Blind MIMO Cooperative Jamming: Secrecy via ISI Heterogeneity Without CSIT

Jean de Dieu Mutangana, *Student Member, IEEE*, and Ravi Tandon, *Senior Member, IEEE*

***Abstract*— We investigate the secure degrees of freedom (SDoF) of the multiple-input multiple-output (MIMO) wiretap channel with intersymbol interference (ISI) in the presence of a multi-antenna cooperative jammer. We focus on the practically relevant setting with no channel state information at the transmitters (CSIT). More specifically, the legitimate transmitter and the cooperative jammer only have statistical knowledge of the channel in terms of the effective number of ISI channel taps, i.e., channel impulse response (CIR) lengths, toward the legitimate receiver and the eavesdropper. Our main contribution is to show that in the absence of CSIT, positive SDoF can be achieved by carefully exploiting: 1) the heterogeneity of the CIR lengths toward both receivers and 2) the relative number of antennas at the four terminals. To achieve secrecy, we propose a scheme in which the transmitter strategically sends a mixture of information and artificial noise symbols in a way that exploits the heterogeneity of CIR lengths. Additionally, the cooperative jammer transmits artificial noise symbols in a way that completely masks all the information symbols that are received at the eavesdropping node. Under the proposed scheme, positive SDoF can be achieved, even when the number of antennas at the legitimate receiver is less than the number of antennas at the eavesdropper.**

***Index Terms*— MIMO wiretap channel, cooperative jammer, intersymbol interference (ISI) heterogeneity, secure degrees of freedom (SDoF), statistical channel state information (CSI).**

I. Introduction

THE key idea behind achieving physical (PHY) layer security lies in the exploitation of the inherent randomness in the wireless channel such as fading or noise. Starting from the pioneering work of Wyner [1] on the degraded wiretap channel, the capacity of the non-degraded wiretap channel was characterized by Csiszár and Körner [2]. The capacity of Gaussian wiretap channel was obtained in [3]. Subsequently, numerous other multi-terminal problems, and architectures/methodologies have been studied with secrecy constraints. For instance, cooperative jamming refers to a scenario in which a cooperative jammer (in addition to the information bearing transmitter) purposefully transmits interfering artificial noise to jam the eavesdropper's signal while minimizing the impact at the legitimate receiver [4]–[9].

The majority of aforementioned developments have been made under the assumptions of availability of channel state information at the transmitter (CSIT)–be it instantaneous [10]–[12], delayed [13], [14], or alternating [15]. For the MIMO Gaussian wiretap channel, recent work [16] has shown that even in the absence of CSIT, positive SDoF can be achieved whenever the number of antennas at the eavesdropper is less than the number of antennas at the legitimate receiver. Most of the research progress has been particularly focused on memoryless channels with secrecy constraints. We refer the reader to [17]–[19] for detailed surveys on this topic.

Within the class of *channels with memory*, an important sub class are channels with intersymbol interference (ISI). The capacity of the Gaussian ISI channel was characterized in [20] (also see multi-user generalizations in [21], [22]). Recently, the capacity of the MIMO wiretap channels with ISI and with full CSIT was characterized in [23]. In particular, [23] uses the discrete Fourier transform (DFT) methods introduced in [20]–[22] to create an equivalent set of parallel memoryless MIMO wiretap channels from the original MIMO ISI wiretap channel. Subsequently, the results on the capacity of parallel wiretap channels [24] are then leveraged to characterize the capacity of MIMO wiretap channel with ISI and full CSIT.

In this paper, we focus on the MIMO ISI wiretap channel with a cooperative jammer as shown in Fig. 1. The system consists of a transmitter (Alice) who wishes to communicate securely to Bob, in presence of an eavesdropper (Eve), through the help of a cooperative jammer (Charlie). All the channels are ISI channels, and most importantly, there is no instantaneous knowledge of CSI at either Alice or Charlie. The main novel aspect of this paper is to show that in the presence of statistical heterogeneity in ISI link lengths, statistical channel knowledge alone is in fact sufficient to achieve positive 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 [25]–[27]. CSI at the transmitters (CSIT) is traditionally obtained through piloting mechanisms where, after estimating the channel coefficients, the receiver feeds them back to the transmitter. This, however, is not practically feasible in the wiretap channel setting since an eavesdropper cannot be expected to cooperate with the legitimate transmitter in such manner. For robust and realistically

Manuscript received February 13, 2019; revised May 13, 2019; accepted June 6, 2019. Date of publication June 17, 2019; date of current version September 16, 2019. This work was supported by U.S. NSF through Grants CNS-1715947 and CAREER-1651492. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Lifeng Lai. *(Corresponding author: Ravi Tandon.)*

The authors are with the Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721 USA (e-mail: mutangana@email.arizona.edu; tandonr@email.arizona.edu).

Digital Object Identifier 10.1109/TIFS.2019.2923340

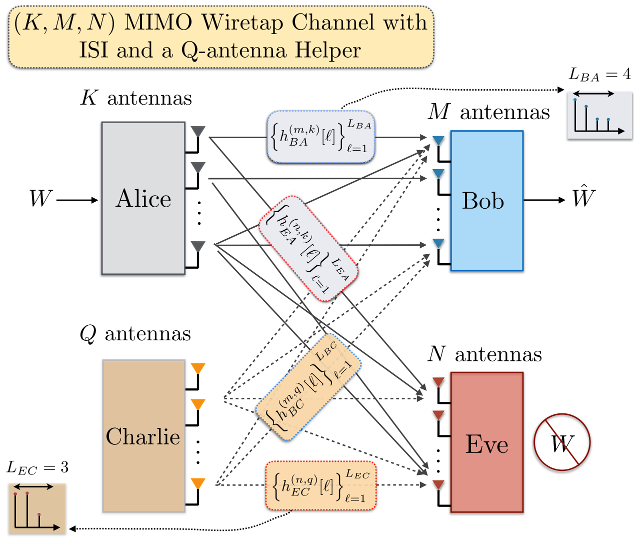
(K, M, N) MIMO Wiretap Channel with ISI and a Q-antenna Helper
K antennas
W
Alice
M antennas
Bob
$\hat{W}$
$L_{BA} = 4$
$\left\{h_{BA}^{(m,k)}[\ell]\right\}_{\ell=1}^{L_{BA}}$
$\left\{h_{EA}^{(n,k)}[\ell]\right\}_{\ell=1}^{L_{EA}}$
Q antennas
Charlie
$\left\{h_{BC}^{(m,q)}[\ell]\right\}_{\ell=1}^{L_{BC}}$
N antennas
Eve
W
$L_{EC} = 3$
$\left\{h_{EC}^{(n,q)}[\ell]\right\}_{\ell=1}^{L_{EC}}$

Fig. 1. The (K, M, N) MIMO ISI Wiretap Channel with a Q-antenna Cooperative Jammer. $L_{BA}(L_{BC})$ and $L_{EA}(L_{EC})$ denote the number of effective channel taps for the channels between Alice (Charlie) and Bob (Bob) and Alice (Charlie) and Eve (Eve), respectively.

secure communication, it thus remains imperative to devise schemes that can achieve security with little or no knowledge of CSI.

Contributions: We now summarize our main contributions:

- We show that for the MIMO ISI wiretap channel with a cooperative jammer, positive SDoF are achievable even in the absence of CSIT. The legitimate transmitter (Alice) and the cooperative jammer (Charlie) only have statistical knowledge of the channels in terms of the effective number of channel taps (i.e., CIR lengths) between the transmitting and the receiving terminals.
- We present a general methodology to leverage the ISI heterogeneity, in terms of CIR lengths between the transmitting and the receiving terminals. Using this statistical knowledge about the ISI channel, the legitimate transmitter uses varying number of transmit antennas to strategically send a mixture of information and artificial noise symbols. Similarly, the cooperative jammer transmits artificial noise symbols only in a manner that, along with the artificial noise symbols from the information bearing transmitter, allows the decodability of information symbols at the legitimate receiver while keeping these information symbols fully immersed in artificial noise at the eavesdropper.
- We obtain a general SDoF expression for the proposed scheme as a function of the number of antennas at the four terminals and the characteristics of the ISI channels (in terms of CIR length parameters). We further show that, when each of the four terminals has only one antenna, the result of this paper becomes a generalization of the single-input single-output (SISO) model studied in [28]. Furthermore, the result of this paper reverts to the result that we presented in [29], when the cooperative jammer is absent. Moreover, we also present numerical results which illustrate the ergodic secrecy rate behavior of the proposed scheme under finite signal-to-noise (SNR) regime.

II. System Model

We consider the MIMO ISI wiretap channel, 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) through the help of a cooperative jammer, Charlie (C) (with Q antennas) as shown in Fig. 1. The channels from Alice (Charlie) to Bob (Bob) and Eve (Eve) are assumed to be ISI channels, where $\left\{h_{BA}^{(m,k)}[\ell]\right\}_{\ell=1}^{L_{BA}}$ denotes the channel impulse response (CIR) between the kth antenna at Alice and the mth antenna at Bob, where $k = 1, \ldots, K$ and $m = 1, \ldots, M$. Here, L_{BA} is the ISI link length parameter, i.e., the number of effective channel taps between Alice and Bob. Similarly, $\left\{h_{EA}^{(n,k)}[\ell]\right\}_{\ell=1}^{L_{EA}}$ denotes the CIR between the kth antenna at Alice and the nth antenna at Eve, where $k = 1, \ldots, K$ and $n = 1, \ldots, N$. Furthermore, $\left\{h_{BC}^{(m,q)}[\ell]\right\}_{\ell=1}^{L_{BC}}$ denotes the CIR between the qth antenna at Charlie and the mth antenna at Bob, where $q = 1, \ldots, Q$ and $m = 1, \ldots, M$ while $\left\{h_{EC}^{(n,q)}[\ell]\right\}_{\ell=1}^{L_{EC}}$ denotes the CIR between the qth antenna at Charlie and the nth antenna at Eve, where $q = 1, \ldots, Q$ and $n = 1, \ldots, N$. All CIR coefficients are assumed to be independent and identically distributed (i.i.d.) and drawn from a continuous distribution. Moreover, we assume that the CIR coefficients are time invariant over the transmission block.

The assumptions on CSI availability are as follows:

- Alice and Charlie do not have any CSI, i.e., do not know any channel coefficients (CIRs). They only know the ISI link length parameters L_{BA}, L_{BC}, L_{EA}, and L_{EC}.
- Bob only knows his local channel coefficients. That is $\left\{h_{BA}^{(m,k)}[\ell]\right\}_{\ell=1}^{L_{BA}}$, $k = 1, \ldots, K$ and $m = 1, \ldots, M$, and $\left\{h_{BC}^{(m,q)}[\ell]\right\}_{\ell=1}^{L_{BC}}$, $q = 1, \ldots, Q$ and $m = 1, \ldots, M$, which are necessary for coherent decoding at Bob.
- Eve has access to all channel coefficients, i.e., can access all CIRs, which is the worst case scenario.

Let $\mathbf{X_A}[t]$ of size $K \times 1$ and $\mathbf{X_C}[t]$ of size $Q \times 1$ be the respective input signal vectors transmitted by Alice and Charlie at time t, then the respective output signal vectors seen at Bob and Eve are given by

$$\begin{aligned}\mathbf{Y_B}[t] &= \sum_{\ell=1}^{L_{BA}} \mathbf{H_{BA}}[\ell]\mathbf{X_A}[t-\ell+1] \\ &\quad + \sum_{\ell=1}^{L_{BC}} \mathbf{H_{BC}}[\ell]\mathbf{X_C}[t-\ell+1] + \mathbf{Z_B}[t] \qquad (1)\\ \mathbf{Y_E}[t] &= \sum_{\ell=1}^{L_{EA}} \mathbf{H_{EA}}[\ell]\mathbf{X_A}[t-\ell+1] \\ &\quad + \sum_{\ell=1}^{L_{EC}} \mathbf{H_{EC}}[\ell]\mathbf{X_C}[t-\ell+1] + \mathbf{Z_E}[t], \qquad (2)\end{aligned}$$

where $(\mathbf{H_{BA}}[\ell])_{(m,k)} = h_{BA}^{(m,k)}[\ell]$, $(\mathbf{H_{BC}}[\ell])_{(m,q)} = h_{BC}^{(m,q)}[\ell]$, $(\mathbf{H_{EA}}[\ell])_{(n,k)} = h_{EA}^{(n,k)}[\ell]$, and $(\mathbf{H_{EC}}[\ell])_{(n,q)} = h_{EC}^{(n,q)}[\ell]$.

$\mathbf{Z_B}[t]$ and $\mathbf{Z_E}[t]$ are channel noise vectors respectively received at Bob and Eve at time t and whose elements are complex Gaussian circularly independent zero-mean and unit-variance random variables. The input signal vectors $\mathbf{X_A}[t]$ and $\mathbf{X_C}[t]$ must satisfy the following average power constraints:

$$\mathbf{E}\left[||\mathbf{X_A}[t]||^2\right] \leq P, \quad \mathbf{E}\left[||\mathbf{X_C}[t]||^2\right] \leq P. \tag{3}$$

Remark 1: We note here that Alice and Charlie can always obtain the ISI link lengths, L_{BA} and L_{BC}, from the legitimate receiver Bob. Furthermore, if Alice and Charlie are not able to directly obtain L_{EA} and L_{EC}, one plausible scenario is that they may only have bounds on L_{EA} and L_{EC}. For instance, if one wants to provide secrecy guarantee in a particular geographical environment, then, from past measurements from legitimate receivers, the transmitters can obtain estimates on the range of the ISI link lengths. These estimates can serve as bounds on the ISI link lengths for any receiver present in the same environment. For the scope of this paper, we assume that Alice and Charlie know the ISI link lengths from both Bob and Eve.

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

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

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

where (4) represents the decoding error probability and (5) represents the uncertainty about the transmitted message W given $\mathbf{Y_E}^{(L)} = \{\mathbf{Y_E}[v]\}_{v=1}^{L}$, the signal observed at Eve. $\hat{W} = g(\mathbf{Y_B}^{(L)})$, where $\mathbf{Y_B}^{(L)} = \{\mathbf{Y_B}[v]\}_{v=1}^{L}$ 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 define the secure degrees of freedom (SDoF) as the pre-log of secrecy capacity

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

The next Section provides the main results of this paper and discusses their immediate consequences as they relate to different antenna and ISI parameter settings.

III. Main Results and Discussion

We divide the main results and discussion into three sections. In Section III-A, we present the main result and provide examples illustrating the core new ideas behind the transmission scheme. We specialize this result for the MIMO ISI wiretap channel in Section III-B, and for the symmetric antenna setting in Section III-C.

A. Main Result and Illustrative Examples

The main contribution of this paper is stated in the following Theorem wherein we show that, under the stated above CSI assumptions, positive SDoF is achievable by carefully leveraging a) the heterogeneity of the ISI link lengths towards the receiving terminals, and b) the relative number of antennas at the four terminals.

Theorem 1: For the (K, M, N) MIMO ISI wiretap channel with a Q-antenna cooperative jammer and with effective ISI link length parameters $(L_{BA}, L_{EA}, L_{BC}, L_{EC})$, the following SDoF is achievable without any CSIT

$$\mathsf{SDoF} \geq \frac{(K+Q-N)^+ \left(\mu_{Bi} - \eta_{Ej}\right)^+}{\mu_{Bi} + \max(L_{Bi}, L_{Ej}) - 1}, \tag{7}$$

where $\mu_{Bi} = \left\lceil \frac{M(L_{Bi}-1)}{K+Q-M} \right\rceil$ and $\eta_{Ej} = \frac{N(L_{Ej}-1)}{K+Q-N}$ for $i, j \in \{A, C\}$, $(x)^+ \overset{\Delta}{=} \max(x, 0)$, and $\lceil x \rceil \overset{\Delta}{=} \min\{n \in \mathbb{Z} | n \geq x\}$.

The expression of inequality (7) corresponds to four cases where parameters $\Omega_B = L_{BC} - L_{BA}$, $\Omega_E = L_{EC} - L_{EA}$, and $\Delta_B = \mu_{BA} - \mu_{BC}$ are related as follows:

- *Case 1.a: if $\Delta_B \geq \max(\Omega_B, \Omega_E)$,*
  then $(\mu_{Bi}, \eta_{Ej}) = (\mu_{BA}, \eta_{EA})$.
- *Case 1.b: if $\Omega_B \leq \Delta_B \leq \Omega_E$,*
  then $(\mu_{Bi}, \eta_{Ej}) = (\mu_{BA}, \eta_{EC})$.
- *Case 2.a: if $\Omega_E \leq \Delta_B \leq \Omega_B$,*
  then $(\mu_{Bi}, \eta_{Ej}) = (\mu_{BC}, \eta_{EA})$.
- *Case 2.b: if $\Delta_B \leq \min(\Omega_B, \Omega_E)$,*
  then $(\mu_{Bi}, \eta_{Ej}) = (\mu_{BC}, \eta_{EC})$.

The proof of Theorem 1 is provided in Section IV.

We next present illustrative examples that highlight the core idea of our scheme, and show how to leverage ISI heterogeneity in order to achieve positive SDoF.

Example 1: Consider the $(K, M, N) = (3, 2, 2)$ MIMO ISI wiretap channel with a cooperative jammer equipped with $Q = 2$ antennas and ISI link length parameters $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (4, 3, 2, 1)$. This means that any symbol transmitted by Alice will be seen over $L_{BA} = 4$ time slots at each of Bob's $M = 2$ antennas and over $L_{EA} = 2$ time slots at each of Eve's $N = 2$ antennas. Similarly, any symbol sent by Charlie will be seen over $L_{BC} = 3$ time slots at each of Bob's $M = 2$ antennas and over $L_{EC} = 1$ time slot at each of Eve's $N = 2$ antennas. Our goal is to show that these parameters, which correspond to Theorem 1 Case 1.a, lead to the SDoF of 4/5. Using direct substitution for the above antenna and ISI link length parameters, we obtain $\mu_{BA} = \left\lceil \frac{M(L_{BA}-1)}{K+Q-M} \right\rceil = \left\lceil \frac{2(4-1)}{3+2-2} \right\rceil = 2$, $\mu_{BC} = \left\lceil \frac{M(L_{BC}-1)}{K+Q-M} \right\rceil = \left\lceil \frac{2(3-1)}{3+2-2} \right\rceil = 2$, $\eta_{EA} = \left\lceil \frac{N(L_{EA}-1)}{K+Q-N} \right\rceil = \left\lceil \frac{2(2-1)}{3+2-2} \right\rceil = 1$, $\Omega_B = L_{BC} - L_{BA} = -1$, $\Omega_B = L_{EC} - L_{EA} = -1$, and $\Delta_B = \mu_{BA} - \mu_{BC} = 0$. Therefore, since $\Delta_B \geq \max\{\Omega_B, \Omega_E\}$, this corresponds to Theorem 1 Case 1.a. This in turn implies that $(\mu_{Bi}, \eta_{Ej}) = (\mu_{BA}, \eta_{EA})$. Moreover, by direct substitution, this scheme which is illustrated by Fig. 2, has a transmission block of duration $T = \left\lceil \frac{M(L_{BA}-1)}{K+Q-M} \right\rceil + \max(L_{BA}, L_{EA}) - 1 = 5$ time slots and is able to securely deliver $(K + Q - N)\left(\left\lceil \frac{M(L_{BA}-1)}{K+Q-M} \right\rceil - \frac{N(L_{EA}-1)}{K+Q-N}\right) = 4$ information symbols, and thus leads to $\mathsf{SDoF} \geq \frac{\left((K+Q-N)(\mu_{BA}-\eta_{EA})\right)^+}{\mu_{BA}+\max(L_{BA},L_{EA})-1} = \frac{4}{5}$. We next show how, for the same parameters, the above SDoF is obtained through the detailed transmission scheme procedure.

1) Transmission by Alice: In the first time slot, respectively over each of her $K = 3$ antennas, Alice transmits two information symbols S_1 and S_2 followed by an artificial noise symbol U_1, i.e., a vector $\mathbf{X}_A[1] = [S_1 \ S_2 \ U_1]^\top$. Similarly, in the second time slot, Alice transmits two information symbols S_3 and S_4 followed by an artificial noise symbol U_2,

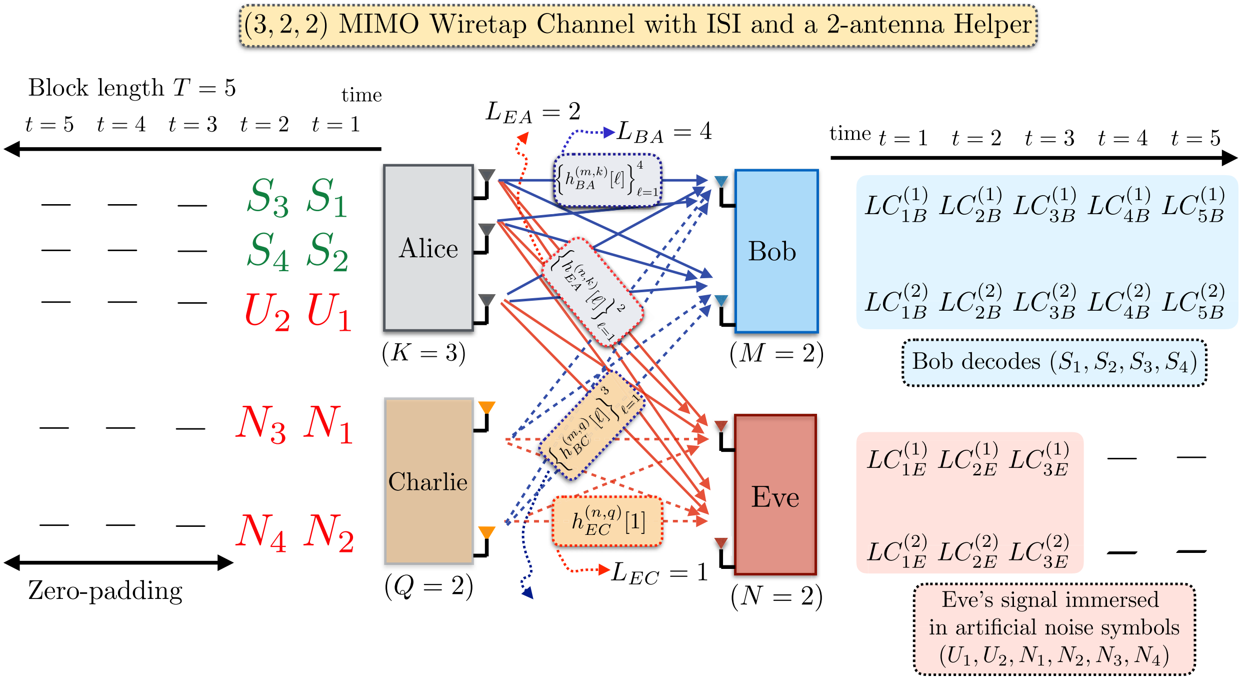
(3, 2, 2) MIMO Wiretap Channel with ISI and a 2-antenna Helper
Block length $T = 5$
time
$t = 5$ $t = 4$ $t = 3$ $t = 2$ $t = 1$
S_3 S_1
S_4 S_2
U_2 U_1
N_3 N_1
N_4 N_2
Zero-padding
Alice
$(K = 3)$
Charlie
$(Q = 2)$
$L_{EA} = 2$
$L_{BA} = 4$
$\{h_{BA}^{(m,k)}[\ell]\}_{\ell=1}^{4}$
$\{h_{EA}^{(n,k)}[\ell]\}_{\ell=1}^{2}$
$\{h_{BC}^{(m,q)}[\ell]\}_{\ell=1}^{3}$
$h_{EC}^{(n,q)}[1]$
$L_{EC} = 1$
Bob
$(M = 2)$
Eve
$(N = 2)$
time $t = 1$ $t = 2$ $t = 3$ $t = 4$ $t = 5$
$LC_{1B}^{(1)}$ $LC_{2B}^{(1)}$ $LC_{3B}^{(1)}$ $LC_{4B}^{(1)}$ $LC_{5B}^{(1)}$
$LC_{1B}^{(2)}$ $LC_{2B}^{(2)}$ $LC_{3B}^{(2)}$ $LC_{4B}^{(2)}$ $LC_{5B}^{(2)}$
Bob decodes (S_1, S_2, S_3, S_4)
$LC_{1E}^{(1)}$ $LC_{2E}^{(1)}$ $LC_{3E}^{(1)}$
$LC_{1E}^{(2)}$ $LC_{2E}^{(2)}$ $LC_{3E}^{(2)}$
Eve's signal immersed in artificial noise symbols $(U_1, U_2, N_1, N_2, N_3, N_4)$

Fig. 2. Illustrative example for the $(K, M, N) = (3, 2, 2)$ MIMO ISI wiretap channel with a $(Q = 2)$-antenna cooperative jammer where $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (4, 3, 2, 1)$. Here, we can achieve SDoF of 4/5 by securely sending 4 information symbols to Bob over 5 time slots.

i.e., a vector $\mathbf{X}_A[2] = [S_3\ S_4\ U_2]^\top$. Alice, then remains silent for the remainder of the transmission block, i.e., over the third, fourth, and fifth time slots. This can also be viewed as zero-padding, i.e., $\mathbf{X}_A[3] = \mathbf{X}_A[4] = \mathbf{X}_A[5] = [0\ 0\ 0]^\top$.

2) Transmission by Charlie: In the first time slot, respectively over each of his $K = 2$ antennas, Charlie transmits two artificial noise symbols N_1 and N_2, i.e., a vector $\mathbf{X}_C[1] = [N_1\ N_2]^\top$. Similarly, in the second time slot, Charlie transmits two artificial noise symbols N_3 and N_4, i.e., a vector $\mathbf{X}_C[2] = [N_3\ \ N_4]^\top$. Charlie, then remains silent for the remainder of the transmission block, i.e., over the third, fourth, and fifth time slots. This can also be viewed as zero-padding, i.e., $\mathbf{X}_C[3] = \mathbf{X}_C[4] = \mathbf{X}_C[5] = [0\ 0]^\top$.

3) Decodability at Bob: Since the channel coefficients are i.i.d continuous random variables, Bob who is equipped with $M = 2$ antennas observes $M\left(\left\lceil\frac{M(L_{BA}-1)}{K+Q-M}\right\rceil + L_{BA} - 1\right) = 10$ independent linear equations over the total transmission block length, i.e, for $t = 1, 2, \ldots, 5$. See Fig. 2.

Linear combinations seen at the first antenna:

- $t = 1$: $LC_{1B}^{(1)}(S_1, S_2, U_1, N_1, N_2)$
- $t = 2$: $LC_{2B}^{(1)}(S_1, S_2, U_1, N_1, N_2, S_3, S_4, U_2, N_3, N_4)$
- $t = 3$: $LC_{3B}^{(1)}(S_1, S_2, U_1, N_1, N_2, S_3, S_4, U_2, N_3, N_4)$
- $t = 4$: $LC_{4B}^{(1)}(S_1, S_2, U_1, S_3, S_4, U_2, N_3, N_4)$
- $t = 5$: $LC_{5B}^{(1)}(S_3, S_4, U_2)$

Linear combinations seen at the second antenna:

- $t = 1$: $LC_{1B}^{(2)}(S_1, S_2, U_1, N_1, N_2)$
- $t = 2$: $LC_{2B}^{(2)}(S_1, S_2, U_1, N_1, N_2, S_3, S_4, U_2, N_3, N_4)$
- $t = 3$: $LC_{3B}^{(2)}(S_1, S_2, U_1, N_1, N_2, S_3, S_4, U_2, N_3, N_4)$
- $t = 4$: $LC_{4B}^{(2)}(S_1, S_2, U_1, S_3, S_4, U_2, N_3, N_4)$
- $t = 5$: $LC_{5B}^{(2)}(S_3, S_4, U_2)$

From these equations, Bob is able to solve for information symbols (S_1, S_2, S_3, S_4) and discard the remaining artificial noise symbols $(U_1, U_2, N_1, N_2, N_3, N_4)$.

4) Secrecy at Eve: Eve who has $N = 2$ antennas receives $N\left(\left\lceil\frac{M(L_{BA}-1)}{K+Q-M}\right\rceil + L_{EA} - 1\right) = 6$ independent linear equations only over the first three time slots, where all the information symbols are fully immersed in the artificial noise symbols. She observes nothing over the remainder of the transmission block (this is in part due to the zero-padding by Alice and Charlie during the transmission phase).

Linear combinations seen at the first antenna:

- $t = 1$: $LC_{1E}^{(1)}(S_1, S_2, U_1, N_1, N_2)$
- $t = 2$: $LC_{2E}^{(1)}(S_1, S_2, U_1, S_3, S_4, U_2, N_3, N_4)$
- $t = 3$: $LC_{3E}^{(1)}(S_3, S_4, U_2)$
- $t = 4, 5$: Nothing is received in these time slots.

Linear combinations seen at the second antenna:

- $t = 1$: $LC_{1E}^{(2)}(S_1, S_2, U_1, N_1, N_2)$
- $t = 2$: $LC_{2E}^{(2)}(S_1, S_2, U_1, S_3, S_4, U_2, N_3, N_4)$
- $t = 3$: $LC_{3E}^{(2)}(S_3, S_4, U_2)$
- $t = 4, 5$: Nothing is received in these time slots.

Therefore, Eve who only receives six independent linear equations (i.e., equivalent to the total number of independent artificial noise symbols) with ten unknowns over the whole transmission block length duration is not able to solve for (S_1, S_2, S_3, S_4). This, in turn, means that the devised above transmission scheme allows us to securely transmit 4 information symbols using 5 time slots, i.e., achieving SDoF of 4/5. This matches the expression of Theorem 1.

We note here that the formal proof of secrecy and SDoF calculation will be shown in Section IV-C.

Example 2: For a $(3, 2, 2)$ wiretap channel with a $Q = 2$ cooperative jammer and ISI link length parameters $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (5, 3, 1, 3)$, similar substitution steps as the above lead to Theorem 1 Case 1.b for which we obtain SDoF of 5/7.

Example 3: For a $(3, 2, 2)$ wiretap channel with a $Q = 2$ cooperative jammer and ISI link length parameters $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (5, 8, 4, 2)$, similar substitution leads to Theorem 1 Case 2.a and SDoF of 3/4.

Example 4: For a $(3, 2, 2)$ wiretap channel with a $Q = 2$ cooperative jammer and ISI link length parameters $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (3, 4, 1, 2)$, similar substitution leads to Theorem 1 Case 2.b and SDoF of 4/5.

The following example illustrates how, under the proposed scheme, positive SDoF can be achieved through the exploitation of ISI link length heterogeneity when the number of antennas at the legitimate receiver (Bob) is less than the number of antennas at the eavesdropper (Eve).

Example 5: Consider the $(K, M, N) = (3, 1, 2)$ MIMO ISI wiretap channel with a cooperative jammer equipped with $Q = 2$ antennas and ISI link length parameters $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (9, 3, 2, 1)$. We follow similar steps as those in Example 1. This scheme has a transmission block of duration $T = 10$ time slots and is able to securely deliver four information symbols. Our goal is to show that we can achieve SDoF of 2/5.

5) Transmission by Alice: In the first time slot, respectively over each of her $K = 3$ antennas, Alice transmits two information symbols S_1 and S_2 followed by an artificial noise symbol U_1, i.e., a vector $\mathbf{X}_A[1] = [S_1 \;\; S_2 \;\; U_1]^\top$. Similarly, in the second time slot, Alice transmits two information symbols S_3 and S_4 followed by an artificial noise symbol U_2, i.e., a vector $\mathbf{X}_A[2] = [S_3 \; S_4 \; U_2]^\top$. Alice, then remains silent for the remainder of the transmission block, i.e., from the third to the tenth time slots. This can also be viewed as zero-padding, i.e., $\mathbf{X}_A[3] = \mathbf{X}_A[4] = \cdots = \mathbf{X}_A[10] = [0 \; 0 \; 0]^\top$.

6) Transmission by Charlie: In the first time slot, respectively over each of his $K = 2$ antennas, Charlie transmits two artificial noise symbols N_1 and N_2, i.e., a vector $\mathbf{X}_C[1] = [N_1 \; N_2]^\top$. Similarly, in the second time slot, Charlie transmits two artificial noise symbols vector $\mathbf{X}_C[2] = [N_3 \;\; N_4]^\top$. Charlie, then remains silent for the remainder of the transmission block. This can also be viewed as zero-padding, i.e., $\mathbf{X}_C[3] = \mathbf{X}_C[4] = \cdots = \mathbf{X}_C[10] = [0 \; 0]^\top$.

7) Decodability at Bob: Bob observes ten independent linear equations over the total transmission block length (i.e, for $t = 1, 2, \ldots, 10$). Bob is thus able to solve for information symbols (S_1, S_2, S_3, S_4) and discard the remaining artificial noise symbols $(U_1, U_2, N_1, N_2, N_3, N_4)$.

8) Secrecy at Eve: Eve only observes six independent linear equations over the first three time slots (where all the information symbols are fully immersed in the same subspace as the artificial noise symbols), and observes nothing over the remainder of the transmission block. Consequently, she is not able to solve for the information symbols (S_1, S_2, S_3, S_4). Hence, this transmission scheme allows us to securely transmit 4 information symbols using 10 time slots, i.e., achieving SDoF of 2/5. This matches the expression of Theorem 1.

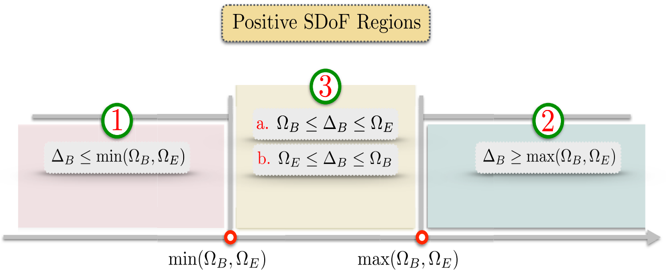
Positive SDoF Regions
1
$\Delta_B \leq \min(\Omega_B, \Omega_E)$
3
a. $\Omega_B \leq \Delta_B \leq \Omega_E$
b. $\Omega_E \leq \Delta_B \leq \Omega_B$
2
$\Delta_B \geq \max(\Omega_B, \Omega_E)$
$\min(\Omega_B, \Omega_E)$
$\max(\Omega_B, \Omega_E)$

Fig. 3. Illustrative figure of positive SDoF resulting from the four cases described in Theorem 1.

The above four cases of Theorem 1, where positive SDoF is achievable, are illustrated by the regions in Fig. 3, by comparing the parameters Δ_B, $\boldsymbol{\Omega}_B$, and $\boldsymbol{\Omega}_E$. In Fig. 3, region 1 represents positive SDoF for Case 2.b, region 2 represents positive SDoF for Case 1.a, whereas region 3 represents positive SDoF for Case 1.b and Case 2.a.

Remark 2 (Interplay between antenna and ISI link length parameters): From the numerator of equation (7), we have that positive SDoF is achievable when $(K + Q - N) > 0$ and $\left(\mu_{Bi} - \eta_{Ej}\right) > 0$ for $i, j \in \{A, C\}$. For example, when $i = A$ and $j = A$, then $\mu_{Bi} = \mu_{BA} = \left\lceil \frac{M(L_{BA}-1)}{K+Q-M} \right\rceil$ and $\eta_{Ej} = \frac{N(L_{EA}-1)}{K+Q-N}$, which corresponds to the first case. Thus, as a consequence of algebraic manipulation, we can obtain following ISI link length parameters and antenna number relationship for positive SDoF $\frac{L_{BA}-1}{L_{EA}-1} > \frac{N(K+Q-M)}{M(K+Q-N)}$. Furthermore, because the numerator of the SDoF in Equation (7) depends on the product of the two terms as follows $(K + Q - N)\left(\mu_{Bi} - \eta_{Ej}\right)$, if the antenna parameters are fixed, one would wish to increase the first term of the second factor, i.e., increase μ_{BA}, by increasing L_{BA}. However, although this increase may seem beneficial, it also leads to the increase in the transmission block $T = \mu_{BA} + L_{BA} - 1$, which is the denominator of equation (7). We refer the reader to Fig. 4 (for fixed L_{EA} and varying L_{BA}) and Fig. 5 (for fixed L_{BA} and varying L_{EA}) for parametric examples illustrating how varying the antenna and ISI link lengths may affect SDoF. A similar analogy can be followed for other cases of the Theorem 1.

From Fig. 4, we observe that for fixed values of the ISI link lengths from Alice to Eve (L_{EA}) and increasing the ISI link lengths from Alice to Bob (L_{BA}), the SDoF increases. Of course, as can also be seen from the figure, this also depends on the number of antennas at all the terminals. From Fig. 5, we observe that for fixed values of the ISI link lengths from Alice to Bob (L_{BA}) and increasing the ISI link lengths from Alice to Eve (L_{EA}), the SDoF decreases towards zero. Similarly, this also depends on the number of antennas at all the terminals.

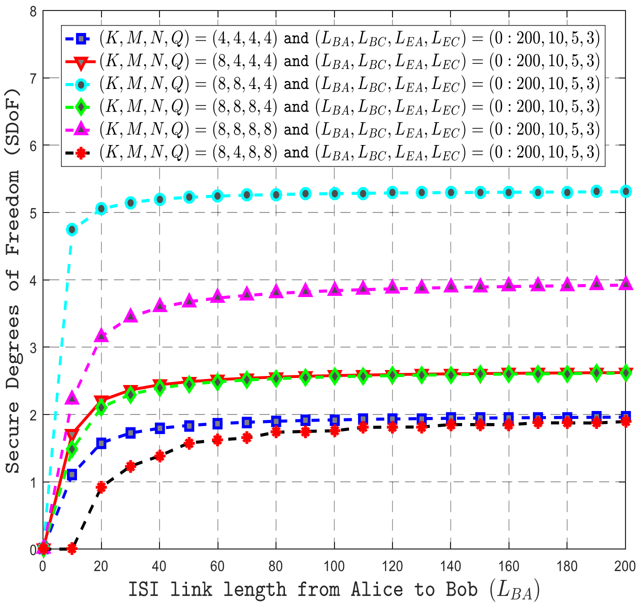

Fig. 4. SDoF versus varying antenna and L_{BA} parameters.

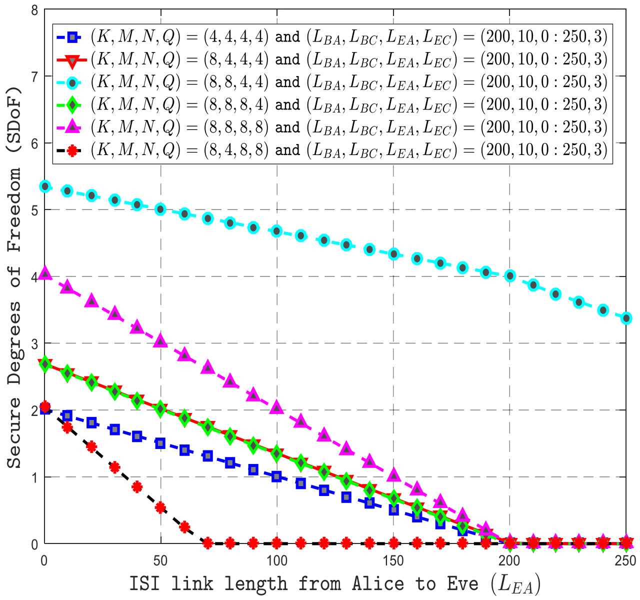

Fig. 5. SDoF versus varying antenna and L_{EA} parameters.

B. MIMO ISI Wiretap Channel Without CSIT

The following Corollary is an immediate consequence of setting $Q = 0$, i.e., removing the cooperative jammer from the system model. It states that the general result of Theorem 1 reverts to the main result of the MIMO ISI wiretap channel without CSIT as was derived in [29].

Corollary 1: For the (K, M, N) MIMO ISI wiretap channel without CSIT and with effective ISI link length parameters L_{BA} and L_{EA} from Alice to the receivers (Bob and Eve), respectively, the following SDoF is achievable [29]:

$$\mathsf{SDoF} \geq \frac{\left((K-N)\left(\left\lceil\frac{M(L_{BA}-1)}{K-M}\right\rceil - \frac{N(L_{EA}-1)}{K-N}\right)\right)^{+}}{\left\lceil\frac{M(L_{BA}-1)}{K-M}\right\rceil + \max(L_{BA}, L_{EA}) - 1}. \tag{8}$$

An interesting aspect about the result of Corollary 1 is that it implies that positive SDoF can be achieved even when the number of antennas at the eavesdropper is larger than the number of antennas at the legitimate receiver. This is the case when $L_{BA} > L_{EA}$, i.e, when the number of taps between Alice and Bob exceeds the number of taps between Alice and Eve. On the other hand, when $L_{BA} < L_{EA}$, positive SDoF can still be achieved when $M > N$, i.e., when the number of antennas at Bob is larger than the number of antennas at Eve.

Remark 3 (Difference between the MIMO ISI wiretap channel with a cooperative jammer and the MIMO ISI wiretap channel without a cooperative jammer): We note here that the (K, M, N, Q) MIMO ISI wiretap channel with a cooperative jammer (of the current paper) differs from the (K+Q, M, N) MIMO ISI wiretap channel without a cooperative jammer. That is, if we remove Charlie (who has Q antennas) from the network and instead equip Alice (who originally has K antennas) with $K + Q$ antennas, the resulting networks may differ due to ISI heterogeneity in $(L_{BA}, L_{BC}, L_{EA}, L_{EC})$. For example, by Theorem 1, the $(K, M, N, Q) = (5, 2, 3, 4)$ MIMO wiretap channel with a helper and with ISI parameters $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (4, 9, 2, 3)$ leads to achievable SDoF of 1.09*, whereas the $(K + Q, M, N, Q) = (9, 2, 3)$ MIMO ISI wiretap channel without a helper and with ISI parameters $(L_{BA}, L_{EA}) = (4, 2)$ leads to achievable SDoF of* 0.75.

C. Symmetric Antenna MIMO ISI Wiretap Channel With a Cooperative Jammer and No CSIT

The following Corollary is an immediate consequence of setting $K = M = N = Q$, i.e., when all the terminals have an equal number of antennas.

Corollary 2: For the (K, K, K) MIMO ISI wiretap channel with a K-antenna cooperative jammer and with effective ISI link length parameters $(L_{BA}, L_{EA}, L_{BC}, L_{EC})$, the following SDoF is achievable without any CSIT

$$\mathsf{SDoF} \geq \frac{K\left(L_{Bi} - L_{Ej}\right)^{+}}{L_{Bi} + \max(L_{Bi}, L_{Ej}) - 2}, \tag{9}$$

where $i, j \in \{A, C\}$.

The expression of inequality (9) *corresponds to four cases where parameters $\Omega_B = L_{BC} - L_{BA}$ and $\Omega_E = L_{EC} - L_{EA}$ are related as follows:*

- Case 1.a: *if $\Omega_B \geq \max(0, \Omega_E)$,*
  then $(L_{Bi}, L_{Ej}) = (L_{BA}, L_{EA})$.
- Case 1.b: *if $0 \leq \Omega_B \leq \Omega_E$,*
  then $(L_{Bi}, L_{Ej}) = (L_{BA}, L_{EC})$.
- Case 2.a: *if $\Omega_E \leq \Omega_B \leq 0$,*
  then $(L_{Bi}, L_{Ej}) = (L_{BC}, L_{EA})$.
- Case 2.b: *if $\Omega_B \leq \min(0, \Omega_E)$,*
  when $(L_{Bi}, L_{Ej}) = (L_{BC}, L_{EC})$.

We note that when $K = M = N = Q = 1$, Corollary 2 becomes a generalization of the result in [28]. That is, it becomes the SISO ISI wiretap channel with a single antenna cooperative jammer in the absence of channel state information at all the transmitting terminals. This is because [28] only considered the channel impulse response (CIR) link lengths to be symmetric. The effective number of channel taps from

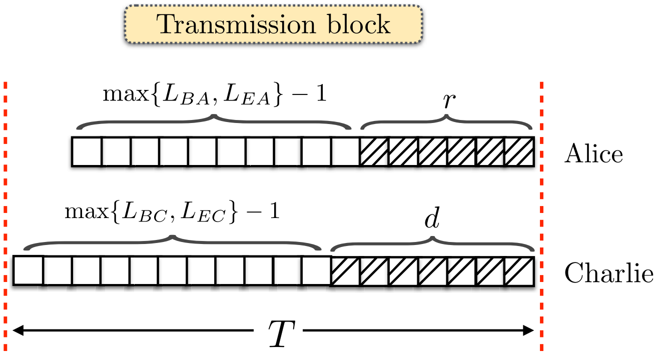

Fig. 6. Illustration of transmission block length T for the proposed scheme.

Alice (Alice) to Bob (Eve) was assumed to be equivalent to the effective number of channel taps from the Charlie (Charlie) to Bob (Eve). This assumption in [28] of ISI symmetry towards the receivers, i.e., that $L_{BA} = L_{BC}$ and $L_{EA} = L_{EC}$, was used in order to introduce the basic idea behind ISI heterogeneity exploitation to achieve secrecy. In other terms, the result of Corollary 2 can be thought of as a secure communication system consisting of a set of K parallel and independent SISO ISI wiretap channels, each with a single antenna cooperative jammer.

On the other hand, we note here that for the non-symmetric antenna case, as an immediate consequence of having symmetric ISI link lengths like those in [28], the general result of Theorem 1 reverts to the single antenna setting.

IV. Proof of Theorem 1

We divide the proof of Theorem 1 into three Sections. In Section IV-A, we explain the transmission scheme. In Section IV-B, we describe the transmitted signal, the ISI channel matrices, and the received signal vectors. In Section IV-C, we calculate the secrecy rate and the achievable SDoF of the proposed scheme.

A. Transmission Scheme

The general scheme works over a transmission block of duration T as shown in Fig 6. Alice transmits a combination of information symbols and artificial noise symbols during the first r time slots and remains silent during the last $(\max(L_{BA}, L_{EA}) - 1)$ time slots. Therefore, Alice uses a total of $T_A = r + \max(L_{BA}, L_{EA}) - 1$ time slots. Similarly, Charlie transmits artificial noise symbols during the first d time slots and remains silent during the last $(\max(L_{BC}, L_{EC}) - 1)$ time slots. Therefore, Charlie uses a total of $T_C = d + \max(L_{BC}, L_{EC}) - 1$ time slots. The proposed transmission scheme is under the assumption that the received signals are observed at discrete and synchronous time slots. This leads to a transmission block of total duration

$$\begin{aligned} T &= \max(T_A, T_C) \\ &= \max(r + L_{BA}, r + L_{EA}, d + L_{BC}, d + L_{EC}) - 1. \quad (10) \end{aligned}$$

1) Transmission by Alice: In each of the first r time slots, Alice sends α_t independent information symbols and $(K - \alpha_t) = \beta_t$ independent artificial noise symbols on her K antennas, for $t = 1, 2, \ldots, r$. This implies that Alice transmits a total of $\sum_{t=1}^{r} \alpha_t$ information symbols (IS) and a total of $rK - \sum_{t=1}^{r} \alpha_t = \sum_{t=1}^{r} \beta_t$ artificial noise (AN) symbols over r time slots. All ISs and ANs satisfy the power constraints in (3). Due to ISI heterogeneity resulting from multipath propagation of wireless signals, symbols transmitted during each such time slot will be observed over L_{BA} time slots at Bob and over L_{EA} time slots at Eve.

2) Transmission by Charlie: In each of the first d time slots, Charlie sends γ_t independent artificial noise symbols on his Q antennas, for $t = 1, 2, \ldots, d$, where $\gamma_t \leq Q$. This implies that Charlie transmits a total of $\sum_{t=1}^{d} \gamma_t \leq dQ$ artificial noise (AN) symbols, each satisfying power constraints in (3), over d time slots. Due to ISI heterogeneity, symbols transmitted during each such time slot will be observed over L_{BC} time slots at Bob and over L_{EC} time slots at Eve.

3) Decodability at Bob: We guarantee Bob to decode both information symbols and artificial noise symbols. This is made feasible by keeping a condition that the total number of symbols (ISs + ANs), i.e., $\sum_{t=1}^{r} \alpha_t + \sum_{t=1}^{r} \beta_t + \sum_{t=1}^{d} \gamma_t \leq rK + dQ$, is no larger than the number of linearly independent equations received at Bob. That is

$$M\left(\max(r + L_{BA}, d + L_{BC}) - 1\right) \geq \sum_{t=1}^{r} \alpha_t + \sum_{t=1}^{r} \beta_t + \sum_{t=1}^{d} \gamma_t, \quad (11)$$

where the left hand side of the inequality (11) represents the number of equations seen at Bob.

4) Secrecy at Eve: In order to preserve secrecy, we guarantee that the signal space at Eve be completely immersed in artificial noise symbols (from Alice and Charlie). In particular, we must keep the total number of ANs, i.e., $\sum_{t=1}^{r} \beta_t + \sum_{t=1}^{d} \gamma_t \leq rK - \sum_{t=1}^{r} \alpha_t + dQ$, at least as large as the number of independent equations seen at Eve. This leads to the constraint

$$N(\max(r + L_{EA}, d + L_{EC}) - 1) \leq \sum_{t=1}^{r} \beta_t + \sum_{t=1}^{d} \gamma_t, \quad (12)$$

where the left hand side of the inequality (12) represents the number of equations seen at Eve. We note that the description of the above secure scheme is for each block. Moreover, in order to achieve perfect secrecy, the proposed scheme can be combined with an outer standard wiretap code [1].

The above decodability and secrecy constraints lead to four cases:

Case 1.a: $M\left(\max(r + L_{BA}, d + L_{BC}) - 1\right) = M(r + L_{BA} - 1)$ and $N(\max(r + L_{EA}, d + L_{EC}) - 1) = N(r + L_{EA} - 1)$. As a direct consequence of this case, r and d must thus satisfy

$$r \leq \left\lceil \frac{M(L_{BA} - 1)}{K + Q - M} \right\rceil \quad \text{and} \quad d \geq \left\lceil \frac{M(L_{BC} - 1)}{K + Q - M} \right\rceil, \quad (13)$$

when $d \geq r$. From substitution into (10), we obtain the following expression for the transmission block

$$T \leq \left\lceil \frac{M(L_{BA} - 1)}{K + Q - M} \right\rceil + \max(L_{BA}, L_{EA}) - 1). \quad (14)$$

Case 1.b: $M\left(\max(r + L_{BA}, d + L_{BC}) - 1\right) = M(r + L_{BA} - 1)$ and $N(\max(r + L_{EA}, d + L_{EC}) - 1) = N(d + L_{EC} - 1)$. Similarly, for r and d satisfying the inequalities in (13), this case and substitution into (10) lead to

$$T \leq \left\lceil \frac{M(L_{BA}-1)}{K+Q-M} \right\rceil + \max(L_{BA}, L_{EC}) - 1). \tag{15}$$

Case 2.a: $M\,(\max(r+L_{BA}, d+L_{BC})-1) = M(d+L_{BC}-1)$ and $N(\max(r+L_{EA}, d+L_{EC})-1) = N(r+L_{EA}-1)$. As a direct consequence of this case, r and d must thus satisfy

$$r \geq \left\lceil \frac{M(L_{BA}-1)}{K+Q-M} \right\rceil \quad \text{and} \quad d \leq \left\lceil \frac{M(L_{BC}-1)}{K+Q-M} \right\rceil, \tag{16}$$

where $d \geq r$. From substitution into (10), we obtain the following expression for the transmission block

$$T \leq \left\lceil \frac{M(L_{BC}-1)}{K+Q-M} \right\rceil + \max(L_{BC}, L_{EA}) - 1). \tag{17}$$

Case 2.b: $M\,(\max(r+L_{BA}, d+L_{BC})-1) = M(d+L_{BC}-1)$ and $N(\max(r+L_{EA}, d+L_{EC})-1) = N(d+L_{EC}-1)$. Similarly, for r and d satisfying the inequalities in (16), this case and substitution into (10) lead to

$$T \leq \left\lceil \frac{M(L_{BC}-1)}{K+Q-M} \right\rceil + \max(L_{BC}, L_{EC}) - 1). \tag{18}$$

We will use constraints (11) and (12) for the secrecy rate and SDoF calculations in Section IV-C.

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 by Alice, whose components are the $K \times 1$ subvectors $\mathbf{X_A}[t]$ transmitted during the tth time slot, for $t = 1, 2, \ldots, r$, satisfying the power constraint in (3). Let $\mathbf{X_C}$ be a composite signal vector of size $dQ \times 1$, consisting of artificial noise symbols transmitted by Charlie, whose components are the $Q \times 1$ subvectors $\mathbf{X_C}[t]$ transmitted during the tth time slot, for $t = 1, 2, \ldots, d$, satisfying the power constraint in (3). Over the course of the 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 Section IV-C.

Combining the properties of the system model equations (1) and (2) and the described above input vectors, the outputs at Bob and Eve over the transmission block can be written in matrix form as follows:

$$\mathbf{Y_B} = \mathbf{H_{BA}X_A} + \mathbf{H_{BC}X_C} + \mathbf{Z_B} \tag{19}$$

$$\mathbf{Y_E} = \mathbf{H_{EA}X_A} + \mathbf{H_{EC}X_C} + \mathbf{Z_E}. \tag{20}$$

To simplify the notation, for the signal vector received at Bob $\mathbf{Y_B}$, we will only consider the output vector dimensions for the case where $L_b = \max(r+L_{BA}-1, d+L_{BC}-1) = r+L_{BA}-1$. We note that an analogous received signal structure can be obtained when $L_b = \max(r+L_{BA}-1, d+L_{BC}-1) = d+L_{BC}-1$. Similarly, for the notation of the signal vector received at Eve $\mathbf{Y_E}$, we will only consider the case where $L_e = \max(r+L_{EA}-1, d+L_{EC}-1) = r+L_{EA}-1$. We note that an analogous received signal structure can be obtained when $L_e = \max(r+L_{EA}-1, d+L_{EC}-1) = d+L_{EC}-1$. In other words, in this proof, we focus on the transmission Case 1.a. The other cases follow similar steps and are thus omitted here.

Starting from equation (1), we can write the composite signal vector $\mathbf{Y_B} = \left[\mathbf{Y_B}[1]^\top \ \mathbf{Y_B}[2]^\top \ \ldots \ \mathbf{Y_B}[L_b]^\top\right]^\top$ as shown in (19), where $\mathbf{Y_B}$ is of size $M(r+L_{BA}-1) \times 1$. $\mathbf{X_A} = \left[\mathbf{X_A}[1]^\top \ \mathbf{X_A}[2]^\top \ \ldots \ \mathbf{X_A}[r]^\top\right]^\top = \left[\mathbf{S}_{\alpha_1}^\top \ \mathbf{U}_{\beta_1}^\top \ \mathbf{S}_{\alpha_2}^\top \ \mathbf{U}_{\beta_2}^\top \ \ldots \ \mathbf{S}_{\alpha_r}^\top \ \mathbf{U}_{\beta_r}^\top\right]^\top$ is the $rK \times 1$ composite signal vector transmitted by Alice over the whole transmission block, where $\mathbf{S}_{\alpha_\mathbf{t}}$ is an $\alpha_t \times 1$ vector consisting of all the information symbols transmitted by Alice over α_t antennas in the tth time slot, for $t = 1, 2, \ldots, r$, and $\mathbf{U}_{\beta_\mathbf{t}}$ is a $(K-\alpha_t) \times 1$ vector consisting of all the artificial noise symbols transmitted by Alice over $\beta_t = K - \alpha_t$ antennas in the tth time slot. $\mathbf{X_C} = \left[\mathbf{X_C}[1]^\top \ \mathbf{X_C}[2]^\top \ldots \mathbf{X_C}[d]^\top\right]^\top = \left[\mathbf{N}_{\gamma_1}^\top \ \mathbf{N}_{\gamma_2}^\top \ldots \mathbf{N}_{\gamma_d}^\top\right]^\top$ is the $rQ \times 1$ composite artificial noise symbols vector transmitted by Charlie over the whole transmission, where $\mathbf{N}_{\gamma_\mathbf{t}}$ is a $\gamma_t \times 1$ vector consisting of all the artificial noise symbols transmitted by Charlie over $\gamma_t \leq Q$ antennas in the tth time slot, for $t = 1, 2, \ldots, d$. $(\mathbf{H_{BA}}[\ell])_{(m,k)} = h_{BA}^{(m,k)}[\ell]$, for $\ell = 1, 2, \ldots, L_{BA}$, and $\mathbf{H_{BA}}[\ell]$ is an $M \times K$ matrix. $\mathbf{H_{BA}}$ is the composite $M(r+L_{BA}-1) \times rK$ channel matrix seen at Bob from Alice. $(\mathbf{H_{BC}}[\ell])_{(m,q)} = h_{BC}^{(m,q)}[\ell]$, for $\ell = 1, 2, \ldots, L_{BC}$, and $\mathbf{H_{BC}}[\ell]$ is an $M \times Q$ matrix. Since for the considered case, $M(d+L_{BC}-1) \leq M(r+L_{BA}-1)$, we have that $\mathbf{H_{BC}}$ is the composite $M(r+L_{BA}-1) \times rQ$ channel matrix seen at Bob from Charlie. To preserve vector/matrix addition properties, we note that the top nonzero matrix portion of $\mathbf{H_{BC}}$ in (19), that we denote as $\tilde{\mathrm{H}}_{\mathrm{BC}}$, is of size $M(d+L_{BC}-1) \times rQ$, whereas $\mathbf{Z_B}$ is the $M(r+L_{BA}-1) \times 1$ composite channel noise vector seen at Bob.

Starting from equation (2), we can write the composite signal vector $\mathbf{Y_E} = \left[\mathbf{Y_E}[1]^\top \ \mathbf{Y_E}[2]^\top \ \ldots \ \mathbf{Y_E}[L_e]^\top\right]^\top$ as shown in (20), where $\mathbf{Y_E}$ is of size $N(r+L_{EA}-1) \times 1$. $\mathbf{H_{EA}}$ is the composite $N(r+L_{EA}-1) \times (rK+dQ)$ channel matrix seen at Eve from Alice. $(\mathbf{H_{EA}}[\ell])_{(n,k)} = h_{EA}^{(n,k)}[\ell]$, for $\ell = 1, 2, \ldots, L_{EA}$, and $\mathbf{H_{EA}}[\ell]$ is an $N \times K$ matrix. Similarly, since for the considered case, $N(d+L_{EC}-1) \leq N(r+L_{EA}-1)$, we have that $\mathbf{H_{EC}}$ is the composite $N(r+L_{EA}-1) \times rQ$ channel matrix seen at Eve from Charlie. To preserve vector/matrix addition properties, we note that the top nonzero portion of $\mathbf{H_{EC}}$ in (20), that we denote as $\tilde{\mathrm{H}}_{\mathrm{EC}}$, is of size $N(d+L_{EC}-1) \times rQ$. $(\mathbf{H_{EC}}[\ell])_{(n,q)} = h_{EC}^{(n,q)}[\ell]$, for $\ell = 1, 2, \ldots, L_{EC}$, and $\mathbf{H_{EC}}[\ell]$ is an $N \times Q$ matrix, whereas $\mathbf{Z_E}$ is the $N(r+L_{EA}-1) \times 1$ composite channel noise vector seen at Eve.

We note that the above received signal representations can be rearranged further in order to isolate the information and artificial noise symbols carrying submatrices. Using properties of the system model equations (1)-(2) and their matrix form representation in (19)-(20), we can further rewrite $\mathbf{Y_B}$ and $\mathbf{Y_E}$ by splitting the channel matrices as

$$\mathbf{Y_B} = \mathbf{H_{BA}^S S} + \mathbf{H_{BA}^U U} + \mathbf{H_{BC}^N N} + \mathbf{Z_B} \tag{23}$$

$$\mathbf{Y_E} = \mathbf{H_{EA}^S S} + \mathbf{H_{EA}^U U} + \mathbf{H_{EC}^N N} + \mathbf{Z_E}, \tag{24}$$

where $\left[\mathbf{H_{BA}^S} \ \mathbf{H_{BA}^U}\right] = \mathbf{H_{BA}}$. $\mathbf{H_{BA}^S}$ is the information symbol carrying submatrix of size $M(r+L_{BA}-1) \times \sum_{t=1}^{r} \alpha_t$, whereas $\mathbf{H_{BA}^U}$ is the artificial noise carrying submatrix of size $M(r+L_{BA}-1) \times \sum_{t=1}^{r} \beta_t$. In order to preserve vector/matrix addition, $\mathbf{H_{BC}^N}$ is the artificial noise symbol carrying submatrix

$$\mathbf{Y_B} = \underbrace{\begin{bmatrix} \mathbf{H^S_{BA}}[1] & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{H^S_{BA}}[2] & \mathbf{H^S_{BA}}[1] & \dots & \mathbf{0} \\ \vdots & \mathbf{H^S_{BA}}[2] & \ddots & \vdots \\ \vdots & \vdots & \ddots & \mathbf{0} \\ \mathbf{H^S_{BA}}[L_{BA}] & \vdots & \ddots & \mathbf{H^S_{BA}}[1] \\ \mathbf{0} & \mathbf{H^S_{BA}}[L_{BA}] & \vdots & \mathbf{H^S_{BA}}[2] \\ \mathbf{0} & \mathbf{0} & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H^S_{BA}}[L_{BA}] \end{bmatrix}}_{\mathbf{H^S_{BA}}} \underbrace{\begin{bmatrix} \mathbf{S}_{\alpha_1} \\ \mathbf{S}_{\alpha_2} \\ \vdots \\ \mathbf{S}_{\alpha_\mathrm{r}} \end{bmatrix}}_{\mathbf{S}} + \underbrace{\begin{bmatrix} \mathbf{H^U_{BA}}[1] & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{H^U_{BA}}[2] & \mathbf{H^U_{BA}}[1] & \dots & \mathbf{0} \\ \vdots & \mathbf{H^U_{BA}}[2] & \ddots & \vdots \\ \vdots & \vdots & \ddots & \mathbf{0} \\ \mathbf{H^U_{BA}}[L_{BA}] & \vdots & \ddots & \mathbf{H^U_{BA}}[1] \\ \mathbf{0} & \mathbf{H^U_{BA}}[L_{BA}] & \vdots & \mathbf{H^U_{BA}}[2] \\ \mathbf{0} & \mathbf{0} & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H^U_{BA}}[L_{BA}] \end{bmatrix}}_{\mathbf{H^U_{BA}}} \underbrace{\begin{bmatrix} \mathbf{U}_{\beta_1} \\ \mathbf{U}_{\beta_2} \\ \vdots \\ \mathbf{U}_{\beta_\mathrm{r}} \end{bmatrix}}_{\mathbf{U}} + \mathbf{H_{BC}X_C} + \mathbf{Z_B} \tag{21}$$

$$\mathbf{Y_E} = \underbrace{\begin{bmatrix} \mathbf{H^S_{EA}}[1] & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{H^S_{EA}}[2] & \mathbf{H^S_{EA}}[1] & \dots & \mathbf{0} \\ \vdots & \mathbf{H^S_{EA}}[2] & \ddots & \vdots \\ \vdots & \vdots & \ddots & \mathbf{0} \\ \mathbf{H^S_{EA}}[L_{EA}] & \vdots & \ddots & \mathbf{H^S_{BA}}[1] \\ \mathbf{0} & \mathbf{H^S_{EA}}[L_{EA}] & \vdots & \mathbf{H^S_{EA}}[2] \\ \mathbf{0} & \mathbf{0} & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H^S_{EA}}[L_{EA}] \end{bmatrix}}_{\mathbf{H^S_{EA}}} \underbrace{\begin{bmatrix} \mathbf{S}_{\alpha_1} \\ \mathbf{S}_{\alpha_2} \\ \vdots \\ \mathbf{S}_{\alpha_\mathrm{r}} \end{bmatrix}}_{\mathbf{S}} + \underbrace{\begin{bmatrix} \mathbf{H^U_{EA}}[1] & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{H^U_{EA}}[2] & \mathbf{H^U_{BA}}[1] & \dots & \mathbf{0} \\ \vdots & \mathbf{H^U_{EA}}[2] & \ddots & \vdots \\ \vdots & \vdots & \ddots & \mathbf{0} \\ \mathbf{H^U_{EA}}[L_{EA}] & \vdots & \ddots & \mathbf{H^U_{EA}}[1] \\ \mathbf{0} & \mathbf{H^U_{EA}}[L_{EA}] & \vdots & \mathbf{H^U_{EA}}[2] \\ \mathbf{0} & \mathbf{0} & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H^U_{EA}}[L_{EA}] \end{bmatrix}}_{\mathbf{H^U_{EA}}} \underbrace{\begin{bmatrix} \mathbf{U}_{\beta_1} \\ \mathbf{U}_{\beta_2} \\ \vdots \\ \mathbf{U}_{\beta_\mathrm{r}} \end{bmatrix}}_{\mathbf{U}} + \mathbf{H_{EC}X_C} + \mathbf{Z_E} \tag{22}$$

of size $M(r+L_{BA}-1)\times\sum_{t=1}^{d}\gamma_t$ whose top nonzero submatrix portion is $\tilde{\mathbf{H}}_{\mathbf{EC}}$ of size $M(d+L_{BC}-1)\times\sum_{t=1}^{d}\gamma_t$. Similarly, $[\mathbf{H^S_{EA}}\ \mathbf{H^U_{EA}}] = \mathbf{H_{EA}}$. $\mathbf{H^S_{EA}}$ is the information symbol carrying submatrix of size $N(r+L_{EA}-1)\times\sum_{t=1}^{r}\alpha_t$, whereas $\mathbf{H^U_{EA}}$ is the artificial noise carrying submatrix of size $N(r+L_{EA}-1)\times\sum_{t=1}^{r}\beta_t$. Similarly, $\mathbf{H^N_{EC}}$ is the artificial noise symbol carrying submatrix of size $N(r+L_{EA}-1)\times\sum_{t=1}^{d}\gamma_t$ whose top nonzero submatrix portion is $\tilde{\mathbf{H}}^N_{EC}$ of size $N(d+L_{EC}-1)\times\sum_{t=1}^{d}\gamma_t$. $\mathbf{S} = \begin{bmatrix}\mathbf{S}_{\alpha_1}{}^\top & \mathbf{S}^\top_{\alpha_2} & \dots & \mathbf{S}^\top_{\alpha_r}\end{bmatrix}^\top$ is the information symbols subvector of $\mathbf{X_A}$ and $\mathbf{U} = \begin{bmatrix}\mathbf{U}_{\beta_1}{}^\top & \mathbf{U}^\top_{\beta_2} & \dots & \mathbf{U}^\top_{\beta_r}\end{bmatrix}^\top$ is the artificial noise symbols subvector of $\mathbf{X_A}$, whereas $\mathbf{N} = \begin{bmatrix}\mathbf{N}^\top_{\gamma_1} & \mathbf{N}^\top_{\gamma_2} & \dots & \mathbf{N}^\top_{\gamma_d}\end{bmatrix}^\top = \mathbf{X_C}$ is the composite artificial noise vector from Charlie.

Using the above description of (23) and (24), we can thus explicitly rewrite the received signal vectors at Bob and Eve, i.e., $\mathbf{Y_B}$ and $\mathbf{Y_E}$, as shown in (21) and (22), shown at the top of this page, where both $\mathbf{H_{BA}}$ and $\mathbf{H_{EA}}$ have been split into information and artificial noise symbol carrying submatrices. We next use these received signal structures for secrecy rate and SDoF calculations.

C. Secrecy Rate and SDoF Calculation

The secure achievable rate R_s over the transmission block of duration T is defined as follows

$$R_s = \frac{I(\mathbf{S};\mathbf{Y_B}) - I(\mathbf{S};\mathbf{Y_E})}{T}, \tag{25}$$

where $I(\mathbf{S};\mathbf{Y_B})$ (respectively, $I(\mathbf{S};\mathbf{Y_E})$), is the mutual information between the information symbols vector $\mathbf{S}$ transmitted by Alice and the composite signal vector $\mathbf{Y_B}$ received at Bob (respectively, $\mathbf{Y_E}$ received at Eve). Using differential entropy, these mutual information terms can be expanded as

$$I(\mathbf{S};\mathbf{Y_B}) = h(\mathbf{Y_B}) - h(\mathbf{Y_B}|\mathbf{S}) \tag{26}$$

$$I(\mathbf{S};\mathbf{Y_E}) = h(\mathbf{Y_E}) - h(\mathbf{Y_E}|\mathbf{S}). \tag{27}$$

Furthermore, we now use equation (19) to write $h(\mathbf{Y_B})$ as

$$h(\mathbf{Y_B}) = h(\mathbf{H_{BA}X_A} + \mathbf{H_{BC}X_C} + \mathbf{Z_B}) \tag{28}$$

$$= h(\mathbf{H_B X} + \mathbf{Z_B}) \tag{29}$$

$$= \log(\pi e)^{M(r+L_{BA}-1)}\det(\mathbf{I_B} + P\mathbf{H_B H_B}^{\mathsf{H}}), \tag{30}$$

where equation (29) follows from the notation $\mathbf{H_B} = \begin{bmatrix}\mathbf{H_{BA}}\ \mathbf{H_{BC}}\end{bmatrix}$, i.e., the composite channel matrix seen at Bob, and $\mathbf{X} = \left[\mathbf{X}_{\mathbf{A}}^{\top}\ \mathbf{X}_{\mathbf{C}}^{\top}\right]^{\top}$, i.e., the composite input signal vector comprising of both signal vectors from Alice and Charlie. Equation (30) follows from [30] and $\mathbf{I_B} + P\mathbf{H_B}\mathbf{H_B}^{\mathsf{H}}$ is the covariance matrix of $\mathbf{Y_B}$. $\mathbf{I_B}$ is an $M(r + L_{BA} - 1) \times M(r + L_{BA} - 1)$ covariance matrix of the channel noise vector $\mathbf{Z_B}$. P is the symbol transmission power from constraints (3). Lemma 1 shows that the matrix $\mathbf{H_B}$ is of rank $rK + dQ$, almost surely. $\mathbf{F}^{\mathsf{H}}$ denotes the Hermitian transpose of the matrix $\mathbf{F}$.

Using equation (23), we expand $h(\mathbf{Y_B}|\mathbf{S})$ of (26) as follows

$$h(\mathbf{Y_B}|\mathbf{S}) = h(\mathbf{H}_{\mathbf{BA}}^{\mathbf{S}}\mathbf{S} + \mathbf{H}_{\mathbf{BA}}^{\mathbf{U}}\mathbf{U} + \mathbf{H}_{\mathbf{BC}}^{\mathbf{N}}\mathbf{N} + \mathbf{Z_B}|\mathbf{S}) \quad (31)$$

$$= h(\mathbf{H}_{\mathbf{BA}}^{\mathbf{U}}\mathbf{U} + \mathbf{H}_{\mathbf{BC}}^{\mathbf{N}}\mathbf{N} + \mathbf{Z_B}) \quad (32)$$

$$= \log(\pi e)^{M(r+L_{BA}-1)} \det(\mathbf{I_B} + P\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]^{\mathsf{H}}}), \quad (33)$$

where (32) follows due to the independence of $\mathbf{S}$ from $(\mathbf{U}, \mathbf{N}, \mathbf{Z_B})$. $\mathbf{I_B}$ is the channel noise covariance matrix identical to the one in (30). $\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]} = \left[\mathbf{H}_{\mathbf{BA}}^{\mathbf{U}}\ \mathbf{H}_{\mathbf{BC}}^{\mathbf{N}}\right]$, i.e., the noise carrying submatrix of the composite channel matrix seen at Bob. Lemma 1 shows that $\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}$ is of rank $N(r + L_{EA} - 1$, almost surely. $\mathbf{I_B} + P\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]^{\mathsf{H}}}$ is the covariance matrix of $\mathbf{H}_{\mathbf{BA}}^{\mathbf{U}}\mathbf{U} + \mathbf{H}_{\mathbf{BC}}^{\mathbf{N}}\mathbf{N} + \mathbf{Z_B}$.

By plugging (30) and (33) into (26), we thus obtain

$$I(\mathbf{S}; \mathbf{Y_B})$$

$$= \log \frac{\det(\mathbf{I_B} + P\mathbf{H_B}\mathbf{H_B}^{\mathsf{H}})}{\det(\mathbf{I_B} + P\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]^{\mathsf{H}}})} \quad (34)$$

$$= \log \frac{\det(\mathbf{I_B} + P\Psi_{\mathbf{B}}\Lambda_{\mathbf{B}}\Lambda_{\mathbf{B}}^{\mathsf{H}}\Psi_{\mathbf{B}}^{\mathsf{H}})}{\det(\mathbf{I_B} + P\Psi_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}\Lambda_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}\Lambda_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]^{\mathsf{H}}}\Psi_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]^{\mathsf{H}}})} \quad (35)$$

$$= \log \frac{\det(\mathbf{I_B} + P\mathbf{Q}\Lambda_{\mathbf{B}})}{\det(\mathbf{I}_{\mathbf{B_N}} + P\mathbf{Q}\Lambda_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]})} \quad (36)$$

$$= \sum_{i=1}^{\mathsf{rank}(\mathbf{H_B})}\log(1 + P|\lambda_{B_i}|^2) - \sum_{i=1}^{\mathsf{rank}(\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]})}\log(1 + P|\lambda_{B_i}^{[\mathbf{U},\mathbf{N}]}|^2), \quad (37)$$

where both the numerator and the denominator of (35) follow from the singular value decomposition (SVD) of $\mathbf{H_B}$ into $\Psi_{\mathbf{B}}\Lambda_{\mathbf{B}}\mathbf{V_B}^{\mathsf{H}}$ and $\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}$ into $\Psi_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}\Lambda_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}\mathbf{V}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]^{\mathsf{H}}}$, respectively. The numerator of (36) is due to Sylvester's determinant identity property $\det(\mathbf{I} + \mathbf{AB}) = \det(\mathbf{I} + \mathbf{BA})$, matrix scalar multiplication, associativity, and commutativity properties, and the fact that $\Psi_{\mathbf{B}}$ and $\mathbf{V_B}^{\mathsf{H}}$ are unitary matrices whose product is an identity matrix. Similarly, the denominator of (36) 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 $\Psi_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}$ and $\mathbf{V}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]^{\mathsf{H}}}$ are unitary matrices. In (37), λ_{B_i} denotes the ith ordered singular value of the matrix $\mathbf{H_B}$, and $\lambda_{B_i}^{[\mathbf{U},\mathbf{N}]}$ denotes the ith ordered singular value of the matrix $\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}$.

We now use equation (20) to expand the first term of equation (27) as

$$h(\mathbf{Y_E}) = h(\mathbf{H_{EA}}\mathbf{X_A} + \mathbf{H_{EC}}\mathbf{X_C} + \mathbf{Z_E}) \quad (38)$$

$$= h(\mathbf{H_E}\mathbf{X} + \mathbf{Z_E}) \quad (39)$$

$$= \log(\pi e)^{N(r+L_{EA}-1)} \det(\mathbf{I_E} + P\mathbf{H_E}\mathbf{H_E}^{\mathsf{H}}), \quad (40)$$

where equation (39) follows from the notation $\mathbf{H_E} = \left[\mathbf{H_{EA}}\ \mathbf{H_{EC}}\right]$, i.e., the composite channel matrix seen at Eve and $\mathbf{X} = \left[\mathbf{X_A}^{\top}\ \mathbf{X_C}^{\top}\right]^{\top}$. $\mathbf{I_E} + P\mathbf{H_E}\mathbf{H_E}^{\mathsf{H}}$ is the covariance matrix of $\mathbf{Y_E}$, whereas $\mathbf{I_E}$ is an $N(r + L_{EA} - 1) \times N(r + L_{EA} - 1)$ covariance matrix of the channel noise vector $\mathbf{Z_E}$. Lemma 2 shows that the matrix $\mathbf{H_E}$ is of rank $N(r + L_{BA} - 1)$, almost surely.

Using equation (24), we expand the second term of (27) as

$$h(\mathbf{Y_E}|\mathbf{S}) = h(\mathbf{H}_{\mathbf{EA}}^{\mathbf{S}}\mathbf{S} + \mathbf{H}_{\mathbf{EA}}^{\mathbf{U}}\mathbf{U} + \mathbf{H}_{\mathbf{EC}}^{\mathbf{N}}\mathbf{N} + \mathbf{Z_E}|\mathbf{S}) \quad (41)$$

$$= h(\mathbf{H}_{\mathbf{EA}}^{\mathbf{U}}\mathbf{U} + \mathbf{H}_{\mathbf{EC}}^{\mathbf{N}}\mathbf{N} + \mathbf{Z_E}) \quad (42)$$

$$= \log(\pi e)^{N(r+L_{EA}-1)} \det(\mathbf{I_E} + P\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]}\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]^{\mathsf{H}}}), \quad (43)$$

where (42) is due to the independence of $\mathbf{S}$ from $(\mathbf{U}, \mathbf{N}, \mathbf{Z_E})$. $\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]} = \left[\mathbf{H}_{\mathbf{EA}}^{\mathbf{U}}\ \mathbf{H}_{\mathbf{EC}}^{\mathbf{N}}\right]$, i.e., the noise carrying submatrix of the composite channel matrix seen at Eve. Lemma 2 shows that $\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]}$ is of rank $N(r + L_{EA} - 1$, almost surely. $\mathbf{I_E}$ is the channel noise covariance matrix identical to that in (40).

By plugging (40) and (43) into (27), we thus obtain

$$I(\mathbf{S}; \mathbf{Y_E})$$

$$= \log \frac{\det(\mathbf{I_E} + P\mathbf{H_E}\mathbf{H_E}^{\mathsf{H}})}{\det(\mathbf{I_E} + P\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]}\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]^{\mathsf{H}}})} \quad (44)$$

$$= \sum_{i=1}^{\mathsf{rank}(\mathbf{H_E})}\log(1 + P|\lambda_{E_i}|^2) - \sum_{i=1}^{\mathsf{rank}(\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]})}\log(1 + P|\lambda_{E_i}^{[\mathbf{U},\mathbf{N}]}|^2), \quad (45)$$

where (44)-(45) follow from similar arguments as (34)-(37).

We next observe that equations (37) and (45) depend on the rank of the four matrices, $\mathbf{H_B}$, $\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}$, $\mathbf{H_E}$, and $\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]}$, as stated in the following two Lemmas.

Lemma 1: The channel matrices $\mathbf{H_B}$, *and* $\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}$ *satisfy*:

$$\mathsf{rank}(\mathbf{H_B}) \overset{a.s.}{=} rK + dQ$$

$$\mathsf{rank}(\mathbf{H}_{\mathbf{B}}^{[\mathbf{U},\mathbf{N}]}) \overset{a.s.}{=} N(r + L_{EA} - 1),$$

where a.s. stands for "almost surely."

Lemma 2: The channel matrices $\mathbf{H_E}$, *and* $\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]}$ *satisfy*:

$$\mathsf{rank}(\mathbf{H_E}) \overset{a.s.}{=} N(r + L_{EA} - 1)$$

$$\mathsf{rank}(\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]}) \overset{a.s.}{=} N(r + L_{EA} - 1).$$

The proofs for Lemmas 1 and 2 are given in Appendix.

The core essense of the transmission scheme is to make sure that all the information symbols seen at Eve are completely immersed in the space occupied by artificial noise. This is formally equivalent to the statement of Lemma 2, i.e., the ranks of the matrices $\mathbf{H_E}$ and $\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]}$ are the same.

Combining the definition of SDoF (6), the definition of secrecy rate (25), and the expansions of the mutual information equations (26) and (27) into (37) and (45), we obtain

$$\mathsf{SDoF} \geq \lim_{P\to\infty} \frac{R_s}{\log(P)} \quad (46)$$

$$= \lim_{P\to\infty} \frac{I(\mathbf{S}; \mathbf{Y_B}) - I(\mathbf{S}; \mathbf{Y_E})}{T\log(P)} \quad (47)$$

$$
\begin{aligned}
&= \lim_{P\to\infty} \Bigg(\frac{\sum_{i=1}^{\mathrm{rank}(\mathbf{H_B})} \log\,(1+P|\lambda_{B_i}|^2)}{T\log(P)} \\
&\quad - \frac{\sum_{i=1}^{\mathrm{rank}(\mathbf{H_B^{[U,N]}})} \log\,(1+P|\lambda_{B_i}^{[\mathbf{U},\mathbf{N}]}|^2)}{T\log(P)}\Bigg) \\
&\quad - \lim_{P\to\infty} \Bigg(\frac{\sum_{i=1}^{\mathrm{rank}(\mathbf{H_E})} \log\,(1+P|\lambda_{E_i}|^2)}{T\log(P)} \\
&\quad - \frac{\sum_{i=1}^{\mathrm{rank}(\mathbf{H_E^{[U,N]}})} \log\,(1+P|\lambda_{E_i}^{[\mathbf{U},\mathbf{N}]}|^2)}{T\log(P)}\Bigg) \qquad (48)\\
&= \lim_{P\to\infty} \Bigg(\frac{\sum_{i=1}^{rK+dQ} \log\,(1+P|\lambda_{B_i}|^2)}{T\log(P)} \\
&\quad - \frac{\sum_{i=1}^{N(r+L_{EA}-1)} \log\,(1+P|\lambda_{B_i}^{[\mathbf{U},\mathbf{N}]}|^2)}{T\log(P)}\Bigg) \\
&\quad - \lim_{P\to\infty} \Bigg(\frac{\sum_{i=1}^{N(r+L_{EA}-1)} \log\,(1+P|\lambda_{E_i}|^2)}{T\log(P)} \\
&\quad - \frac{\sum_{i=1}^{N(r+L_{EA}-1)} \log\,(1+P|\lambda_{E_i}^{[\mathbf{U},\mathbf{N}]}|^2)}{T\log(P)}\Bigg) \qquad (49)\\
&= \Bigg(\frac{rK+dQ-N(r+L_{EA}-1)}{T}\Bigg) \\
&\quad - \Bigg(\frac{N(r+L_{EA}-1)-N(r+L_{EA}-1)}{T}\Bigg) \qquad (50)\\
&= \frac{rK+dQ-N(r+L_{EA}-1)}{T} \qquad (51)\\
&\geq \frac{r(K+Q-N)-N(L_{EA}-1)}{T} \qquad (52)\\
&= (K+Q-N)\Bigg(\frac{r-\frac{N(L_{EA}-1)}{K+Q-N}}{T}\Bigg), \qquad (53)
\end{aligned}
$$

where (49) is due to the "decodability at Bob" condition (11), "secrecy at Eve" condition (12), Lemma 1, and Lemma 2. The inequality (52) follows from (13). By plugging r and T from (13) and (14) into (53), we obtain the SDoF expression of Theorem 1 Case 1.a. The derivations of SDoF expressions for Theorem 1 Case 1.b, Case 2.a, and Case 2.b follow a similar analogy as that of the derivation of Case 1.a and, hence, will be omitted here. This completes the proof of Theorem 1. □

V. Simulations and Discussions

A. Secrecy Rate Under Finite SNR Regime

In this section, we present numerical simulation results highlighting the behavior of the ergodic secrecy rate R_s for the transmission scheme of Theorem 1 under finite signal transmission power P settings, i.e., under finite SNR regime.

As illustrated by Fig. 7, following the scheme of Theorem 1: a) We run Monte Carlo simulation using antenna and ISI link length parameters used in Example 1 for the MIMO ISI wiretap channel with a cooperative jammer. That is, for the $(K, M, N) = (3, 2, 2)$ MIMO ISI wiretap channel with a $(Q = 2)$-antenna cooperative jammer where $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (4, 3, 2, 1)$. The resulting ergodic secrecy rate R_s behavior over the duration of the transmission block T is illustrated by the blue curve (with diamonds). b) Similarly, we run Monte Carlo simulation to investigate R_s behavior for the antenna and ISI link length parameters of Example 5. That is, for the $(K, M, N) = (3, 1, 2)$ MIMO ISI wiretap channel with a $(Q = 2)$-antenna cooperative jammer where $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (9, 3, 2, 1)$. The resulting ergodic secrecy rate behavior is illustrated by the red curve (with squares).

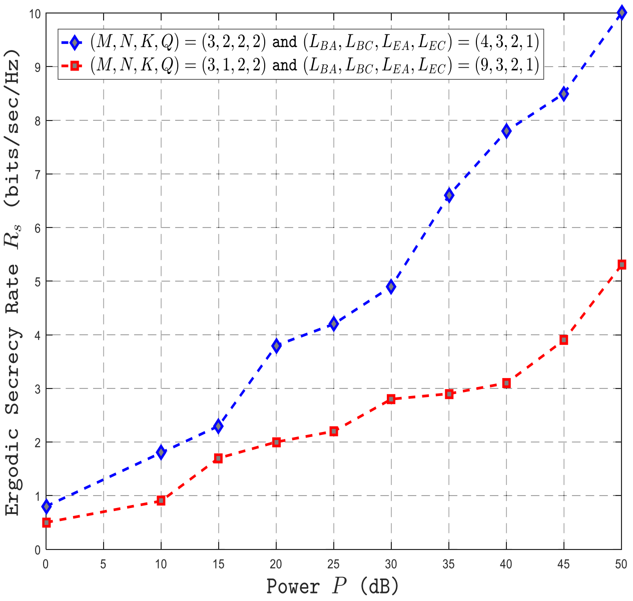

Fig. 7. The secrecy rate R_s behavior under finite SNR regime for the MIMO wiretap channels with ISI and a cooperative jammer.

To generate these R_s plots, we use the above antenna and ISI link length parameters to generate random signal vectors and channel matrices of similar structures as those described in (19)-(24). We then apply the secrecy rate (25) and SVD based expressions derived in (37) and (45). These parameters are used in equation (25) for incrementally increasing signal transmission power (P), where P is generated under the input signal power constraint (3). Running Monte Carlo simulations for both Examples 1 and 5 using 5000 iterations, for each example, leads to the secrecy rate R_s behavior displayed by Fig. 4.

At very low values of power P, the secrecy rate R_s rises very slowly. However, as we slowly increase P up towards 50 decibels (dB), then the more and more the R_s values (in bits/sec/hertz) start to increase towards secrecy rate saturation values. We observe from Fig. 7 that when both the legitimate receiver (Bob) and the eavesdropper (Eve) have an equal number of antennas, i.e., when $M = N = 2$, the resulting R_s values (as shown by the blue curve (with diamonds)) are higher than those obtained when Bob has a lesser number of antennas than the eavesdropper (as shown by the red curve (with squares)), i.e., when $M = 1$ and $N = 2$. We note that this difference in R_s values under low SNR parallels that in SDoF values as was numerically shown by Example 1 and Example 5 under high SNR regime. It is also interesting to observe from the red curve (with squares) that positive R_s is still achievable under the ISI link length heterogeneity exploitation scheme that we have proposed, even when the number of antennas at the legitimate receiver is less than that of the number of the antennas at the eavesdropper.

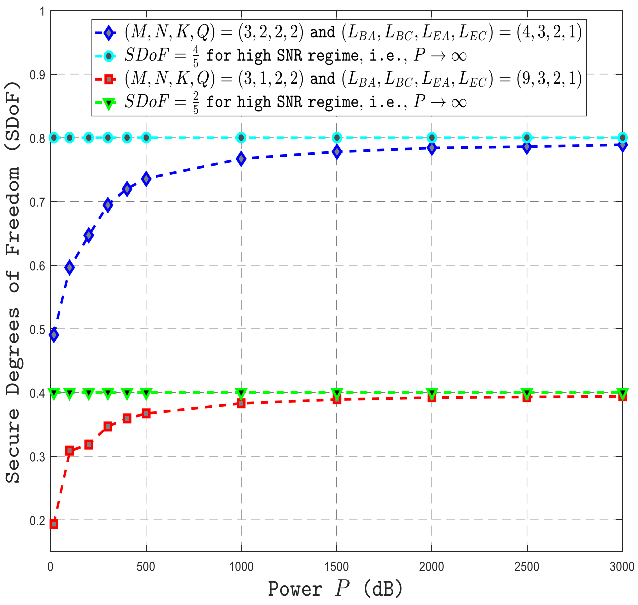

Fig. 8. The secrecy rate R_s behavior per $\log(P)$ for increasing SNR for the MIMO wiretap channels with ISI and a cooperative jammer.

B. Convergence Towards SDoF Values in High SNR Regime

In this section, we present numerical simulation results highlighting the SDoF behavior for the transmission scheme of Theorem 1 under an increasing signal transmission power P settings, i.e., under high SNR regime.

As illustrated by Fig. 8, following the scheme of Theorem 1, we run Monte Carlo simulation using antenna and ISI link length parameters for MIMO ISI wiretap channel with a cooperative jammer as those used in: a) Example 1. That is, for $(K, M, N, Q) = (3, 2, 2, 2)$ and $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (4, 3, 2, 1)$. The resulting ergodic secrecy rate R_s over $\log(P)$ during the transmission block T is illustrated by the blue curve (with diamonds). b) Example 5. That is, for $(K, M, N, Q) = (3, 1, 2, 2)$ and $(L_{BA}, L_{BC}, L_{EA}, L_{EC}) = (9, 3, 2, 1)$. The resulting ergodic SDoF behavior is illustrated by the red curve (with squares).

To generate these plots, we use the above antenna and ISI link length parameters to generate random signal vectors and channel matrices of similar structures as those described in (19)-(24). We then apply the secrecy rate (25) and SVD based expressions derived in (37) and (45). These parameters are used in equation (6) for increasing signal transmission power P, generated under the input power constraint (3). We run the Monte Carlo simulations for both Examples 1 and 5 using 5000 iterations, each.

At low values of power P, the SDoF values rise fast. However, as P approaches 2000 decibels (dB), then the resulting values converge towards the SDoF values $\frac{4}{5}$ and $\frac{2}{5}$ obtained in Example 1 and Example 5, respectively.

VI. Conclusion

We have presented a novel approach to leverage ISI heterogeneity to achieve positive SDoF for the MIMO ISI wiretap channel with a cooperative jammer in the absence of CSIT. In particular, we showed that Alice can use the CIR lengths towards Bob and the eavesdropper (Eve) to carry out a transmission that mixes both the information and artificial noise symbols and, along with the artificial noise from Charlie, be able to achieve secure communication. This scheme remains robust against eavesdropping, even when the number of antennas at the eavesdropper is larger than the number of antennas at the legitimate receiver. The proposed methodology can serve as a foundation for several future research directions: a) application to multi-user networks to achieve robust secrecy without any instantaneous CSIT; b) extension to the MIMO wiretap channel with ISI where CSI from the legitimate receiver (Bob) is available at the transmitters; c) further investigation to obtain information-theoretic upper bounds on the SDoF with no CSIT for the current model; and d) generalization to correlated channel distributions.

Appendix

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

A. Proof of Lemma 1

Proof: Here, we provide the proof of the rank of $\mathbf{H_B}$. The rank for its noise carrying submatrix $\mathbf{H_B^{[U,N]}}$ follows similar arguments, and hence will be omitted here due to space limitations. In order to prove the rank for $\mathbf{H_B}$, we first consider the explicit structure of the received channel matrix at the mth antenna at Bob. Let $\mathbf{H}_\mathbf{B}^{m} = \left[\mathbf{H}_\mathbf{BA}^{m}\ \mathbf{H}_\mathbf{BC}^{m}\right]$, the composite channel matrix received at the m^{th} antenna at Bob, be a channel matrix of size $(r + L_{BA} - 1) \times (rK + dQ)$ whose nonzero elements in the first K columns $\mathbf{C}_\mathbf{BA}^{(m,1)}, \mathbf{C}_\mathbf{BA}^{(m,2)}, \ldots, \mathbf{C}_\mathbf{BA}^{(m,K)}$ are the i.i.d. continuous random channel coefficients from the kth antenna at Alice, for $k = 1, 2, \ldots, K$, to the mth antenna at Bob, for $m = 1, 2, \ldots, M$, such that $\mathbf{C}_\mathbf{AB}^{(m,K)} = \left[h_{BA}^{(m,k)}[1]\ h_{BA}^{(m,k)}[2] \ldots h_{BA}^{(m,k)}[L_{BA}]\ 0 \ldots 0\right]^\top$. Let the subsequent $rK - K$ columns of $\mathbf{H}_\mathbf{B}^{m}$ be $r - 1$ simultaneous vertically circular permutations of the first K columns, respectively. Then, after these first rK columns, let the next Q columns of $\mathbf{H}_\mathbf{B}^{m}$ be $\mathbf{C}_\mathbf{BC}^{(m,1)}, \mathbf{C}_\mathbf{BC}^{(m,2)}, \ldots, \mathbf{C}_\mathbf{BC}^{(m,Q)}$, the i.i.d. continuous random channel coefficients from the qth antenna at Charlie, for $q = 1, 2, \ldots, Q$, to the mth antenna at Bob, for $m = 1, 2, \ldots, M$, such that $\mathbf{C}_\mathbf{BC}^{(m,q)} = \left[h_{BC}^{(m,q)}[1]\ h_{BC}^{(m,q)}[2] \ldots h_{BC}^{(m,q)}[L_{BC}]\ 0 \ldots 0\right]^\top$. Let the subsequent $dQ - Q$ columns of $\mathbf{H}_\mathbf{B}^{m}$ be $d - 1$ simultaneous vertically circular permutations of the previous Q columns, respectively.

Consider the first K columns $\mathbf{C}_\mathbf{BA}^{(m,1)}, \mathbf{C}_\mathbf{BA}^{(m,2)}, \ldots, \mathbf{C}_\mathbf{BA}^{(m,K)}$ of the matrix $\mathbf{H}_\mathbf{BA}^{m}$ and let $\Theta = [\theta_1\ \theta_2\ \ldots\ \theta_{rK}]^\top$ be some vector of size $rK \times 1$. Then, consider the top left corner $L_{BA} \times K$ submatrix of $\mathbf{H}_\mathbf{BA}^{m}$ whose structure is described above, i.e., the nonzero portion of the first K columns. Next, consider the first Q columns $\mathbf{C}_\mathbf{BC}^{(m,1)}, \mathbf{C}_\mathbf{BC}^{(m,2)}, \ldots, \mathbf{C}_\mathbf{BC}^{(m,Q)}$ of the matrix $\mathbf{H}_\mathbf{BC}^{m}$ and let $\Sigma = \left[\sigma_1\ \sigma_2\ \ldots\ \sigma_{dQ}\right]^\top$ be some vector of size $dQ \times 1$. Then, consider the top left corner $L_{BC} \times Q$ submatrix of $\mathbf{H}_\mathbf{BC}^{m}$ whose structure is described above, i.e., the nonzero portion of the first Q columns. We can deduce the following four cases:

•Case 1: $\min(K, L_{BA}) = K$ and $\min(Q, L_{BC}) = Q$.

For $\min(K, L_{BA}) = K$*:* Since each column of the $L_{BA} \times K$ nonzero submatrix of the first K columns of $\mathbf{H}_{\mathbf{B}}^{m}$ is formed by i.i.d. continuous random channel coefficients, this implies that $\theta_1 \mathbf{C}_{\mathbf{BA}}^{(m,1)} + \theta_2 \mathbf{C}_{\mathbf{BA}}^{(m,2)} + \cdots + \theta_K \mathbf{C}_{\mathbf{BA}}^{(m,K)} = 0$, if and only if $[\theta_1\, \theta_2\, \ldots\, \theta_K] = [0\, 0\, \ldots\, 0]$, almost surely. That is $\mathsf{rank}\left(\left[\mathbf{C}_{\mathbf{BA}}^{(m,1)}, \mathbf{C}_{\mathbf{BA}}^{(m,2)}\, \ldots\, \mathbf{C}_{\mathbf{BA}}^{(m,K)}\right]\right) = K$. By inductively following the same logical argument for the subsequent K columns of $\mathbf{H}_{\mathbf{BA}}^{m}$, i.e, for $\mathbf{C}_{\mathbf{BA}}^{(m,K+1)}\, \mathbf{C}_{\mathbf{BA}}^{(m,K+2)}\, \ldots\, \mathbf{C}_{\mathbf{BA}}^{(m,2K)}$, and repeating this for a total of r times, we reach the conclusion that $\mathsf{rank}(\mathbf{H}_{\mathbf{BA}}^{m}) \geq r + K - 1$. Also, recall that $r+K-1 \leq r+L_{BA}-1$ since $\min(K, L_{BA}) = K$. Here we note that doing simultaneously circular shifts of the first K columns for a total of r shifts as stated above leads to a matrix of size $(r + L_{BA} - 1) \times rK$. This newly created $(r + L_{BA} - 1) \times rK$ matrix thus contains a full rank maximally square submatrix of size $\min(r + L_{BA} - 1, rK) \times \min(r + L_{BA} - 1, rK)$. This directly implies that $\mathsf{rank}(\mathbf{H}_{\mathbf{BA}}^{m}) = \min(r+L_{BA}-1, rK)$. Here we are assuming that $\min(r + L_{BA} - 1, rK) = r + L_{BA} - 1$, otherwise, there is nothing to prove because rK represents the total number of information and artificial noise symbols (transmitted by Alice) that we want to solve for. Moreover, $\mathsf{rank}(\mathbf{H}_{\mathbf{BA}}^{m}) = \min(r + L_{BA} - 1, rK) = r + L_{BA} - 1$ instead of $r + K - 1$ because, given that $K \leq L_{BA}$, we can have the r circular permutations to be of the top left $L_{BA} \times K$ submatrix of $\mathbf{H}_{\mathbf{BA}}^{m}$ instead of $K \times K$ submatrix.

For $\min(Q, L_{BC}) = Q$*:* Since each column of the $L_{BC} \times Q$ nonzero submatrix of the first Q columns of $\mathbf{H}_{\mathbf{BC}}^{m}$ is formed by i.i.d. continuous random channel coefficients, this implies that $\sigma_1 \mathbf{C}_{\mathbf{BC}}^{(m,1)} + \sigma_2 \mathbf{C}_{\mathbf{BC}}^{(m,2)} + \cdots + \sigma_Q \mathbf{C}_{\mathbf{BC}}^{(m,Q)} = 0$, if and only if $\left[\sigma_1\, \sigma_2\, \ldots\, \sigma_Q\right] = [0\, 0\, \ldots\, 0]$, almost surely. That is $\mathsf{rank}\left(\left[\mathbf{C}_{\mathbf{BC}}^{(m,1)}, \mathbf{C}_{\mathbf{BC}}^{(m,2)}\, \ldots\, \mathbf{C}_{\mathbf{BC}}^{(m,Q)}\right]\right) = Q$. By inductively following the same logical argument for the subsequent Q columns of $\mathbf{H}_{\mathbf{BC}}^{m}$, i.e, for $\mathbf{C}_{\mathbf{BC}}^{(m,Q+1)}\, \mathbf{C}_{\mathbf{BC}}^{(m,Q+2)}\, \ldots\, \mathbf{C}_{\mathbf{BC}}^{(m,2Q)}$, and repeating this for a total of d times, we reach the conclusion that $\mathsf{rank}(\mathbf{H}_{\mathbf{BC}}^{m}) \geq d+Q-1$. Also, recall that $d+Q-1 \leq d + L_{BC} - 1$ since $\min(Q, L_{BC}) = Q$. Here we note that doing simultaneously circular shifts of the first Q columns for a total of d shifts as stated above leads to a matrix of size $(d + L_{BC} - 1) \times dQ$. This newly created $(d + L_{BC} - 1) \times dQ$ matrix thus contains a full rank maximally square submatrix of size $\min(d + L_{BC} - 1, dQ) \times \min(d + L_{BC} - 1, dQ)$. This directly implies that $\mathsf{rank}(\mathbf{H}_{\mathbf{BC}}^{m}) = \min(d + L_{BC} - 1, dQ)$. We assume that $\min(d + L_{BC} - 1, dQ) = d + L_{BC} - 1$, otherwise, there is nothing to prove because dQ represents the total number of all artificial noise symbols (transmitted by Charlie) that we want to solve for. Moreover, $\mathsf{rank}(\mathbf{H}_{\mathbf{BC}}^{m}) = \min(r + L_{BC} - 1, dQ) = r + L_{BC} - 1$ instead of $r + Q - 1$ because, given that $Q \leq L_{BC}$, we can have the d circular permutations to be of the top left $L_{BC} \times Q$ submatrix of $\mathbf{H}_{\mathbf{BC}}^{m}$ instead of $Q \times Q$ submatrix.

Recall that, for the purpose of this proof, we are only considering the case where $L_b = \max(r + L_{BA} - 1, d + L_{BC} - 1) = r + L_{BA} - 1$ as provided in the description of (19). Therefore, using the fact that $\mathbf{H}_{\mathbf{B}}^{m} = \left[\mathbf{H}_{\mathbf{BA}}^{m}\ \mathbf{H}_{\mathbf{BC}}^{m}\right]$ is a horizontal concatenation of the two matrices whose rank properties are described above, we deduce that its rank is $\max(\mathsf{rank}(\mathbf{H}_{\mathbf{BA}}^{m}), \mathsf{rank}(\mathbf{H}_{\mathbf{BC}}^{m})) = \max(r + L_{BA} - 1, d + L_{BC} - 1) = r + L_{BA} - 1$. Now, consider the $M(r + L_{BA} - 1) \times (rK + dQ)$ composite channel matrix $\mathbf{H}_{\mathbf{B}}$ seen at Bob, which is a vertical concatenation of M independent channel matrices $\mathbf{H}_{\mathbf{B}}^{1}, \mathbf{H}_{\mathbf{B}}^{2}, \ldots, \mathbf{H}_{\mathbf{B}}^{M}$ respectively seen at each of his M antennas. This matrix, by definition, consists of $M(r + L_{BA} - 1)$ rows whose elements are the random i.i.d channel coefficients. From this, we therefore conclude that $\mathsf{rank}(\mathbf{H}_{\mathbf{B}}) = \min(M(r + L_{BA} - 1), rK + dQ) = rK + dQ$, by the "decodability at Bob" condition in (11) which is a direct consequence of the devised transmission scheme. We refer the reader to [31], [32] for more on ranks of concatenated matrices.

•Case 2: $\min(K, L_{BA}) = L_{BA}$ and $\min(Q, L_{BC}) = L_{BC}$.

For $\min(K, L_{BA}) = L_{BA}$*:* Since each column of the $L_{BA} \times K$ nonzero submatrix of the first L_{BA} columns of $\mathbf{H}_{\mathbf{B}}^{m}$ is formed by i.i.d. continuous random channel coefficients, this implies that $\theta_1 \mathbf{C}_{\mathbf{BA}}^{(m,1)} + \theta_2 \mathbf{C}_{\mathbf{BA}}^{(m,2)} + \cdots + \theta_{L_{BA}} \mathbf{C}_{\mathbf{BA}}^{(m,L_{BA})} = 0$, if and only if $\left[\theta_1\, \theta_2\, \ldots\, \theta_{L_{BA}}\right] = [0\, 0\, \ldots\, 0]$, almost surely. That is $\mathsf{rank}\left(\left[\mathbf{C}_{\mathbf{BA}}^{(m,1)}, \mathbf{C}_{\mathbf{BA}}^{(m,2)} \ldots \mathbf{C}_{\mathbf{BA}}^{(m,L_{BA})}\right]\right) = L_{BA}$. By inductively following the same logical argument for the subsequent K columns of $\mathbf{H}_{\mathbf{BA}}^{m}$, i.e, for $\mathbf{C}_{\mathbf{BA}}^{(m,K+1)}\mathbf{C}_{\mathbf{BA}}^{(m,K+2)} \ldots \mathbf{C}_{\mathbf{BA}}^{(m,2K)}$, and repeating this for a total of r times, we reach the conclusion that $\mathsf{rank}(\mathbf{H}_{\mathbf{BA}}^{m}) = r + L_{BA} - 1$. Here we note that doing simultaneously circular shifts of the first K columns for a total of r shifts as stated above leads to a matrix of size $(r + L_{BA} - 1) \times rK$. This newly created $(r + L_{BA} - 1) \times rK$ matrix thus contains a full rank maximally square submatrix of size $\min(r + L_{BA} - 1, rK) \times \min(r + L_{BA} - 1, rK)$. This directly implies that $\mathsf{rank}(\mathbf{H}_{\mathbf{BA}}^{m}) = \min(r + L_{BA} - 1, rK)$. We also assume that $\min(r + L_{BA} - 1, rK) = r + L_{BA} - 1$, otherwise, there is nothing to prove. Moreover, $\min(r+L_{BA}-1, rK) = r + L_{BA} - 1$ because, given that $K \geq L_{BA}$, then we have $rK - (r + L_{BA} - 1) = r(K - 1) - (L_{BA} - 1) \geq r(K - 1) - (K - 1) = (K - 1)(r - 1) \geq 0$ for $K,\ r \geq 1$.

For $\min(Q, L_{BC}) = L_{BC}$*:* Since each column of the $L_{BC} \times Q$ nonzero submatrix of the first L_{BC} columns of $\mathbf{H}_{\mathbf{BC}}^{m}$ is formed by i.i.d. continuous random channel coefficients, this implies that $\sigma_1 \mathbf{C}_{\mathbf{BC}}^{(m,1)} + \sigma_2 \mathbf{C}_{\mathbf{BC}}^{(m,2)} + \cdots + \sigma_{L_{BC}} \mathbf{C}_{\mathbf{BC}}^{(m,L_{BC})} = 0$, if and only if $\left[\sigma_1\, \sigma_2\, \ldots\, \sigma_{L_{BC}}\right] = [0\, 0\, \ldots\, 0]$, almost surely. That is $\mathsf{rank}\left(\left[\mathbf{C}_{\mathbf{BC}}^{(m,1)}, \mathbf{C}_{\mathbf{BC}}^{(m,2)} \ldots \mathbf{C}_{\mathbf{BC}}^{(m,L_{BC})}\right]\right) = L_{BC}$. By inductively following the same logical argument for the subsequent Q columns of $\mathbf{H}_{\mathbf{BC}}^{m}$, i.e, for $\mathbf{C}_{\mathbf{BC}}^{(m,Q+1)}\mathbf{C}_{\mathbf{BC}}^{(m,Q+2)} \ldots \mathbf{C}_{\mathbf{BC}}^{(m,2Q)}$, and repeating this for a total of d times, we reach the conclusion that $\mathsf{rank}(\mathbf{H}_{\mathbf{BC}}^{m}) = d + L_{BC} - 1$. Here we note that doing simultaneously circular shifts of the first Q columns for a total of d shifts as stated above leads to a matrix of size $(d + L_{BC} - 1) \times dQ$. This newly created $(d + L_{BC} - 1) \times dQ$ matrix thus contains a full rank maximally square submatrix of size $\min(d + L_{BC} - 1, dQ) \times \min(d + L_{BC} - 1, dQ)$. This directly implies that $\mathsf{rank}(\mathbf{H}_{\mathbf{BC}}^{m}) = \min(d + L_{BC} - 1, dQ)$. We assume that $\min(d + L_{BC} - 1, dQ) = d + L_{BC} - 1$, otherwise, there is nothing to prove. Moreover, $\min(d+L_{BC}-1, dQ) = d + L_{BC} - 1$ because, given that $Q \geq L_{BC}$, then we have $dQ - (d + L_{BC} - 1) = d(Q - 1) - (L_{BC} - 1) \geq d(Q - 1) - (Q - 1) = (Q - 1)(d - 1) \geq 0$ for $Q,\ d \geq 1$.

Recall that, for the purpose of this proof, we are only considering the case where $L_b = \max(r+L_{BA}-1, d+L_{BC}-1) = r+L_{BA}-1$ as provided in the description of (19). Using the fact that $\mathbf{H}_{\mathbf{B}}^{m} = \left[\mathbf{H}_{\mathbf{BA}}^{m}\ \mathbf{H}_{\mathbf{BC}}^{m}\right]$ is a horizontal concatenation of the above two matrices, we can thus infer that its rank is $\max(r+L_{BA}-1, d+L_{BC}-1) = r+L_{BA}-1$. Now, consider the $M(r+L_{BA}-1)\times(rK+dQ)$ composite channel matrix $\mathbf{H_B}$ seen at Bob, which is a vertical concatenation of M independent channel matrices $\mathbf{H}_{\mathbf{B}}^{1}$, $\mathbf{H}_{\mathbf{B}}^{2}$, $\ldots$, $\mathbf{H}_{\mathbf{B}}^{M}$. This matrix, by definition, consists of $M(r+L_{BA}-1)$ rows whose elements are the random i.i.d channel coefficients. From this, we can infer that $\mathsf{rank}(\mathbf{H_B}) = \min(M(r+L_{BA}-1), rK+dQ) = rK+dQ$, by the "decodability at Bob" condition in (11) which is a direct consequence of the devised transmission scheme.

•**Case 3:** $\min(K, L_{BA}) = K$ and $\min(Q, L_{BC}) = L_{BC}$.

Following analogous arguments to those used in Case 1 for $\min(K, L_{BA}) = K$ and those used in Case 2 for $\min(Q, L_{BC}) = L_{BC}$, we obtain that $\mathbf{H}_{\mathbf{B}}^{m} = \left[\mathbf{H}_{\mathbf{BA}}^{m}\ \mathbf{H}_{\mathbf{BC}}^{m}\right]$ is of rank $\max(r+L_{BA}-1, d+L_{BC}-1) = r+L_{BA}-1$. Similarly, with arguments analogous to those in the cases 1 and 2 above, we can obtain that the composite channel matrix $\mathbf{H_B}$ is of rank $\mathsf{rank}(\mathbf{H_B}) = \min(M(r+L_{BA}-1), rK+dQ) = rK+dQ$, by the "decodability at Bob" condition in (11) which is a direct consequence of the devised transmission scheme.

•**Case 4:** $\min(Q, L_{BC}) = Q$ and $\min(K, L_{BA}) = L_{BA}$.

Following analogous arguments to those used in Case 1 for $\min(Q, L_{BC}) = Q$ and those used in Case 2 for $\min(K, L_{BA}) = L_{BA}$, we obtain that $\mathbf{H}_{\mathbf{B}}^{m} = \left[\mathbf{H}_{\mathbf{BA}}^{m}\ \mathbf{H}_{\mathbf{BC}}^{m}\right]$ is of rank $\max(r+L_{BA}-1, d+L_{BC}-1) = r+L_{BA}-1$. Similarly, with arguments analogous to those in the cases 1 and 2 above, we can obtain that the composite channel matrix $\mathbf{H_B}$ is of rank $\mathsf{rank}(\mathbf{H_B}) = \min(M(r+L_{BA}-1), rK+dQ) = rK+dQ$, by the "decodability at Bob" condition in (11) which is a direct consequence of the devised transmission scheme. This concludes the proof of Lemma 1. □

B. Proof of Lemma 2

Proof: Here, we provide a brief for the proof of the rank of $\mathbf{H_E}$. The rank for its noise carrying submatrix $\mathbf{H}_{\mathbf{E}}^{[\mathbf{U},\mathbf{N}]}$ follows similar arguments, and hence will be omitted here due to space limitations. We now consider the explicit structure of the received channel matrix at the nth antenna at Eve. Let $\mathbf{H}_{\mathbf{E}}^{\mathbf{n}} = \left[\mathbf{H}_{\mathbf{EA}}^{n}\ \ \mathbf{H}_{\mathbf{EC}}^{n}\right]$, the composite channel matrix received at the n^{th} antenna at Eve, be a channel matrix of size $(r+L_{EA}-1)\times(rK+dQ)$ whose nonzero elements in the first K columns $\mathbf{C}_{\mathbf{EA}}^{(n,1)}, \mathbf{C}_{\mathbf{EA}}^{(n,2)}, \ldots, \mathbf{C}_{\mathbf{EA}}^{(n,K)}$ are the i.i.d. continuous Gaussian random channel coefficients from the kth antenna at Alice, for $k = 1, 2, \ldots, K$, to the nth antenna at Eve, for $n = 1, 2, \ldots, N$, such that $\mathbf{C}_{\mathbf{EA}}^{(n,k)} = \left[h_{EA}^{(n,k)}[1]\ h_{EA}^{(n,k)}[2]\ \ldots\ h_{EA}^{(n,k)}[L_{EA}]\ 0\ \ldots\ 0\right]^{\top}$. Let the subsequent $rK-K$ columns of $\mathbf{H}_{\mathbf{E}}^{\mathbf{n}}$ be $r-1$ simultaneous vertically circular permutations of the first K columns, respectively. Then, after these first rK columns, let the next Q columns of $\mathbf{H}_{\mathbf{E}}^{n}$ be $\mathbf{C}_{\mathbf{EC}}^{(n,1)}, \mathbf{C}_{\mathbf{EC}}^{(n,2)}, \ldots, \mathbf{C}_{\mathbf{EC}}^{(n,Q)}$, the i.i.d. continuous random channel coefficients from the qth antenna at Charlie, for $q = 1, 2, \ldots, Q$, to the nth antenna at Eve, for $n = 1, 2, \ldots, N$, such that $\mathbf{C}_{\mathbf{EC}}^{(n,q)} = \left[h_{EC}^{(n,q)}[1]\ h_{EC}^{(n,q)}[2]\ \ldots\ h_{EC}^{(n,q)}[L_{EC}]\ 0\ \ldots\ 0\right]^{\top}$. Let the subsequent $dQ-Q$ columns of $\mathbf{H}_{\mathbf{E}}^{\mathbf{n}}$ be $d-1$ simultaneous vertically circular permutations of the previous Q columns, respectively. The matrix $\mathbf{H_E}$ is thus a vertical concatenation of N independent channel matrices $\mathbf{H}_{\mathbf{E}}^{\mathbf{1}}$, $\mathbf{H}_{\mathbf{E}}^{\mathbf{2}}$ $\ldots$, $\mathbf{H}_{\mathbf{E}}^{\mathbf{N}}$ respectively seen at each of the N antennas at Eve. Similarly to the proof of Lemma 1, we can deduce four cases from the structure of $\mathbf{H}_{\mathbf{E}}^{\mathbf{n}}$, for which the arguments are analogous to those of Lemma 1, and use the "secrecy at Eve" constraint in (12). We omit the detailed steps as they follow in a similar manner as in Lemma 1. □

References

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

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

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

[5] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[6] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[7] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 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 Int. Conf. Commun.*, Jun. 2015, pp. 4169–4174.

[9] M. Nafea and A. Yener, "Secure degrees of freedom for the MIMO wiretap channel with a multi-antenna cooperative jammer," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7420–7441, Nov. 2017.

[10] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[12] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[13] R. Tandon, P. Piantanida, and S. Shamai (Shitz), "On multi-user MISO wiretap channels with delayed CSIT," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2014, pp. 211–215.

[14] S. Lashgari and A. S. Avestimehr, "Secrecy DoF of blind MIMOME wiretap channel with delayed CSIT," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 478–489, Feb. 2018.

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

[16] 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 Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2655–2669, May 2015.

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

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

[19] H. V. Poor and R. F. Schaefer, “Wireless physical layer security,” *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[20] W. Hirt and J. L. Massey, “Capacity of the discrete-time Gaussian channel with intersymbol interference,” *IEEE Trans. Inf. Theory*, vol. IT-34, no. 3, p. 38, May 1988.

[21] R. S. Cheng and S. Verdú, “Gaussian multiaccess channels with ISI: Capacity region and multiuser water-filling,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 773–785, May 1993.

[22] A. J. Goldsmith and M. Effros, “The capacity region of broadcast channels with intersymbol interference and colored Gaussian noise,” *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 219–240, Jan. 2001.

[23] N. Shlezinger, D. Zahavi, Y. Murin, and R. Dabora, “The secrecy capacity of Gaussian MIMO channels with finite memory,” *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1874–1897, Mar. 2017.

[24] Z. Li, R. Yates, and W. Trappe, *Secrecy Capacity of Independent Parallel Channels*. Boston, MA, USA: Springer, 2010, pp. 1–18.

[25] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[26] N. Lee, “A blind interference management technique for the K-user interference channel with ISI: Interference-free OFDM,” in *Proc. IEEE Int. Conf. Commun.*, May 2017, pp. 1–6.

[27] Y.-S. Jeon, N. Lee, and R. Tandon, “Degrees of freedom and achievable rate of wide-band multi-cell multiple access channels with no CSIT,” *IEEE Trans. Commun.*, vol. 66, no. 4, pp. 1772–1786, Apr. 2018.

[28] J. de Dieu Mutangana, R. Tandon, and N. Lee, “Blind cooperative jamming: Exploiting ISI heterogeneity to achieve positive secure DoF,” in *Proc. IEEE Global Commun. Conf. Commun.*, Dec. 2017, pp. 1–6.

[29] J. de Dieu Mutangana, D. Kumar, and R. Tandon, “MIMO wiretap channel with ISI heterogeneity—Achieving secure DoF with no CSI,” in *Proc. 51st Asilomar Conf. Signals, Syst., Comput.*, Oct./Nov. 2017, pp. 1687–1691.

[30] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.

[31] S. H. Friedberg, A. J. Insel, and L. E. Spence, *Linear Algebra*. London, U.K.: Pearson Education, 2003.

[32] G. H. Golub and C. F. Van Loan, *Matrix Computations*. Baltimore, MD, USA: The Johns Hopkins Univ. Press, 1996.

Jean de Dieu Mutangana (S’19) received the B.S. degree in systems engineering (telecommunications) from the University of Arkansas at Little Rock in 2012, and the M.S. degree in electrical and computer engineering (control, communications, and signal processing) from the University of California at Santa Barbara in 2014. He is currently pursuing the Ph.D. degree in electrical and computer engineering with The University of Arizona. Prior to joining The University of Arizona in 2016, he was an Electrical Product Design and Development Engineer (RF connectivity and signal integrity) at Panduit Corporation, Chicago, from 2014 to 2016. He spent 2018 as a Systems Engineer Graduate Technical Intern (mobile communications) at Intel Corporation, Santa Clara, CA, USA. His current research interests include wireless communications, physical layer security, network information and coding theory, machine learning applications for next wireless generations, and signal processing.

Ravi Tandon (SM’17) received the B.Tech. degree in electrical engineering from the IIT Kanpur in 2004 and the Ph.D. degree in electrical and computer engineering from the University of Maryland at College Park (UMCP) in 2010. He is an Assistant Professor with the Department of ECE, University of Arizona. Prior to joining the University of Arizona in 2015, he was a Research Assistant Professor at Virginia Tech with positions in the Bradley Department of ECE, Hume Center for National Security and Technology and at the Discovery Analytics Center, Department of Computer Science. From 2010 to 2012, he was a Post-Doctoral Research Associate at Princeton University. His current research interests include information theory and its applications to wireless networks, communications, security and privacy, machine learning, and data mining. He was a recipient of the 2018 Keysight Early Career Professor Award, the NSF CAREER Award in 2017, and the Best Paper Award at IEEE GLOBECOM 2011. He currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.