Real Interference Alignment for 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.) when the channel gains are fixed for the duration of the communication. We provide optimal achievable schemes based on a combination of Gaussian signaling and real interference alignment for all regimes of N and K.**

I. Introduction

We consider the two-user $N \times N \times N \times K$ 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 gains are drawn from a continuous distribution prior to the start of the communication and then remain fixed for the duration of the communication. When the channel gains are fading, the optimal sum secure degrees of freedom (s.d.o.f.) of this channel is established in [1]. The optimal achievable schemes presented in [1] exploit the channel variations over multiple time slots. These schemes do not extend to channels with fixed gains. In this paper, we present new achievable schemes for the case of fixed channel gains based on a combination of real interference alignment and Gaussian signaling, which achieve the optimal sum s.d.o.f.

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, Gaussian signaling and real interference alignment techniques [2], [3]. 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 antennas is sufficiently small ($K \leq \frac{N}{2}$) and the optimal scheme is Gaussian signaling in the nullspace of the eavesdropper channel.

When the number of eavesdropper antennas $K \geq \frac{N}{2}$, the optimal scheme either uses Gaussian signaling alone or combined with real interference alignment techniques. In the regime $\frac{N}{2} \leq K \leq \frac{4N}{3}$, the optimal sum s.d.o.f. is 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 suffices. However, when $l \neq 0$, the s.d.o.f. has a fractional part, and Gaussian signaling alone is not optimal. This is also observed in the achievable schemes in [4], [5] 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, references [4], [5] 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, 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.

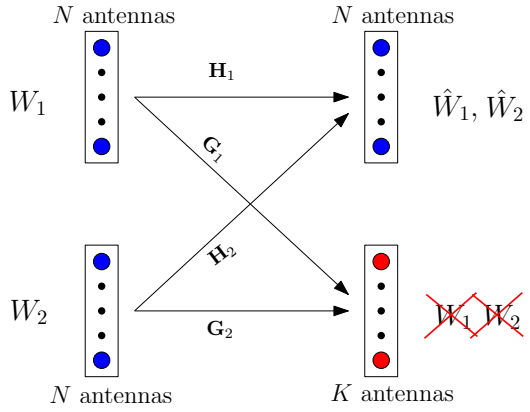

Fig. 1. The MIMO multiple access wiretap channel.

In this paper, we consider real channel gains. In order to handle the fractional s.d.o.f., 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 presented in [1]. 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 [6]. 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

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

alignment [3] 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 the Gaussian signaling suffices. In fact, the schemes presented in [1] for fading channel gains can also be used and are optimal. When $K \geq \frac{3N}{2}$, the multiple access wiretap channel reduces to a wiretap channel with one helper and the scheme in [5] for the wiretap channel with one helper is optimal here.

The main contribution of this paper is the achievable scheme based on asymptotic real interference alignment for the $2 \times 2 \times 2 \times 2$ multiple access wiretap channel. To the best of our knowledge, this is the first scheme which uses *asymptotic* alignment for the multiple access channel. Further, we show how to use real interference alignment based structured signaling in conjunction with Gaussian signaling to achieve the optimal sum s.d.o.f. with fixed real channel gains.

Related Work: The multiple access wiretap channel is introduced by [7], [8], where the technique of cooperative jamming is introduced to improve the rates achievable with Gaussian signaling. Reference [9] 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 [7]–[9] all yield zero s.d.o.f. Reference [10] 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 [6], [11] 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. Reference [1] determines the optimal sum s.d.o.f. of the $N \times N \times N \times K$ MIMO multiple access wiretap channel with fading channel gains. 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 [6] and [4], [5], and in [12] and [13], respectively.

II. System Model

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

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

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

where $\mathbf{X}_i$ is an N dimensional column vector denoting the ith user's channel input, $\mathbf{Y}$ is an N dimensional vector denoting the legitimate receiver's channel output, and $\mathbf{Z}$ is a K dimensional vector denoting the eavesdropper's channel output. In addition, $\mathbf{N}_1$ and $\mathbf{N}_2$ 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, $\mathbf{H}_i$ and $\mathbf{G}_i$ are the $N \times N$ and $K \times N$ channel matrices from transmitter i to the legitimate receiver and the eavesdropper, respectively. 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 prior to the start of communication and remain fixed for the duration of communication. We assume that the channel matrices $\mathbf{H}_i$ and $\mathbf{G}_i$ are known with full precision at all terminals. All channel inputs satisfy the average power constraint $E[\|\mathbf{X}_i\|^2] \leq P,\ i = 1, 2$, where $\|\mathbf{X}\|$ denotes the Euclidean (or the spectral norm) of the vector (or matrix) $\mathbf{X}$.

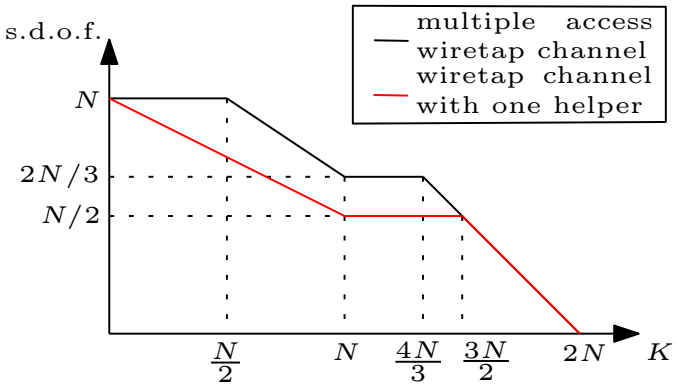

Fig. 2. d_s versus K.

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, $\Pr[W_i \neq \hat{W}_i] \to 0$, for $i = 1, 2$, and the secrecy constraint, namely,

$$\frac{1}{n} I(W_1, W_2; \mathbf{Z}^n) \to 0 \quad (3)$$

as $n \to \infty$. An s.d.o.f. pair (d_1, d_2) is 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.

III. Main Result

In this paper, we determine the optimal sum s.d.o.f. of the MIMO multiple access wiretap channel with fixed channel gains, stated in 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*

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

for almost all channel gains.

The converse proof for this theorem is the same as the one presented in [1] for the fading channel case and is omitted

here. We note that optimal achievable schemes for the fading channel gains are also presented in [1]. However, in some regimes of N and K, the optimal schemes for fading channel gains cannot be used with fixed channel gains. Here, we present optimal achievable schemes for fixed channel gains, showing that the sum s.d.o.f. in Theorem 1 is achievable, thereby settling the optimal sum s.d.of. for the MIMO multiple access wiretap channel with fixed channel gains.

Fig. 2 shows the variation of the optimal sum s.d.o.f. with the number of eavesdropper antennas K. Note that 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 same as the optimal s.d.o.f. of the wiretap channel with helpers.

IV. Achievable Schemes for Fixed Channel Gains

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, which can be achieved by Gaussian signaling orthogonal to the eavesdropper's channel. The scheme, also presented in [1] for fading channel gains, is the following: Transmitter 1 sends $(N-K)$ independent Gaussian symbols along $(N-K)$ directions that span the $(N-K)$ dimensional nullspace of the eavesdropper's channel $\mathbf{G}_i$, while transmitter 2 sends K independent Gaussian symbols in directions that are orthogonal to the eavesdropper's channel; this can be done since $K \leq N-K$ in this regime. The security is guaranteed since the symbols are not received at the eavesdropper. Since the legitimate receiver has N antennas, it can decode the total of N Gaussian symbols to within noise distortion. Thus, the sum s.d.o.f. of N is achieved.

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

The optimal sum s.d.o.f. in this regime is $\frac{2}{3}(2N-K)$. Note that the schemes presented in [1] for this regime with fading channel gains exploit the diversity of channel gains over three time slots; thus, those schemes cannot be used in the fixed channel gains case. Therefore, we now propose new achievable schemes for this regime. Our schemes are based on real interference alignment [2], [3]. We first present a scheme for the $2 \times 2 \times 2 \times 2$ system, which will be later used for general achievable scheme.

1) 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 $M \triangleq m^{\Gamma}$, where Γ will be specified later. The channel inputs are given by

$$\mathbf{X}_1 = \mathbf{G}_1^{-1}\mathbf{G}_2\mathbf{H}_2^{-1}\begin{pmatrix} \mathbf{t}_1^T\mathbf{v}_{11} \\ \mathbf{t}_2\mathbf{v}_{12} \end{pmatrix} + \mathbf{H}_1^{-1}\begin{pmatrix} \mathbf{t}_1^T\mathbf{u}_{11} \\ \mathbf{t}_2\mathbf{u}_{12} \end{pmatrix} \quad (5)$$

$$\mathbf{X}_2 = \mathbf{G}_2^{-1}\mathbf{G}_1\mathbf{H}_1^{-1}\begin{pmatrix} \mathbf{t}_1^T\mathbf{v}_{21} \\ \mathbf{t}_2\mathbf{v}_{22} \end{pmatrix} + \mathbf{H}_2^{-1}\begin{pmatrix} \mathbf{t}_1^T\mathbf{u}_{21} \\ \mathbf{t}_2\mathbf{u}_{22} \end{pmatrix} \quad (6)$$

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

$$C(a,Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \quad (7)$$

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

$$\begin{aligned}\mathbf{Y} =& \mathbf{A}\begin{pmatrix} \mathbf{t}_1^T\mathbf{v}_{11} \\ \mathbf{t}_2\mathbf{v}_{12} \end{pmatrix} + \mathbf{B}\begin{pmatrix} \mathbf{t}_1^T\mathbf{v}_{21} \\ \mathbf{t}_2\mathbf{v}_{22} \end{pmatrix} \\ &+ \begin{pmatrix} \mathbf{t}_1^T(\mathbf{u}_{11}+\mathbf{u}_{21}) \\ \mathbf{t}_2(\mathbf{u}_{12}+\mathbf{u}_{22}) \end{pmatrix} + \mathbf{N}_1 \quad (8)\\ \mathbf{Z} =& \mathbf{G}_1\mathbf{H}_1^{-1}\begin{pmatrix} \mathbf{t}_1^T(\mathbf{u}_{11}+\mathbf{v}_{21}) \\ \mathbf{t}_2(\mathbf{u}_{12}+\mathbf{v}_{22}) \end{pmatrix} \\ &+ \mathbf{G}_2\mathbf{H}_2^{-1}\begin{pmatrix} \mathbf{t}_1^T(\mathbf{u}_{21}+\mathbf{v}_{11}) \\ \mathbf{t}_2(\mathbf{u}_{22}+\mathbf{v}_{12}) \end{pmatrix} + \mathbf{N}_2 \quad (9)\end{aligned}$$

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

$$\begin{pmatrix} \mathbf{t}_2^T(a_{12}\mathbf{v}_{12} + b_{12}\mathbf{v}_{22}) + \mathbf{t}_1^T(a_{11}\mathbf{v}_{11} + b_{11}\mathbf{v}_{21} + \sum_{i=1}^{2}\mathbf{u}_{i1}) \\ \mathbf{t}_1^T(a_{21}\mathbf{v}_{11} + b_{21}\mathbf{v}_{21}) + \mathbf{t}_2^T(a_{22}\mathbf{v}_{12} + b_{22}\mathbf{v}_{22} + \sum_{i=1}^{2}\mathbf{u}_{i2}) \end{pmatrix} \quad (10)$$

We define

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

$$T_2 = \{a_{22}^{r_1}b_{22}^{r_2}, r_i \in \{0,\ldots,m-1\}\} \quad (12)$$

Letting $\Gamma = 2$, we note that

$$|T_1| = |T_2| = M \quad (13)$$

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. Also, the elements of T_i can be verified to be rationally independent of the elements of T_j, if $i \neq j$. 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,

$$\tilde{T}_1 = \{a_{11}^{r_1}b_{11}^{r_2}, r_i \in \{0,\ldots,m\}\} \quad (14)$$

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. Note that the elements of $a_{12}T_2$ and $b_{12}T_2$ are rationally independent and thus, $\mathbf{v}_{12}$ and $\mathbf{v}_{22}$ occupy separate rational dimensions. Also they are separate from the interference space $\tilde{T}_1$. 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 Similarly, we can define

$$\tilde{T}_2 = \{a_{22}^{r_1} b_{22}^{r_2}, r_i \in \{0, \ldots, m\}\} \tag{15}$$

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 [14]

$$\sup \sum_{i=1}^{2} R_i \geq I(\mathbf{V}; \mathbf{Y}) - I(\mathbf{V}; \mathbf{Z}) \tag{16}$$

where $\mathbf{V} \triangleq \{\mathbf{v}_{ij}, i, j \in \{1, 2\}\}$. In order to bound the term $I(\mathbf{V}; \mathbf{Y})$, we first bound the probability of error. Let $M_S \triangleq 2m^2 + (m+1)^2$ be the number of rational dimensions at each receiver antenna. Also let $\mathbf{V}_i = \{\mathbf{v}_{kj}, k = 1, 2; j \neq i\}$ be the desired symbols at the ith antenna of the receiver. In order to decode, the receiver makes an estimate $\hat{V}_i$ 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 $\mathbf{V} = \{\mathbf{V}_i, i = 1, 2\}$,

$$\Pr(\mathbf{V} \neq \hat{\mathbf{V}}) \leq 2 \exp\left(-\eta_\gamma P^\delta\right) \tag{17}$$

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

$$\begin{aligned}
I(\mathbf{V}; \mathbf{Y}) &= H(\mathbf{V}) - H(\mathbf{V}|\hat{\mathbf{V}}) && (18)\\
&\geq \log(|\mathcal{V}|) - 1 - \Pr(\mathbf{V} \neq \hat{\mathbf{V}}) \log(|\mathcal{V}|) && (19)\\
&= \log(|\mathcal{V}|) - o(\log P) && (20)\\
&= \frac{4M(1-\delta)}{M_S + \delta} \left(\frac{1}{2} \log P\right) + o(\log P) && (21)
\end{aligned}$$

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

$$I(\mathbf{V}; \mathbf{Z}) \leq I\left(\{\mathbf{v}_{ij}, i, j = 1, 2\}; \left\{\mathbf{v}_{ij} + \mathbf{u}_{\hat{i}j}, \begin{array}{c} \hat{i} \neq i, \\ i, j = 1, 2 \end{array}\right\}\right) \tag{22}$$

$$\leq \sum_{i,j=1,\hat{i}\neq i}^{2} H(\mathbf{v}_{ij} + \mathbf{u}_{\hat{i}j}) - H(\mathbf{u}_{\hat{i}j}) \tag{23}$$

$$\leq 4M \log(4Q+1) - 4M \log(2Q+1) \tag{24}$$

$$\leq 4M = o(\log P) \tag{25}$$

Using (21) and (25) in (16), we have

$$\sup \sum_{i=1}^{2} R_i \geq \frac{4M(1-\delta)}{M_S + \delta} \left(\frac{1}{2} \log P\right) + o(\log P) \tag{26}$$

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

2) The General Scheme: We use structured PAM signaling along with Gaussian signaling. Let $d = \lfloor \frac{2K-N}{3} \rfloor$, and $l = (2K - N) \bmod 3 = (2N - K) \bmod 3$. Let $\mathbf{v}_i^{(1)} = \{v_{ij}, j = 1, \ldots, d\}$, 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 $\tilde{\mathbf{v}}_i = \{\tilde{v}_{ij}, j = 1, \ldots, N-K\}$ denote the symbols that can be transmitted securely by beamforming orthogonal to the eavesdropper channel. Transmitter i sends:

$$\mathbf{X}_i = \mathbf{G}_i^\perp \tilde{\mathbf{v}}_i + \mathbf{P}_i \mathbf{v}_i + \mathbf{H}_i^{-1} \mathbf{Q} \mathbf{u}_i \tag{27}$$

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 $\mathbf{u}_i^{(1)} = \{u_{ij}, j = 1, \ldots, d\}$ 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:

$$\begin{aligned}
\mathbf{Y} =& \mathbf{H}_1 \mathbf{G}_1^\perp \tilde{\mathbf{v}}_1 + \mathbf{H}_1 \mathbf{P}_1 \mathbf{v}_1 + \mathbf{H}_2 \mathbf{P}_2 \mathbf{v}_2 \\
&+ \mathbf{H}_2 \mathbf{G}_2^\perp \tilde{\mathbf{v}}_2 + \mathbf{Q}(\mathbf{u}_1 + \mathbf{u}_2) + \mathbf{N}_1 && (28)\\
\mathbf{Z} =& \mathbf{G}_1 \mathbf{P}_1 \mathbf{v}_1 + \mathbf{G}_2 \mathbf{H}_2^{-1} \mathbf{Q} \mathbf{u}_2 \\
&+ \mathbf{G}_2 \mathbf{P}_2 \mathbf{v}_2 + \mathbf{G}_1 \mathbf{H}_1^{-1} \mathbf{Q} \mathbf{u}_1 + \mathbf{N}_2 && (29)
\end{aligned}$$

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 $\mathbf{F}^T = [\mathbf{H}_1 \mathbf{G}_1^\perp \quad \mathbf{H}_2 \mathbf{G}_2^\perp \quad \mathbf{H}_1 \mathbf{P}_1^{(1)} \quad \mathbf{H}_1 \mathbf{P}_1^{(1)} \quad \mathbf{Q}^{(1)}]^T$. 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

$$\mathbf{E} = \begin{pmatrix} \mathbf{D}_{l \times N} \\ \mathbf{I}_{N-l} \quad \mathbf{0}_{(N-l) \times l} \end{pmatrix} \tag{30}$$

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

$$\begin{aligned}
\tilde{\mathbf{Y}} =& \mathbf{D} \mathbf{H}_1 \mathbf{P}_1^{(2)} \mathbf{v}_1^{(2)} + \mathbf{D} \mathbf{H}_2 \mathbf{P}_2^{(2)} \mathbf{v}_2^{(2)} \\
&+ (\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}) + \mathbf{D} \mathbf{N}_1 && (31)
\end{aligned}$$

Note that (31) 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 (31) with (8). 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 $2(N-K)+3d \le N-l$, $\tilde{\mathbf{v}}_i$ and $\mathbf{v}_i^{(1)}$ can also be decoded from $\tilde{\mathbf{Y}}$. We compute

$$\begin{aligned} I(\mathbf{v}_1,\mathbf{v}_2,\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2;\mathbf{Y}) =& I(\mathbf{v}_1^{(1)},\mathbf{v}_2^{(1)},\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2;\mathbf{Y}|\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)}) \\ &+ I(\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)};\mathbf{Y}) \end{aligned} \tag{32}$$

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

$$\begin{aligned} I(\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)};\mathbf{Y}) =& \log(2Q+1)^2 + o(\log P) && (33)\\ =& 2\frac{1-\delta}{(3+\delta)}\left(\frac{1}{2}\log P\right) + o(\log P) && (34) \end{aligned}$$

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

$$I(\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)};\mathbf{Y}) = \frac{4M(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{35}$$

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

$$I(\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)};\mathbf{Y}) = \frac{2l}{3}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{36}$$

Noting that $\mathbf{v}_1^{(1)},\mathbf{v}_2^{(1)},\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2$ can be decoded to within noise variation from $\mathbf{Y}$, given $\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)}$, the first term of (32) is

$$\begin{aligned} I(\mathbf{v}_1^{(1)},\mathbf{v}_2^{(1)},\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2;\mathbf{Y}|\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)}) \ge& 2(d+N-K)\left(\frac{1}{2}\log P\right) \\ &+ o(\log P) \end{aligned} \tag{37}$$

Using (36) and (37) in (32), we have,

$$\begin{aligned} I(\mathbf{v}_1,\mathbf{v}_2,\tilde{\mathbf{v}}_1,\tilde{\mathbf{v}}_2;\mathbf{Y}) \ge& 2\left(d+N-K+\frac{l}{3}\right)\left(\frac{1}{2}\log P\right) \\ &+ o(\log P) && (38)\\ =& \frac{2}{3}(2N-K)\left(\frac{1}{2}\log P\right) + o(\log P) && (39) \end{aligned}$$

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

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

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 $\mathbf{v}_i^{(1)} = \{v_{ij}, j=1,\ldots,d\}$ are drawn in an i.i.d. fashion $\sim \mathcal{N}(0,\alpha P)$, and the entries of $\mathbf{v}_i^{(2)} = \{v_{ij}, j=d+1,\ldots,d+l\}$ 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 $\mathbf{u}_i^{(1)} = \{u_{ij}, j=1,\ldots,d\}$ are drawn in an i.i.d. fashion $\sim \mathcal{N}(0,\alpha P)$, and the entries of $\mathbf{u}_i^{(2)} = \{u_{ij}, j=d+1,\ldots,d+l\}$ are structured PAM signals independent of $\mathbf{v}_j, j=1,2$ and $\mathbf{u}_j, j\neq i$. Transmitter i sends

$$\mathbf{X}_i = \mathbf{P}_i\mathbf{v}_i + \mathbf{H}_i^{-1}\mathbf{Q}\mathbf{u}_i \tag{40}$$

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

$$\mathbf{Y} = \mathbf{H}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{Q}(\mathbf{u}_1+\mathbf{u}_2) + \mathbf{N}_1 \tag{41}$$

$$\begin{aligned} \mathbf{Z} =& \mathbf{G}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 \\ &+ \mathbf{G}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 + \mathbf{N}_2 \end{aligned} \tag{42}$$

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

$$\mathbf{G}_i\mathbf{P}_i = \mathbf{G}_j\mathbf{H}_j^{-1}\mathbf{Q} \tag{43}$$

We rewrite the conditions in (43) as

$$\mathbf{\Psi}\begin{bmatrix} \mathbf{P}_1^T & \mathbf{P}_2^T & \mathbf{Q}^T \end{bmatrix}^T = \mathbf{0}_{2K\times(d+l)} \tag{44}$$

where

$$\mathbf{\Psi} \triangleq \begin{bmatrix} \mathbf{G}_1 & \mathbf{0}_{K\times N} & -\mathbf{G}_2\mathbf{H}_2^{-1} \\ \mathbf{0}_{K\times N} & \mathbf{G}_2 & -\mathbf{G}_1\mathbf{H}_1^{-1} \end{bmatrix} \tag{45}$$

Note that $\mathbf{\Psi}$ has a nullity $3N-2K$. This alignment is feasible if $3N-2K \ge d+l$, i.e., if $K \le 4d+l$. This is satisfied since, in this regime, $K \le 4d+l+\frac{1}{3}l$, which implies $K \le 4d+1$ for integers N and K, since $0 \le l \le 2$. 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 $\mathbf{F}^T = [\mathbf{H}_1\mathbf{P}_1^{(1)} \quad \mathbf{H}_1\mathbf{P}_1^{(1)} \quad \mathbf{Q}^{(1)}]^T$. 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 (30). We have

$$\begin{aligned} \tilde{\mathbf{Y}} =& \mathbf{D}\mathbf{H}_1\mathbf{P}_1^{(2)}\mathbf{v}_1^{(2)} + \mathbf{D}\mathbf{H}_2\mathbf{P}_2^{(2)}\mathbf{v}_2^{(2)} \\ &+ (\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}) + \mathbf{D}\mathbf{N}_1 \end{aligned} \tag{46}$$

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 proba-

bility 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 (46) with (8). 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 $3d\leq N-l$, $\mathbf{v}_i^{(1)}=\{v_{ij}, j=1,\ldots,d\}$ can also be decoded to within noise variation from $\mathbf{Y}$. As in (34)-(35),

$$I(\mathbf{v}_1^{(2)},\mathbf{v}_2^{(2)};\mathbf{Y})=\frac{2l}{3}\left(\frac{1}{2}\log P\right)+o(\log P) \tag{47}$$

Also, as in (37), we have

$$I(\mathbf{v}_1^{(1)},\mathbf{v}_2^{(1)};\mathbf{Y}|\mathbf{v}_1^{(2)},v_2^{(2)})\geq 2d\left(\frac{1}{2}\log P\right)+o(\log P) \tag{48}$$

Using (47) and (48), we have

$$I(\mathbf{v}_1,\mathbf{v}_2;\mathbf{Y})\geq 2\left(d+\frac{l}{3}\right)\left(\frac{1}{2}\log P\right)+o(\log P) \tag{49}$$

$$=\frac{2}{3}N\left(\frac{1}{2}\log P\right)+o(\log P) \tag{50}$$

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

The optimal s.d.o.f. in this regime is $2N-K$. Gaussian signaling suffices in this case. 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 $\left\{\mathbf{v}_2\in\mathbb{R}^{3N-2K}\right\}$. The transmitted signals are

$$\mathbf{X}_1=\mathbf{R}_1\tilde{\mathbf{v}}+\mathbf{P}_1\mathbf{v}_1+\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 \tag{51}$$

$$\mathbf{X}_2=\mathbf{R}_2\tilde{\mathbf{u}}+\mathbf{P}_2\mathbf{v}_2+\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 \tag{52}$$

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 i.i.d. $\sim\mathcal{N}(0,\alpha P)$. 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

$$\begin{aligned}\mathbf{Y}=&\mathbf{H}_1\mathbf{R}_1\tilde{\mathbf{v}}+\mathbf{H}_1\mathbf{P}_1\mathbf{v}_1+\mathbf{H}_2\mathbf{P}_2\mathbf{v}_2+\mathbf{H}_2\mathbf{R}_2\tilde{\mathbf{u}}\\&+\mathbf{Q}(\mathbf{u}_1+\mathbf{u}_2)\end{aligned} \tag{53}$$

$$\begin{aligned}\mathbf{Z}=&\mathbf{G}_1\mathbf{R}_1\tilde{\mathbf{v}}+\mathbf{G}_2\mathbf{R}_2\tilde{\mathbf{u}}+\mathbf{G}_1\mathbf{P}_1\mathbf{v}_1+\mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2\\&+\mathbf{G}_2\mathbf{P}_2\mathbf{v}_2+\mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1\end{aligned} \tag{54}$$

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

$$\mathbf{G}_1\mathbf{R}_1=\mathbf{G}_2\mathbf{R}_2 \tag{55}$$

$$\mathbf{G}_i\mathbf{P}_i=\mathbf{G}_j\mathbf{H}_j^{-1}\mathbf{Q} \tag{56}$$

for $i\neq j$. We can satisfy (56) as in (43). To satisfy (55), 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 see the decodablity, we can rewrite the observation at the legitimate receiver as $\mathbf{Y}=\mathbf{\Phi}[\tilde{\mathbf{v}}^T,\mathbf{v}_1^T,\mathbf{v}_2^T,\tilde{\mathbf{u}}^T,(\mathbf{u}_1+\mathbf{u}_2)^T]^T$ where $\mathbf{\Phi}$ is the $N\times N$ matrix defined as $\mathbf{\Phi}\triangleq[\mathbf{H}_1\mathbf{R}_1\quad\mathbf{H}_1\mathbf{P}_1\quad\mathbf{H}_2\mathbf{P}_2\quad\mathbf{H}_2\mathbf{R}_2\quad\mathbf{Q}]$. Since $\mathbf{\Phi}$ 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. 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].

V. 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, with fixed real channel gains. We provided optimal schemes that use real alignment based techniques in conjunction with Gaussian signaling. In particular, we provided a scheme based on asymptotic real interference alignment for the multiple access wiretap channel with two antennas at each terminal. This is the first instance where asymptotic alignment is needed and used for the multiple access wiretap channel.

References

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

[2] 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].

[3] 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.

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

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

[6] 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.

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

[8] 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.

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

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

[11] J. Xie and S. Ulukus. Secure degrees of freedom region of the Gaussian multiple access wiretap channel. In *Asilomar Conf.*, Nov. 2013.

[12] J. Xie and S. Ulukus. Secure degrees of freedom of K-user Gaussian interference channels: A unified view. *IEEE Trans. on Inf. Theory*, 61(5):2647–2661, May 2015.

[13] K. Banawan and S. Ulukus. Secure degrees of freedom of the Gaussian MIMO interference channel. In *Asilomar Conf.*, Nov. 2015.

[14] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure DoF of the single-antenna MAC. In *IEEE ISIT*, Jun. 2010.