MIMO One Hop Networks with No Eve CSIT

Pritam Mukherjee Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
pritamm@umd.edu *ulukus@umd.edu*

***Abstract*— Two fundamental multi-user channel models: the multiple-input multiple-output (MIMO) wiretap channel with one helper (WTH) and the MIMO multiple access wiretap channel (MAC-WT) are considered. In each case, the eavesdropper has K antennas while the remaining terminals have N antennas. We consider a fast fading channel where the channel state information (CSI) of the legitimate receiver is available at the transmitters but no channel state information at the transmitters (CSIT) is available for the eavesdropper's channel. The optimal sum secure degrees of freedom (s.d.o.f.) for each channel model is determined for the regime $K \leq N$, and we show that in this regime, the MAC-WT channel reduces to the WTH in the absence of eavesdropper CSIT. For the regime $N \leq K \leq 2N$, we obtain the optimal *linear* s.d.o.f., and show that the MAC-WT channel and the WTH have the same optimal s.d.o.f. when restricted to linear encoding strategies. In the absence of any such restrictions, we provide an upper bound for the sum s.d.o.f. of the MAC-WT chanel in the regime $N \leq K \leq 2N$. Our results show that unlike in the single-input single-output (SISO) case, there is loss of s.d.o.f. for even the WTH due to lack of eavesdropper CSIT, when $K \geq N$.**

I. Introduction

We consider two multi-user models: the multiple-input multiple-output (MIMO) wiretap channel with one helper (WTH) where the transmitter, the helper and the legitimate receiver have N antennas each, and the eavesdropper has K antennas; see Fig. 1, and the MIMO multiple access wiretap channel (MAC-WT), where both transmitters and the legitimate receiver have N antennas each and the eavesdropper has K antennas; see Fig. 2. In both cases, the channel is fast fading and the channel gains vary in an independent and identically distributed (i.i.d.) fashion across the links and time. We consider the case when the eavesdropper's channel state information (CSI) is not available at the transmitters. Our goal in this paper is to investigate the optimal sum secure degrees of freedom (s.d.o.f.) of the MIMO WTH and the MIMO MAC-WT channel as a function of N and K.

To that end, we provide an achievable scheme based on vector space alignment [1], that attains $\frac{1}{2}(2N-K)$ s.d.o.f. for the WTH for all values of $0 \leq K \leq 2N$. Note that when $K \leq N$, this value coincides with the optimal s.d.o.f. for the WTH in the case where full eavesdropper CSIT is available. Therefore, for the regime $K \leq N$, there is no loss of s.d.o.f. for the WTH due to the lack of eavesdropper CSIT. Further, the proposed scheme which does not require eavesdropper CSIT, is optimal. The achievable scheme for the WTH also suffices as an achievable scheme for the MAC-WT channel, since we can treat one of the transmitters as a helper and use time-sharing among the two transmitters.

To prove the optimality of the proposed scheme for the MAC-WT channel, we next provide a matching converse for the regime $K \leq N$. Besides using MIMO versions of the *secrecy penalty lemma* and the *role of a helper lemma* [2], the converse proof relies on exploiting channel symmetry at the eavesdropper. Since the transmitters do not have the eavesdropper's CSIT, the output at the K antennas of the eavesdropper are *entropy symmetric* [3], i.e., any two subsets of the antenna outputs have the same differential entropy, if the subsets are of equal size. Finally, we use a MIMO version of the *least alignment lemma* [4], [5], which states that the differential entropy at the output of the terminal which does not provide CSIT is the greatest among terminals having equal number of antennas. Intuitively, this holds since no signal alignment is possible at the output of the terminal which does not provide CSIT. The converse in the regime $K \leq N$ shows that the sum s.d.o.f. cannot exceed $\frac{1}{2}(2N-K)$ for the MAC-WT channel. Note that a converse for the MAC-WT channel is valid for the WTH as well. Further, together with the achievable scheme, it shows that the optimal s.d.o.f. for both the WTH and the MAC-WT channel in this regime is $\frac{1}{2}(2N-K)$; therefore, as in the SISO case [6], [7], which is a subset of this regime with $N=K=1$, the MAC-WT channel reduces to the WTH when the eavesdropper's CSIT is not available. Recalling that with full eavesdropper CSIT, the optimal sum s.d.o.f. of the MAC-WT channel in this regime is $\min(N, \frac{2}{3}(2N-K))$ [8], [9], this also illustrates the loss of s.d.o.f. for the MAC-WT channel due to the lack of eavesdropper's CSIT.

Next, we consider the regime $N \leq K \leq 2N$. In this regime, we provide an upper bound which shows that the sum s.d.o.f. of the MAC-WT channel cannot be larger than $\min\left(\frac{N}{2}, \frac{2N(2N-K)}{4N-K}\right)$. Noting that $\frac{2N(2N-K)}{4N-K} < (2N-K)$, we conclude that there will be loss of s.d.o.f. due to lack of eavesdropper CSIT, even for the WTH, in the regime $\frac{4N}{3} \leq K \leq 2N$, where $\min\left(\frac{N}{2}, 2N-K\right)$ s.d.o.f. is achievable with full eavesdropper CSIT [10].

In order to further investigate the optimality of $\frac{1}{2}(2N-K)$ as the sum s.d.o.f. for the MAC-WT channel in the regime $N \leq K \leq 2N$, we then restrict ourselves to *linear* encoding strategies [11], [12], where the channel input of each antenna in every time slot is restricted to be a linear combination

This work was supported by NSF Grants CNS 13-14733, CCF 14-22111, CCF 14-22129 and CNS 15-26608.

of some information symbols intended for the legitimate receiver and some artificial noise symbols to provide secrecy at the eavesdropper. We show that under this restriction to linear encoding schemes, the *linear* sum s.d.o.f. can be no larger than $\frac{1}{2}(2N-K)$. The key idea of the proof is that since no alignment is possible at the eavesdropper, the artificial noise symbols should asymptotically occupy the maximum number of dimensions available at the eavesdropper; consequently, the dimension of the linear signal space at the eavesdropper should be $Kn+o(n)$ in n channel uses.

Related Work: The MAC-WT channel is introduced by [13], [14], where the technique of cooperative jamming is introduced to improve the rates achievable with Gaussian signaling. Reference [15] provides outer bounds and identifies cases where these outer bounds are within 0.5 bits per channel use of the rates achievable by Gaussian signaling. While the exact secrecy capacity remains unknown, the achievable rates in [13]–[15] all yield zero s.d.o.f. Positive s.d.o.f. can be obtained by either structured signaling [16] or non-i.i.d. Gaussian signaling [17]. The exact optimal sum s.d.o.f. of the wiretap channel with M helpers and the K-user MAC-WT channel are established to be $\frac{M}{M+1}$ and $\frac{K(K-1)}{K(K-1)+1}$, respectively in [2], when full eavesdropper's CSIT is available. References [6], [7] show that without eavesdropper's CSIT, the optimal s.d.o.f. for the wiretap channel with M helpers is still $\frac{M}{M+1}$, while the optimal sum s.d.o.f. of the K-user MAC-WT channel decreases to $\frac{K-1}{K}$. The two-user MIMO WTH, with full eavesdropper CSIT is considered in [10], [18], and the optimal s.d.o.f. is determined for the case when the transmitter and the receiver each has N antennas, the helper has K antennas and the eavesdropper has M antennas. References [8], [9], [19] determine the optimal sum s.d.o.f. for the two user MIMO MAC-WT channel when each transmitter and the receiver have N antennas while the eavesdropper has K antennas, and full eavesdropper CSIT is available.

II. System Model

In this paper, we consider two fundamental channel models: the MIMO WTH and the MIMO MAC-WT. In each case, we assume that the channel gains are non-zero and are drawn from a common continuous distribution with bounded support in an i.i.d. fashion in each channel use. The common continuous distribution is known at all the terminals in the system. We assume no eavesdropper CSIT, that is, the channel gains to the eavesdropper are not available at any transmitter. In the following three subsections we describe each channel model and provide the relevant definitions.

A. Wiretap Channel with a Helper

The MIMO WTH, see Fig. 1, is described by,

$$\mathbf{Y}(t) =\mathbf{H}_1(t)\mathbf{X}_1(t)+\mathbf{H}_2(t)\mathbf{X}_2(t)+\mathbf{N}_1(t) \tag{1}$$

$$\mathbf{Z}(t) =\mathbf{G}_1(t)\mathbf{X}_1(t)+\mathbf{G}_2(t)\mathbf{X}_2(t)+\mathbf{N}_2(t) \tag{2}$$

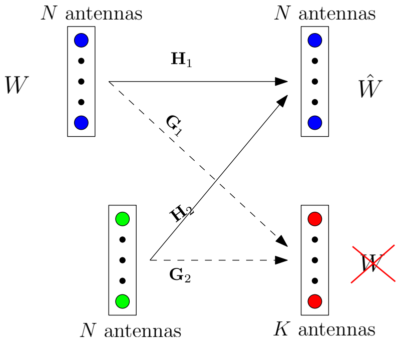

Fig. 1: Wiretap channel with a helper (WTH).

where $\mathbf{X}_1(t)$ and $\mathbf{X}_2(t)$ are N dimensional column vectors denoting the input of the legitimate transmitter and the helper, respectively, $\mathbf{Y}(t)$ is an N dimensional vector denoting the legitimate receiver's channel output, and $\mathbf{Z}(t)$ is a K dimensional vector denoting the eavesdropper's channel output, at time t. In addition, $\mathbf{N}_1(t)$ and $\mathbf{N}_2(t)$ are N and K dimensional white Gaussian noise vectors, respectively, with $\mathbf{N}_1 \sim \mathcal{N}(\mathbf{0},\mathbf{I}_N)$ and $\mathbf{N}_2 \sim \mathcal{N}(\mathbf{0},\mathbf{I}_K)$, where $\mathbf{I}_N$ denotes the $N\times N$ identity matrix. Here, $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are the $N\times N$ and $K\times N$ channel matrices from transmitter i to the legitimate receiver and the eavesdropper, respectively, at time t. The entries of $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are drawn from a fixed continuous distribution with bounded support in an i.i.d. fashion at every time slot t. We assume that the channel matrices at the legitimate receiver, $\mathbf{H}_i(t)$, are known with full precision at all terminals, at time t. However, the channel matrices to the eavesdropper, $\mathbf{G}_i(t)$ are not known at any transmitter. All channel inputs satisfy the average power constraint $E[\|\mathbf{X}_i(t)\|^2]\leq P$, $i=1,2$, where $\|\mathbf{X}\|$ denotes the Euclidean (or spectral) norm of the vector (or matrix) $\mathbf{X}$.

The transmitter wishes to send a message W, uniformly distributed in $\mathcal{W}$, securely to the legitimate receiver in the presence of the eavesdropper. A secure rate R, with $R=\frac{\log|\mathcal{W}|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receiver, namely, $\Pr[W\neq\hat{W}]\leq\epsilon_n$, for $i=1,2$, and the secrecy constraint, namely,

$$\frac{1}{n}I(W;\mathbf{Z}^n)\leq\epsilon_n \tag{3}$$

where $\epsilon_n \to 0$ as $n\to\infty$. An s.d.o.f. d is said to be achievable if a rate R is achievable with

$$d=\lim_{P\to\infty}\frac{R}{\frac{1}{2}\log P} \tag{4}$$

B. Multiple Access Wiretap Channel

The two-user MIMO MAC-WT, see Fig. 2, is as follows:

$$\mathbf{Y}(t) =\mathbf{H}_1(t)\mathbf{X}_1(t)+\mathbf{H}_2(t)\mathbf{X}_2(t)+\mathbf{N}_1(t) \tag{5}$$

$$\mathbf{Z}(t) =\mathbf{G}_1(t)\mathbf{X}_1(t)+\mathbf{G}_2(t)\mathbf{X}_2(t)+\mathbf{N}_2(t) \tag{6}$$

where $\mathbf{X}_i(t)$ is an N dimensional column vector denoting the ith user's channel input, $\mathbf{Y}(t)$ is an N dimensional vector denoting the legitimate receiver's channel output, and $\mathbf{Z}(t)$ is a K dimensional vector denoting the eavesdropper's channel

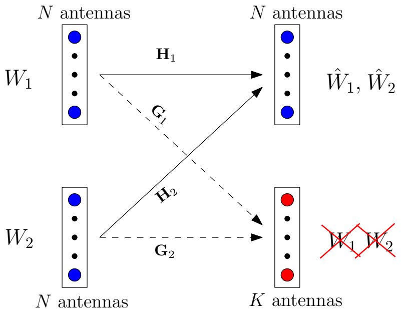

Fig. 2: Multiple access wiretap channel (MAC-WT).

output, at time t. In addition, $\mathbf{N}_1(t)$ and $\mathbf{N}_2(t)$ are N and K dimensional white Gaussian noise vectors, respectively, with $\mathbf{N}_1 \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$ and $\mathbf{N}_2 \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_K)$, where $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. Here, $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are the $N \times N$ and $K \times N$ channel matrices from transmitter i to the legitimate receiver and the eavesdropper, respectively, at time t. The entries of $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are drawn from a fixed continuous distribution with bounded support in an i.i.d. fashion at every time slot t. We assume that the channel matrices to the legitimate receiver, $\mathbf{H}_i(t)$, are known with full precision at all terminals, at time t. However, the channel matrices to the eavesdropper, $\mathbf{G}_i(t)$, are not available at the transmitters. All channel inputs satisfy the average power constraint $E[\|\mathbf{X}_i(t)\|^2] \leq P,\ i = 1, 2$.

Transmitter i wishes to send a message W_i, uniformly distributed in $\mathcal{W}_i$, securely to the legitimate receiver in the presence of the eavesdropper. A secure rate pair (R_1, R_2), with $R_i = \frac{\log |\mathcal{W}_i|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receiver, namely, $\Pr[W_i \neq \hat{W}_i] \leq \epsilon_n$, for $i = 1, 2$, and the secrecy constraint, namely,

$$\frac{1}{n} I(W_1, W_2; \mathbf{Z}^n) \leq \epsilon_n \tag{7}$$

where $\epsilon_n \to 0$ as $n \to \infty$. An s.d.o.f. pair (d_1, d_2) is said to be achievable if a rate pair (R_1, R_2) is achievable with

$$d_i = \lim_{P \to \infty} \frac{R_i}{\frac{1}{2} \log P} \tag{8}$$

The sum s.d.o.f. d_s is the largest achievable $d_1 + d_2$.

C. A Linear Secure Degrees of Freedom Perspective

In this paper, we also consider *linear* coding strategies as defined in [11], [20]. In such cases, the degrees of freedom simply represents the dimension of the linear subspace of transmitted signals.

When we focus on linear coding schemes, we consider a communication scheme of blocklength n, where transmitter i wishes to send $m_i(n)$ *information* symbols $\mathbf{v}_i \in \mathbb{R}^{m_i(n)}$ to the legitimate receiver reliably and securely. In case of the WTH, $m_2(n) = 0$. Each information symbol is a zero-mean Gaussian random variable with variance αP, where α is a constant chosen to ensure that the power constraints are satisfied at each transmitter. In addition to the information symbols, transmitter i can use $n_i(n)$ artificial noise symbols, $\mathbf{u}_i \in \mathbb{R}^{n_i(n)}$ each of which is a zero-mean Gaussian random variable with variance αP. These artificial noise symbols need not be decoded at the receiver; instead they drown out the information symbols at the eavesdropper for security.

At each time t, the information symbols $\mathbf{v}_i$ at transmitter i are modulated by a precoding matrix $\mathbf{P}_i(t) \in \mathbb{R}^{N \times m_i(n)}$, while the artificial noise symbols $\mathbf{u}_i$ are modulated using a precoding matrix $\mathbf{Q}_i(t) \in \mathbb{R}^{N \times n_i(n)}$. Since the channel gains $\mathbf{H}_i(t),\ i = 1, 2$ are known at both transmitters at time t, the precoding matrices $\mathbf{P}_i(t)$ and $\mathbf{Q}_i(t)$ can each depend on $\{\mathbf{H}_1(k), \mathbf{H}_2(k), k = 1, \ldots, t\}$. However, since the channel gains $\mathbf{G}_i(t)$ are not available at any transmitter, $\mathbf{P}_i$ and $\mathbf{Q}_i$ are independent of $\{\mathbf{G}_i(t), t = 1, \ldots, n\}$.

At time t, transmitter i sends a linear combination of the information and the artificial noise symbols:

$$\mathbf{X}_i(t) = \mathbf{P}_i(t)\mathbf{v}_i + \mathbf{Q}_i(t)\mathbf{u}_i \tag{9}$$

The channel outputs at time t are, therefore,

$$\begin{aligned} \mathbf{Y}(t) =& \mathbf{H}_1(t)\mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{H}_2(t)\mathbf{P}_2(t)\mathbf{v}_2 \\ &+ \mathbf{H}_1(t)\mathbf{Q}_1(t)\mathbf{u}_1 + \mathbf{H}_2(t)\mathbf{Q}_2(t)\mathbf{u}_2 + \mathbf{N}_1(t) \quad (10) \\ \mathbf{Z}(t) =& \mathbf{G}_1(t)\mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{G}_2(t)\mathbf{P}_2(t)\mathbf{v}_2 \\ &+ \mathbf{G}_1(t)\mathbf{Q}_1(t)\mathbf{u}_1 + \mathbf{G}_2(t)\mathbf{Q}_2(t)\mathbf{u}_2 + \mathbf{N}_2(t) \quad (11) \end{aligned}$$

Now letting $\bar{\mathbf{P}}_i = [\mathbf{P}_i(1), \ldots, \mathbf{P}_i(n)]^T$, $\bar{\mathbf{Q}}_i = [\mathbf{Q}_i(1), \ldots, \mathbf{Q}_i(n)]$, we can compactly write the channel outputs as

$$\bar{\mathbf{Y}} = \bar{\mathbf{H}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2\mathbf{v}_2 + \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1\mathbf{u}_1 + \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2\mathbf{u}_2 + \bar{\mathbf{N}}_1 \tag{12}$$

$$\bar{\mathbf{Z}} = \bar{\mathbf{G}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2\mathbf{v}_2 + \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1\mathbf{u}_1 + \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2\mathbf{u}_2 + \bar{\mathbf{N}}_2 \tag{13}$$

where $\bar{\mathbf{H}}_i$ and $\bar{\mathbf{G}}_i$ are the $Nn \times Nn$ and $Kn \times Nn$ block diagonal matrices

$$\bar{\mathbf{H}}_i = \begin{bmatrix} \mathbf{H}_i(1) & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_i(2) & \ldots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & \mathbf{H}_i(n) \end{bmatrix} \tag{14}$$

$$\bar{\mathbf{G}}_i = \begin{bmatrix} \mathbf{G}_i(1) & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_i(2) & \ldots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & \mathbf{G}_i(n) \end{bmatrix} \tag{15}$$

and $\bar{\mathbf{N}}_i = [\mathbf{N}_i(1), \ldots, \mathbf{N}_i(n)]^T$ for $i = 1, 2$.

At the legitimate receiver, the interference subspace is

$$\mathcal{I}_B = \text{colspan}([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]) \tag{16}$$

Let $\mathcal{I}_B^c$ denote the orthogonal subspace of $\mathcal{I}_B$. If we ignore the additive Gaussian noise, i.e., in the high transmit power regime, the decodability of $\mathbf{v}_1$ and $\mathbf{v}_2$ at the legitimate receiver corresponds to the constraint that the projection of the subspace $\text{colspan}([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2])$ onto $\mathcal{I}_B^c$ must have dimension $m_1(n) + m_2(n)$, i.e.,

$$\begin{aligned}
&\dim\left(\text{Proj}_{\mathcal{I}_B^c}\text{colspan}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2]\right)\right) \\
&\quad = \dim\left(\text{colspan}\left([\bar{\mathbf{P}}_1]\right)\right) + \dim\left(\text{colspan}\left([\bar{\mathbf{P}}_2]\right)\right) \\
&\quad = m_1(n) + m_2(n) \qquad (17)
\end{aligned}$$

This can be rewritten as requiring that

$$\begin{aligned}
&\text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) \\
&\quad - \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) = m_1(n) + m_2(n) \qquad (18)
\end{aligned}$$

On the other hand, at the eavesdropper, we require that

$$\lim_{n\to\infty}\frac{1}{n}\dim\left(\text{Proj}_{\mathcal{I}_E^c}\text{colspan}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2]\right)\right) = 0,\ a.s. \qquad (19)$$

where $\mathcal{I}_E = \text{colspan}([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2])$.

The security requirement in (19) can be reformulated as follows: Let $L(n)$ be the number of *leakage dimensions* defined as

$$\begin{aligned}
L(n) =& \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \\
&- \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \qquad (20)
\end{aligned}$$

Then, we want

$$\lim_{n\to\infty}\frac{L(n)}{n} = 0,\ a.s. \qquad (21)$$

In other words, we want the artificial noise symbols to occupy the full received signal space at the eavesdropper asymptotically. This secrecy requirement is a weaker version of the original constraint $\frac{1}{n}I(W_1, W_2; \mathbf{Z}^n) \to 0$. Indeed, it is analogous to requiring that $\lim_{n\to\infty}\lim_{P\to\infty}\frac{I(W_1,W_2;\mathbf{Z}^n)}{\log P} = 0$. However, this does not lead to any loss of generality in our case because the proposed achievable scheme which satisfies the weakened secrecy requirement may be modified using stochastic encoding techniques [21] to obtain a scheme that satisfies the stronger security constraint as well. Note that a converse with the weaker secrecy requirement suffices as a converse for the case of the stronger secrecy requirement.

For the WTH, a *linear* s.d.o.f. d with $d = m_1(n)/n$ is said to be achievable if there exists a sequence of precoding matrices $\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}_1, \bar{\mathbf{Q}}_2$ such that both the reliability constraints in (17) and the security constraints in (19) are satisfied.

For the MAC-WT channel, a *linear* s.d.o.f. pair (d_1, d_2), with $d_i = m_i(n)/n$ is said to be achievable if there exists a sequence of precoding matrices $\bar{\mathbf{P}}_i, \bar{\mathbf{Q}}_i$ such that both the reliability constraints in (17) and the security constraints in (19) are satisfied. The *linear* sum s.d.o.f. d_s is the supremum of $d_1 + d_2$, such that the pair (d_1, d_2) is achievable.

III. Main Results

The main result of this paper is the determination of the optimal linear sum s.d.o.f. for the MIMO WTH and the MIMO MAC-WT channel. We have the following theorem.

Theorem 1 *For both the $N \times N \times N \times K$ WTH and the MAC-WT channel with no eavesdropper CSIT, the optimal linear sum s.d.o.f. d_s is*

$$d_s = \max\left(\frac{1}{2}(2N - K), 0\right) \qquad (22)$$

for almost all channel gains. Further, without any linearity constraints, the optimal sum s.d.o.f. d_s is

$$d_s \begin{cases} = \frac{1}{2}(2N-K), & 0 \le K \le N \\ \le \min\left(\frac{N}{2}, \frac{2N(2N-K)}{4N-K}\right), & N \le K \le 2N \\ = 0, & K \ge 2N \end{cases} \qquad (23)$$

We also have the following corollary.

Corollary 1 *For the $N \times N \times N \times K$ MAC-WT channel with no eavesdropper CSIT, the linear s.d.o.f. region is given by the set of all nonnegative pairs (d_1, d_2) that satisfy,*

$$d_1 + d_2 = \frac{1}{2}(2N - K) \qquad (24)$$

The proof of the corollary follows from the observation that every point in the given region can be achieved by time sharing between the points $\left(\frac{1}{2}(2N-K), 0\right)$ and $\left(0, \frac{1}{2}(2N-K)\right)$, which can themselves be attained by treating the MAC-WT channel as a WTH. Also, no point outside the given region is achievable since the sum s.d.o.f. is bounded by $\frac{1}{2}(2N-K)$ from Theorem 1.

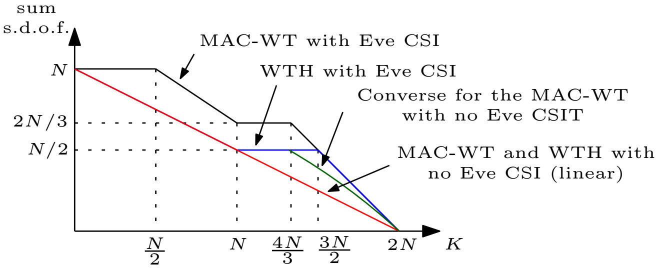

Fig. 3: Sum s.d.o.f. with number of eavesdropper antennas.

Fig. 3 shows the optimal linear sum s.d.o.f. for the WTH and the MAC-WT channel with and without eavesdropper CSIT. Similar to the SISO case [7], the MIMO MAC-WT channel reduces to the WTH when the eavesdropper CSIT is not available for the regime $0 \le K \le N$, and at least from a linear s.d.o.f. perspective in the regime $N \le K \le 2N$. However, unlike in the SISO case [7], the linear s.d.o.f. for the WTH decreases due to the lack of eavesdropper CSIT. Even without any linearity constraints, the optimal s.d.o.f. for the WTH does decrease due to lack of eavesdropper CSIT, as can be seen from the general upper bound, especially in the regime $\frac{4N}{3} \le K \le 2N$.

IV. Proof of Theorem 1

In this section, we will prove Theorem 1 by providing an achievable scheme and a converse. Since Theorem 1 implies that the WTH and the MAC-WT channel have the same linear sum s.d.o.f., we first note that it suffices to provide a linear achievable scheme for the WTH, since the MAC-WT channel can be treated as a WTH with time sharing between the users. Also, since any rate achievable for the WTH is achievable for the MAC-WT channel, a converse for the MAC-WT channel suffices as a converse for the WTH as well. Thus, in the following subsections, we provide an achievable scheme for the WTH and a converse for the MAC-WT channel.

A. Achievable Scheme for the WTH

In this scheme, the transmitter sends $(2N-K)$ information symbols reliably and securely to the legitimate receiver in two time slots, in order to achieve $\frac{1}{2}(2N-K)$ s.d.o.f. At each time slot, transmitter 1 sends a linear combination of $(2N-K)$ information symbols $\mathbf{v}_1$ and K artificial noise symbols $\mathbf{u}_1$ as in (9). Transmitter 2 sends a linear combination of its K artificial noise symbols $\mathbf{u}_2$. Since transmitter 2 does not have any information symbols $\mathbf{v}_2$ for the WTH, there is no $\mathbf{P}_2$ in that case. The channel outputs can be written compactly as in (12)-(13) as:

$$\bar{\mathbf{Y}} = \bar{\mathbf{H}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1\mathbf{u}_1 + \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2\mathbf{u}_2 + \bar{\mathbf{N}}_1 \tag{25}$$

$$\bar{\mathbf{Z}} = \bar{\mathbf{G}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1\mathbf{u}_1 + \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2\mathbf{u}_2 + \bar{\mathbf{N}}_2 \tag{26}$$

It remains to choose the precoding matrices $\bar{\mathbf{P}}_1$, $\bar{\mathbf{Q}}_1$ and $\bar{\mathbf{Q}}_2$ appropriately. We make the following selection:

$$\bar{\mathbf{Q}}_i = \bar{\mathbf{H}}_i^{-1}\bar{\mathbf{Q}}, \quad i = 1, 2 \tag{27}$$

where $\bar{\mathbf{Q}}$ is a $2N \times K$ matrix with rank K. Also choose $\bar{\mathbf{P}}_1$ to be a $2N \times (2N-K)$ matrix with rank $2N-K$, such that the matrix $[\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}]$ has rank $2N$. Note that this condition will be satisfied almost surely if the elements of $\bar{\mathbf{P}}_1$ and $\bar{\mathbf{Q}}$ are chosen from any continuous distribution in an i.i.d. fashion. With this selection, the channel outputs are:

$$\bar{\mathbf{Y}} =\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{Q}}_1(\mathbf{u}_1 + \mathbf{u}_2) + \bar{\mathbf{N}}_1 \tag{28}$$

$$\bar{\mathbf{Z}} =\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{G}}_1\bar{\mathbf{H}}_1^{-1}\bar{\mathbf{Q}}\mathbf{u}_1 + \bar{\mathbf{G}}_2\bar{\mathbf{H}}_2^{-1}\bar{\mathbf{Q}}\mathbf{u}_2 + \bar{\mathbf{N}}_2 \tag{29}$$

The decodability of $\mathbf{v}_1$ at the legitimate receiver in the high transmit power regime follows immediately since the matrix $[\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}]$ has rank $2N$ by our choice of $\bar{\mathbf{P}}_1$ and $\bar{\mathbf{Q}}$. On the other hand, the number of *leakage dimensions* L is

$$\begin{aligned} L =&\text{rank}[\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_1\bar{\mathbf{H}}_1^{-1}\bar{\mathbf{Q}}, \bar{\mathbf{G}}_2\bar{\mathbf{H}}_2^{-1}\bar{\mathbf{Q}}] \\ &- \text{rank}[\bar{\mathbf{G}}_1\bar{\mathbf{H}}_1^{-1}\bar{\mathbf{Q}}, \bar{\mathbf{G}}_2\bar{\mathbf{H}}_2^{-1}\bar{\mathbf{Q}}] && (30) \\ \leq& 2K - 2K && (31) \\ =&0 && (32) \end{aligned}$$

where we have used the fact that for any full-rank $\bar{\mathbf{Q}}$ chosen independently of $\bar{\mathbf{G}}_1, \bar{\mathbf{G}}_2$, $\text{rank}[\bar{\mathbf{G}}_1\bar{\mathbf{H}}_1^{-1}\bar{\mathbf{Q}}, \bar{\mathbf{G}}_2\bar{\mathbf{H}}_2^{-1}\bar{\mathbf{Q}}] = 2K$ for almost all channel realizations of $(\bar{\mathbf{G}}_1, \bar{\mathbf{G}}_2)$. This follows from the following lemma by noting that each row and each column of $\bar{\mathbf{G}}_i$ has at least one entry drawn from a continuous distribution in an i.i.d. fashion and the matrices $\bar{\mathbf{H}}_i^{-1}\bar{\mathbf{Q}}$ for $i = 1, 2$ do not depend on the $\bar{\mathbf{G}}_i$s.

Lemma 1 *Let $\mathbf{P}_1 \in \mathbb{R}^{N\times m_1}$ and $\mathbf{P}_2 \in \mathbb{R}^{N\times m_2}$ fixed matrices with ranks p_1 and p_2, respectively. Let $\mathbf{G}_1$ and $\mathbf{G}_2$ be $K \times N$ matrices whose each row and each column has at least one entry that is drawn from some continuous distribution in an i.i.d. fashion, and the remaining elements are arbitrary but fixed. Then, almost surely,*

$$K \geq \text{rank}[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2] \geq \min(p_1 + p_2, K) \tag{33}$$

The proof of this lemma is relegated to Appendix I.

Therefore, the security requirement in (21) is satisfied as well. This completes the achievable scheme. We remark here that though the achievability has been shown for linear framework, it can be easily shown that the leakage $I(\mathbf{v}_1; \bar{\mathbf{Z}}) \leq o(\log P)$, as done in [8]. Further by using stochastic encoding techniques, one can obtain an achievable scheme for which the leakage $\frac{1}{n}I(W; \mathbf{Z}^n) \to 0$ as $n \to \infty$.

B. Converse

In this section, we will prove the converse for the MAC-WT channel. To that end, we consider two regimes of K. When $0 \leq K \leq N$, we prove the converse for general transmission schemes without any restrictions of linearity. For the regime $N \leq K \leq 2N$, we prove the converse under the assumption of linear coding schemes only. We also provide a general upper bound in this regime which does not match the achievablity; nevertheless, it shows that there is loss in s.d.o.f. for the WTH and the MAC-WT channel due to no eavesdropper CSIT.

1) $0 \leq K \leq N$: Converse with No Restrictions: We wish to show that:

$$d_1 + d_2 \leq \frac{1}{2}(2N - K) \tag{34}$$

Let us first state three lemmas which are useful for the proof.

Lemma 2 (Channel symmetry [3, Lemma 3]) *Let $Z^K = \{Z_1, \ldots, Z_K\}$ be entropy symmetric, i.e., for any subsets A and B of $\{1, \ldots, K\}$, with $|A| = |B| \leq K$,*

$$h(\{Z_i, i \in A\}) = h(\{Z_i, i \in B\}) \tag{35}$$

Then, for any $M \geq N$, the following holds:

$$\frac{1}{N}h(Z^N) \geq \frac{1}{M}h(Z^M) \tag{36}$$

Lemma 3 (Least alignment lemma [5, Lemma 3]) *Consider two receivers, each with L antennas. Suppose the channel gains to receiver 2 are not available at the transmitters. If $\mathbf{Y}$ and $\mathbf{Z}$ denote the channel outputs at receivers 1 and 2, respectively, we have*

$$h(\mathbf{Z}^n) \geq h(\mathbf{Y}^n) + no(\log P) \tag{37}$$

Combining the two lemmas, we have the following lemma.

Lemma 4 *For the $N \times N \times N \times K$ MIMO MAC-WT channel with no eavesdropper CSIT, with $K \leq N$*

$$h(\mathbf{Z}^n) \geq \frac{K}{N}h(\mathbf{Y}^n) + no(\log P) \tag{38}$$

We relegate the proof of this lemma to Appendix II.

Let us now proceed with the converse proof. As in [2], [8], [10], we define noisy versions of $\mathbf{X}_i$ as $\tilde{\mathbf{X}}_i = \mathbf{X}_i + \tilde{\mathbf{N}}_i$

where $\tilde{\mathbf{N}}_i \sim \mathcal{N}(\mathbf{0}, \rho_i^2 \mathbf{I}_N)$ with $\rho_i^2 < \min\left(\frac{1}{\|\mathbf{H}_i\|^2}, \frac{1}{\|\mathbf{G}_i\|^2}\right)$. The *secrecy penalty lemma* [2] can then be derived as

$$\begin{aligned}
n(R_1+R_2) \leq& I(W_1, W_2; \mathbf{Y}^n | \mathbf{Z}^n) + n\epsilon \qquad (39)\\
\leq& h(\mathbf{Y}^n | \mathbf{Z}^n) + no(\log P) \qquad (40)\\
=& h(\mathbf{Y}^n, \mathbf{Z}^n) - h(\mathbf{Z}^n) + no(\log P) \qquad (41)\\
\leq& h(\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + no(\log P) \qquad (42)\\
=& h(\tilde{\mathbf{X}}_1^n) + h(\tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + no(\log P) \qquad (43)
\end{aligned}$$

The *role of a helper lemma* [2] also generalizes to the MIMO case as

$$\begin{aligned}
nR_1 \leq& I(\mathbf{X}_1^n; \mathbf{Y}^n) \qquad (44)\\
=& h(\mathbf{Y}^n) - h(\mathbf{H}_2^n \mathbf{X}_2^n + \mathbf{N}_1^n) \qquad (45)\\
\leq& h(\mathbf{Y}^n) - h(\tilde{\mathbf{X}}_2^n) + no(\log P) \qquad (46)
\end{aligned}$$

By symmetry, we also have

$$nR_2 \leq h(\mathbf{Y}^n) - h(\tilde{\mathbf{X}}_1^n) + no(\log P) \qquad (47)$$

Adding (43), (46) and (47), we have

$$\begin{aligned}
2n(R_1+R_2) \leq& 2h(\mathbf{Y}^n) - h(\mathbf{Z}^n) + no(\log P) \qquad (48)\\
\leq& 2h(\mathbf{Y}^n) - \frac{K}{N} h(\mathbf{Y}^n) + no(\log P) \qquad (49)\\
=& \frac{2N-K}{N} h(\mathbf{Y}^n) + no(\log P) \qquad (50)\\
\leq& (2N-K)\left(\frac{n}{2}\log P\right) + no(\log P) \qquad (51)
\end{aligned}$$

where (49) follows from Lemma 4 and we have used the fact that $h(\mathbf{Y}^n) \leq \frac{N}{2}\log P + no(\log P)$. Therefore, we have,

$$R_1 + R_2 \leq \frac{1}{2}(2N-K)\left(\frac{1}{2}\log P\right) + o(\log P) \qquad (52)$$

Dividing by $\frac{1}{2}\log P$ and taking the limit $P \to \infty$, we have

$$d_1 + d_2 \leq \frac{1}{2}(2N-K) \qquad (53)$$

which completes the proof of the converse for the regime $0 \leq K \leq N$.

2) $N \leq K \leq 2N$: Converse with Linear Coding Strategies: We begin with the following lemma.

Lemma 5 *For the $N \times N \times N \times K$ MAC-WT channel, and for any* linear *achievable scheme satisfying both the reliability and security constraints, and also $d_1 + d_2 > 0$,*

$$\begin{aligned}
&\lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad = \lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) = K \qquad (54)
\end{aligned}$$

We relegate the proof of this lemma to Appendix III.

To proceed with the upper bound, first note that since strictly positive sum s.d.o.f. is achievable for the MAC-WT channel using linear schemes, we can safely discard the case $d_1 + d_2 = 0$ for the purpose of the converse. Therefore, from Lemma 5, the rank of the vector space spanned by the output at the eavesdropper is $Kn + o(n)$, i.e.,

$$\begin{aligned}
&\lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad = \lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) = K \qquad (55)
\end{aligned}$$

We have,

$$\begin{aligned}
&m_1(n) + m_2(n)\\
&= \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad - \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) \qquad (56)\\
&\leq \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad - \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad - \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad + \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) + o(n) \qquad (57)\\
&\leq \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad - \frac{1}{2}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad - \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad + \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) + o(n) \qquad (58)\\
&\leq \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad + \frac{1}{2}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad - \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) + o(n) \qquad (59)\\
&\leq \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad - \frac{1}{2}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) + o(n) \qquad (60)\\
&\leq Nn - \frac{1}{2}Kn + o(n) \qquad (61)\\
&= \frac{(2N-K)n}{2} + o(n) \qquad (62)
\end{aligned}$$

where (56) follows from the decodability constraint, (57) follows from the secrecy constraint (21), and (58) follows from the following:

$$\begin{aligned}
&2 \times \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right)\\
&\quad \geq \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1]\right) + \text{rank}\left([\bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) \qquad (63)\\
&\quad = \text{rank}\left([\bar{\mathbf{Q}}_1]\right) + \text{rank}\left([\bar{\mathbf{Q}}_2]\right) \qquad (64)\\
&\quad = \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1]\right) + \text{rank}\left([\bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \qquad (65)\\
&\quad \geq \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \qquad (66)
\end{aligned}$$

The above equalities all hold almost surely since $\bar{\mathbf{H}}_i$ and $\bar{\mathbf{G}}_i$ are both full column rank almost surely.

Now dividing by n and taking limit $n \to \infty$, we have

$$d_1 + d_2 \leq \frac{1}{2}(2N-K) \qquad (67)$$

3) $N \leq K \leq 2N$: Converse with No Restrictions: We have the following lemma.

Lemma 6 *For the $N \times N \times N \times K$ MIMO MAC-WT channel with no eavesdropper CSIT, with $K \leq 2N$*

$$h(\mathbf{Z}^n) \geq \frac{K}{2N} h(\mathbf{Y}^n, \mathbf{Z}^n) + no(\log P) \qquad (68)$$

The proof of this lemma is relegated to Appendix IV.

Now we proceed as in the case of $0 \leq K \leq N$:

$$\begin{aligned} n(R_1+R_2) \leq& I(W_1,W_2;\mathbf{Y}^n|\mathbf{Z}^n)+n\epsilon && (69)\\ \leq& h(\mathbf{Y}^n,\mathbf{Z}^n)-h(\mathbf{Z}^n)+no(\log P) && (70)\\ \leq& \left(1-\frac{K}{2N}\right)h(\mathbf{Y}^n,\mathbf{Z}^n)+no(\log P) && (71)\\ \leq& \frac{2N-K}{2N}\left(h(\tilde{\mathbf{X}}_1^n)+h(\tilde{\mathbf{X}}_2^n)\right)+no(\log P) && (72)\end{aligned}$$

The *role of the helper* lemma yields, for $i \neq j$:

$$nR_i \leq h(\mathbf{Y}^n)-h(\tilde{\mathbf{X}}_j^n)+no(\log P) \tag{73}$$

Eliminating $h(\tilde{\mathbf{X}}_1^n)$ and $h(\tilde{\mathbf{X}}_2^n)$ using (72) and (73),

$$\begin{aligned} n(R_1+R_2) \leq& \frac{2(2N-K)}{4N-K}h(\mathbf{Y}^n)+no(\log P) && (74)\\ \leq& \frac{2N(2N-K)}{4N-K}\left(\frac{n}{2}\log P\right)+no(\log P) && (75)\end{aligned}$$

Dividing by n and letting $n \to \infty$, we have

$$R_1+R_2 \leq \frac{2N(2N-K)}{4N-K}\left(\frac{1}{2}\log P\right)+o(\log P) \tag{76}$$

Now dividing by $\frac{1}{2}\log P$ and letting $P \to \infty$,

$$d_1+d_2 \leq \frac{2N(2N-K)}{4N-K} \tag{77}$$

Also, $d_1+d_2 \leq \frac{N}{2}$, since $\frac{N}{2}$ is the optimal sum s.d.o.f. when $K=N$, and the sum s.d.o.f. is non-increasing in K.

V. Conclusions

In this paper, we considered two fundamental multi-user channel models: the MIMO WTH and the MIMO MAC-WT channel. In each case, the eavesdropper has K antennas while the remaining terminals have N antennas. We assumed that the CSIT of the legitimate receiver is available but no eavesdropper CSIT is available. We determined the optimal sum s.d.o.f. for each channel model for the regime $K \leq N$, and showed that in this regime, the MAC-WT channel reduces to the WTH in the absence of eavesdropper CSIT. For the regime $N \leq K \leq 2N$, we obtained the optimal *linear* s.d.o.f., and showed that the MAC-WT channel and the WTH have the same optimal s.d.o.f. when restricted to linear encoding strategies. In the absence of any such restrictions, we provided an upper bound for the sum s.d.o.f. of the MAC-WT channel in the regime $N \leq K \leq 2N$. Our results showed that unlike in the SISO case, there is loss of s.d.o.f. for even the WTH due to lack of eavesdropper CSIT, especially when $K \geq N$.

Appendix I
Proof of Lemma 1

First note when $N \leq K$, $\mathbf{G}_i$s have full column rank almost surely. Therefore,

$$\text{rank}[\mathbf{G}_i\mathbf{P}_i]=\text{rank}[\mathbf{P}_i]=p_i \tag{78}$$

almost surely. On the other hand, when $N \geq K$, we have

$$\text{rank}[\mathbf{G}_i\mathbf{P}_i] \geq \text{rank}[\mathbf{G}_i\hat{\mathbf{P}}_i] \tag{79}$$

where $\hat{\mathbf{P}}_i$ is a $N \times p_i$ submatrix of $\mathbf{P}_i$ with full column rank. Let $\bar{p}_i=\min(K,p_i)$. Now, the determinant of any $\bar{p}_i \times \bar{p}_i$ submatrix of $\mathbf{G}_i\hat{\mathbf{P}}_i$ is a multi-variate polynomial of the random entries of $\mathbf{G}_i$ and is zero for only finitely many realizations. Therefore, $\mathbf{G}_i\hat{\mathbf{P}}_i$ has rank $\bar{p}_i$. Note that when $N \leq K$, $\bar{p}_i=p_i$ is satisfied trivially.

Therefore, there exists a set $I_i \subseteq \{1,\dots,m_i\}$ such that $|I_i|=\bar{p}_i$ and the collection of column vectors $\mathbf{C}_i=\{\mathbf{c}_{ij}, j \in I_i\}$ are linearly independent, where $\mathbf{c}_{ij}$ denotes the jth column of $\mathbf{G}_i\mathbf{P}_i$. Clearly,

$$\text{rank}[\mathbf{G}_1\mathbf{P}_1,\mathbf{G}_2\mathbf{P}_2] \geq \text{rank}[\mathbf{C}_1,\mathbf{C}_2] \tag{80}$$

The matrix $[\mathbf{C}_1,\mathbf{C}_2]$ is a $K \times (\bar{p}_1+\bar{p}_2)$ matrix. Now, if $K \leq \bar{p}_1+\bar{p}_2$, consider any $K \times K$ submatrix of $[\mathbf{C}_1,\mathbf{C}_2]$. The determinant of this submatrix is a multi-variate polynomial function of the random entries of $\mathbf{G}_1$ and $\mathbf{G}_2$, and therefore, the determinant can be zero for only finitely many realizations, corresponding to the roots of the multi-variate polynomial function. Note that this is true if each row and each column of $\bar{\mathbf{G}}_i$ has at least one random entry. Also, the polynomial function is not identically zero. Therefore,

$$\text{rank}[\mathbf{C}_1,\mathbf{C}_2]=K \tag{81}$$

On the other hand, if $K \geq \bar{p}_1+\bar{p}_2$, we can consider a $(\bar{p}_1+\bar{p}_2)\times(\bar{p}_1+\bar{p}_2)$ submatrix of $[\mathbf{C}_1,\mathbf{C}_2]$, and using a similar argument, we can claim that

$$\text{rank}[\mathbf{C}_1,\mathbf{C}_2]=\bar{p}_1+\bar{p}_2 \tag{82}$$

Combining (80), (81) and (82), we have

$$\begin{aligned} &\text{rank}[\mathbf{G}_1\mathbf{P}_1,\mathbf{G}_2\mathbf{P}_2]\\ &\quad \geq \min(\bar{p}_1+\bar{p}_2,K) && (83)\\ &\quad =\min(\min(p_1,K)+\min(p_2,K),K) && (84)\\ &\quad =\min(\min(p_1+p_2,K+p_1,K+p_2,2K),K) && (85)\\ &\quad =\min(p_1+p_2,K) && (86)\end{aligned}$$

Finally, it trivially holds that $K \geq \text{rank}[\mathbf{G}_1\mathbf{P}_1,\mathbf{G}_2\mathbf{P}_2]$. This completes the proof of the lemma.

Appendix II
Proof of Lemma 4

Note that $K \leq N$. Consider $N-K$ additional outputs $\hat{\mathbf{Z}}$ at the eavesdropper as:

$$\hat{\mathbf{Z}}(t)=\hat{\mathbf{G}}_1(t)\mathbf{X}_1(t)+\hat{\mathbf{G}}_2(t)\mathbf{X}_2(t)+\hat{\mathbf{N}}_2(t) \tag{87}$$

where each $\hat{\mathbf{G}}_i$ is a $(N-K)\times N$ matrix whose entries are drawn in an i.i.d. fashion from the same continuous distribution as the entries of $\mathbf{G}_i$, and the entries of $\hat{\mathbf{N}}_2$ are i.i.d. zero-mean unit-variance Gaussian noise. Assume that the $\hat{\mathbf{G}}_i$s are not available at the transmitters either. Then, the enhanced output $\bar{\mathbf{Z}}(t)=(\mathbf{Z}(t),\hat{\mathbf{Z}}(t))$ is clearly entropy symmetric. Therefore, using Lemma 2, we have

$$h(\mathbf{Z}^n) \geq \frac{K}{N} h(\bar{\mathbf{Z}}^n) \tag{88}$$

Now, since the $\mathbf{G}_i$s and $\hat{\mathbf{G}}_i$s are not available at the transmitters, using Lemma 3, we have

$$h(\bar{\mathbf{Z}}^n) \geq h(\mathbf{Y}^n) + no(\log P) \tag{89}$$

Combining (88) and (89), we get the desired result that

$$h(\mathbf{Z}^n) \geq \frac{K}{N} h(\mathbf{Y}^n) + no(\log P) \tag{90}$$

Appendix III
Proof of Lemma 5

Since $d_1 + d_2 > 0$, without loss of generality, assume $d_1 > 0$. We wish to prove that

$$\begin{aligned} &\lim_{n\to\infty} \frac{1}{n} \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right) \\ &\qquad = \lim_{n\to\infty} \frac{1}{n} \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right) = K \end{aligned} \tag{91}$$

For the sake of contradiction, suppose $\lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right) < K$. We have

$$\begin{aligned} &\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right) \\ &\quad \geq \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right) && (92) \\ &\quad = \text{rank}\left([\bar{\mathbf{G}}_1[\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}_1], \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right) && (93) \\ &\quad \geq \min\left(\text{rank}\left([\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}_1] \right) + \text{rank}\left([\bar{\mathbf{Q}}_2] \right), Kn \right) && (94) \\ &\quad = \min\left(\text{rank}\left([\bar{\mathbf{P}}_1] \right) + \text{rank}\left([\bar{\mathbf{Q}}_1] \right) + \text{rank}\left([\bar{\mathbf{Q}}_2] \right), Kn \right) && (95) \\ &\quad = \min\left(m_1(n) + \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1] \right) + \text{rank}\left([\bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right), Kn \right) && (96) \\ &\quad \geq \min\left(m_1(n) + \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right), Kn \right) && (97) \end{aligned}$$

where (94) follows from Lemma 1, (95) follows from the decodability requirement, and (96) follows almost surely since $\bar{\mathbf{G}}_i$ is full column rank almost surely as long as $K > N$. Therefore,

$$\begin{aligned} &\lim_{n\to\infty} \frac{1}{n} \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right) \\ &\quad \geq \min\left(d_1 + \lim_{n\to\infty} \frac{1}{n} \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right), K \right) && (98) \\ &\quad > \lim_{n\to\infty} \frac{1}{n} \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2] \right) && (99) \end{aligned}$$

which contradicts the security requirement in (21).

Appendix IV
Proof of Lemma 6

Consider $2N-K$ additional outputs $\hat{\mathbf{Z}}$ at the eavesdropper:

$$\hat{\mathbf{Z}}(t) = \hat{\mathbf{G}}_1(t)\mathbf{X}_1(t) + \hat{\mathbf{G}}_2(t)\mathbf{X}_2(t) + \hat{\mathbf{N}}_2(t) \tag{100}$$

where each $\hat{\mathbf{G}}_i$ is a $(2N-K) \times N$ matrix whose entries are drawn in an i.i.d. fashion from the same continuous distribution as the entries of $\mathbf{G}_i$, and the entries of $\hat{\mathbf{N}}_2$ are i.i.d. zero-mean unit-variance Gaussian noise. Assume that the $\hat{\mathbf{G}}_i$s are not available at the transmitters either. Then, the enhanced output $\bar{\mathbf{Z}}(t) = (\mathbf{Z}(t), \hat{\mathbf{Z}}(t))$ is clearly entropy symmetric. Therefore, using Lemma 2, we have

$$h(\mathbf{Z}^n) \geq \frac{K}{2N} h(\bar{\mathbf{Z}}^n) \tag{101}$$

Now, given $\bar{\mathbf{Z}}^n$, we can decode both inputs $\mathbf{X}_1^n$ and $\mathbf{X}_2^n$ to within noise variance, and therefore, also $\mathbf{Y}^n$ and $\mathbf{Z}^n$. Thus, we have

$$h(\bar{\mathbf{Z}}^n) \geq h(\mathbf{Y}^n, \mathbf{Z}^n) + no(\log P) \tag{102}$$

Combining (101) and (102), we get the desired result that

$$h(\mathbf{Z}^n) \geq \frac{K}{2N} h(\mathbf{Y}^n, \mathbf{Z}^n) + no(\log P) \tag{103}$$

References

[1] V. R. Cadambe and S. A. Jafar. Interference alignment and degrees of freedom of the K-user interference channel. *IEEE Trans. on Inf. Theory*, 54(8):3425–3441, Aug. 2008.

[2] J. Xie and S. Ulukus. Secure degrees of freedom of one-hop wireless networks. *IEEE Trans. on Inf. Theory*, 60(6):3359–3378, Jun. 2014.

[3] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai. Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT. *IEEE Trans. on Inf. Theory*, 59(9):5244–5256, Sep. 2013.

[4] A. G. Davoodi and S. A. Jafar. Aligned image sets under channel uncertainty: Settling a conjecture by Lapidoth, Shamai and Wigger on the collapse of degrees of freedom under finite precision CSIT. Available at [arXiv:1403.1541].

[5] S. Lashgari and S. Avestimehr. Blind MIMOME wiretap channel with delayed CSIT. Available at [arXiv:1405.0521].

[6] P. Mukherjee and S. Ulukus. Secure degrees of freedom of the multiple access wiretap channel with no eavesdropper CSI. In *IEEE ISIT*, Jul. 2015.

[7] P. Mukherjee, J. Xie, and S. Ulukus. Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT. *IEEE Trans. on Inf. Theory*, submitted Jun. 2015. Also available at [arXiv:1506.06114].

[8] P. Mukherjee and S. Ulukus. Secure degrees of freedom of the MIMO multiple access wiretap channel. In *Asilomar Conf.*, Nov. 2015.

[9] P. Mukherjee and S. Ulukus. Secure degrees of freedom of the multiple access wiretap channel with multiple antennas. *IEEE Trans. on Inf. Theory*, submitted Feb. 2016. Also available at [arXiv:1604.03541].

[10] M. Nafea and A. Yener. Secure degrees of freedom of $N \times N \times M$ wiretap channel with a K-antenna cooperative jammer. In *IEEE ICC*, Jun. 2015.

[11] S. Lashgari, S. Avestimehr, and C. Suh. Linear degrees of freedom of the X-channel with delayed CSIT. *IEEE Trans. on Inf. Theory*, 60(4):2180–2189, Apr. 2014.

[12] S. Lashgari and A. S. Avestimehr. Blind wiretap channel with delayed csit. In Proc. *IEEE International Symposium on Information Theory*, pages 36–40, Jun. 2014.

[13] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. on Inf. Theory*, 54(12):5747–5755, Dec. 2008.

[14] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. on Inf. Theory*, 54(6):2735–2751, Jun. 2008.

[15] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *Allerton Conf.*, Sep. 2008.

[16] X. He and A. Yener. Providing secrecy with structured codes: Two-user Gaussian channels. *IEEE Trans. on Inf. Theory*, 60(4):2121–2138, Apr. 2014.

[17] R. Bassily and S. Ulukus. Ergodic secret alignment. *IEEE Trans. on Inf. Theory*, 58(3):1594–1611, Mar. 2012.

[18] M. Nafea and A. Yener. Secure degrees of freedom for the MIMO wiretap channel with a multiantenna cooperative jammer. In *IEEE ITW*, Nov. 2014.

[19] P. Mukherjee and S. Ulukus. Real interference alignment for the MIMO multiple access wiretap channel. In *IEEE ICC*, May 2016.

[20] G. Bresler, D. Cartwright, and D. Tse. Feasibility of interference alignment for the MIMO interference channel. *IEEE Trans. on Inf. Theory*, 60(9):5573–5586, Sep. 2014.

[21] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, Oct. 1975.