Secure Degrees of Freedom of the Multiple Access Wiretap Channel With Multiple Antennas

Pritam Mukherjee, *Member, IEEE*, and Sennur Ulukus, *Fellow, IEEE*

***Abstract*—We consider a two-user multiple-input multiple-output multiple access wiretap channel with N antennas at each transmitter, N antennas at the legitimate receiver, and K antennas at the eavesdropper. We determine the optimal sum secure degrees of freedom (s.d.o.f.) for this model for all values of N and K. We subdivide our problem into several regimes based on the values of N and K, and provide achievable schemes based on vector space alignment and real alignment techniques for fixed and fading channel gains. To prove the optimality of the achievable schemes, we provide matching converses for each regime. Our results show how the number of eavesdropper antennas affects the optimal sum s.d.o.f. of the multiple access wiretap channel.**

***Index Terms*—Secure degrees of freedom, multiple access wiretap channel, multiple-input multiple-output (MIMO), interference alignment.**

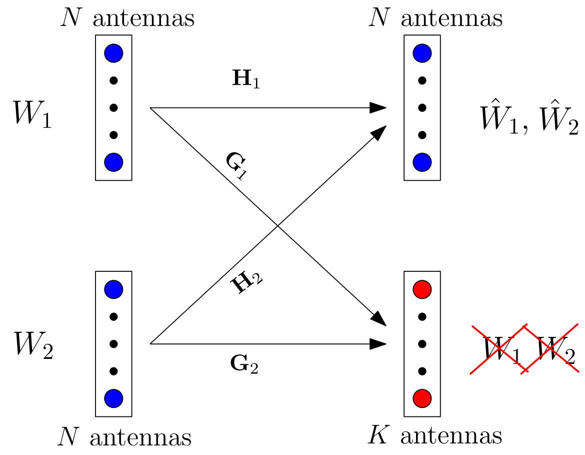

Fig. 1. The MIMO multiple access wiretap channel.

I. Introduction

We consider the two-user multiple-input multiple-output (MIMO) multiple access wiretap channel where each transmitter has N antennas, the legitimate receiver has N antennas and the eavesdropper has K antennas; see Fig. 1. We consider the case when the channel gains are fixed throughout the duration of the communication, as well as the case when the channel is fast fading and the channel gains vary in an i.i.d. fashion across time. Our goal in this paper is to characterize how the optimal sum secure degrees of freedom (s.d.o.f.) of the MIMO multiple access wiretap channel varies with the number of antennas at the legitimate users and the eavesdropper.

To that end, we partition the range of K into various regimes, and propose achievable schemes for each regime. Our schemes are based on a combination of zero-forcing beamforming and vector space interference alignment techniques. When the number of antennas at the eavesdropper is less than the number of antennas at the transmitters, the nullspace of the eavesdropper channel can be exploited to send secure signals to the legitimate transmitter. This strategy is, in fact, optimal when the number of antennas at the eavesdropper is sufficiently small ($K \leq \frac{N}{2}$) and the optimal sum s.d.o.f. of N is limited by the decoding capability of the legitimate receiver. We note that the optimal scheme requires a single channel use and thus, can be used for both fixed and fading channel gains.

However, zero-forcing beamforming does not suffice when $K \geq \frac{N}{2}$. In the regime $\frac{N}{2} \leq K \leq \frac{4N}{3}$, we use vector space interference alignment [1] over three time slots to achieve the optimal sum s.d.o.f. The structure of the optimal signaling scheme is inspired by ideas from the optimal real alignment scheme presented in [2] for the single-input single-output (SISO) multiple access wiretap channel. The proposed schemes work for both fixed and fading channel gains. We also provide a new real alignment based achievable scheme for fixed channel gains. The optimal s.d.o.f. in this regime is $\max(\frac{2}{3}(2N-K), \frac{2N}{3})$, i.e., in the form $2(d+\frac{l}{3})$, where d and l are both integers. For the case $l=0$, the sum s.d.o.f. is an integer and carefully precoded Gaussian signaling suffices to achieve the optimal s.d.o.f. in a single slot. When $l \neq 0$, the s.d.o.f. has a fractional part, and Gaussian signaling over a single time slot is not optimal. This is also observed in the achievable schemes in [3] and [4] for the MIMO wiretap channel with one helper, where structured signaling is used when the optimal s.d.o.f. is not an integer. However, [3], [4] consider complex channel gains, for which an s.d.o.f. of the form $\left(d+\frac{1}{2}\right)$ can be obtained by using d complex symbols (which comprise two real symbols) and one real symbol,

Manuscript received February 29, 2016; revised October 15, 2017; accepted December 30, 2017. Date of publication January 15, 2018; date of current version February 15, 2018. This work was supported by NSF under Grant CNS 13-14733, Grant CCF 14-22111, Grant CCF 14-22129, and Grant CNS 15-26608. This paper was presented in part at the 2015 Asilomar Conference on Signals, Systems and Computers and the 2016 IEEE ICC.

P. Mukherjee was with the Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park, MD 20742 USA. He is now with the Electrical Engineering Department, Stanford University, Stanford, CA 94305 USA (e-mail: pritamm@stanford.edu).

S. Ulukus is with the Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park, MD 20742 USA (e-mail: ulukus@umd.edu).

Communicated by A. Khisti, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2018.2793848

where each real symbol belongs to the same PAM constellation and carries $\frac{1}{2}$ s.d.o.f. In our case, the s.d.o.f. is of the form $2\left(d+\frac{l}{3}\right)$, $l=0,1,2$, and such simplification is not possible even with complex channel gains.

In this paper, we consider real channel gains. In order to handle the fractional s.d.o.f. with the real interference based achievable scheme, we decompose the channel input at each transmitter into two parts: a Gaussian signaling part carrying d (the integer part) d.o.f. of information securely, and a structured signaling part carrying $\frac{l}{3}$ (the fractional part) d.o.f. of information securely. The structure of the Gaussian signals carrying the integer s.d.o.f. resembles that of the schemes for the fading channel gains. When $l=1$, we design the structured signals carrying $\frac{2}{3}$ sum s.d.o.f. according to the real interference alignment based SISO scheme of [2]. However, when $l=2$, a new scheme is required to achieve $\frac{4}{3}$ sum s.d.o.f. on the MIMO multiple access wiretap channel with two antennas at every terminal. To that end, we provide a novel optimal scheme for the canonical $2\times2\times2\times2$ MIMO multiple access wiretap channel. Interestingly, the scheme relies on asymptotic real interference alignment [5] at each antenna of the legitimate receiver.

When the number of eavesdropper antennas K is large enough $K\geq\frac{4N}{3}$, the optimal sum s.d.o.f. is given by $(2N-K)$, which is always an integer. In this regime Gaussian signaling along with vector space alignment techniques suffices to achieve the optimal s.d.o.f. in one time slot. When the number of antennas at the eavesdropper is very large ($K\geq\frac{3N}{2}$), the two-user multiple access wiretap channel reduces to a wiretap channel with one helper, and, thus, the scheme for the MIMO wiretap channel with one helper in [4] is optimal.

To establish the optimality of our achievable schemes, we present matching converses in each regime. A simple upper bound is obtained by allowing cooperation between the two transmitters. This reduces the two-user multiple access wiretap channel to a MIMO wiretap channel with $2N$ antennas at the transmitter, N antennas at the legitimate receiver and K antennas at the eavesdropper. The optimal s.d.o.f. of this MIMO wiretap channel is well known to be $\min((2N-K)^+,N)$ [6], [7], and this serves as an upper bound for the sum s.d.o.f. of the two-user multiple access wiretap channel. This bound is optimal when the number of eavesdropper antennas K is either quite small ($K\leq\frac{N}{2}$), or quite large ($K\geq\frac{4N}{3}$). When K is small, the sum s.d.o.f. is limited by the decoding capability of the legitimate receiver, and the optimal sum s.d.o.f. is N which is optimal even without any secrecy constraints. When K is large, the s.d.o.f. is limited by the requirement of secrecy from a very strong eavesdropper. For intermediate values of K, the distributed nature of the transmitters dominates, and we employ a generalization of the SISO converse techniques of [2] for the converse proof in the MIMO case, similar to [4].

A. Related Work

The multiple access wiretap channel is introduced by [8] and [9], where the technique of cooperative jamming is introduced to improve the rates achievable with Gaussian signaling. Reference [10] 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 [8]–[10] all yield zero s.d.o.f. Reference [11] proposes scaling-based and ergodic alignment techniques to achieve a sum s.d.o.f. of $\frac{K-1}{K}$ for the K-user multiple access wiretap channel; thus, showing that an alignment based scheme strictly outperforms i.i.d. Gaussian signaling with or without cooperative jamming at high SNR. Finally, [2], [12] establish the optimal sum s.d.o.f. to be $\frac{K(K-1)}{K(K-1)+1}$ and the full s.d.o.f. region, respectively, for the SISO multiple access wiretap channel. Other related channel models are the wiretap channel with helpers and the interference channel with confidential messages, for which the optimal sum s.d.o.f. is known for the SISO and MIMO cases in [2] and [3], [4], [13], and in [14] and [15], respectively.

A related line of research investigates the multiple access wiretap channel with an *arbitrarily varying* eavesdropper [16]. The eavesdropper's channel is assumed to be arbitrary, without any assumptions on its distribution, and security is guaranteed for *every* realization of the eavesdropper's channel. This models an exceptionally strong eavesdropper, which may control its own channel in an adversarial manner. Hence, the optimal sum s.d.o.f. is zero if $K\geq N$, since the eavesdropper's channel realizations may be exactly equal to the legitimate user's channel realizations. On the other hand, in our model, the eavesdropper's channel gains are drawn from an arbitrary but fixed continuous distribution with bounded support. We show that, with this mild assumption, strictly positive s.d.o.f. can be achieved even $K\geq N$ for *almost all* channel realizations for the multiple access wiretap channel.

II. System Model

The two-user multiple access wiretap channel, see Fig. 1, is described by,

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

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

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 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. When the channel gains are fixed, $\mathbf{H}_i(t)=\mathbf{H}_i$ and $\mathbf{G}_i(t)=\mathbf{G}_i$, for all $t=1,\dots,n$, where the entries of $\mathbf{H}_i$ and $\mathbf{G}_i$ are drawn from an arbitrary but fixed continuous distribution with bounded support in an i.i.d. fashion, i.e., the channel gains remain fixed throughout the duration of the communication. When the channel gains are fading, the entries of $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$, $t=1,\dots,n$, are drawn from the fixed continuous distribution with bounded support in an i.i.d. fashion. We assume that all the channel matrices $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$, $t = 1, \ldots, n$, are known with full precision at all terminals, at time $t = 0$, i.e., before the start of the communication. 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 the spectral norm) of the vector (or matrix) $\mathbf{X}$.

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,

$$\frac{1}{n} I(W_1, W_2; \mathbf{Z}^n) \leq \epsilon_n \tag{3}$$

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

$$d_i = \lim_{P \to \infty} \frac{R_i}{\frac{1}{2}\log P} \tag{4}$$

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

III. Main Result

The main result of this paper is the determination of the optimal sum s.d.o.f. of the MIMO multiple access wiretap channel. We have the following theorem.

Theorem 1: The optimal sum s.d.o.f. of the MIMO multiple access wiretap channel with N antennas at the transmitters, N antennas at the legitimate receiver and K antennas at the eavesdropper is given by

$$d_s = \begin{cases} N, & \text{if } K \leq \frac{1}{2}N \\ \frac{2}{3}(2N-K), & \text{if } \frac{1}{2}N \leq K \leq N \\ \frac{2}{3}N, & \text{if } N \leq K \leq \frac{4}{3}N \\ 2N-K, & \text{if } \frac{4}{3}N \leq K \leq 2N \\ 0, & \text{if } K \geq 2N. \end{cases} \tag{5}$$

for fading channel gains, and almost surely for fixed channel gains.

We present the converse proof for this theorem in Section IV. The achievable schemes for the case of fading channel gains are presented in Section V, while the achievable schemes for the case of fixed channel gains are presented in Appendix.

Note that in the case of fixed channel gains, the s.d.o.f. results stated in Theorem 1 hold for *almost* all channel gains, not all channel gains. Indeed, it is clear that when $K \geq N$, we cannot guarantee secrecy for any of the users for all channel gains; simply consider the case when the channel gains from each transmitter to the eavesdropper (with N antennas) are exactly the same as the channel gains to the legitimate receiver. Reference [16] determines the optimal s.d.o.f. for the case of the arbitrarily varying eavesdropper where secrecy has to be guaranteed for all channel gains. In practice, such a strong secrecy requirement may be pessimistic and we can achieve higher rates by relaxing to *almost* all channel gains; in particular, we achieve positive secrecy rates even when $K \geq N$, as long as $K < 2N$.

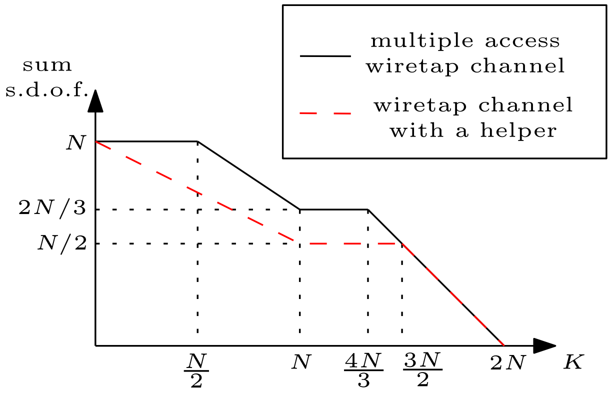

Fig. 2. d_s versus K.

Also, note that though the results presented here are for the case where all legitimate terminals have equal number of antennas, we believe our techniques can be extended to analyze the case of arbitrary number of antennas at each terminal. Indeed, [13] considers the closely related model of the wiretap channel with one helper and determines the optimal s.d.o.f. for arbitrary number of antennas at each terminal. The main approach is to subdivide the problem into many regimes based on the number of antennas and then use techniques similar to those used here to analyze each regime. Here, we consider the simpler scenario to focus on the effect of the number of eavesdropper antennas on the s.d.o.f. and to highlight the various techniques used to construct the achievable schemes and the converse proofs.

Fig. 2 shows the variation of the optimal sum s.d.o.f. with the number of eavesdropper antennas K. Note that as in the SISO case, the optimal sum s.d.o.f. is higher for the multiple access wiretap channel than for the wiretap channel with one helper [4], when $K < 3N/2$. However, when the number of eavesdropper antennas K is large enough, i.e., when $K \geq 3N/2$, the optimal sum s.d.o.f. of the multiple access wiretap channel is the same as the optimal s.d.o.f. of the wiretap channel with a helper.

Further, note that when the number of eavesdropper antennas K is small enough ($K \leq \frac{N}{2}$), the optimal sum s.d.o.f. is N, which is the optimal d.o.f. of the multiple access channel without any secrecy constraints. Thus, there is no penalty for imposing the secrecy constraints in this regime. Also note that allowing cooperation beteen the transmitters does not increase the sum s.d.o.f. in this regime. Heuristically, the eavesdropper is quite weak in this regime, and the optimal sum s.d.o.f. is limited by the decoding capabilities of the legitimate receiver.

On the other hand, when the number of antennas K is quite large ($K \geq \frac{4N}{3}$), the optimal sum s.d.o.f. is $(2N-K)$, which is the optimal s.d.o.f. obtained by allowing cooperation between the transmitters. Intuitively, the eavesdropper is very strong in this regime and the sum s.d.o.f. is limited by the requirement of secrecy from this strong eavesdropper. In the intermediate regime, when $\frac{N}{2} \leq K \leq \frac{4N}{3}$, the distributed nature of the transmitters becomes a key factor and the upper bound

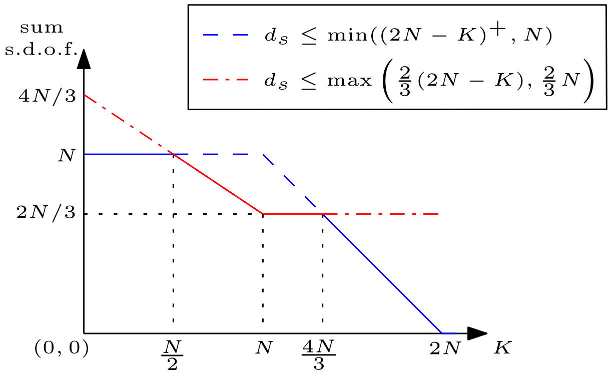

Fig. 3. The two upper bounds.

obtained by allowing cooperation between the transmitters is no longer achievable; see Fig. 3.

IV. Proof of the Converse

We prove the following upper bounds which are combined to give the converse for the full range of N and K,

$$d_1 + d_2 \le \min((2N-K)^+, N) \tag{6}$$

$$d_1 + d_2 \le \max\left(\frac{2}{3}(2N-K), \frac{2}{3}N\right) \tag{7}$$

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

It can be verified from Fig. 3 that the minimum of the two bounds in (6)-(7) gives the converse to the sum s.d.o.f. stated in (5) for all ranges of N and K. Thus, we next provide proofs of each of the bounds in (6) and (7).

A. Proof of $d_1 + d_2 \le min((2N-K)^+, N)$

This bound follows by allowing cooperation between the transmitters, which reduces the two-user multiple access wiretap channel to a single-user MIMO wiretap channel with $2N$ antennas at the transmitter, N antennas at the legitimate receiver and K antennas at the eavesdropper. The optimal s.d.o.f. for this MIMO wiretap channel is known to be $\min((2N-K)^+, N)$ [6], [7].

B. Proof of $d_1 + d_2 \le max(\frac{2}{3}(2N-K), \frac{2}{3}N)$

We only show that $d_1 + d_2 \le \frac{2}{3}(2N-K)$, when $K \le N$, and note that the bound $d_1 + d_2 \le \frac{2}{3}N$ for $K > N$ follows from the fact that increasing the number of eavesdropper antennas cannot increase the sum s.d.o.f.; thus, the sum s.d.o.f. when $K > N$ is upper-bounded by the sum s.d.o.f. for the case of $K = N$, which is $\frac{2}{3}N$.

To prove $d_1 + d_2 \le \frac{2}{3}(2N-K)$ when $K \le N$, we follow [2], [4]. 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

$$\begin{aligned} n(R_1+R_2) &\le I(W_1, W_2; \mathbf{Y}^n|\mathbf{Z}^n) + n\epsilon && (8)\\ &\le h(\mathbf{Y}^n|\mathbf{Z}^n) + nc_1 && (9)\\ &= h(\mathbf{Y}^n, \mathbf{Z}^n) - h(\mathbf{Z}^n) + nc_1 && (10)\\ &\le h(\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + nc_2 && (11)\\ &\le h(\tilde{\mathbf{X}}_1^n) + h(\tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + nc_2 && (12) \end{aligned}$$

where (9) follows since $h(\mathbf{Y}^n|\mathbf{Z}^n, W_1, W_2) \ge h(\mathbf{Y}^n|\mathbf{Z}^n, \mathbf{X}_1^n, \mathbf{X}_2^n) = o(\log P)$, (11) follows since $h(\mathbf{Y}^n, \mathbf{Z}^n) = h(\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n) + h(\mathbf{Y}^n, \mathbf{Z}^n|\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n) - h(\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n|\mathbf{Y}^n, \mathbf{Z}^n)$, where $h(\mathbf{Y}^n, \mathbf{Z}^n|\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n) \le o(\log P)$ while $h(\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n|\mathbf{Y}^n, \mathbf{Z}^n) = o(\log P)$ due to the fact that $\mathbf{X}_1^n$ and $\mathbf{X}_2^n$ (and consequently, $\tilde{\mathbf{X}}_1^n$ and $\tilde{\mathbf{X}}_2^n$) can be reconstructed within noise variance given $\mathbf{Y}^n$ and $\mathbf{Z}^n$. Finally, (12) follows since $\mathbf{X}_1^n$, $\mathbf{X}_2^n$, $\tilde{\mathbf{N}}_1^n$ and $\tilde{\mathbf{N}}_2^n$ are all independent of each other.

Now consider a stochastically equivalent version of $\mathbf{Z}$ given by $\tilde{\mathbf{Z}} = \mathbf{G}_1\tilde{\mathbf{X}}_1 + \mathbf{G}_2\mathbf{X}_2 + \mathbf{N}_Z$, where $\mathbf{N}_Z$ is an independent Gaussian noise vector, distributed as $\mathcal{N}(\mathbf{0}, \mathbf{I}_K - \rho_1^2\mathbf{G}_1\mathbf{G}_1^H)$. Further, let $\mathbf{G}_1 = [\tilde{\mathbf{G}}_1 \;\; \hat{\mathbf{G}}_1]$ and $\tilde{\mathbf{X}}_1^T = [\tilde{\mathbf{X}}_{1a}^T \;\; \tilde{\mathbf{X}}_{1b}^T]^T$, where $\tilde{\mathbf{G}}_1$ is the matrix with the first K columns of $\mathbf{G}_1$, $\hat{\mathbf{G}}_1$ has the last $N-K$ columns of $\mathbf{G}_1$, $\tilde{\mathbf{X}}_{1a}$ is a vector with the top K elements of $\tilde{\mathbf{X}}_1$, while $\tilde{\mathbf{X}}_{1b}$ has the remaining $N-K$ elements of $\tilde{\mathbf{X}}_1$. Then, we have

$$\begin{aligned} h(\mathbf{Z}^n) = h(\tilde{\mathbf{Z}}^n) &= h(\mathbf{G}_1^n\tilde{\mathbf{X}}_1^n + \mathbf{G}_2^n\mathbf{X}_2^n + \mathbf{N}_Z^n) && (13)\\ &\ge h(\mathbf{G}_1^n\tilde{\mathbf{X}}_1^n) && (14)\\ &= h(\tilde{\mathbf{G}}_1^n\tilde{\mathbf{X}}_{1a}^n + \hat{\mathbf{G}}_1^n\tilde{\mathbf{X}}_{1b}^n) && (15)\\ &\ge h(\tilde{\mathbf{G}}_1^n\tilde{\mathbf{X}}_{1a}^n|\tilde{\mathbf{X}}_{1b}^n) && (16)\\ &= h(\tilde{\mathbf{X}}_{1a}^n|\tilde{\mathbf{X}}_{1b}^n) + nc_3 && (17) \end{aligned}$$

Using (17) in (12), we have

$$n(R_1+R_2) \le h(\tilde{\mathbf{X}}_{1b}^n) + h(\tilde{\mathbf{X}}_2^n) + nc_4 \tag{18}$$

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

$$\begin{aligned} nR_1 &\le I(\mathbf{X}_1^n; \mathbf{Y}^n) && (19)\\ &= h(\mathbf{Y}^n) - h(\mathbf{H}_2^n\mathbf{X}_2^n + \mathbf{N}_1^n) && (20)\\ &\le h(\mathbf{Y}^n) - h(\tilde{\mathbf{X}}_2^n) + nc_5 && (21) \end{aligned}$$

Adding (18) and (21), we have

$$\begin{aligned} n(2R_1+R_2) &\le h(\mathbf{Y}^n) + h(\tilde{\mathbf{X}}_{1b}^n) + nc_6 && (22)\\ &\le N\frac{n}{2}\log P + (N-K)\frac{n}{2}\log P + nc_7 && (23)\\ &= (2N-K)\frac{n}{2}\log P + nc_7 && (24) \end{aligned}$$

First dividing by n and letting $n \to \infty$, and then dividing by $\frac{1}{2}\log P$ and letting $P \to \infty$, we have

$$2d_1 + d_2 \le 2N - K \tag{25}$$

By reversing the roles of the transmitters, we have

$$d_1 + 2d_2 \le 2N - K \tag{26}$$

Combining (25) and (26), we have the required bound

$$d_1 + d_2 \le \frac{2}{3}(2N-K) \tag{27}$$

This completes the proof of the converse of Theorem 1.

V. Achievable Schemes

We provide separate achievable schemes for each of the following regimes:

1) $K \leq N/2$
2) $N/2 \leq K \leq N$
3) $N \leq K \leq 4N/3$
4) $4N/3 \leq K \leq 3N/2$
5) $3N/2 \leq K \leq 2N$

Each scheme described in the following sections can be outlined as follows. We neglect the impact of noise at high SNR. Then, to achieve a certain sum s.d.o.f., d_s, we achieve the s.d.o.f. pair (d_1, d_2) with $d_s = d_1+d_2$. We send n_1 symbols $\mathbf{v}_1 = \left(v_{11}, \ldots, v_{1n_1}\right)$ and n_2 symbols $\mathbf{v}_2 = \left(v_{21}, \ldots, v_{2n_2}\right)$ from the first and second transmitters, respectively, in n_B slots, such that $d_1 = n_1/n_B$ and $d_2 = n_2/n_B$. Finally, we show that the leakage of information symbols at the eavesdropper is $o(\log P)$. We however want a stronger guarantee of security, namely,

$$\frac{1}{n} I(W_1, W_2; \mathbf{Z}^n) \to 0 \tag{28}$$

as $n \to \infty$. To achieve this, we view the n_B slots described in the scheme as a block and treat the equivalent channel from $\mathbf{v}_1$ and $\mathbf{v}_2$ to $\mathbf{Y}$ and $\mathbf{Z}$ as a memoryless multiple access wiretap channel with $\mathbf{Y}$ being the output at the legitimate receiver and $\mathbf{Z}$ being the output at the eavesdropper. The following sum secure rate is achievable [17]:

$$\sup(R_1 + R_2) \geq I(\mathbf{V}; \mathbf{Y}) - I(\mathbf{V}; \mathbf{Z}) \tag{29}$$

where $\mathbf{V} \stackrel{\Delta}{=} \{\mathbf{v}_1, \mathbf{v}_2\}$. Using the proposed scheme, $\mathbf{v}_1$ and $\mathbf{v}_2$ can be reconstructed from $\mathbf{Y}$ to within noise distortion. Thus,

$$I(\mathbf{V}; \mathbf{Y}) = (n_1 + n_2)\frac{1}{2}\log P + o(\log P) \tag{30}$$

Also, for each scheme, by design

$$I(\mathbf{V}; \mathbf{Z}) = o(\log P) \tag{31}$$

Thus, from (29), the achievable sum secure rate in each block is $(n_1 + n_2)\frac{1}{2}\log P + o(\log P)$. Since our block contains n_B channel uses, the effective sum secure rate is

$$\sup(R_1 + R_2) \geq \left(\frac{n_1 + n_2}{n_B}\right)\frac{1}{2}\log P + o(\log P) \tag{32}$$

Thus, the achievable sum s.d.o.f. is $\frac{n_1+n_2}{n_B}$, with the stringent security requirement as well.

In the following subsections, we present the achievable scheme for each regime.

A. $K \leq N/2$

In this regime, the optimal sum s.d.o.f. is N. In our scheme, transmitter 1 sends $(N - K)$ independent Gaussian symbols $\mathbf{v}_1 \in \mathbb{R}^{N-K}$ while transmitter 2 sends K independent Gaussian symbols $\mathbf{v}_2 \in \mathbb{R}^K$, in one time slot. This can be done by beamforming the information streams at both transmitters to directions that are orthogonal to the eavesdropper's channel. To this end, the transmitted signals are:

$$\mathbf{X}_1 = \mathbf{P}_1\mathbf{v}_1 \tag{33}$$

$$\mathbf{X}_2 = \mathbf{P}_2\mathbf{v}_2 \tag{34}$$

where $\mathbf{P}_1 \in \mathbb{R}^{N\times(N-K)}$ is a matrix whose $(N - K)$ columns span the $(N - K)$ dimensional nullspace of $\mathbf{G}_1$, and $\mathbf{P}_2 \in \mathbb{R}^{N\times K}$ is a matrix with K linearly independent vectors drawn from the $(N - K)$ dimensional nullspace of $\mathbf{G}_2$. This can be done since $K \leq N - K$. The channel outputs are:

$$\mathbf{Y} = [\mathbf{H}_1\mathbf{P}_1 \quad \mathbf{H}_2\mathbf{P}_2]\begin{bmatrix}\mathbf{v}_1\\ \mathbf{v}_2\end{bmatrix} + \mathbf{N}_1 \tag{35}$$

$$\mathbf{Z} = \mathbf{N}_2 \tag{36}$$

Note that $[\mathbf{H}_1\mathbf{P}_1 \quad \mathbf{H}_2\mathbf{P}_2]$ is an $N \times N$ matrix with full rank almost surely, and thus, both $\mathbf{v}_1$ and $\mathbf{v}_2$ can be decoded at the legitimate receiver to within noise variance. On the other hand, they do not appear in the eavesdropper's observation and thus their security is guaranteed.

B. $N/2 \leq K \leq N$

The optimal sum s.d.o.f. in this regime is $\frac{2}{3}(2N - K)$. If $N = K = 1$, real interference alignment can be used to achieve an s.d.o.f. of $\frac{2}{3}$ [2] for fixed channel gains. If $N > 1$, transmitter i sends $(2N - K)$ Gaussian symbols $\left\{\mathbf{v}_i \in \mathbb{R}^{2K-N}, \tilde{\mathbf{v}}_i(t) \in \mathbb{R}^{N-K}, t = 1, 2, 3\right\}$, each drawn independently from $\mathcal{N}(0, \bar{P})$, in 3 time slots for $i = 1, 2$, where $\bar{P} = \alpha P$ and α is chosen to satisfy the power constraint. Intuitively, transmitter i sends the $(N - K)$ symbols $\mathbf{w}_i(t)$ by beamforming orthogonal to the eavesdropper in each time slot $t = 1, 2, 3$. The remaining $(2K - N)$ symbols are sent over 3 time slots using a scheme similar to the SISO scheme of [2], [18]. Thus, the transmitted signals at time t are:

$$\mathbf{X}_1(t) = \mathbf{G}_1(t)^{\perp}\mathbf{w}_1(t) + \mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{H}_1(t)^{-1}\mathbf{Q}(t)\mathbf{u}_1 \tag{37}$$

$$\mathbf{X}_2(t) = \mathbf{G}_2(t)^{\perp}\mathbf{w}_2(t) + \mathbf{P}_2(t)\mathbf{v}_2 + \mathbf{H}_2(t)^{-1}\mathbf{Q}(t)\mathbf{u}_2 \tag{38}$$

where $\mathbf{G}_i(t)^{\perp}$ is an $N \times (N - K)$ full rank matrix with $\mathbf{G}_i(t)\mathbf{G}_i(t)^{\perp} = \mathbf{0}_{N\times(N-K)}$, $\mathbf{u}_i$ is a $(2K - N)$ dimensional vector whose entries are drawn in an i.i.d. fashion from $\mathcal{N}(0, \bar{P})$, and $\mathbf{P}_i$ and $\mathbf{Q}$ are $N \times (2K - N)$ precoding matrices that will be fixed later. The channel outputs are:

$$\begin{aligned}\mathbf{Y}(t) &= \mathbf{H}_1(t)\mathbf{G}_1(t)^{\perp}\mathbf{w}_1(t) + \mathbf{H}_1(t)\mathbf{P}_1(t)\mathbf{v}_1\\ &\quad + \mathbf{H}_2(t)\mathbf{P}_2(t)\mathbf{v}_2 + \mathbf{H}_2(t)\mathbf{G}_2(t)^{\perp}\mathbf{w}_2(t)\\ &\quad + \mathbf{Q}(t)(\mathbf{u}_1 + \mathbf{u}_2) + \mathbf{N}_1(t) \qquad (39)\\ \mathbf{Z}(t) &= \mathbf{G}_1(t)\mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{G}_2(t)\mathbf{H}_2(t)^{-1}\mathbf{Q}(t)\mathbf{u}_2\\ &\quad + \mathbf{G}_2(t)\mathbf{P}_2(t)\mathbf{v}_2 + \mathbf{G}_1(t)\mathbf{H}_1(t)^{-1}\mathbf{Q}(t)\mathbf{u}_1 + \mathbf{N}_2(t) \qquad (40)\end{aligned}$$

Let us define

$$\tilde{\mathbf{P}}_i \stackrel{\Delta}{=} \begin{bmatrix}\mathbf{P}_i(1)\\ \mathbf{P}_i(2)\\ \mathbf{P}_i(3)\end{bmatrix}, \quad \tilde{\mathbf{Q}} \stackrel{\Delta}{=} \begin{bmatrix}\mathbf{Q}(1)\\ \mathbf{Q}(2)\\ \mathbf{Q}(3)\end{bmatrix} \tag{41}$$

Further, if we define

$$\tilde{\mathbf{H}}_i \stackrel{\Delta}{=} \begin{bmatrix}\mathbf{H}_i(1) & \mathbf{0}_{N\times N} & \mathbf{0}_{N\times N}\\ \mathbf{0}_{N\times N} & \mathbf{H}_i(2) & \mathbf{0}_{N\times N}\\ \mathbf{0}_{N\times N} & \mathbf{0}_{N\times N} & \mathbf{H}_i(3)\end{bmatrix} \tag{42}$$

and, $\tilde{\mathbf{G}}_i$, $\tilde{\mathbf{G}}_i^{\perp}$ similarly, we can compactly represent the channel outputs over all 3 time slots as

$$\begin{aligned}\tilde{\mathbf{Y}} &= \tilde{\mathbf{H}}_1\tilde{\mathbf{G}}_1^{\perp}\tilde{\mathbf{w}}_1 + \tilde{\mathbf{H}}_1\tilde{\mathbf{P}}_1\mathbf{v}_1 + \tilde{\mathbf{H}}_2\tilde{\mathbf{P}}_2\mathbf{v}_2 \\ &\quad + \tilde{\mathbf{H}}_2\tilde{\mathbf{G}}_2^{\perp}\tilde{\mathbf{w}}_2 + \tilde{\mathbf{Q}}(\mathbf{u}_1 + \mathbf{u}_2) + \tilde{\mathbf{N}}_1 \qquad (43)\\ \tilde{\mathbf{Z}} &= \tilde{\mathbf{G}}_1\tilde{\mathbf{P}}_1\mathbf{v}_1 + \tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1}\tilde{\mathbf{Q}}\mathbf{u}_2 + \tilde{\mathbf{G}}_2\tilde{\mathbf{P}}_2\mathbf{v}_2 \\ &\quad + \tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1}\tilde{\mathbf{Q}}\mathbf{u}_1 + \tilde{\mathbf{N}}_2 \qquad (44)\end{aligned}$$

where $\tilde{\mathbf{w}}_i = [\mathbf{w}_i(1)^T \quad \mathbf{w}_i(2)^T \quad \mathbf{w}_i(3)^T]^T$, and $\tilde{\mathbf{N}}_i$, $\tilde{\mathbf{Y}}$ and $\tilde{\mathbf{Z}}$ are defined similarly.

We now choose $\tilde{\mathbf{Q}}$ to be any $3N \times (2K - N)$ matrix with full column rank, and choose

$$\tilde{\mathbf{P}}_i = \tilde{\mathbf{G}}_i^T(\tilde{\mathbf{G}}_i\tilde{\mathbf{G}}_i^T)^{-1}(\tilde{\mathbf{G}}_j\tilde{\mathbf{H}}_j^{-1})\tilde{\mathbf{Q}} \qquad (45)$$

where $i, j \in \{1, 2\}, i \neq j$. It can be verified that this selection aligns $\mathbf{v}_i$ with $\mathbf{u}_j$, $i \neq j$, at the eavesdropper, and this guarantees that the information leakage is $o(\log P)$. On the other hand, the legitimate receiver decodes the desired signals $\left\{\mathbf{w}_i(t) \in \mathbb{R}^{N-K}, t \in \{1, 2, 3\}\right\}$, $\left\{\mathbf{v}_i \in \mathbb{R}^{2K-N}, i = 1, 2\right\}$ and the aligned artificial noise symbols $\mathbf{u}_1 + \mathbf{u}_2 \in \mathbb{R}^{2K-N}$, i.e., $6(N - K) + 3(2K - N) = 3N$ symbols using $3N$ observations in 3 time slots, to within noise variance. This completes the scheme for the regime $N/2 \leq K \leq N$.

C. $N \leq K \leq 4N/3$

In this regime, the optimal sum s.d.o.f. is $\frac{2}{3}N$. Therefore, transmitter i in our scheme sends N Gaussian symbols, $\mathbf{v}_i \in \mathbb{R}^N$, in 3 time slots. The transmitted signals in time slot t are given by

$$\begin{aligned}\mathbf{X}_1(t) &= \mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{H}_1(t)^{-1}\mathbf{Q}(t)\mathbf{u}_1 \qquad (46)\\ \mathbf{X}_2(t) &= \mathbf{P}_2(t)\mathbf{v}_2 + \mathbf{H}_1(t)^{-1}\mathbf{Q}(t)\mathbf{u}_2 \qquad (47)\end{aligned}$$

where the $\mathbf{P}_1(t)$, $\mathbf{Q}(t)$, and $\mathbf{P}_2(t)$ are $N \times N$ precoding matrices to be designed. As in the previous scheme, we can compactly represent the channel outputs over 3 channel uses as

$$\begin{aligned}\tilde{\mathbf{Y}} &= \tilde{\mathbf{H}}_1\tilde{\mathbf{P}}_1\mathbf{v}_1 + \tilde{\mathbf{H}}_2\tilde{\mathbf{P}}_2\mathbf{v}_2 + \tilde{\mathbf{Q}}(\mathbf{u}_1 + \mathbf{u}_2) + \tilde{\mathbf{N}}_1 \qquad (48)\\ \tilde{\mathbf{Z}} &= \tilde{\mathbf{G}}_1\tilde{\mathbf{P}}_1\mathbf{v}_1 + \tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1}\tilde{\mathbf{Q}}\mathbf{u}_2 + \tilde{\mathbf{G}}_2\tilde{\mathbf{P}}_2\mathbf{v}_2 \\ &\quad + \tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1}\tilde{\mathbf{Q}}\mathbf{u}_1 + \tilde{\mathbf{N}}_2 \qquad (49)\end{aligned}$$

To ensure secrecy, we impose the following conditions

$$\begin{aligned}\tilde{\mathbf{G}}_1\tilde{\mathbf{P}}_1 &= \tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1}\tilde{\mathbf{Q}} \qquad (50)\\ \tilde{\mathbf{G}}_2\tilde{\mathbf{P}}_2 &= \tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1}\tilde{\mathbf{Q}} \qquad (51)\end{aligned}$$

We rewrite the conditions in (50)-(51) as

$$\Psi \begin{bmatrix} \tilde{\mathbf{P}}_1 \\ \tilde{\mathbf{P}}_2 \\ \tilde{\mathbf{Q}} \end{bmatrix} = \mathbf{0}_{6K \times N} \qquad (52)$$

where

$$\Psi \overset{\Delta}{=} \begin{bmatrix} \tilde{\mathbf{G}}_1 & \mathbf{0}_{3K \times 3N} & -\tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1} \\ \mathbf{0}_{3K \times 3N} & \tilde{\mathbf{G}}_2 & -\tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1} \end{bmatrix} \qquad (53)$$

Note that Ψ has a nullity $9N - 6K$. Since $9N - 6K \geq N$ in this regime, we can choose N vectors of dimension $9N$ randomly such that they are linearly independent and lie in the nullspace of Ψ. We can then assign to $\tilde{\mathbf{P}}_1$, $\tilde{\mathbf{P}}_2$ and $\tilde{\mathbf{Q}}$, the top, the middle and the bottom $3N$ rows of the matrix comprising the N chosen vectors. This guarantees secrecy of the message symbols at the eavesdropper.

To see the decodability, we rewrite the received signal at the legitimate receiver as

$$\tilde{\mathbf{Y}} = \Phi \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{u}_1 + \mathbf{u}_2 \end{bmatrix} + \tilde{\mathbf{N}}_1 \qquad (54)$$

where $\Phi \overset{\Delta}{=} [\tilde{\mathbf{H}}_1\tilde{\mathbf{P}}_1 \quad \tilde{\mathbf{H}}_2\tilde{\mathbf{P}}_2 \quad \tilde{\mathbf{Q}}]$. We note that Φ is $3N \times 3N$ and full rank almost surely; thus, the desired signals $\mathbf{v}_1$ and $\mathbf{v}_2$ can be decoded at the legitimate receiver within noise distortion at high SNR.

D. $4N/3 \leq K \leq 3N/2$

The optimal s.d.o.f. in this regime is $2N - K$. To achieve this s.d.o.f., the first transmitter sends $K - N$ Gaussian symbols $\left\{\mathbf{v}_1 \in \mathbb{R}^{3N-2K}, \tilde{\mathbf{v}} \in \mathbb{R}^{3K-4N}\right\}$, while the second transmitter sends $3N - 2K$ Gaussian symbols $\left\{\mathbf{v}_2 \in \mathbb{R}^{3N-2K}\right\}$, in one time slot. The scheme is as follows. The transmitted signals are

$$\begin{aligned}\mathbf{X}_1 &= \mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 \qquad (55)\\ \mathbf{X}_2 &= \mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{P}_2\mathbf{v}_2 + \mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 \qquad (56)\end{aligned}$$

where $\tilde{\mathbf{u}} \in \mathbb{R}^{3K-4N}$ and $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{R}^{3N-2K}$ are artificial noise vectors, whose entries are drawn in an i.i.d. fashion from $\mathcal{N}(0, \bar{P})$. The precoding matrices $\mathbf{R}_i \in \mathbb{R}^{N \times (3K-4N)}$, and $\mathbf{P}_i, \mathbf{Q}_i \in \mathbb{R}^{N \times (3N-2K)}$ will be chosen later. The channel outputs are

$$\begin{aligned}\mathbf{Y} &= \mathbf{H}_1\mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{H}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_2\mathbf{P}_2\mathbf{v}_2 \\ &\quad + \mathbf{H}_2\mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{Q}(\mathbf{u}_1 + \mathbf{u}_2) + \mathbf{N}_1 \qquad (57)\\ \mathbf{Z} &= \mathbf{G}_1\mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{G}_2\mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{G}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 \\ &\quad + \mathbf{G}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 + \mathbf{N}_2 \qquad (58)\end{aligned}$$

To ensure secrecy, we want to impose the following conditions:

$$\begin{aligned}\mathbf{G}_1\mathbf{R}_1 &= \mathbf{G}_2\mathbf{R}_2 \qquad (59)\\ \mathbf{G}_1\mathbf{P}_1 &= \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q} \qquad (60)\\ \mathbf{G}_2\mathbf{P}_2 &= \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q} \qquad (61)\end{aligned}$$

To satisfy (59), we choose $\mathbf{R}_1$ and $\mathbf{R}_2$ to be the first and the last N rows of a $2N \times 3K - 4N$ matrix whose columns consist of any $3K - 4N$ linearly independent vectors drawn randomly from the nullspace of $[\mathbf{G}_1 \quad -\mathbf{G}_2]$. This is possible since, $3K - 4N \leq 2N - K$ in this regime. To satisfy (60)-(61), we let $\mathbf{P}_1$, $\mathbf{P}_2$ and $\mathbf{Q}$ to be the first, the second and the last N rows of a $3N \times (3N - 2K)$ matrix whose columns are randomly chosen to span the $(3N - 2K)$ dimensional nullspace of the matrix Λ given by

$$\Lambda \overset{\Delta}{=} \begin{bmatrix} \mathbf{G}_1 & \mathbf{0}_{K \times N} & -\mathbf{G}_2\mathbf{H}_2^{-1} \\ \mathbf{0}_{K \times N} & \mathbf{G}_2 & -\mathbf{G}_1\mathbf{H}_1^{-1} \end{bmatrix} \qquad (62)$$

To see the decodablity, we can rewrite the observation at the legitimate receiver as

$$\mathbf{Y} = \Phi \begin{bmatrix} \tilde{\mathbf{v}} \\ \mathbf{v}_1 \\ \mathbf{v}_2 \\ \tilde{\mathbf{u}} \\ \mathbf{u}_1 + \mathbf{u}_2 \end{bmatrix} + \mathbf{N}_1 \tag{63}$$

where Φ is the $N \times N$ matrix defined as

$$\Phi = [\mathbf{H}_1\mathbf{R}_1 \quad \mathbf{H}_1\mathbf{P}_1 \quad \mathbf{H}_2\mathbf{P}_2 \quad \mathbf{H}_2\mathbf{R}_2 \quad \mathbf{Q}] \tag{64}$$

Since Φ is full rank almost surely, the legitimate receiver can decode its desired symbols $\tilde{\mathbf{v}}, \mathbf{v}_1$, and $\mathbf{v}_2$.

E. $3N/2 \leq K \leq 2N$

In this regime, it is clear from Fig. 2 that the multiple access wiretap channel has the same optimal sum s.d.o.f. as the optimal s.d.o.f. of the wiretap channel with one helper. Thus, an optimal achievable scheme for the wiretap channel with one helper suffices as the scheme for the multiple access wiretap channel as well. Such an optimal scheme, based on real interference alignment, is provided in [4] for the wiretap channel with one helper with fixed channel gains. Here, we provide a scheme based on vector space alignment.

In order to achieve the optimal sum s.d.o.f. of $2N - K$ in this regime, the first transmitter sends $2N - K$ independent Gaussian symbols $\mathbf{v} \in \mathbb{R}^{2N-K}$ securely, in one time slot. The second transmitter just transmits artificial noise symbols $\mathbf{u} \in \mathbb{R}^{2N-K}$, whose entries are drawn in an i.i.d. fashion from $\mathcal{N}(0, \bar{P})$. The transmitted signals are

$$\mathbf{X}_1 = \mathbf{P}\mathbf{v} \tag{65}$$

$$\mathbf{X}_2 = \mathbf{Q}\mathbf{u} \tag{66}$$

where $\mathbf{P}$ and $\mathbf{Q}$ are $N \times (2N - K)$ precoding matrices to be fixed later. The received signals are

$$\mathbf{Y} = \mathbf{H}_1\mathbf{P}\mathbf{v} + \mathbf{H}_2\mathbf{Q}\mathbf{u} + \mathbf{N}_1 \tag{67}$$

$$\mathbf{Z} = \mathbf{G}_1\mathbf{P}\mathbf{v} + \mathbf{G}_2\mathbf{Q}\mathbf{u} + \mathbf{N}_2 \tag{68}$$

To ensure security, we wish to ensure that

$$\mathbf{G}_1\mathbf{P} = \mathbf{G}_2\mathbf{Q} \tag{69}$$

This can be done by choosing $\mathbf{P}$ and $\mathbf{Q}$ to be the top and the bottom N rows of a $2N \times (2N - K)$ matrix whose linearly independent columns are drawn randomly from the nullspace of $[\mathbf{G}_1 \quad -\mathbf{G}_2]$. The decodability is ensured by noting that the matrix $[\mathbf{H}_1\mathbf{P} \quad \mathbf{H}_2\mathbf{Q}]$ is full column rank and $2(2N - K) \leq N$ in this regime.

VI. Conclusions

In this paper, we determined the optimal sum s.d.o.f. of the two-user MIMO multiple access wiretap channel with N antennas at each transmitter, N antennas at the legitimate receiver and K antennas at the eavesdropper. We provided vector space alignment based achievable schemes that exploit the channel variation over multiple time slots in general for both fixed and fading channel gains. When the channel gains are fixed, we also provided single time-slot schemes that use real interference alignment on structured signaling. We also provided matching converses to establish the optimality of the achievable schemes for both fixed and fading channel gains. Our results highlight the effect of the number of eavesdropper antennas on the s.d.o.f. of the multiple access wiretap channel.

Appendix
Real Alignment Based Achievable Schemes for Fixed Channel Gains

We note that the achievable schemes proposed for the fading channel gains in the regimes $K \leq \frac{N}{2}$ and $\frac{4N}{2} \leq K \leq 2N$ are single time-slot schemes and suffice for the fixed channel gains case. Here we present single time-slot real interference alignment schemes for the regime $\frac{N}{2} \leq K \leq \frac{4N}{3}$. In this regime, the optimal sum s.d.o.f. is $\max(\frac{2}{3}(2N - K), \frac{2N}{3})$, i.e., of the form $2\left(d + \frac{l}{3}\right)$, $l = 0, 1, 2$, where d is an integer. When $l = 0$, the sum s.d.o.f. is an integer and carefully precoded Gaussian signaling provides a single time-slot scheme. However, when $l \neq 0$, the s.d.o.f. has a fractional part, and Gaussian signaling alone cannot achieve the optimal s.d.o.f. in one time slot, since Gaussian signals with full power cannot carry fractional d.o.f. of information.

The general structure of our schemes is as follows: We decompose the channel input at each transmitter into three parts: a Gaussian signaling part that is transmitted orthogonal to the eavesdropper's channel, if possible, a Gaussian signaling part carrying d (the integer part) d.o.f. of information securely, and a structured signaling part carrying $\frac{l}{3}$ (the fractional part) d.o.f. of information securely. The structure of the Gaussian signals carrying the integer s.d.o.f. d are the same as that of the corresponding schemes for the fading channel gains. This ensures security at the eavesdropper as well as decodability at the legitimate receiver as long as the structured signals carrying the fractional s.d.o.f. $\frac{2l}{3}$ from both transmitters can be decoded at the legitimate receiver. The design of the structured signals is motivated from the SISO scheme of [2]. In fact, when $l = 1$, we use the signal structure of the scheme in [2], where real interference alignment is used to transmit $\frac{2}{3}$ sum s.d.o.f. on the SISO multiple access wiretap channel. However, when $l = 2$, a new scheme is required to achieve $\frac{4}{3}$ sum s.d.o.f. on the MIMO multiple access wiretap channel with two antennas at every terminal. To that end, we first provide a novel scheme, based on asymptotic real interference alignment [5], [19], for the canonical $2 \times 2 \times 2 \times 2$ MIMO multiple access wiretap channel.

A. Scheme for the $2 \times 2 \times 2 \times 2$ System

The optimal sum s.d.o.f. is $\frac{4}{3}$. Since the legitimate receiver has 2 antennas, we achieve $\frac{2}{3}$ s.d.o.f. on each antenna. The scheme is as follows.

Let m be a large integer. Define $M \overset{\Delta}{=} m^{\Gamma}$, where Γ will be specified later. The channel inputs are given by

$$\mathbf{X}_1 = \mathbf{G}_1^{-1}\mathbf{G}_2\mathbf{H}_2^{-1} \begin{pmatrix} \mathbf{t}_1^T\mathbf{v}_{11} \\ \mathbf{t}_2^T\mathbf{v}_{12} \end{pmatrix} + \mathbf{H}_1^{-1} \begin{pmatrix} \mathbf{t}_1^T\mathbf{u}_{11} \\ \mathbf{t}_2^T\mathbf{u}_{12} \end{pmatrix} \tag{70}$$

$$\mathbf{X}_2 = \mathbf{G}_2^{-1}\mathbf{G}_1\mathbf{H}_1^{-1}\begin{pmatrix}\mathbf{t}_1^T\mathbf{v}_{21}\\ \mathbf{t}_2^T\mathbf{v}_{22}\end{pmatrix} + \mathbf{H}_2^{-1}\begin{pmatrix}\mathbf{t}_1^T\mathbf{u}_{21}\\ \mathbf{t}_2^T\mathbf{u}_{22}\end{pmatrix} \quad (71)$$

where $\mathbf{t}_i, i = 1,2$ are M dimensional precoding vectors which will be fixed later, and $\mathbf{u}_{ij}, \mathbf{v}_{ij}$ are independent random variables drawn uniformly from the same PAM constellation $C(a, Q)$ given by

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \quad (72)$$

where Q is a positive integer and a is a real number used to normalize the transmission power. The exact values of a and Q will be specified later. The variables $\mathbf{v}_{ij}$ denote the information symbols of transmitter i, while $\mathbf{u}_{ij}$ are the cooperative jamming signals being transmitted from transmitter i.

The channel outputs are given by

$$\begin{aligned}\mathbf{Y} &= \mathbf{A}\begin{pmatrix}\mathbf{t}_1^T\mathbf{v}_{11}\\ \mathbf{t}_2^T\mathbf{v}_{12}\end{pmatrix} + \mathbf{B}\begin{pmatrix}\mathbf{t}_1^T\mathbf{v}_{21}\\ \mathbf{t}_2^T\mathbf{v}_{22}\end{pmatrix}\\ &\quad + \begin{pmatrix}\mathbf{t}_1^T(\mathbf{u}_{11}+\mathbf{u}_{21})\\ \mathbf{t}_2^T(\mathbf{u}_{12}+\mathbf{u}_{22})\end{pmatrix} + \mathbf{N}_1 &(73)\\ \mathbf{Z} &= \mathbf{G}_1\mathbf{H}_1^{-1}\begin{pmatrix}\mathbf{t}_1^T(\mathbf{u}_{11}+\mathbf{v}_{21})\\ \mathbf{t}_2^T(\mathbf{u}_{12}+\mathbf{v}_{22})\end{pmatrix}\\ &\quad + \mathbf{G}_2\mathbf{H}_2^{-1}\begin{pmatrix}\mathbf{t}_1^T(\mathbf{u}_{21}+\mathbf{v}_{11})\\ \mathbf{t}_2^T(\mathbf{u}_{22}+\mathbf{v}_{12})\end{pmatrix} + \mathbf{N}_2 &(74)\end{aligned}$$

where $\mathbf{A} = \mathbf{H}_1\mathbf{G}_1^{-1}\mathbf{G}_2\mathbf{H}_2^{-1}$ and $\mathbf{B} = \mathbf{H}_2\mathbf{G}_2^{-1}\mathbf{G}_1\mathbf{H}_1^{-1}$. Note that the information symbols $\mathbf{v}_{ij}$ are buried in the cooperative jamming signals $\mathbf{u}_{kj}$, where $k \neq i$, at the eavesdropper. Intuitively, this ensures security of the information symbols at the eavesdropper. At the legitimate receiver, we can express the received signal $\mathbf{Y}$ more explicitly as

$$\begin{pmatrix}\mathbf{t}_2^T(a_{12}\mathbf{v}_{12}+b_{12}\mathbf{v}_{22})\\ \qquad +\mathbf{t}_1^T(a_{11}\mathbf{v}_{11}+b_{11}\mathbf{v}_{21}+\mathbf{u}_{11}+\mathbf{u}_{21})\\ \mathbf{t}_1^T(a_{21}\mathbf{v}_{11}+b_{21}\mathbf{v}_{21})\\ \qquad +\mathbf{t}_2^T(a_{22}\mathbf{v}_{12}+b_{22}\mathbf{v}_{22}+\mathbf{u}_{12}+\mathbf{u}_{22})\end{pmatrix}$$

We define

$$T_1 = \left\{a_{11}^{r_1}b_{11}^{r_2}, r_i \in \{0,\ldots,m-1\}\right\} \quad (75)$$

$$T_2 = \left\{a_{22}^{r_1}b_{22}^{r_2}, r_i \in \{0,\ldots,m-1\}\right\} \quad (76)$$

Letting $\Gamma = 2$, we note that

$$|T_1| = |T_2| = M \quad (77)$$

We choose $\mathbf{t}_i$ to be the M dimensional vector that has all the elements of T_i. We note that all elements in T_i are rationally independent, since the channel gains are drawn independently from a continuous distribution. With the above selections, let us analyze the structure of the received signal at the legitimate receiver.

At the first antenna, $\mathbf{u}_{11}$ and $\mathbf{u}_{21}$ arrive along the dimensions of T_1. The signals $\mathbf{v}_{11}$ and $\mathbf{v}_{21}$ arrive along dimensions $a_{11}T_1$ and $b_{11}T_1$ and, thus, they align with $\mathbf{u}_{11}$ and $\mathbf{u}_{21}$ in $\tilde{T}_1$, where,

$$\tilde{T}_1 = \left\{a_{11}^{r_1}b_{11}^{r_2}, r_i \in \{0,\ldots,m\}\right\} \quad (78)$$

Thus, $\mathbf{v}_{11}$ and $\mathbf{v}_{21}$ cannot be reliably decoded from the observation of the first antenna. However, the desired signals $\mathbf{v}_{12}$ and $\mathbf{v}_{22}$ arrive along dimensions $a_{12}T_2$ and $b_{12}T_2$, respectively. Therefore, we need to verify that the elements of $a_{12}T_2$, $b_{12}T_2$ and $\tilde{T}_1$ are rationally independent. Note that in our case $\mathbf{A}$ and $\mathbf{B}$ are related; in fact $\mathbf{A} = \mathbf{B}^{-1}$, and therefore, $b_{ii} = ca_{jj}$ and $b_{ij} = -ca_{ij}$, $i \neq j$ for $i, j \in \{1,2\}$, where $c = \det(\mathbf{A})^{-1}$. Therefore, the elements in T_1 and T_2 can be represented as:

$$T_1 = \left\{a_{11}^{r_1}a_{22}^{r_2}c^{r_2}, r_i \in \{0,\ldots,m-1\}\right\} \quad (79)$$

$$T_2 = \left\{a_{22}^{r_1}a_{11}^{r_2}c^{r_2}, r_i \in \{0,\ldots,m-1\}\right\} \quad (80)$$

Now, first note that the elements of $\tilde{T}_1$ are rationally independent of those in $\{a_{12}T_2\}\bigcup\{b_{12}T_2\}$ since a_{12} is not present as a factor in the elements of $\tilde{T}_1$ (note that $b_{12}T_2 = ca_{12}T_2$). Next, note that elements of $a_{12}T_2$ and $b_{12}T_2$ are also rationally independent since $b_{12} = -ca_{12}$. Therefore, $\mathbf{v}_{12}$ and $\mathbf{v}_{22}$ can be reliably decoded at high SNR. Heuristically, the s.d.o.f. achieved using the first antenna is $\frac{2|T_1|}{2|T_1|+|\tilde{T}_2|} = \frac{2m^2}{2m^2+(m+1)^2} \approx \frac{2}{3}$ for large enough m.

At the second antenna, a similar analysis holds. The signals $\mathbf{v}_{12}$, $\mathbf{v}_{22}$, $\mathbf{u}_{12}$ and $\mathbf{u}_{22}$ align with each other in the dimensions of $\tilde{T}_2$, which is defined as

$$\tilde{T}_2 = \left\{a_{22}^{r_1}b_{22}^{r_2}, r_i \in \{0,\ldots,m\}\right\} \quad (81)$$

The signals $\mathbf{v}_{11}$ and $\mathbf{v}_{21}$ arrive along dimensions that are separate from each other as well as from the dimensions in $\tilde{T}_2$, and thus, can be decoded reliably. The s.d.o.f. achieved in the second antenna is also $\frac{2m^2}{2m^2+(m+1)^2} \approx \frac{2}{3}$ for large m. Therefore, the sum s.d.o.f. achieved using both antennas is $\frac{4}{3}$, as desired.

Formally, an achievable sum rate is given in equation (29), where $\mathbf{V} \overset{\Delta}{=} \left\{\mathbf{v}_{ij}, i, j \in \{1,2\}\right\}$. In order to bound the term $I(\mathbf{V};\mathbf{Y})$, we first bound the probability of error. Let $M_S \overset{\Delta}{=} 2m^2 + (m+1)^2$ be the number of rational dimensions at each receiver antenna. Also let $\mathbf{V}_i = \left\{\mathbf{v}_{kj}, k = 1,2; j \neq i\right\}$ be the desired symbols at the ith antenna of the receiver. In order to decode, the receiver makes an estimate $\hat{\mathbf{V}}_i$ of $\mathbf{V}_i$ by choosing the closest point in the constellation based on the signal received at antenna i. For any $\delta > 0$, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(M_S+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$, then for almost all channel gains the average power constraint is satisfied and the probability of error, $\Pr(\mathbf{V}_i \neq \hat{\mathbf{V}}_i)$, is upper-bounded by $\exp\left(-\eta_\gamma P^\delta\right)$, where η_γ is a positive constant which is independent of P. Since $\mathbf{V} = \{\mathbf{V}_i, i = 1,2\}$,

$$\Pr(\mathbf{V} \neq \hat{\mathbf{V}}) \leq 2\exp\left(-\eta_\gamma P^\delta\right) \quad (82)$$

By Fano's inequality and the Markov chain $\mathbf{V} \to \mathbf{Y} \to \hat{\mathbf{V}}$,

$$\begin{aligned}I(\mathbf{V};\mathbf{Y}) &= H(\mathbf{V}) - H(\mathbf{V}|\hat{\mathbf{V}}) &(83)\\ &\geq \log(|\mathcal{V}|) - 1 - \Pr(\mathbf{V} \neq \hat{\mathbf{V}})\log(|\mathcal{V}|) &(84)\\ &= \log(|\mathcal{V}|) - o(\log P) &(85)\\ &= \frac{4M(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) &(86)\end{aligned}$$

where $\mathcal{V}$ is the alphabet of $\mathbf{V}$ with cardinality $(2Q+1)^{4M} = (2Q+1)^{4m^2}$. Next, we compute

$$I(\mathbf{V};\mathbf{Z}) \leq I\left(\left\{\mathbf{v}_{ij}, i, j = 1,2\right\}; \left\{\mathbf{v}_{ij} + \mathbf{u}_{\hat{i}j}, \begin{matrix}\hat{i} \neq i,\\ i, j = 1,2\end{matrix}\right\}\right) \quad (87)$$

$$
\begin{aligned}
&\leq \sum_{i,j=1,\hat{i}\neq i}^{2} H(\mathbf{v}_{ij}+\mathbf{u}_{\hat{i}j}) - H(\mathbf{u}_{\hat{i}j}) && (88)\\
&\leq 4M\log(4Q+1) - 4M\log(2Q+1) && (89)\\
&\leq 4M = o(\log P) && (90)
\end{aligned}
$$

Using (86) and (90) in (29), we have

$$
\sup(R_1+R_2) \geq \frac{4M(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \quad (91)
$$

By choosing δ small enough and m large enough, we can make the sum s.d.o.f. arbitrarily close to $\frac{4}{3}$.

B. Achievable Schemes for $\frac{N}{2} \leq K \leq N$

We use structured PAM signaling along with Gaussian signaling. Let $d = \lfloor\frac{2K-N}{3}\rfloor$, and $l = (2K-N)\text{mod } 3 = (2N-K)\text{mod } 3$. Let $\mathbf{v}_i^{(1)} = \left\{v_{ij}, j=1,\ldots,d\right\}$, where each $v_{ij}, j=1,\ldots,d$ is drawn in an i.i.d. fashion $\sim \mathcal{N}(0,\alpha P)$, and $\mathbf{v}_i^{(2)} = \left\{v_{i(d+1)},\ldots,v_{i(d+l)}\right\}$ are structured PAM signals to be specified later. When $l=0$, $\mathbf{v}_i^{(2)}$ is the empty set. Let $\mathbf{v}_i = \left(\mathbf{v}_i^{(1)},\mathbf{v}_i^{(2)}\right)$. Also, let $\tilde{\mathbf{v}}_i = \left\{\tilde{v}_{ij}, j=1,\ldots,N-K\right\}$ denote the symbols that can be transmitted securely by beamforming orthogonal to the eavesdropper channel. Transmitter i sends:

$$
\mathbf{X}_i = \mathbf{G}_i^{\perp}\tilde{\mathbf{v}}_i + \mathbf{P}_i\mathbf{v}_i + \mathbf{H}_i^{-1}\mathbf{Q}\mathbf{u}_i \quad (92)
$$

where $\mathbf{G}_i^{\perp}$ is an $N\times(N-K)$ full rank matrix with $\mathbf{G}_i\mathbf{G}_i^{\perp} = \mathbf{0}_{N\times(N-K)}$, $\mathbf{u}_i = \left(\mathbf{u}_i^{(1)},\mathbf{u}_i^{(2)}\right)$ is a $(d+l)$ dimensional vector with the entries of $\mathbf{u}_i^{(1)} = \left\{u_{ij}, j=1,\ldots,d\right\}$ being drawn independently of $\mathbf{v}$ and each other from $\mathcal{N}(0,\alpha P)$, and the structure of $\mathbf{u}_i^{(2)} = \left\{u_{i(d+1)},\ldots,u_{i(d+l)}\right\}$ will be specified later. $\mathbf{P}_i$ and $\mathbf{Q}$ are $N\times(d+l)$ precoding matrices that will also be fixed later. The received signals are:

$$
\begin{aligned}
\mathbf{Y} &= \mathbf{H}_1\mathbf{G}_1^{\perp}\tilde{\mathbf{v}}_1 + \mathbf{H}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{H}_2\mathbf{G}_2^{\perp}\tilde{\mathbf{v}}_2\\
&\quad + \mathbf{Q}(\mathbf{u}_1+\mathbf{u}_2) + \mathbf{N}_1 && (93)\\
\mathbf{Z} &= \mathbf{G}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 + \mathbf{G}_2\mathbf{P}_2\mathbf{v}_2\\
&\quad + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 + \mathbf{N}_2 && (94)
\end{aligned}
$$

We now choose $\mathbf{Q}$ to be any $N\times(d+l)$ matrix with full column rank, and choose $\mathbf{P}_i = \mathbf{G}_i^T(\mathbf{G}_i\mathbf{G}_i^T)^{-1}(\mathbf{G}_j\mathbf{H}_j^{-1})\mathbf{Q}$, where $i,j\in\{1,2\}, i\neq j$. It can be verified that this selection aligns $\mathbf{v}_i$ with $\mathbf{u}_j$, $i\neq j$, at the eavesdropper, and this guarantees that the information leakage is $o(\log P)$. Next, let $\mathbf{P}_i^{(1)}$, $\mathbf{Q}^{(1)}$ be matrices containing the first d columns of $\mathbf{P}_i$ and $\mathbf{Q}$, respectively, while $\mathbf{P}_i^{(2)}$ and $\mathbf{Q}^{(2)}$ contain the last l columns of $\mathbf{P}_i$ and $\mathbf{Q}$, respectively. Let $\mathbf{B}$ be a matrix whose columns lie in the nullspace of the matrix $\mathbf{F}^T = [\mathbf{H}_1\mathbf{G}_1^{\perp}\ \ \mathbf{H}_2\mathbf{G}_2^{\perp}\ \ \mathbf{H}_1\mathbf{P}_1^{(1)}\ \ \mathbf{H}_1\mathbf{P}_1^{(1)}\ \ \mathbf{Q}^{(1)}]^T$. Note that $\mathbf{F}$ is a $(N-l)\times N$ matrix and thus there exists a $N\times l$ matrix $\mathbf{B}$ such that $\mathbf{FB}=\mathbf{0}$. We consider the filtered output $[\tilde{\mathbf{Y}},\hat{\mathbf{Y}}]^T = \mathbf{EY}$, where

$$
\mathbf{E} = \begin{pmatrix} & \mathbf{D}_{l\times N} \\ \mathbf{I}_{N-l} & \mathbf{0}_{(N-l)\times l}\end{pmatrix} \quad (95)
$$

and $\mathbf{D} = (\mathbf{B}^T\mathbf{Q}^{(2)})^{-1}\mathbf{B}^T$ and let

$$
\tilde{\mathbf{Y}} = \mathbf{D}\mathbf{H}_1\mathbf{P}_1^{(2)}\mathbf{v}_1^{(2)} + \mathbf{D}\mathbf{H}_2\mathbf{P}_2^{(2)}\mathbf{v}_2^{(2)} + (\mathbf{u}_1^{(2)}+\mathbf{u}_2^{(2)}) + \mathbf{D}\mathbf{N}_1 \quad (96)
$$

Note that (96) represents the output at the receiver of a multiple access wiretap channel with l antennas at each terminal. If $l=1$, we let $\mathbf{v}_i^{(2)} = v_{i(d+1)}$ be drawn uniformly and independently from the PAM constellation $C(a,Q)$, with $Q = P^{\frac{1-\delta}{2(3+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$. Also, $\mathbf{u}_i^{(2)} = u_{i(d+1)}$ is chosen uniformly from $C(a,Q)$ and independently from $\mathbf{v}_j$, $j=1,2$. The receiver can then decode $v_{1(d+1)}$, $v_{2(d+1)}$ and $(u_{1(d+1)} + u_{2(d+1)})$ with vanishing probability of error. On the other hand, if $l=2$, we choose $\mathbf{v}_i^{(2)}$ and $\mathbf{u}_i^{(2)}$ as in the $2\times2\times2\times2$ multiple access wiretap channel, i.e., $v_{i(d+k)} = \mathbf{t}_k^T\hat{\mathbf{v}}_{ik}, k=1,2$, where $\hat{\mathbf{v}}_{ik}$ is an M dimensional vector whose entries are drawn from the PAM constellation $C(a,Q)$ with $Q = P^{\frac{1-\delta}{2(M_S+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$, and $\mathbf{t}_i$ is chosen appropriately analogous to the selection for the $2\times2\times2\times2$ multiple access wiretap channel, noting the similarity of (96) with (73). The cooperative jamming signal $\mathbf{u}_i^{(2)}$ is chosen similarly. Then, the receiver can decode $\mathbf{v}_i^{(2)}$ and also $\mathbf{u}_1^{(2)}+\mathbf{u}_2^{(2)}$ with vanishing probability of error.

Thus, for $l=1,2$, $\mathbf{v}_i^{(2)}$ and $\mathbf{u}_1^{(2)}+\mathbf{u}_2^{(2)}$ can be eliminated from $\hat{\mathbf{Y}}$. Noting that $2(N-K)+3d\leq N-l$, $\tilde{\mathbf{v}}_i$ and $\mathbf{v}_i^{(1)}$ can also be decoded from $\tilde{\mathbf{Y}}$. We compute

$$
\begin{aligned}
I(\mathbf{v}_1,\mathbf{v}_2,\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2;\mathbf{Y}) &= I(\mathbf{v}_1^{(1)},\mathbf{v}_2^{(1)},\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2;\mathbf{Y}|\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)})\\
&\quad + I(\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)};\mathbf{Y}) \qquad (97)
\end{aligned}
$$

The second term depends on the value of l. When $l=1$,

$$
\begin{aligned}
I(\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)};\mathbf{Y}) &= \log(2Q+1)^2 + o(\log P) && (98)\\
&= 2\frac{1-\delta}{(3+\delta)}\left(\frac{1}{2}\log P\right) + o(\log P) && (99)
\end{aligned}
$$

On the other hand, when $l=2$, we have

$$
I(\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)};\mathbf{Y}) = \frac{4M(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \quad (100)
$$

Thus, in either case, by choosing δ sufficiently small and m large enough when $l=2$, we have

$$
I(\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)};\mathbf{Y}) = \frac{2l}{3}\left(\frac{1}{2}\log P\right) + o(\log P) \quad (101)
$$

Noting that $\mathbf{v}_1^{(1)},\mathbf{v}_2^{(1)},\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2$ can be decoded to within noise variance from $\mathbf{Y}$, given $\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)}$, the first term of (97) is

$$
\begin{aligned}
&I(\mathbf{v}_1^{(1)},\mathbf{v}_2^{(1)},\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2;\mathbf{Y}|\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)})\\
&\qquad \geq 2(d+N-K)\left(\frac{1}{2}\log P\right) + o(\log P) \qquad (102)
\end{aligned}
$$

Using (101) and (102) in (97), we have,

$$
\begin{aligned}
&I(\mathbf{v}_1,\mathbf{v}_2,\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2;\mathbf{Y})\\
&\quad \geq 2\left(d+N-K+\frac{l}{3}\right)\left(\frac{1}{2}\log P\right) + o(\log P) && (103)\\
&\quad = \frac{2}{3}(2N-K)\left(\frac{1}{2}\log P\right) + o(\log P) && (104)
\end{aligned}
$$

This completes the achievable schemes for the regime $\frac{N}{2}\leq K\leq N$.

C. Achievable Schemes for $N \leq K \leq \frac{4N}{3}$

As in the previous regime, we use structured PAM signaling along with Gaussian signaling. Let $d = \lfloor \frac{N}{3} \rfloor$ and $l = N \bmod 3$. Let $\mathbf{v}_i = \left(\mathbf{v}_i^{(1)}, \mathbf{v}_i^{(2)}\right)$ be the information symbols such that the entries of $\mathbf{v}_i^{(1)} = \left\{v_{ij}, j = 1, \ldots, d\right\}$ are drawn in an i.i.d. fashion $\sim \mathcal{N}(0, \alpha P)$, and the entries of $\mathbf{v}_i^{(2)} = \left\{v_{ij}, j = d+1, \ldots, d+l\right\}$ are structured PAM signals to be designed later. Let $\mathbf{u}_i = \left(\mathbf{u}_i^{(1)}, \mathbf{u}_i^{(2)}\right)$ denote the cooperative jamming symbols such that the entries of $\mathbf{u}_i^{(1)} = \left\{u_{ij}, j = 1, \ldots, d\right\}$ are drawn in an i.i.d. fashion $\sim \mathcal{N}(0, \alpha P)$, and the entries of $\mathbf{u}_i^{(2)} = \left\{u_{ij}, j = d+1, \ldots, d+l\right\}$ are structured PAM signals independent of $\mathbf{v}_j, j = 1, 2$ and $\mathbf{u}_j, j \neq i$. Transmitter i sends

$$\mathbf{X}_i = \mathbf{P}_i \mathbf{v}_i + \mathbf{H}_i^{-1} \mathbf{Q} \mathbf{u}_i \tag{105}$$

where the $\mathbf{P}_1$, $\mathbf{Q}$, and $\mathbf{P}_2$ are $N \times (d+l)$ precoding matrices to be designed. The channel outputs are given by

$$\mathbf{Y} = \mathbf{H}_1 \mathbf{P}_1 \mathbf{v}_1 + \mathbf{H}_2 \mathbf{P}_2 \mathbf{v}_2 + \mathbf{Q}(\mathbf{u}_1 + \mathbf{u}_2) + \mathbf{N}_1 \tag{106}$$

$$\begin{aligned} \mathbf{Z} = \mathbf{G}_1 \mathbf{P}_1 \mathbf{v}_1 + \mathbf{G}_2 \mathbf{H}_2^{-1} \mathbf{Q} \mathbf{u}_2 + \mathbf{G}_2 \mathbf{P}_2 \mathbf{v}_2 \\ + \mathbf{G}_1 \mathbf{H}_1^{-1} \mathbf{Q} \mathbf{u}_1 + \mathbf{N}_2 \end{aligned} \tag{107}$$

To ensure secrecy, we impose that for $i \neq j$

$$\mathbf{G}_i \mathbf{P}_i = \mathbf{G}_j \mathbf{H}_j^{-1} \mathbf{Q} \tag{108}$$

We rewrite the conditions in (108) as

$$\Psi \begin{bmatrix} \mathbf{P}_1^T & \mathbf{P}_2^T & \mathbf{Q}^T \end{bmatrix}^T = \mathbf{0}_{2K \times (d+l)} \tag{109}$$

where

$$\Psi \triangleq \begin{bmatrix} \mathbf{G}_1 & \mathbf{0}_{K \times N} & -\mathbf{G}_2 \mathbf{H}_2^{-1} \\ \mathbf{0}_{K \times N} & \mathbf{G}_2 & -\mathbf{G}_1 \mathbf{H}_1^{-1} \end{bmatrix} \tag{110}$$

Note that Ψ has a nullity $3N - 2K$. This alignment is feasible if $3N - 2K \geq d + l$, i.e., if $K \leq 4d + l$. This is satisfied since, in this regime, $K \leq 4d + l + \frac{1}{3}l$, which implies $K \leq 4d + 1$ for integers N and K, since $0 \leq l \leq 2$. This guarantees security and the information leakage is $o(\log P)$. Next, let $\mathbf{P} = \left(\mathbf{P}_i^{(1)}, \mathbf{P}_i^{(2)}\right)$ such that $\mathbf{P}_i^{(1)}$, contains the first d columns of $\mathbf{P}_i$. We define $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$ similarly. Let $\mathbf{B}$ be a matrix whose columns lie in the nullspace of the matrix $\mathbf{F}^T = [\mathbf{H}_1 \mathbf{P}_1^{(1)} \;\; \mathbf{H}_1 \mathbf{P}_1^{(1)} \;\; \mathbf{Q}^{(1)}]^T$. Note that $\mathbf{F}$ is a $(N - l) \times N$ matrix and thus there exists a non-zero $N \times l$ matrix $\mathbf{B}$ such that $\mathbf{FB} = \mathbf{0}$. We consider the filtered output $[\tilde{\mathbf{Y}}, \hat{\mathbf{Y}}]^T = \mathbf{EY}$, where $\mathbf{E}$ is as in (95). We have

$$\tilde{\mathbf{Y}} = \mathbf{D}\mathbf{H}_1 \mathbf{P}_1^{(2)} \mathbf{v}_1^{(2)} + \mathbf{D}\mathbf{H}_2 \mathbf{P}_2^{(2)} \mathbf{v}_2^{(2)} + (\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}) + \mathbf{D}\mathbf{N}_1 \tag{111}$$

When $l = 1$, we choose $\mathbf{v}_i^{(2)} = v_{i(d+1)}$ and $\mathbf{u}_i^{(2)} = u_{i(d+1)}$ to be PAM signals drawn independently from $C(a, Q)$ with $Q = P^{\frac{1-\delta}{2(3+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$. The receiver can then decode $v_{1(d+1)}$, $v_{2(d+1)}$ and $(u_{1(d+1)} + u_{2(d+1)})$ with vanishing probability of error. When $l = 2$, we choose $\mathbf{v}_i^{(2)}$ and $\mathbf{u}_i^{(2)}$ analogous to the case of the $2 \times 2 \times 2 \times 2$ multiple access wiretap channel, i.e., $v_{i(d+k)} = \mathbf{t}_k^T \hat{\mathbf{v}}_{ik}, k = 1, 2$, where $\hat{\mathbf{v}}_{ik}$ is an M dimensional vector whose entries are drawn from the PAM constellation $C(a, Q)$ with $Q = P^{\frac{1-\delta}{2(M_S+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$, and $\mathbf{t}_i$ is chosen appropriately, noting the similarity of (111) with (73). The cooperative jamming signals $\mathbf{u}_i^{(2)}, i = 1, 2$ are chosen similarly. Such a selection allows the receiver to decode $\mathbf{v}_i^{(2)}$ and also $\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}$ with vanishing probability of error. Thus, they can be eliminated from the received observation $\mathbf{Y}$.

Thus, we can eliminate $\mathbf{v}_i^{(2)}$ and $\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}$ from $\hat{\mathbf{Y}}$. Noting that $3d \leq N - l$, $\mathbf{v}_i^{(1)} = \left\{v_{ij}, j = 1, \ldots, d\right\}$ can also be decoded to within noise variance from $\mathbf{Y}$. As in (99)-(100),

$$I(\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}; \mathbf{Y}) = \frac{2l}{3}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{112}$$

Also, as in (102), we have

$$I(\mathbf{v}_1^{(1)}, \mathbf{v}_2^{(1)}; \mathbf{Y} | \mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}) \geq 2d\left(\frac{1}{2}\log P\right) + o(\log P) \tag{113}$$

Using (112) and (113), we have

$$\begin{aligned} I(\mathbf{v}_1, \mathbf{v}_2; \mathbf{Y}) &\geq 2\left(d + \frac{l}{3}\right)\left(\frac{1}{2}\log P\right) + o(\log P) && (114) \\ &= \frac{2}{3}N\left(\frac{1}{2}\log P\right) + o(\log P) && (115) \end{aligned}$$

References

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

[2] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[3] M. Nafea and A. Yener, "Secure degrees of freedom for the MIMO wiretap channel with a multiantenna cooperative jammer," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2014, pp. 626–630.

[4] M. Nafea and A. Yener, "Secure degrees of freedom of $N \times N \times M$ wiretap channel with a K-antenna cooperative jammer," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 4169–4174.

[5] A. S. Motahari, S. Oveis-Gharan, M.-A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4799–4810, Aug. 2014.

[6] 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.

[7] 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.

[8] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[9] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[10] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 1014–1021.

[11] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, Mar. 2012.

[12] J. Xie and S. Ulukus, "Secure degrees of freedom regions of multiple access and interference channels: The polytope structure," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 2044–2069, Apr. 2016.

[13] 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. [Online]. Available: http://ieeexplore.ieee.org

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

[15] K. Banawan and S. Ulukus, "Secure degrees of freedom of the Gaussian MIMO interference channel," in *Proc. 49th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2015, pp. 40–44.

[16] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.

[17] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure DoF of the single-antenna MAC," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2010, pp. 2588–2592.

[18] P. Mukherjee, J. Xie, and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1898–1922, Mar. 2017.

[19] A. S. Motahari, S. O. Gharan, and A. K. Khandani. (Aug. 2009). "Real interference alignment with real numbers." [Online]. Available: https://arxiv.org/abs/0908.1208

Pritam Mukherjee received his B. Tech (Hons) with a major in Electronics and Electrical Communication Engineering and a minor in Computer Science and Engineering from Indian Institute of Technology (IIT), Kharagpur in 2010. He obtained a Ph.D in Electrical and Computer Engineering at the University of Maryland, College Park under the guidance of Prof. Sennur Ulukus, in 2016. Currently, he is a postdoctoral researcher in the Electrical Engineering department at Stanford University with Prof. Tsachy Weissman and Prof. Ayfer Ozgur.

He received the Kulkarni Summer Research Fellowship at University of Maryland, College Park, in 2016. His research interests include information theoretic physical layer security and network information theory for wireless networks.

Sennur Ulukus (S'90–M'98–SM'15–F'16) is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received her Ph.D. degree in Electrical and Computer Engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University. Her research interests are in wireless communications, information theory, signal processing, and networks, with recent focus on information theoretic physical layer security, private information retrieval, energy harvesting communications, and wireless energy and information transfer.

Dr. Ulukus is a fellow of the IEEE, and a Distinguished Scholar-Teacher of the University of Maryland. She received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, the 2005 NSF CAREER Award, the 2010–2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 ECE George Corcoran Education Award. She is on the Editorial Board of the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING (2016–). She was an Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS–SERIES ON GREEN COMMUNICATIONS AND NETWORKING (2015–2016), IEEE TRANSACTIONS ON INFORMATION THEORY (2007–2010), and IEEE TRANSACTIONS ON COMMUNICATIONS (2003–2007). She was a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (2015 and 2008), *Journal of Communications and Networks* (2012), and IEEE TRANSACTIONS ON INFORMATION THEORY (2011). She was a general TPC co-chair of 2017 IEEE ISIT, 2016 IEEE Globecom, 2014 IEEE PIMRC, and 2011 IEEE CTW.