Real Interference Alignment for Vector Channels

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 present a real interference alignment technique for multiple-input multiple-output (MIMO) networks. This technique is based on a theorem due to Dirichlet and Khintchine for simultaneous Diophantine approximation and uses the outputs of all the antennas at the receiver simultaneously for decoding, instead of using them in an antenna-by-antenna basis. This allows us to forgo *asymptotic* real interference alignment for several multi-user scenarios such as the two-user MIMO interference channel with confidential messages and the two-user MIMO multiple access wiretap channel.**

I. Introduction

Real interference alignment, introduced in [1], has been widely used with great success to achieve the optimal degrees of freedom (d.o.f.) in various multi-user networks, with or without security constraints, mostly in the context of single antenna terminals. Examples of such networks include the interference channel and the X-channel without secrecy constraints [1], interference channel with an external eavesdropper and confidential messages, the multiple access wiretap channel and the wiretap channel with helpers [2], [3]. In this paper, we develop a generalization of the real interference technique for multiple-input multiple-output (MIMO) multi-user networks.

Real interference alignment has been used in MIMO networks in the literature. Reference [4] studies the MIMO wiretap channel with one deaf helper and determines the optimal secure degrees of freedom (s.d.o.f.) in terms of the number of antennas at the various terminals. In this case, the optimal s.d.o.f. is of the form $\left(d+\frac{l}{2}\right)$, where d and $l \leq 1$ are nonnegative integers. When $l=0$, real interference alignment is not required and channel precoding and Gaussian signaling suffice. When $l=1$, however, structured signaling is necessary. To decode, the receiver uses a filtering operation to isolate one *data stream* of structured signals, essentially reducing the system to a single-input single-output (SISO) system, for which the design of the structured signaling scheme is known [3]. Once this stream is decoded, it can be removed from the output and the remaining data streams can be decoded using the diversity of the multiple antennas.

The simplicity of the scheme for the wiretap channel with a helper does not easily extend to other MIMO multi-user scenarios such as the multiple access wiretap channel [5] and the interference channel with confidential messages [6]. In both of these cases, 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 $l=0$, real interference alignment is not required and Gaussian signaling with channel precoding is optimal. The case of $l=1$ can also be dealt with as in [4] by using a filtering operation to reduce the MIMO system to a SISO system for which the optimal signaling scheme is known [3]. However, when $l=2$, the filtering operation reduces the general MIMO system to a simpler but still MIMO system with two antennas at each terminal. For this two-antenna system, references [5] and [6] use asymptotic interference alignment where the receiver decodes the output of each antenna separately.

In this paper, we provide a real interference scheme where such asymptotic alignment is not required. While real interference alignment uses the Khintchine-Groshev theorem to bound the minimum distance in the received constellation and thereby bound the probability of error, we use a theorem due to Dirichlet and Khintchine on simultaneous Diophantine approximation [7] that allows us to bound the minimum distance in a multi-dimensional received constellation. This, in turn, allows us to bound the probability of error in a multi-dimensional constellation that results due to the presence of multiple antennas at the terminals. While the receiver decodes each antenna output separately in the asymptotic alignment scheme of [6] and [5], in our scheme, the receiver must decode by using the outputs at all the antennas jointly. This method yields much simpler schemes that are natural generalizations of the schemes for the SISO case. This allows us to eschew the complexity and high SNR requirements of asymptotic alignment schemes in MIMO systems.

In this paper, we illustrate our method by recovering a few known results. We start with the MIMO point-to-point channel with N antennas at each terminal, and show how to achieve N d.o.f. using our scheme. Note that the capacity for this channel is well known [8]; however, we use this channel as a toy example to elucidate our decoding scheme in a scenario which does not involve any alignment. Next, we consider the interference channel with confidential messages and the multiple access wiretap channel, both with two antennas at each terminal, and show how to achieve the optimal sum s.d.o.f. of $\frac{4}{3}$ in each case without taking recourse to asymptotic interference alignment.

II. Preliminaries

We will consider several channel models in the following sections: the point-to-point channel, the interference channel with confidential messages, and the multiple access wiretap

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

channel. Here, we formalize some of the common terms and assumptions used in each of the channel models.

A rate tuple $(R_1, \ldots, R_K)$ is said to be achievable if there exists a sequence of codes indexed by the codelength n such that the probability of error at the intended receivers in transmitting the message tuple $(W_1, \ldots, W_K) \in \mathcal{W}_1 \times \ldots \times \mathcal{W}_K$ goes to zero as the codelength $n \to \infty$, and $R_i = \frac{1}{n} \log |\mathcal{W}_i|$. If additional security constraints are satisfied, the rate tuple is called *secure*. The security constraints, if any, will be specified later as part of the model.

In this paper, we are concerned with the achievable d.o.f. (secure or otherwise) of a network. A (secure) d.o.f. tuple $(d_1, \ldots, d_K)$ is said to be achievable if there exists an (secure) achievable rate tuple $(R_1, \ldots, R_K)$ for the network with $d_i = \lim_{P \to \infty} \frac{R_i}{\frac{1}{2} \log P}$.

We consider fixed channel gains. The channel gain of each link is drawn in an i.i.d. fashion from a continuous distribution with finite support prior to the start of the communication and remains fixed throughout the duration of the communication. This assumption ensures that any finite collection of channel gains are rationally independent almost surely.

III. Main Contribution

In this paper, we provide a new technique to use real interference techniques for systems with multiple antennas. We note that real interference alignment has been used for MIMO systems in the literature. Reference [4] provides real interference alignment based optimal schemes for the MIMO wiretap channel with a helper. These schemes combine channel precoding to exploit the spatial diversity of multiple antennas along with real interference alignment based techniques for complex channel gains to achieve the optimal sum s.d.o.f. A similar strategy is used in references [5], [6], for the cases of the multiple access wiretap channel and the interference channel with confidential messages, respectively. However, in these cases, the optimal schemes are based on *asymptotic* real interference alignment, and the decoding at each receiver is done on an antenna-by-antenna basis. Thus, the schemes are high in complexity and are quite different in structure from the schemes in the SISO case [3]. In this paper, we propose real alignment based schemes where the decoding is done by considering all the available antenna outputs simultaneously. To do so, we exploit a theorem on simultaneous Diophantine approximation. As a result, the proposed scheme does not require asymptotic alignment and structurally resembles the SISO schemes closely.

IV. MIMO Point-to-point Channel

To illustrate our scheme, we start with a MIMO Gaussian point-to-point channel. For simplicity, we assume that both the transmitter and the receiver are equipped with N antennas. The channel is given by:

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N} \tag{1}$$

where $\mathbf{N} \sim \mathcal{N}(\mathbf{0}, I_N)$ is the white Gaussian noise and I_N denotes the $N \times N$ identity matrix. Further, the channel input $\mathbf{X}$ satisfies the average power constraint $\mathbb{E}[||\mathbf{X}||^2] \leq P$. Note that the capacity of this channel is well known [8], and can be obtained by simply performing a singular value decomposition of the channel matrix that converts the MIMO channel to a channel with N parallel sub-channels. The optimal d.o.f. is N. To achieve the capacity, no alignment is necessary. We use this channel as a toy example to elucidate our scheme, in particular, the decoding procedure without any signal alignment. The scheme is as follows:

Encoding: The transmitter first decomposes its messages into L independent sub-messages, each of which is encoded with the help of input symbols chosen from a discrete constellation. For each sub-message, we use the constellation

$$C(a, Q, N) = a \left\{-Q, -Q+1, \ldots, 0, \ldots, Q-1, Q\right\}^N \tag{2}$$

where A^N denotes the N-ary Cartesian product of the set A. The values of a and Q will be appropriately chosen later. Note that each point in the constellation is a tuple of N integers, scaled by a real number. Using this constellation, the transmitter creates a random codebook for the sub-message by imposing a uniform distribution on the constellation.

To send the L sub-messages, the transmitter sends:

$$\mathbf{X} = \sum_{i=1}^{L} \mathbf{T}_i \mathbf{u}_i \tag{3}$$

where $\mathbf{u}_i \in C(a, Q, N)$ and $\mathbf{T}_i$ are $N \times N$ precoding matrices with real entries. The entries of $\mathbf{T}_i$ are such that there exists a row in the concatenated matrix $\tilde{\mathbf{T}} \stackrel{\Delta}{=} [\mathbf{T}_1, \ldots, \mathbf{T}_L]$ for which the row elements are rationally independent. This ensures that the mapping from $\mathbf{u} \stackrel{\Delta}{=} (\mathbf{u}_1, \ldots, \mathbf{u}_L)$ to $\mathbf{X}$ is one-to-one. To see this, let $\hat{\mathbf{u}} = (\hat{\mathbf{u}}_1, \ldots, \hat{\mathbf{u}}_L)$ be another tuple such that $\sum_{i=1}^{L} \mathbf{T}_i \mathbf{u}_i = \sum_{i=1}^{L} \mathbf{T}_i \hat{\mathbf{u}}_i$, i.e., $\sum_{i=1}^{L} \mathbf{T}_i (\mathbf{u}_i - \hat{\mathbf{u}}_i) = \mathbf{0}$. This can be rewritten as

$$\tilde{\mathbf{T}} \begin{pmatrix} \mathbf{u}_1 - \hat{\mathbf{u}}_1 \\ \vdots \\ \mathbf{u}_L - \hat{\mathbf{u}}_L \end{pmatrix} = \mathbf{0} \tag{4}$$

Since the elements of at least one row of $\tilde{\mathbf{T}}$ are rationally independent, $\mathbf{u}_i - \hat{\mathbf{u}}_i = \mathbf{0}$ for all $i = 1, \ldots, L$, i.e., $\mathbf{u} = \hat{\mathbf{u}}$.

Decoding: As in [1], the decoding is in two steps. First, the receiver tries to remove the impact of the noise by mapping the received signal

$$\mathbf{Y} = \mathbf{H} \sum_{i=1}^{L} \mathbf{T}_i \mathbf{u}_i + \mathbf{N} \tag{5}$$

to the nearest point in the received constellation $C_R(a, Q, N) = \mathbf{H} \sum_{i=1}^{L} \mathbf{T}_i C(a, Q, N)$. This step may incur an error, if the noise is too large. However, if there is no error, the processed output is $\hat{\mathbf{Y}} = \mathbf{H} \sum_{i=1}^{L} \mathbf{T}_i \mathbf{u}_i$. In the next step, the receiver computes $\mathbf{H}^{-1} \hat{\mathbf{Y}}$ and then, using the one-to-one relation between $(\mathbf{u}_1, \ldots, \mathbf{u}_L)$ and $\sum_{i=1}^{L} \mathbf{T}_i \mathbf{u}_i$, it can recover $(\mathbf{u}_1, \ldots, \mathbf{u}_L)$ from $\mathbf{H}^{-1} \hat{\mathbf{Y}}$. By design of the $\mathbf{T}_i$s, this step does not incur any errors.

Performance Analysis: In order to bound the probability of

error in the first stage of decoding, we need to first bound the minimum distance in the received constellation $C_R(a, Q, N)$. We use a theorem due to Dirichlet and Khintchine on simultaneous Diophantine approximation [7], stated as follows:

Theorem 1 *Let $\omega(\boldsymbol{A})$, the Diophantine exponent for the $m \times n$ matrix $\boldsymbol{A}$, be the supremum of $\nu > 0$ for which there exists infinitely many $\boldsymbol{q} \in \mathbb{Z}^n$ such that*

$$\|\boldsymbol{A}\boldsymbol{q} + \boldsymbol{p}\|_\infty < \|\boldsymbol{q}\|_\infty^{-\nu} \tag{6}$$

for some $\boldsymbol{p} \in \mathbb{Z}^m$. Then,

$$\omega(\boldsymbol{A}) = \frac{n}{m} \tag{7}$$

for Lebesgue almost every $\boldsymbol{A}$.

It follows from this theorem that there are only finitely many solutions $\boldsymbol{p} \in \mathbb{Z}^m$, $\boldsymbol{q} \in \mathbb{Z}^n$ for the equation

$$\|\boldsymbol{A}\boldsymbol{q} + \boldsymbol{p}\|_\infty < \|\boldsymbol{q}\|_\infty^{-\frac{n}{m}-\epsilon} \tag{8}$$

for any $\epsilon > 0$. Therefore, it is possible to find a constant $\kappa(\epsilon) > 0$ such that

$$\|\boldsymbol{A}\boldsymbol{q} + \boldsymbol{p}\|_\infty > \kappa(\epsilon)\, \|\boldsymbol{q}\|_\infty^{-\frac{n}{m}-\epsilon} \tag{9}$$

holds for all $\boldsymbol{p} \in \mathbb{Z}^m$, $\boldsymbol{q} \in \mathbb{Z}^n$.

Consider the Euclidean distance between the received constellation points induced by the input tuples $\mathbf{u} = (\mathbf{u}_1, \ldots, \mathbf{u}_L)$ and $\tilde{\mathbf{u}} = (\tilde{\mathbf{u}}_1, \ldots, \tilde{\mathbf{u}}_L)$, given by

$$d(\mathbf{u}, \tilde{\mathbf{u}}) = a \left\| \mathbf{H} \sum_{i=1}^{L} \mathbf{T}_i (\mathbf{u}_i - \tilde{\mathbf{u}}_i) \right\|_2 \tag{10}$$

To bound $d(\mathbf{u}, \tilde{\mathbf{u}})$, we proceed as follows

$$a \left\| \mathbf{H} \sum_{i=1}^{L} \mathbf{T}_i (\mathbf{u}_i - \tilde{\mathbf{u}}_i) \right\|_2 \tag{11}$$

$$\geq a \sigma_{\mathbf{H}} \sigma_{\mathbf{T}_1} \left\| (\mathbf{u}_1 - \tilde{\mathbf{u}}_1) + \sum_{i=2}^{L} \mathbf{T}_1^{-1} \mathbf{T}_i (\mathbf{u}_i - \tilde{\mathbf{u}}_i) \right\|_2 \tag{12}$$

$$\geq a \sigma_{\mathbf{H}} \sigma_{\mathbf{T}_1} \left\| (\mathbf{u}_1 - \tilde{\mathbf{u}}_1) + \sum_{i=2}^{L} \mathbf{T}_1^{-1} \mathbf{T}_i (\mathbf{u}_i - \tilde{\mathbf{u}}_i) \right\|_\infty \tag{13}$$

$$\geq a \sigma_{\mathbf{H}} \sigma_{\mathbf{T}_1} \kappa(\epsilon) (2Q+1)^{-L+1-\epsilon} \tag{14}$$

where $\sigma_{\boldsymbol{A}}$ denotes the minimum singular value of the matrix $\boldsymbol{A}$. In the above, we have assumed that $\mathbf{T}_1$ is invertible and that the matrix $[\mathbf{T}_1^{-1}\mathbf{T}_2, \ldots, \mathbf{T}_1^{-1}\mathbf{T}_L]$ belongs to the *good* set of matrices for which (7) holds. Of course, the set of such *good* matrices has the full Lebesgue measure. One way to ensure that these two conditions are satisfied simultaneously is to draw the entries of $\mathbf{T}_i$ in an i.i.d. fashion from some continuous distribution. We let

$$d_{\min} \geq a \sigma_{\mathbf{H}} \sigma_{\mathbf{T}_1} \kappa(\epsilon) (2Q+1)^{-L+1-\epsilon} \approx P^{\delta} \tag{15}$$

For sufficiently large power P, we have

$$\frac{a}{Q^{L-1+\epsilon}} \approx \gamma_1 P^{\delta} \tag{16}$$

for some appropriate constant γ_1.

To satisfy the power constraint, we set

$$aQ \approx \gamma_2 P^{\frac{1}{2}} \tag{17}$$

for some appropriate constant γ_2.

Combining (16) and (17), we have

$$a \approx P^{\frac{L-1+\epsilon+2\delta}{2(L+\epsilon)}}, \quad Q \approx P^{\frac{1-\delta}{2(L+\epsilon)}} \tag{18}$$

Now, we can bound the probability of error. The following loose bound on the probability of error can be obtained by considering pairwise error probabilities and the union bound:

$$P_e \leq (2Q+1)^{2NL} e^{-d_{\min}^2/8} \tag{19}$$

$$\approx P^{\frac{2NL(1-\delta)}{2(L+\epsilon)}} e^{-P^{2\delta}/8} \tag{20}$$

which goes to 0 as $P \to \infty$.

We bound the achievable rate for this scheme as in [1],

$$R \geq I(\mathbf{u}_1, \ldots, \mathbf{u}_L; \hat{\mathbf{u}}_1, \ldots, \hat{\mathbf{u}}_L) \tag{21}$$

$$\geq L(1 - P_e) \log(2Q+1)^N - 1 \tag{22}$$

$$\approx LN \frac{1-\delta}{(L+\epsilon)} \left(\frac{1}{2} \log P \right) + o(\log P) \tag{23}$$

at high P, which immediately yields the optimal d.o.f. of N for suitable choice of ϵ and δ.

Note that when $N = 1$, our scheme reduces to the scheme in [1]. For general N, each data stream is an N-tuple transmitted over N antennas, and carries $\frac{N}{L}$ d.o.f. of information.

In the following sections, we apply this technique to two multi-user MIMO scenarios with secrecy constraints: the two-user interference channel with confidential messages and the two-user multiple access wiretap channel.

V. Interference Channel with Confidential Messages

We consider the case when each terminal has two antennas. This case is crucial for the more general case with M transmitter antennas and N receiver antennas in [6].

The two-user interference channel with confidential messages, see Fig. 1, is described by

$$\mathbf{Y} = \mathbf{H}_1 \mathbf{X}_1 + \mathbf{H}_2 \mathbf{X}_2 + \mathbf{N}_1 \tag{24}$$

$$\mathbf{Z} = \mathbf{G}_1 \mathbf{X}_1 + \mathbf{G}_2 \mathbf{X}_2 + \mathbf{N}_2 \tag{25}$$

where $\mathbf{X}_i$ is the two-dimensional channel input of transmitter i, $\mathbf{Y}$ and $\mathbf{Z}$ are the received two-dimensional channel outputs, and $\mathbf{N}_i$ is a zero-mean white Gaussian noise vector with $\mathbf{N}_i \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_2)$. Transmitter i has a message W_i which needs to be sent securely to receiver i. Thus, we require:

$$\frac{1}{n} I(W_1; \mathbf{Z}^n | W_2) \to 0, \quad \frac{1}{n} I(W_2; \mathbf{Y}^n | W_1) \to 0 \tag{26}$$

as $n \to \infty$ As shown in [6], the optimal sum s.d.o.f. in for our model is $\frac{4}{3}$. The channel inputs are:

$$\mathbf{X}_1 = \mathbf{G}_1^{-1} \mathbf{v}_1 + \mathbf{H}_1^{-1} \mathbf{u}_1 \tag{27}$$

$$\mathbf{X}_2 = \mathbf{H}_2^{-1} \mathbf{v}_2 + \mathbf{G}_2^{-1} \mathbf{u}_2 \tag{28}$$

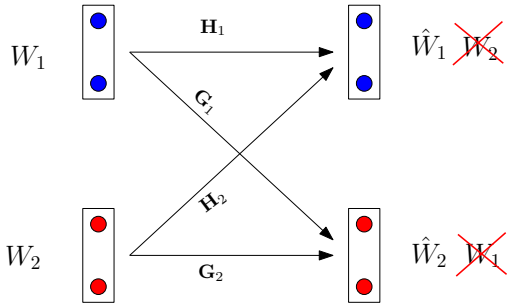

Fig. 1. Interference channel with confidential messages.

where $\mathbf{v}_i$ are the two-dimensional information carrying signal corresponding to the encoding of the message W_i, drawn from the constellation $C(a, Q, 2)$. The vectors $\mathbf{u}_i$ are artificial noise symbols drawn independently and uniformly from the constellation $C(a, Q, 2)$. The channel outputs are:

$$\mathbf{Y} = \mathbf{H}_1\mathbf{G}_1^{-1}\mathbf{v}_1 + (\mathbf{u}_1 + \mathbf{v}_2) + \mathbf{H}_2\mathbf{G}_2^{-1}\mathbf{u}_2 + \mathbf{N}_1 \quad (29)$$

$$\mathbf{Z} = \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{v}_2 + (\mathbf{u}_2 + \mathbf{v}_1) + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{u}_1 + \mathbf{N}_2 \quad (30)$$

Note that $\mathbf{u}_1$ and $\mathbf{v}_2$ arrive at the channel output $\mathbf{Y}$ with the same coefficient, i.e., they are aligned at $\mathbf{Y}$. A similar observation holds for $\mathbf{u}_2$ and $\mathbf{v}_1$. Therefore, intuitively, each receiver decodes three distinct data streams, and one of them is the desired message. Since each terminal has two antennas, each datastream carries $\frac{2}{3}$ d.o.f. Thus, the achievable sum d.o.f. is $\frac{4}{3}$. Further, since the message symbols are buried in the artificial noise symbols at the unintended receivers, we also obtain confidentiality from this scheme.

Formally, from [9], the following rates are achievable

$$R_1 \geq I(\mathbf{v}_1; \mathbf{Y}) - I(\mathbf{v}_1; \mathbf{Z}|\mathbf{v}_2) \quad (31)$$

$$R_2 \geq I(\mathbf{v}_2; \mathbf{Z}) - I(\mathbf{v}_2; \mathbf{Y}|\mathbf{v}_1) \quad (32)$$

To evaluate the lower bound on the rate R_1, we first note that

$$I(\mathbf{v}_1; \mathbf{Z}|\mathbf{v}_2) \leq I(\mathbf{v}_1; \mathbf{v}_1 + \mathbf{u}_2) \quad (33)$$

$$= H(\mathbf{v}_1 + \mathbf{u}_2) - H(\mathbf{u}_2) \quad (34)$$

$$\leq 2\log(4Q+1) - 2\log(2Q+1) \quad (35)$$

$$\leq 2 \quad (36)$$

On the other hand, to bound $I(\mathbf{v}_1; \mathbf{Y})$, we first bound the probability of error. The minimum distance in the received signal constellation can be bounded as follows. Consider two input tuples $(\mathbf{u}_1, \mathbf{v}_1, \mathbf{u}_2, \mathbf{v}_2)$ and $(\tilde{\mathbf{u}}_1, \tilde{\mathbf{v}}_1, \tilde{\mathbf{u}}_2, \tilde{\mathbf{v}}_2)$. The distance in the received constellation at $\mathbf{Y}$ due to these input tuples is almost surely

$$d \geq a \left\| \mathbf{H}_1\mathbf{G}_1^{-1}\hat{\mathbf{v}}_1 + \mathbf{H}_2\mathbf{G}_2^{-1}\hat{\mathbf{u}}_2 + (\hat{\mathbf{u}}_1 + \hat{\mathbf{v}}_2) \right\|_2 \quad (37)$$

$$\geq a \left\| \mathbf{H}_1\mathbf{G}_1^{-1}\hat{\mathbf{v}}_1 + \mathbf{H}_2\mathbf{G}_2^{-1}\hat{\mathbf{u}}_2 + (\hat{\mathbf{u}}_1 + \hat{\mathbf{v}}_2) \right\|_\infty \quad (38)$$

$$\geq \beta a (2Q+1)^{-2-\epsilon} \quad (39)$$

where $\hat{\mathbf{v}}_i = \mathbf{v}_i - \tilde{\mathbf{v}}_i$ and $\hat{\mathbf{u}}_i$ is defined similarly, β is some constant and we have used the fact that $|\hat{\mathbf{v}}_i| \leq (2Q+1)$. Also, the above distance bound holds for almost all $\mathbf{H}_i$ and $\mathbf{G}_i$ since the entries of these channel matrices are drawn from a continuous distribution and the set of *good* matrices satisfying (7) has full Lebesgue measure. Since the bound holds for every pair of input tuples, the minimum distance

$$d_{\min} \geq \beta a (2Q+1)^{-2-\epsilon} \quad (40)$$

As before, we set

$$a(2Q+1)^{-2-\epsilon} \approx \gamma_1 P^{\delta}, \quad aQ \approx \gamma_2 P^{\frac{1}{2}} \quad (41)$$

for the minimum distance and the power constraint, respectively, which leads to

$$a \approx P^{\frac{2+\epsilon+2\delta}{2(3+\epsilon)}}, \quad Q \approx P^{\frac{1-\delta}{2(3+\epsilon)}} \quad (42)$$

Therefore, the probability of error in decoding $\mathbf{v}_1$ can be bounded by $(2Q+1)^{16}e^{-P^{\delta}/8}$ which goes to 0 as $P \to \infty$. Thus, we can bound $I(\mathbf{v}_1; \mathbf{Y})$ in (31) as

$$I(\mathbf{v}_1; \mathbf{Y}) \geq I(\mathbf{v}_1; \hat{\hat{\mathbf{v}}}_1) \quad (43)$$

$$\geq (1 - P_e)\log(2Q+1)^2 - 1 \quad (44)$$

$$= \frac{2(1-\delta)}{3+\epsilon}\left(\frac{1}{2}\log P\right) + o(\log P) \quad (45)$$

where $\hat{\hat{\mathbf{v}}}_1$ is the reconstruction of $\mathbf{v}_1$. Substituting in (31),

$$R_1 \geq \frac{2(1-\delta)}{3+\epsilon}\left(\frac{1}{2}\log P\right) + o(\log P) \quad (46)$$

which yields the s.d.o.f. of $\frac{2}{3}$. Similarly, an s.d.o.f. of $\frac{2}{3}$ can be achieved for the second user. Thus, the sum s.d.o.f. is $\frac{4}{3}$.

Note the differences between our scheme and the one presented in [6]. In the scheme of [6], the decoding at the receivers is on an antenna-by-antenna basis. Thus, asymptotic real interference alignment is used to obtain the optimal sum rate. In our case, the decoding process uses the output at both antennas together and no asymptotic alignment is required.

We next provide another example where our scheme allows us to bypass the need for asymptotic alignment in a multi-user MIMO setting. Specifically, we present the scheme for the two-user MIMO multiple access wiretap channel with two antennas at each terminal.

VI. Multiple Access Wiretap Channel

The two-user multiple access wiretap channel, see Fig. 2, is described by

$$\mathbf{Y} = \mathbf{H}_1\mathbf{X}_1 + \mathbf{H}_2\mathbf{X}_2 + \mathbf{N}_1 \quad (47)$$

$$\mathbf{Z} = \mathbf{G}_1\mathbf{X}_1 + \mathbf{G}_2\mathbf{X}_2 + \mathbf{N}_2 \quad (48)$$

where $\mathbf{X}_i$ is the two-dimensional channel input of transmitter i, $\mathbf{Y}$ and $\mathbf{Z}$ are the received two-dimensional channel outputs at the legitimate receiver and the eavesdropper, respectively, and $\mathbf{N}_i$ is a zero-mean white Gaussian noise vector with $\mathbf{N}_i \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_2)$. Transmitter i has a message W_i which needs to be sent securely to the legitimate receiver in the presence of the eavesdropper; thus, we require:

$$\frac{1}{n} I(W_1, W_2; \mathbf{Z}^n) \to 0 \quad (49)$$

as $n \to \infty$. This model is studied in [10] for the case of

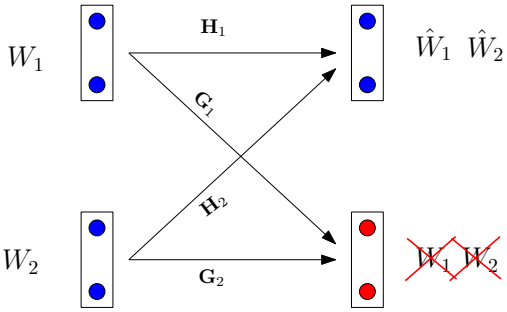

Fig. 2. Multiple access wiretap channel.

varying channel gains and in a more general setting with N antennas at the legitimate parties and K antennas at the eavesdropper. It is shown that the optimal sum s.d.o.f. for our channel with two antennas at each terminal is $\frac{4}{3}$ with varying channel gains. For fixed channel gains, reference [5] presents a scheme based on *asymptotic* real interference alignment. In the following, we present a scheme that does not require asymptotic interference alignment and resembles the scheme for varying channel gains in [10], and the SISO case in [3]. The scheme is as follows. Transmitter i sends

$$\mathbf{X}_i = \mathbf{G}_i^{-1}\mathbf{G}_j\mathbf{H}_j^{-1}\mathbf{v}_i + \mathbf{H}_i^{-1}\mathbf{u}_i \tag{50}$$

for $j \neq i$, where $\mathbf{v}_i$ are the the two-dimensional information carrying symbols in $C(a, Q, 2)$ encoding W_i, and $\mathbf{u}_i$ are artificial noise symbols drawn independently and uniformly from $C(a, Q, 2)$. The channel outputs are

$$\begin{aligned}\mathbf{Y} =&\mathbf{H}_1\mathbf{G}_1^{-1}\mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{v}_1 + \mathbf{H}_2\mathbf{G}_2^{-1}\mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{v}_2 \\ &+ (\mathbf{u}_1 + \mathbf{u}_2) + \mathbf{N}_1 \qquad (51)\\ \mathbf{Z} =&\mathbf{G}_2\mathbf{H}_2^{-1}(\mathbf{v}_1 + \mathbf{u}_2) + \mathbf{G}_1\mathbf{H}_1^{-1}(\mathbf{v}_2 + \mathbf{u}_1) + \mathbf{N}_2 \qquad (52)\end{aligned}$$

Note that at the legitimate receiver, the artificial noise symbols $\mathbf{u}_1$ and $\mathbf{u}_2$ are aligned; thus, effectively there are only three distinct data streams to be decoded. Therefore, with two antennas, each data stream may carry $\frac{2}{3}$ d.o.f. Since two of the three data streams are information carrying symbols, the total d.o.f. is $\frac{4}{3}$. Further, the scheme provides security from the eavesdropper as well, since the information carrying symbol $\mathbf{v}_i$ is buried in the artificial noise $\mathbf{u}_j$, $i \neq j$ at the eavesdropper.

Formally, an achievable sum rate is [11]

$$R_1 + R_2 \geq I(\mathbf{v}_1, \mathbf{v}_2; \mathbf{Y}) - I(\mathbf{v}_1, \mathbf{v}_2; \mathbf{Z}) \tag{53}$$

As in the case of the interference channel, we can bound the leakage term $I(\mathbf{v}_1, \mathbf{v}_2; \mathbf{Z})$ as

$$\begin{aligned}I(\mathbf{v}_1, \mathbf{v}_2; \mathbf{Z}) \leq& I(\mathbf{v}_1, \mathbf{v}_2; (\mathbf{v}_1 + \mathbf{u}_2), (\mathbf{v}_2 + \mathbf{u}_1)) \qquad (54)\\ \leq& H(\mathbf{v}_1 + \mathbf{u}_2) + H(\mathbf{v}_2 + \mathbf{u}_1) - H(\mathbf{u}_1, \mathbf{u}_2) \qquad (55)\\ \leq& 2\log(4Q+1)^2 - \log(2Q+1)^4 \qquad (56)\\ \leq& 4 \qquad (57)\end{aligned}$$

In order to bound $I(\mathbf{v}_1, \mathbf{v}_2; \mathbf{Y})$, we first bound the probability of error in detecting $(\mathbf{v}_1, \mathbf{v}_2)$. As before, the minimum distance of the received constellation at $\mathbf{Y}$ can be lower-bounded by P^δ while satisfying the transmit power constraint by choosing

$$a \approx P^{\frac{2+\epsilon+2\delta}{2(3+\epsilon)}}, \quad Q \approx P^{\frac{1-\delta}{2(3+\epsilon)}} \tag{58}$$

Thus, the probability of error can be bounded by $(2Q+1)^6 e^{-P^\delta/8}$ which goes to zero as $P \to \infty$. Therefore,

$$\begin{aligned}I(\mathbf{v}_1, \mathbf{v}_2; \mathbf{Y}) \geq& I(\mathbf{v}_1, \mathbf{v}_2; \hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2) \qquad (59)\\ =&2(1-P_e)\log(2Q+1)^2 + o(\log P) \qquad (60)\\ =&\frac{4(1-\delta)}{3+\epsilon}\left(\frac{1}{2}\log P\right) + o(\log P) \qquad (61)\end{aligned}$$

where $\hat{\mathbf{v}}_i$ is the reconstruction of $\mathbf{v}_i$. Now, using this along with (57) in (53), we have

$$R_1 + R_2 \geq \frac{4(1-\delta)}{3+\epsilon}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{62}$$

which yields a sum s.d.o.f. of $\frac{4}{3}$ for sufficiently small δ and ϵ.

VII. Conclusion

In this paper, we presented a generalization of the real interference alignment technique for MIMO networks. This scheme, based on a theorem due to Dirichlet and Khintchine on simultaneous Diophantine approximation, uses the outputs at all the antennas in the terminal together instead of using the output at each antenna separately. This allows us to forgo using asymptotic real interference alignment in several multi-user networks. We have demonstrated the use of this technique for two such multi-user scenarios: the two-user interference channel with confidential messages and the two-user multiple access wiretap channel, both with two antennas at each terminal. In both cases, our technique leads to simpler schemes than the asymptotic schemes existing in the literature.

References

[1] 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.

[2] 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.

[3] 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.

[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 *IEEE ICC*, Jun. 2015.

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

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

[7] W. M. Schmidt. *Diophantine Approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer Berlin Heidelberg, 1980.

[8] I Telatar. Capacity of multi-antenna Gaussian channels. *Euro. Trans. on Telecom.*, 10(6):585–595, 1999.

[9] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. on Inf. Theory*, 54(6):2493–2507, Jun. 2008.

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

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