},(-\mathbf{k})}$ is defined as

$$\mathbf{H}_{\mathbf{k}}^{\mathbf{b},\mathbf{K},(-\mathbf{k})} \tag{22}$$
$$= \left[\hat{\mathbf{H}}_{\mathbf{k},\mathbf{1}}^{\mathbf{b}'} \mathbf{F} \ldots \hat{\mathbf{H}}_{\mathbf{k},\mathbf{J}}^{\mathbf{b}'} \mathbf{F} \ldots \hat{\mathbf{H}}_{\mathbf{k},\mathbf{k-1}}^{\mathbf{b}'} \mathbf{F}\ \hat{\mathbf{H}}_{\mathbf{k},\mathbf{k+1}}^{\mathbf{b}'} \mathbf{F} \ldots \hat{\mathbf{H}}_{\mathbf{k},\mathbf{K}}^{\mathbf{b}'} \mathbf{F}\right].$$

Therefore to achieve confidentiality, it is necessary and sufficient that the following interfering channel submatrix $\hat{\mathbf{H}}_{\mathbf{J-1}}^{\mathbf{b}}$, which is only composed of any $J-1$ of the total J cooperative jamming signal carrying matrices (i.e., which carry artificial noises), be of the same rank as the matrix $\mathbf{H}_{\mathbf{k}}^{\mathbf{b},\mathbf{K},(-\mathbf{k})}$. Without loss of generality (and for ease of presentation), we can let $\hat{\mathbf{H}}_{\mathbf{J-1}}^{\mathbf{b}}$ be of composed of the first $J-1$ interfering matrices and define it as follows

$$\hat{\mathbf{H}}_{\mathbf{J-1}}^{\mathbf{b}} = \left[\hat{\mathbf{H}}_{\mathbf{k},\mathbf{1}}^{\mathbf{b}'} \mathbf{F}\ \hat{\mathbf{H}}_{\mathbf{k},\mathbf{2}}^{\mathbf{b}'} \mathbf{F} \ldots \hat{\mathbf{H}}_{\mathbf{k},\mathbf{J-1}}^{\mathbf{b}'} \mathbf{F}\right] \tag{23}$$

$$= \underbrace{\left[\hat{\mathbf{H}}_{\mathbf{k},\mathbf{1}}^{\mathbf{b}'}\ \hat{\mathbf{H}}_{\mathbf{k},\mathbf{2}}^{\mathbf{b}'} \ldots \hat{\mathbf{H}}_{\mathbf{k},\mathbf{J-1}}^{\mathbf{b}'}\right]}_{\hat{\mathbf{H}}_{\mathbf{J-1}}^{\mathbf{b}'}} \begin{bmatrix} \mathbf{F} & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \mathbf{F} & \mathbf{0} & \ldots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{F} & \ldots & \mathbf{0} \\ \vdots & \ddots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \ldots & \ldots & \mathbf{0} & \mathbf{F} \end{bmatrix}. \tag{24}$$

It is important to note that the nonzero rows portion of each matrix $\hat{\mathbf{H}}^{\mathbf{b}'}_{\mathbf{k},\mathbf{i}}$ as shown in (18) is of size $[(N + L_I - 1) + (L_I - 1)] \times N$ where the number of rows exceeds the number of columns. Therefore the composite rectangular concatenation matrix $\hat{\mathbf{H}}^{\mathbf{b}'}_{\mathbf{J-1}}$ is of size $[(N+L_I-1)+(L_I-1)] \times (J-1)N$. This implies that, for the matrix $\hat{\mathbf{H}}^{\mathbf{b}'}_{\mathbf{J-1}}$ to reach *rank saturation*, we have to concatenate enough cooperative jamming matrices to reach the matrix size inequality condition

$$(J-1)N \geq N + L_I - 1 + (L_I - 1). \tag{25}$$

Hence, from (25), we directly observe that confidentiality for the unintended symbols vector X_i^b sent during the bth sub-block is achieved whenever

$$J \geq \left\lceil \frac{2(L_I-1)}{N} \right\rceil + 2. \tag{26}$$

We note that the description of the scheme above is for each block. In order to achieve perfect secrecy, this needs to be applied with an outer standard wiretap code. Moreover, since all the channel coefficients are continuous i.i.d. and our model is under symmetric ISI, the same secrecy achieving strategy applies to all of the B OFDM symbol input vectors sent from any transmitter k over B sub-blocks. We refer the reader for full details in the full version paper [8].

B. SDoF Calculation

We demonstrated that inter-user interference cancellation allows the kth receiver do decode the intended message during the bth sub-block. However, by the design structure of the input signal vector, the full transmission takes place over a total of B transmission blocks. Furthermore, the inter-sub-block interference is unavoidable in the bth sub-block and its preceding neighbor, i.e., the $(b-1)$th sub-block. This is due to the fact that the cyclic prefix is of length is less than the desired ISI link length, i.e., $L_I - 1 < L_D - 1$. Thus, after removing the $L_D - 1$ zeros appended at the end of B blocks of the input signal, by ignoring channel noise terms $\tilde{Z}_k^1, \tilde{Z}_k^2, \ldots, \tilde{Z}_k^B$, we obtain the input-output relationship below

$$\begin{bmatrix} \tilde{Y}_k^1 \\ \tilde{Y}_k^2 \\ \vdots \\ \tilde{Y}_k^B \end{bmatrix} = \begin{bmatrix} \mathbf{F}_c^{\mathsf{H}} \bar{\mathbf{H}}^1_{\mathbf{k},\mathbf{k}} \mathbf{F} & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{F}_c^{\mathsf{H}} \bar{\mathbf{H}}^{1,2}_{\mathbf{k},\mathbf{k}} \mathbf{F} & \mathbf{F}_c^{\mathsf{H}} \bar{\mathbf{H}}^2_{\mathbf{k},\mathbf{k}} \mathbf{F} & \ldots & \mathbf{0} \\ \mathbf{0} & \mathbf{F}_c^{\mathsf{H}} \bar{\mathbf{H}}^{2,3}_{\mathbf{k},\mathbf{k}} \mathbf{F} & \ldots & \mathbf{0} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & \mathbf{F}_c^{\mathsf{H}} \bar{\mathbf{H}}^B_{\mathbf{k},\mathbf{k}} \mathbf{F} \end{bmatrix} \begin{bmatrix} S_k^1 \\ S_k^2 \\ \vdots \\ S_k^B \end{bmatrix}. \tag{27}$$

Note that the interfering channel matrix $\bar{\mathbf{H}}^{b-1,b}_{\mathbf{k},\mathbf{k}}$ seen in the bth sub-block from the $(b-1)$ neighbor is equivalent to the non-trivial submatrix of the non-circulant matrix seen in the $(b-1)$th sub-block [3]. Because there is no inter-sub-block interference in the first sub-block, the receiver is able to solve for the symbols vector S_k^1. The receiver can solve for S_k^2 using $\tilde{Y}_k^2 - \bar{\mathbf{H}}^{1,2}_{\mathbf{k},\mathbf{k}} \mathbf{F} S_k^1 = \mathbf{F}_c^{\mathsf{H}} \bar{\mathbf{H}}^2_{\mathbf{k},\mathbf{k}} \mathbf{F} S_k^2$, ignoring the channel noise terms. The receiver can then iteratively solve for the remaining symbol vectors S_k^b where $b \in \{3, \ldots, B\}$ by removing the effect of the previous sub-block interference by means of the following successive interference cancellation

$$\tilde{Y}_k^b - \bar{\mathbf{H}}^{b-1,b}_{\mathbf{k},\mathbf{k}} \mathbf{F} S_k^{b-1} = \mathbf{F}_c^{\mathsf{H}} \bar{\mathbf{H}}^b_{\mathbf{k},\mathbf{k}} \mathbf{F} S_k^b. \tag{28}$$

Using a similar strategy, each of the $K - J$ out of K receivers is thus able to solve for a total of $B(L_D - L_I)$ symbols, i.e., for symbols vectors $S_k^1, S_k^2, \ldots, S_k^B$ over the whole transmission block of duration $T = BN + L_D - 1$. Recall that for confidentiality, the first $J = \left\lceil \frac{2(L_I-1)}{N} \right\rceil$ out of K transmitters act as cooperative jammers. Therefore, for a total of $K - J$ information bearing communication links, the devised scheme leads to the following SDoF as B arbitrarily increases

$$\mathsf{SDoF} = \lim_{B \to \infty} \frac{\left(\sum_{k=J+1}^{K} B(L_D - L_I) \right)}{B(N + L_I - 1) + L_D - 1}, \tag{29}$$

which matches the expression of Theorem 1. □

V. Conclusion

We introduced a novel scheme showing that SDoF for the K-user IC-CM with symmetric ISI can linearly increase with the number of users without CSIT. Using OFDM multicarrier techniques along with DFT-IDFT based precoding methods, the devised transmission aligns interfering symbols in a separate subspace from that of the desired symbols at the intended receiver's terminal and thereby leading to the interference elimination. Moreover, we use strategic cooperative jamming which guarantees that these interfering symbols are completely masked by artificial noise at the unintended receivers. There are several interesting research directions that directly arise from this work such as: a) obtaining upper bounds (converse) for interference channels with ISI and confidential messages; and b) devising schemes for the case of asymmetric 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] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] J. d. D. Mutangana and R. Tandon, "Interference channels with confidential messages: Leveraging OFDM transmission to scale up secure degrees of freedom with no CSIT," 2019. [Online]. Available: https://www.dropbox.com/s/iunjp1qwdt0p4kn/ISIT-Secrecy-2019-Paper-Full.pdf?dl=0

[9] G. H. Golub and C. F. V. Loan, *Matrix Computations*. The Johns Hopkins University Press, 1996.

[10] R. M. Gray, "Toeplitz and circulant matrices: A review," *Foundations and Trends in Communications and Information Theory*, vol. 2, no. 3, pp. 155–239, 2006.

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