Secure Degrees of Freedom of the MIMO Multiple Access Wiretap Channel

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

***Abstract*—We consider a two-user multiple-input multiple-output (MIMO) 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 alignment based achievable schemes and 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.**

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. The channel is fast fading and the channel gains vary in an i.i.d. fashion across the links and 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 eavesdropper.

To that end, we subdivide 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 eavesdropper is sufficiently small ($K \leq \frac{N}{2}$) and the optimal sum s.d.o.f. is limited by the decoding capability of the legitimate receiver.

However, zero-forcing beamforming does not suffice when the number of eavesdropper antennas is above the threshold. In particular, when the transmitters have equal or fewer antennas than the eavesdropper, such zero-forcing beamforming is not feasible. In such cases, we use interference alignment techniques [1] to design our schemes. We borrow ideas from and generalize the optimal alignment scheme presented in [2] for the single-input single-output (SISO) multiple access wiretap channel. While [2] provided schemes based on real interference alignment [3], [4] for fixed channel gains, we present schemes based on vector space alignment [1] for varying channel gains. Nevertheless, our schemes are motivated by and mirror the real alignment scheme in [2] closely, at least when $K = N$. 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 we present a vector space alignment scheme that resembles the real interference alignment schemes for the MIMO wiretap channel with one helper in [5] and the SISO wiretap channel with one helper in [2].

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

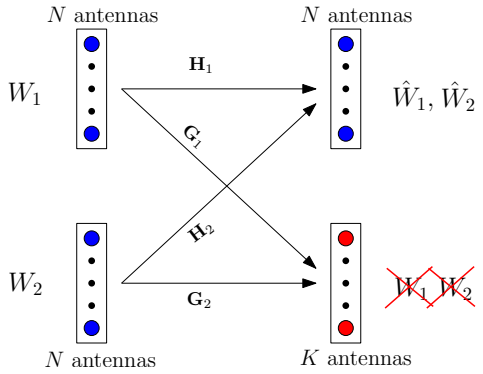

Fig. 1. The MIMO multiple access wiretap channel.

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 [5].

Related Work: The multiple access wiretap channel is introduced by [8], [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 MAC-WT; thus, showing that an alignment based scheme strictly outperforms i.i.d. Gaussian signaling with or without cooperative jamming at high SNR. Finally, references [2], [12] establish the optimal sum s.d.o.f. and the full s.d.o.f. region, respectively, for the SISO multiple access wiretap channel. A related channel model is the wiretap channel with helpers, for which the optimal sum s.d.o.f. is known for the SISO case [2], as well as the the MIMO case [5].

II. System Model

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

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

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

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. The entries of $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are drawn from an arbitrary but fixed continuous distribution with bounded support in an i.i.d. fashion. We assume that the channel matrices $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are known with full precision at all terminals, at time t. 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,

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

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 $d_i = \lim_{P\to\infty} \frac{R_i}{\frac{1}{2}\log P}$. The sum s.d.o.f. is $d_s \triangleq \sup(d_1 + d_2)$, such that (d_1, d_2) is achievable.

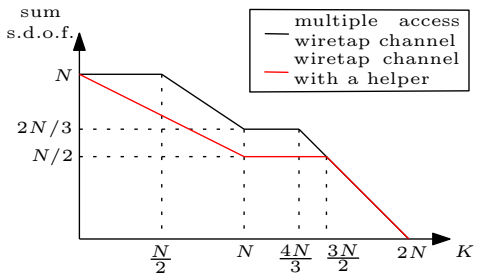

Fig. 2. d_s versus K.

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*

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

We present the converse proof for this theorem in Section IV and the achievable schemes in Section V.

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 [5], 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 between the transmitters does not increase the sum s.d.o.f. in this regime. Heuristically, the eavesdropper is weak in this regime, and the optimal sum s.d.o.f. is limited by the decodability at 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

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,

$$d_1 + d_2 \leq \min((2N-K)^+, N) \tag{5}$$

$$d_1 + d_2 \leq \max\left(\frac{2}{3}(2N-K), \frac{2}{3}N\right) \tag{6}$$

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

It can be verified from Fig. 3 that the minimum of the two bounds in (5)-(6) gives the converse to the sum s.d.o.f. stated in (4) for all ranges of N and K. Thus, we next provide proofs of each of the bounds in (5) and (6).

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

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

We only show that $d_1+d_2 \leq \frac{2}{3}(2N-K)$, when $K \leq N$, and note that the bound $d_1 + d_2 \leq \frac{2}{3}N$ 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 $d_1 + d_2 \leq \frac{2}{3}(2N-K)$ when $K \leq N$, we follow [2], [5]. 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

$$\begin{aligned} n(R_1+R_2) \leq & I(W_1, W_2; \mathbf{Y}^n|\mathbf{Z}^n) + n\epsilon && (7)\\ \leq & h(\mathbf{Y}^n|\mathbf{Z}^n) + nc_1 && (8)\\ = & h(\mathbf{Y}^n, \mathbf{Z}^n) - h(\mathbf{Z}^n) + nc_1 && (9)\\ \leq & h(\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + nc_2 && (10)\\ \leq & h(\tilde{\mathbf{X}}_1^n) + h(\tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + nc_2 && (11) \end{aligned}$$

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 $\mathbf{G}_1 = [\tilde{\mathbf{G}}_1 \quad \hat{\mathbf{G}}_1]$ and $\tilde{\mathbf{X}}_1^T = [\tilde{\mathbf{X}}_{1a}^T \quad \tilde{\mathbf{X}}_{1b}^T]^T$, 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

$$\begin{aligned} h(\mathbf{Z}^n) = h(\tilde{\mathbf{Z}}^n) = & h(\mathbf{G}_1^n\tilde{\mathbf{X}}_1^n + \mathbf{G}_2^n\mathbf{X}_2^n + \mathbf{N}_Z^n) && (12)\\ \geq & h(\mathbf{G}_1^n\tilde{\mathbf{X}}_1^n) && (13)\\ \geq & h(\tilde{\mathbf{G}}_1^n\tilde{\mathbf{X}}_{1a}^n + \hat{\mathbf{G}}_1^n\tilde{\mathbf{X}}_{1b}^n) && (14) \end{aligned}$$

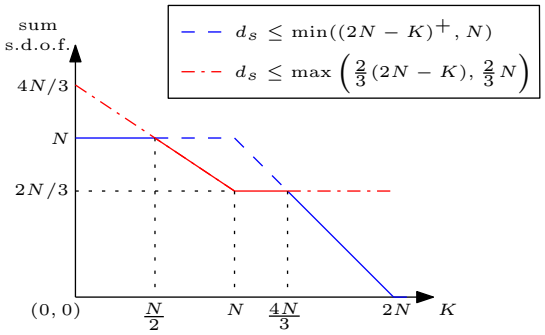

Fig. 3. The two upper bounds.

$$\begin{aligned} \geq & h(\tilde{\mathbf{G}}_1^n\tilde{\mathbf{X}}_{1a}^n|\tilde{\mathbf{X}}_{1b}^n) && (15)\\ = & h(\tilde{\mathbf{X}}_{1a}^n|\tilde{\mathbf{X}}_{1b}^n) + nc_3 && (16) \end{aligned}$$

Using (16) in (11), we have

$$n(R_1+R_2) \leq h(\tilde{\mathbf{X}}_{1b}^n) + h(\tilde{\mathbf{X}}_2^n) + nc_4 \tag{17}$$

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

$$\begin{aligned} nR_1 \leq & I(\mathbf{X}_1^n; \mathbf{Y}^n) && (18)\\ = & h(\mathbf{Y}^n) - h(\mathbf{H}_2^n\mathbf{X}_2^n + \mathbf{N}_1^n) && (19)\\ \leq & h(\mathbf{Y}^n) - h(\tilde{\mathbf{X}}_2^n) + nc_5 && (20) \end{aligned}$$

Adding (17) and (20), we have

$$\begin{aligned} n(2R_1+R_2) \leq & h(\mathbf{Y}^n) + h(\tilde{\mathbf{X}}_{1b}^n) + nc_6 && (21)\\ \leq & N\frac{n}{2}\log P + (N-K)\frac{n}{2}\log P + nc_7 && (22)\\ = & (2N-K)\frac{n}{2}\log P + nc_7 && (23) \end{aligned}$$

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

$$2d_1 + d_2 \leq 2N - K \tag{24}$$

By reversing the roles of the transmitters, we have

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

Combining (24) and (25), we have the required bound

$$d_1 + d_2 \leq \frac{2}{3}(2N-K) \tag{26}$$

This completes the proof of the converse of Theorem 1.

V. Achievable Schemes

We provide achievable schemes for each of the following regimes: *A.* $K \leq N/2$, *B.* $N/2 \leq K \leq N$, *C.* $N \leq K \leq 4N/3$, *D.* $4N/3 \leq K \leq 3N/2$, *E.* $3N/2 \leq K \leq 2N$.

A. $K \leq N/2$

In this regime, the optimal sum s.d.o.f. is N. In our scheme, transmitters 1 and 2 send $(N-K)$ and K independent Gaussian symbols $\mathbf{v}_1 \in \mathbb{R}^{N-K}$, and $\mathbf{v}_2 \in \mathbb{R}^K$, respectively, in one time slot. The entries of $\mathbf{v}_1$ and $\mathbf{v}_2$ are drawn from $\mathcal{N}(0, \bar{P})$, where $\bar{P} = \alpha P$, and α is chosen appropriately to satisfy

the power constraint at the transmitters. 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 channel input at transmitter i is:

$$\mathbf{X}_i = \mathbf{P}_i \mathbf{v}_i \tag{27}$$

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:

$$\mathbf{Y} = [\mathbf{H}_1\mathbf{P}_1 \quad \mathbf{H}_2\mathbf{P}_2] \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{bmatrix} + \mathbf{N}_1 \tag{28}$$

$$\mathbf{Z} = \mathbf{N}_2 \tag{29}$$

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 $\frac{2}{3}(2N-K)$. Thus, 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 $i = 1,2$. Intuitively, transmitter i sends the $(N-K)$ symbols $\tilde{\mathbf{v}}_i(t)$ 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]. Thus, the channel input at transmitter i at time t is:

$$\mathbf{X}_i(t) = \mathbf{G}_i(t)^{\perp}\tilde{\mathbf{v}}_i(t) + \mathbf{P}_i(t)\mathbf{v}_i + \mathbf{H}_i(t)^{-1}\mathbf{Q}(t)\mathbf{u}_i \tag{30}$$

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:

$$\begin{aligned}\mathbf{Y}(t) =& \mathbf{H}_1(t)\mathbf{G}_1(t)^{\perp}\tilde{\mathbf{v}}_1(t) + \mathbf{H}_1(t)\mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{H}_2(t)\mathbf{P}_2(t)\mathbf{v}_2 \\ &+ \mathbf{H}_2(t)\mathbf{G}_2(t)^{\perp}\tilde{\mathbf{v}}_2(t) + \mathbf{Q}(t)(\mathbf{u}_1+\mathbf{u}_2)\end{aligned} \tag{31}$$

$$\begin{aligned}\mathbf{Z}(t) =& \mathbf{G}_1(t)\mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{G}_2(t)\mathbf{H}_2(t)^{-1}\mathbf{Q}(t)\mathbf{u}_2 \\ &+ \mathbf{G}_2(t)\mathbf{P}_2(t)\mathbf{v}_2 + \mathbf{G}_1(t)\mathbf{H}_1(t)^{-1}\mathbf{Q}(t)\mathbf{u}_1\end{aligned} \tag{32}$$

where we have dropped the Gaussian noise at high SNR. We now choose $\mathbf{Q}(t)$ to be any $N \times (2K-N)$ matrix with full column rank, and choose

$$\mathbf{P}_i(t) = \mathbf{G}_i(t)^T(\mathbf{G}_i(t)\mathbf{G}_i(t)^T)^{-1}(\mathbf{G}_j(t)\mathbf{H}_j(t)^{-1})\mathbf{Q}(t) \tag{33}$$

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 $\left\{\tilde{\mathbf{v}}_i(t) \in \mathbb{R}^{N-K}, t \in \{1,2,3\}, \mathbf{v}_i \in \mathbb{R}^{2K-N}, i = 1,2\right\}$ and the aligned artificial noise symbols $\mathbf{u}_1 + \mathbf{u}_2 \in \mathbb{R}^{2K-N}$, i.e., $6(N-K) + 3(2N-K) = 3N$ symbols using $3N$ observations in 3 time slots.

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. Transmitter i sends:

$$\mathbf{X}_i(t) = \mathbf{P}_i(t)\mathbf{v}_i + \mathbf{H}_i(t)^{-1}\mathbf{Q}(t)\mathbf{u}_i \tag{34}$$

where the $\mathbf{P}_1(t)$, $\mathbf{Q}(t)$, and $\mathbf{P}_2(t)$ are $N \times N$ precoding matrices to be designed. Let us define $\tilde{\mathbf{P}}_i \triangleq \left[\mathbf{P}_i(1)^T \quad \mathbf{P}_i(2)^T \quad \mathbf{P}_i(3)^T\right]^T$ and $\tilde{\mathbf{Q}}$ similarly. Further, let

$$\tilde{\mathbf{H}}_i \triangleq \begin{bmatrix} \mathbf{H}_i(1) & \mathbf{0}_{N\times N} & \mathbf{0}_{N\times N} \\ \mathbf{0}_{N\times N} & \mathbf{H}_i(2) & \mathbf{0}_{N\times N} \\ \mathbf{0}_{N\times N} & \mathbf{0}_{N\times N} & \mathbf{H}_i(3) \end{bmatrix} \tag{35}$$

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

$$\tilde{\mathbf{Y}} = \tilde{\mathbf{H}}_1\tilde{\mathbf{P}}_1\mathbf{v}_1 + \tilde{\mathbf{H}}_2\tilde{\mathbf{P}}_2\mathbf{v}_2 + \mathbf{Q}(\mathbf{u}_1+\mathbf{u}_2) \tag{36}$$

$$\tilde{\mathbf{Z}} = \tilde{\mathbf{G}}_1\tilde{\mathbf{P}}_1\mathbf{v}_1 + \tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1}\mathbf{Q}\mathbf{u}_2 + \tilde{\mathbf{G}}_2\tilde{\mathbf{P}}_2\mathbf{v}_2 + \tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1}\mathbf{Q}\mathbf{u}_1 \tag{37}$$

where $\tilde{\mathbf{Y}} \triangleq [\mathbf{Y}(1)^T \quad \mathbf{Y}(2)^T \quad \mathbf{Y}(2)^T]^T$, and $\tilde{\mathbf{Z}}$ is defined similarly. To ensure secrecy, we impose

$$\tilde{\mathbf{G}}_1\tilde{\mathbf{P}}_1 = \tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1}\mathbf{Q} \tag{38}$$

$$\tilde{\mathbf{G}}_2\tilde{\mathbf{P}}_2 = \tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1}\mathbf{Q} \tag{39}$$

We rewrite the conditions in (38)-(39) as

$$\mathbf{\Psi}\left[\tilde{\mathbf{P}}_1^T \quad \tilde{\mathbf{P}}_2^T \quad \mathbf{Q}^T\right]^T = \mathbf{0}_{6K\times N} \tag{40}$$

where

$$\mathbf{\Psi} \triangleq \begin{bmatrix} \tilde{\mathbf{G}}_1 & \mathbf{0}_{3K\times 3N} & \tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1} \\ \mathbf{0}_{3K\times 3N} & \tilde{\mathbf{G}}_2 & \tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1} \end{bmatrix} \tag{41}$$

Note that $\mathbf{\Psi}$ 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 $\mathbf{\Psi}$. 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

$$\tilde{\mathbf{Y}} = \mathbf{\Gamma}\left[\mathbf{v}_1^T \quad \mathbf{v}_2^T \quad (\mathbf{u}_1+\mathbf{u}_2)^T\right]^T \tag{42}$$

where $\mathbf{\Gamma} \triangleq [\tilde{\mathbf{H}}_1\tilde{\mathbf{P}}_1 \quad \tilde{\mathbf{H}}_2\tilde{\mathbf{P}}_2 \quad \mathbf{Q}]$. We note that $\mathbf{\Gamma}$ 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 transmitters send

$$\mathbf{X}_1 = \mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 \tag{43}$$

$$\mathbf{X}_2 = \mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{P}_2\mathbf{v}_2 + \mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 \tag{44}$$

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 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

$$\begin{aligned}\mathbf{Y} =&\mathbf{H}_1\mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{H}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{H}_2\mathbf{R}_2\tilde{\mathbf{u}} \\ &+ \mathbf{Q}(\mathbf{u}_1 + \mathbf{u}_2)\end{aligned} \tag{45}$$

$$\begin{aligned}\mathbf{Z} =&\mathbf{G}_1\mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{G}_2\mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{G}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 \\ &+ \mathbf{G}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1\end{aligned} \tag{46}$$

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

$$\mathbf{G}_1\mathbf{R}_1 = \mathbf{G}_2\mathbf{R}_2 \tag{47}$$

$$\mathbf{G}_1\mathbf{P}_1 = \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q} \tag{48}$$

$$\mathbf{G}_2\mathbf{P}_2 = \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q} \tag{49}$$

To satisfy (47), 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 (48)-(49), 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 $\mathbf{\Lambda}$ given by

$$\mathbf{\Lambda} \triangleq \begin{bmatrix} \mathbf{G}_1 & \mathbf{0}_{K\times N} & -\mathbf{G}_2\mathbf{H}_2^{-1} \\ \mathbf{0}_{K\times N} & \mathbf{G}_2 & -\mathbf{G}_1\mathbf{H}_1^{-1} \end{bmatrix} \tag{50}$$

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

$$\mathbf{Y} = \mathbf{\Phi}\begin{bmatrix}\tilde{\mathbf{v}}^T & \mathbf{v}_1^T & \mathbf{v}_2^T & \tilde{\mathbf{u}}^T & (\mathbf{u}_1+\mathbf{u}_2)^T\end{bmatrix}^T \tag{51}$$

where $\mathbf{\Phi}$ is the $N \times N$ matrix defined as

$$\mathbf{\Phi} = [\mathbf{H}_1\mathbf{R}_1 \quad \mathbf{H}_1\mathbf{P}_1 \quad \mathbf{H}_2\mathbf{P}_2 \quad \mathbf{H}_2\mathbf{R}_2 \quad \mathbf{Q}] \tag{52}$$

Since $\mathbf{\Phi}$ is full rank almost surely, the legitimate receiver can decode the symbols $\tilde{\mathbf{v}}, \mathbf{v}_1$, and $\mathbf{v}_2$ to within noise variance.

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. Therefore, we can treat the multiple access wiretap channel as a helper channel by assigning a zero rate to one of the users, and achieve the optimal sum s.d.o.f. using [5]. We present the scheme here for completeness.

In order to achieve the optimal sum s.d.o.f. of $2N-K$ in this regime, the first transmitter sends $2N-K$ Gaussian independent 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

$$\mathbf{X}_1 = \mathbf{P}\mathbf{v} \tag{53}$$

$$\mathbf{X}_2 = \mathbf{Q}\mathbf{u} \tag{54}$$

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

$$\mathbf{Y} = \mathbf{H}_1\mathbf{P}\mathbf{v} + \mathbf{H}_2\mathbf{Q}\mathbf{u} \tag{55}$$

$$\mathbf{Z} = \mathbf{G}_1\mathbf{P}\mathbf{v} + \mathbf{G}_2\mathbf{Q}\mathbf{u} \tag{56}$$

To ensure security, we wish to ensure that $\mathbf{G}_1\mathbf{P} = \mathbf{G}_2\mathbf{Q}$ 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 fading 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 as well as matching converses to establish the optimality of the achievable schemes. The achievable schemes provided in this paper assume time-varying channel gains, and are *multi-block schemes* in nature, in general. In [13], we provide the optimum (*single-block*) achievable schemes for fixed channel gains.

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] A. S. Motahari, S. Oveis-Gharan, and A. K. Khandani. Real interference alignment with real numbers. *IEEE Trans. on Inf. Theory*, submitted Aug. 2009. Also available at [arXiv:0908.1208].

[4] 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. on Inf. Theory*, 60(8):4799–4810, Aug. 2014.

[5] 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.

[6] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. on Inf. Theory*, 57(8):4961–4972, Aug. 2011.

[7] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas - Part II: The MIMOME wiretap channel. *IEEE Trans. on Inf. Theory*, 56(11):5515–5532, Nov. 2010.

[8] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. on Inf. Theory*, 54(12):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. on Inf. Theory*, 54(6):2735–2751, Jun. 2008.

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

[11] R. Bassily and S. Ulukus. Ergodic secret alignment. *IEEE Trans. on Inf. Theory*, 58(3):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. on Inf. Theory*. To appear. Also available at [arXiv:1404.7478].

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