Secure Degrees of Freedom of the Gaussian MIMO Interference Channel

Karim Banawan Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
kbanawan@umd.edu *ulukus@umd.edu*

***Abstract*—We consider the two-user multiple-input multiple-output (MIMO) interference channel with confidential messages (ICCM). We determine the exact sum secure degrees of freedom (s.d.o.f.) for the symmetric case of M antennas at both transmitters and N antennas at both receivers. We develop the converse by combining the broadcast channel with confidential messages (BCCM) cooperative upper bound, decodability upper bound for the IC with no secrecy constraints, and extensions of the secrecy penalty and role of a helper lemmas. We propose a novel achievable scheme for the 2×2 ICCM, which combines asymptotic real interference alignment with spatial interference alignment. Using this scheme, we provide achievable schemes for any M and N by proper vector space operations.**

I. Introduction

We consider the two-user MIMO ICCM [1], where two users wish to send messages to their respective receivers reliably, while keeping them secure from the unintended receiver. The secrecy capacity region of the ICCM is unknown today. The exact *sum* s.d.o.f. [2], [3] and the entire s.d.o.f. *region* [4] of the single-input single-output (SISO) ICCM are known for arbitrary number of transmitters and receivers. In this paper, we determine the exact sum s.d.o.f. of a two-user MIMO ICCM for the symmetric case of M antennas at the transmitters and N antennas at the receivers (see Fig. 1).

Reference [2] determines the exact s.d.o.f. of several SISO one-hop networks, including the wiretap channel with helpers, the multiple access wiretap channel, and the interference channel with secrecy constraints. For achievability, [2] proposes real interference alignment [5] based achievable schemes that use structured codes in the form of pulse amplitude modulation (PAM). Focusing on the two-user SISO ICCM in [2], for the achievability, each user sends one message-carrying signal and one cooperative jamming signal. Each cooperative jamming signal is aligned with the message-carrying signal of the other user at the user's unintended receiver, thereby protecting it. For the converse, [2] develops two converse lemmas, the *secrecy penalty lemma* and the *role of a helper lemma*, which prove the optimality of the proposed achievable schemes. Reference [3] generalizes the sum s.d.o.f. result of [2] to the case of K-users, and [4] generalizes it to determine the entire s.d.o.f. region.

Reference [6] extends the result for the wiretap channel with helpers in [2] to the case of MIMO nodes for the special case of a single helper. To that end, [6] extends the role of a helper lemma of [2] for the MIMO case by upper bounding the conditional differential entropy of the helper channel input given its channel inputs in the null space of the receiver. [6] provides multiple achievable schemes for different regimes including spatial precoding/alignment, transmission in the null space, and projecting onto a SISO dimension where real interference alignment of [2] is used. Since the s.d.o.f. in the case of a MIMO wiretap channel with a helper is a multiple of $1/2$, the strategy of projecting onto a single dimension and using a SISO achievable scheme as in [2] is sufficient.

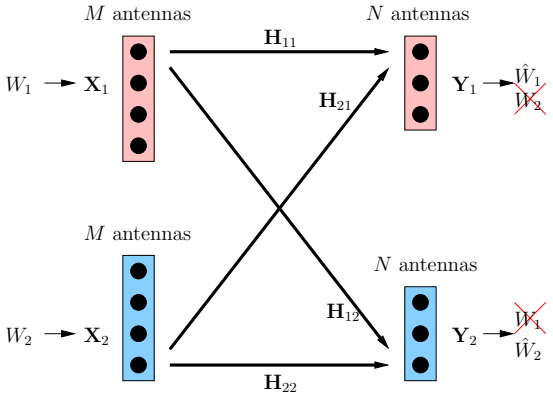

Fig. 1. Two-user MIMO ICCM.

In this paper, we extend the result for the ICCM in [2] to the case of MIMO nodes, for the special case of a two-user system with equal number of antennas at both transmitters (M) and both receivers (N). First, we propose a novel achievable scheme for the 2×2 ICCM system. The 2×2 achievable scheme is central in this paper, since for the ICCM, the final sum s.d.o.f. numbers are multiples of $1/3$. The required achievable scheme depends on the value of the fractional (non-integer) part of the sum s.d.o.f. This fractional part is either 0 or $1/3$ or $2/3$. If it is $1/3$, a projection onto a single SISO dimension as in [6] is sufficient. In this SISO dimension, we use real interference alignment scheme of [2] for ICCM. However, if it is $2/3$, the projection strategy results in a 2×2 ICCM system. In this case, we cannot use the real interference alignment scheme of [2] in individual dimensions. Instead, we use a spatial interference alignment scheme [7] to ensure that the leakage is negligible in the s.d.o.f. sense, and an asymptotic real interference alignment scheme [3] to minimize the required number of irrational dimensions at each antenna

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

for decodability. Any other antenna configuration (any M and N) can be reduced to either a 1×1 (i.e., SISO) or a 2×2 ICCM system after proper vector space operations for the integer part of the sum s.d.o.f. These operations include transmission in the null space of the cross links and spatial alignment.

We develop a matching converse by using three distinct upper bounds: the cooperative upper bound by treating the ICCM as a BCCM; the vectorized version of the upper bounding technique developed in [2] using secrecy penalty and role of a helper lemmas (see also [6]); and the decodability upper bound developed in [8] for the IC without secrecy constraints. The intersection of these three upper bounds gives a tight upper bound for any number of antennas.

II. System Model

The input-output relationships of a two-user MIMO ICCM (see Fig. 1) are:

$$\mathbf{Y}_1 = \mathbf{H}_{11}\mathbf{X}_1 + \mathbf{H}_{21}\mathbf{X}_2 + \mathbf{N}_1 \tag{1}$$

$$\mathbf{Y}_2 = \mathbf{H}_{12}\mathbf{X}_1 + \mathbf{H}_{22}\mathbf{X}_2 + \mathbf{N}_2 \tag{2}$$

where $\mathbf{H}_{ij} \in \mathbb{R}^{N\times M}$ is the channel gain matrix from transmitter i to receiver j, $\mathbf{X}_i$ is the channel input of transmitter i, $\mathbf{Y}_i$ is the channel output of receiver i, and $\mathbf{N}_i$ is the Gaussian noise at receiver i. Transmitter i sends a message W_i chosen uniformly from a message set $\mathcal{W}_i$ by encoding it into an n-letter channel input $\mathbf{X}_i^n$. The message W_i is to be conveyed reliably to receiver i and to be kept secret from receiver j, where $j \neq i$:

$$\mathbb{P}(\hat{W}_1 \neq W_1) \leq \epsilon, \quad \frac{1}{n} I(W_1; \mathbf{Y}_2^n) \leq \epsilon \tag{3}$$

$$\mathbb{P}(\hat{W}_2 \neq W_2) \leq \epsilon, \quad \frac{1}{n} I(W_2; \mathbf{Y}_1^n) \leq \epsilon \tag{4}$$

where $\hat{W}_i$ is the estimate of W_i at receiver i. The channel inputs are subject to average power constraints of P. The rate of user i is $R_i = \frac{1}{n}\log|\mathcal{W}_i|$. The sum s.d.o.f. d_s is:

$$d_s = \lim_{P\to\infty} \frac{R_1 + R_2}{\frac{1}{2}\log P} \tag{5}$$

III. Main Result

Theorem 1 *The sum s.d.o.f. of the two-user $M \times N$ MIMO ICCM is given by,*

$$d_s = \begin{cases} \min\{\frac{2N}{3}, [4M-2N]^+\}, & M \leq N \\ \min\{2N, \frac{4M-2N}{3}\}, & M \geq N \end{cases} \tag{6}$$

for almost all channel gains.

The s.d.o.f. as a function of M for arbitrary N is shown in Fig. 2. We note that when $M = N = 1$ (SISO ICCM), our result reduces to $d_s = 2/3$ in [2].

IV. Upper Bounds for MIMO ICCM

A. For $M < N$

Allowing cooperation between transmitters yields an upper bound. This results in a BCCM with a single transmitter with $2M$ antennas and two receivers with N antennas each. The s.d.o.f. of this BCCM is given by [9]:

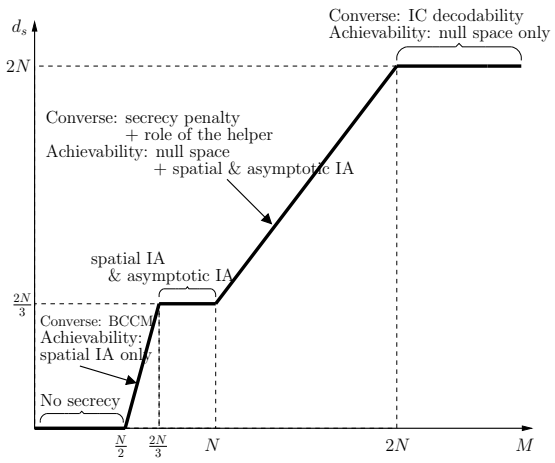

Fig. 2. S.d.o.f. of $M \times N$ MIMO ICCM for given N.

$$d_s \leq 2\min\{N, [2M-N]^+\} = \min\{2N, [4M-2N]^+\} \tag{7}$$

B. For $M \geq N$

Here we present two upper bounds for the MIMO ICCM. First, from the d.o.f. of the two-user IC with no secrecy constraints, $\tilde{d}$, we have the following bound [8]:

$$d_s \leq \tilde{d} = \min\{M_1 + M_2, N_1 + N_2, \max\{M_1, N_2\}, \max\{M_2, N_1\}\} \tag{8}$$

$$= \min\{2N, M\} \tag{9}$$

Second, from the *secrecy penalty lemma* in [2], we have:

$$nR_i \leq h(\tilde{\mathbf{X}}_1^n) + h(\tilde{\mathbf{X}}_2^n) - h(\mathbf{Y}_j^n) + nc_1 \tag{10}$$

where $\tilde{\mathbf{X}}_i^n = \mathbf{X}_i^n + \tilde{\mathbf{N}}_i^n$ is a Gaussian perturbed channel input. In addition, we have the following vectorized version of the *role of a helper lemma* of [2] (see also [6]):

$$h(\tilde{\mathbf{X}}_i^n) \leq h(\mathbf{X}_i^{n^{(2)}}) + h(\mathbf{Y}_j^n) - nR_j + nc_2, \quad i \neq j \tag{11}$$

where $\mathbf{X}_i^{n^{(2)}} = [\tilde{X}_{i_{N+1}}^n \; \tilde{X}_{i_{N+2}}^n \; \dots \; \tilde{X}_{i_M}^n]$. Note that, here, we have, $M \geq N$, therefore, $\mathbf{X}_i^{n^{(2)}}$ is well-defined.

By applying (11) in (10) for both users we obtain:

$$n(2R_1 + R_2) \leq h(\mathbf{X}_1^{n^{(2)}}) + h(\mathbf{X}_2^{n^{(2)}}) + h(\mathbf{Y}_1^n) + nc_3 \tag{12}$$

$$n(R_1 + 2R_2) \leq h(\mathbf{X}_1^{n^{(2)}}) + h(\mathbf{X}_2^{n^{(2)}}) + h(\mathbf{Y}_2^n) + nc_4 \tag{13}$$

Now, adding (12) and (13), and using the fact that Gaussian random variables maximize the differential entropy, we obtain:

$$3n(R_1 + R_2) \leq 2(h(\mathbf{X}_1^{n^{(2)}}) + h(\mathbf{X}_2^{n^{(2)}})) + h(\mathbf{Y}_1^n) + h(\mathbf{Y}_2^n) + nc_5 \tag{14}$$

$$\leq 4(M-N)\cdot\frac{n}{2}\log P + 2N\cdot\frac{n}{2}\log P + nc_6 \tag{15}$$

Dividing by n yields,

$$R_1 + R_2 \leq \frac{4M-2N}{3}\cdot\frac{1}{2}\log P + c_6 \tag{16}$$

and by taking the limit as $P \to \infty$, we obtain:

$$d_s \leq \frac{4M-2N}{3} \tag{17}$$

To combine the two upper bounds obtained in this subsection, (17) and (9), we note that if $M \leq \frac{4M-2N}{3}$ or $2N \leq \frac{4M-2N}{3}$, then $M \geq 2N$. Consequently, we obtain for $M \geq N$:

$$d_s \leq \min\left\{2N, \frac{4M-2N}{3}\right\} \tag{18}$$

C. Combining both Bounds

We note that increasing the number of transmit antennas of both transmitters cannot decrease the s.d.o.f. of ICCM for a fixed number of receiver antennas. Therefore, $d_s \leq \frac{2N}{3}$ bound corresponding to the case of $M = N$ in (18) is a valid upper bound for any $M < N$. Combining the bound in (7) and $d_s \leq \frac{2N}{3}$, we obtain for $M \leq N$:

$$d_s \leq \min\left\{\frac{2N}{3}, [4M-2N]^+\right\} \tag{19}$$

Combining (18) and (19) gives the converse proof for (6).

V. Achievable Scheme for the 2×2 ICCM

The basic building blocks of all achievable schemes are the 1×1 SISO ICCM and the 2×2 MIMO ICCM systems. We can reduce all other regimes to one of these cases by proper vector space manipulations. The achievable scheme for the 1×1 SISO ICCM is given in [2]. In this section, we give an achievable scheme for the 2×2 MIMO ICCM. The achievable scheme for the 2×2 ICCM combines spatial alignment with asymptotic real interference alignment. The spatial alignment ensures that leakage rate is upper bounded by a constant, and the asymptotic real interference alignment minimizes the total irrational dimensions needed for reliable decoding. To use real alignment, we construct the secure signals $\mathbf{V}_i$, cooperative jamming signals $\mathbf{U}_i$ as linear combination of structured signals chosen from a PAM constellation $C(a, Q)$ as in [2] with proper parameters. The transmitted signals are:

$$\mathbf{X}_1 = \mathbf{H}_{12}^{-1}\mathbf{V}_1 + \mathbf{H}_{11}^{-1}\mathbf{U}_1 \tag{20}$$

$$\mathbf{X}_2 = \mathbf{H}_{21}^{-1}\mathbf{V}_2 + \mathbf{H}_{22}^{-1}\mathbf{U}_2 \tag{21}$$

The received signals are:

$$\begin{aligned}\mathbf{Y}_1 &= \mathbf{H}_{11}\mathbf{H}_{12}^{-1}\mathbf{V}_1 + (\mathbf{U}_1 + \mathbf{V}_2) + \mathbf{H}_{21}\mathbf{H}_{22}^{-1}\mathbf{U}_2 \\ &= \mathbf{A}\mathbf{V}_1 + (\mathbf{U}_1 + \mathbf{V}_2) + \mathbf{B}\mathbf{U}_2 \end{aligned} \tag{22}$$

$$\begin{aligned}\mathbf{Y}_2 &= (\mathbf{V}_1 + \mathbf{U}_2) + \mathbf{H}_{12}\mathbf{H}_{11}^{-1}\mathbf{U}_1 + \mathbf{H}_{22}\mathbf{H}_{21}^{-1}\mathbf{V}_2 \\ &= (\mathbf{V}_1 + \mathbf{U}_2) + \bar{\mathbf{B}}\mathbf{U}_1 + \bar{\mathbf{A}}\mathbf{V}_2 \end{aligned} \tag{23}$$

Considering the first receiver, without loss of generality, we note that $\mathbf{A} = \mathbf{H}_{11}\mathbf{H}_{12}^{-1}$, $\mathbf{B} = \mathbf{H}_{21}\mathbf{H}_{22}^{-1}$ are generally non-diagonal with rationally independent elements almost surely. Using exact real interference alignment requires constructing 5 irrational dimensions for reliable decoding of $\mathbf{V}_i$. However, this wastes the observation space of the second antenna and achieves s.d.o.f. of $2/5$ from only one antenna. Hence, we use asymptotic real interference alignment [3]. The idea is that we need one signal component to be in a free irrational dimension at each antenna, while the other secure signal component and the cooperative jamming signals received from the other user should be asymptotically aligned together. This makes the required signal component to cover approximately $1/3$ of the total dimensions.

We define sets of irrational dimensions T_i:

$$T_1 = \left\{ \prod_{i,j=1, i\neq j}^{2} \bar{a}_{ij}^{r_{ij}} \prod_{i,j=1}^{2} \bar{b}_{ij}^{s_{ij}} : r_{ij}, s_{ij} = 1, \ldots, m \right\} \tag{24}$$

$$T_2 = \left\{ \prod_{i,j=1, i\neq j}^{2} a_{ij}^{r_{ij}} \prod_{i,j=1}^{2} b_{ij}^{s_{ij}} : r_{ij}, s_{ij} = 1, \ldots, m \right\} \tag{25}$$

We define $\mathbf{t}_1$, $\mathbf{t}_2$ to be the vectors constructed by enumerating all elements of T_1, T_2 sets, respectively. The cardinality of T_i is $M_T = |T_i| = m^6$. Note that T_i does not contain the channels $a_{ii}, \bar{a}_{ii}$. Hence, multiplying by this channel gain produces new M_T irrational dimensions. On the other hand, multiplying with any channel gain that appears in T_i results in asymptotically aligning this signal within $\tilde{T}_i$ set which is defined as:

$$\tilde{T}_1 = \left\{ \prod_{i,j=1, i\neq j}^{2} \bar{a}_{ij}^{r_{ij}} \prod_{i,j=1}^{2} \bar{b}_{ij}^{s_{ij}} : r_{ij}, s_{ij} = 1, \ldots, m+1 \right\} \tag{26}$$

$$\tilde{T}_2 = \left\{ \prod_{i,j=1, i\neq j}^{2} a_{ij}^{r_{ij}} \prod_{i,j=1}^{2} b_{ij}^{s_{ij}} : r_{ij}, s_{ij} = 1, \ldots, m+1 \right\} \tag{27}$$

with cardinality of $M_R = |\tilde{T}_i| = (m+1)^6$.

Now, we give the explicit structure of the transmitted signals. The vectors $\mathbf{V}_i$, $\mathbf{U}_i$ are 2×1 vectors. Each component is constructed out of irrational combination of M_T PAM signals $\mathbf{v}_{ij} = [v_{ij_1}\, v_{ij_2} \cdots v_{ij_{M_T}}]^T$ representing secure signal components of user i from antenna j. Similarly, generate $\mathbf{u}_{ij} = [u_{ij_1}\, u_{ij_2} \cdots u_{ij_{M_T}}]^T$ cooperative jamming signals:

$$\mathbf{V}_1 = \begin{bmatrix}\mathbf{t}_2^T\mathbf{v}_{11} \\ \mathbf{t}_2^T\mathbf{v}_{12}\end{bmatrix}, \quad \mathbf{U}_1 = \begin{bmatrix}\mathbf{t}_1^T\mathbf{u}_{11} \\ \mathbf{t}_1^T\mathbf{u}_{12}\end{bmatrix} \tag{28}$$

$$\mathbf{V}_2 = \begin{bmatrix}\mathbf{t}_1^T\mathbf{v}_{21} \\ \mathbf{t}_1^T\mathbf{v}_{22}\end{bmatrix}, \quad \mathbf{U}_2 = \begin{bmatrix}\mathbf{t}_2^T\mathbf{v}_{21} \\ \mathbf{t}_2^T\mathbf{v}_{22}\end{bmatrix} \tag{29}$$

This means that the alignment of $\mathbf{V}_1$ and $\mathbf{U}_2$ is carried over the T_2 set, while that of $\mathbf{V}_2$ and $\mathbf{U}_1$ over the T_1 set. Using this construction the received signal at receiver 1, $\mathbf{Y}_1$, is:

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

We finally state that using the combination of asymptotic alignment and spatial alignment illustrated in this section above achieves a sum s.d.o.f. of $d_s \geq 4/3$. Next, we give only a sketch of a proof of this statement due to space limitations here. We first note that using this type of alignment ensures exact alignment of user 2's secure signals with cooperative jamming signal generated by user 1 as in $(\mathbf{u}_{11} + \mathbf{v}_{21})$ terms.

This exact alignment guarantees security as in the SISO case in [2]. In addition, at each antenna, only one secure signal component lies in a separate irrational dimension for decodability as in $a_{11}\mathbf{t}_2^T\mathbf{v}_{11}$ and $a_{22}\mathbf{t}_2^T\mathbf{v}_{12}$, while the other component aligns with user 2's cooperative jamming signal over the set $\tilde{T}_2$. The total number of dimensions needed in this case is $M_\Sigma = |a_{11}T_2 \cup T_1 \cup \tilde{T}_2| = 2m^6 + (m+1)^6$. Therefore, the intended secure signal at each antenna covers M_T dimensions out of M_Σ dimensions. Consequently, achievable s.d.o.f. per antenna is approximately $\frac{M_T}{M_\Sigma}$ which approaches $1/3$ as m gets large. Hence, we achieve a total of $2/3$ s.d.o.f. per user, and a total of $d_s = 4/3$ s.d.o.f. for the system.

VI. Achievable Scheme for $M \times N$ MIMO ICCM

We now present the achievable scheme for arbitrary M and N, i.e., for an arbitrary $M \times N$ MIMO ICCM. Due to the symmetry, the encoding (decoding) strategies are the same for both transmitters (receivers). We thus present for one user only.

A. For $M \leq N$

For $M \leq N$, we have $d_s \leq \min\{\frac{2N}{3}, [4M-2N]^+\}$. We note that for $2M \leq N$, no positive rate can be achieved. The $4M-2N$ upper bound is active if $\frac{1}{2} \leq \frac{M}{N} \leq \frac{2}{3}$, while the $\frac{2N}{3}$ upper bound is active for $\frac{2}{3} \leq \frac{M}{N} \leq 1$.

1) $\frac{1}{2} < \frac{M}{N} \leq \frac{2}{3}$: In this case, the sum s.d.o.f. is an integer. Hence, we use Gaussian codebooks for transmission of secure signal $\mathbf{V}_i$ and cooperative jamming signal $\mathbf{U}_i$. We precode these signals such that the secure signal of one user lies in the same subspace as the cooperative jamming of the other user. Each user transmits $\mathbf{V}_i$, $\mathbf{U}_i$ signals of $2M-N$ dimensions. The transmitted signals are:

$$\mathbf{X}_i = \mathbf{P}_i\mathbf{V}_i + \mathbf{Q}_i\mathbf{U}_i \tag{30}$$

The received signal at receiver 1 is:

$$\mathbf{Y}_1 = \mathbf{H}_{11}\mathbf{P}_1\mathbf{V}_1 + (\mathbf{H}_{11}\mathbf{Q}_1\mathbf{U}_1 + \mathbf{H}_{21}\mathbf{P}_2\mathbf{V}_2) + \mathbf{H}_{21}\mathbf{Q}_2\mathbf{U}_2 \tag{31}$$

The precoding matrices $\mathbf{P}_i$, $\mathbf{Q}_i$ are chosen such that $\text{span}\{\mathbf{H}_{21}\mathbf{P}_2\} \subseteq \text{span}\{\mathbf{H}_{11}\mathbf{Q}_1\}$, and $\text{span}\{\mathbf{H}_{12}\mathbf{P}_1\} \subseteq \text{span}\{\mathbf{H}_{22}\mathbf{Q}_2\}$. This is done by choosing $\mathbf{P}_i$, $\mathbf{Q}_i$ such that:

$$\begin{bmatrix}\mathbf{H}_{11} & -\mathbf{H}_{21}\end{bmatrix}\begin{bmatrix}\mathbf{Q}_1\\ \mathbf{P}_2\end{bmatrix} = \mathbf{0},\ \begin{bmatrix}\mathbf{H}_{12} & -\mathbf{H}_{22}\end{bmatrix}\begin{bmatrix}\mathbf{P}_1\\ \mathbf{Q}_2\end{bmatrix} = \mathbf{0} \tag{32}$$

By this alignment technique, we have:

$$\mathbf{Y}_1 = \mathbf{H}_{11}\mathbf{P}_1\mathbf{V}_1 + \mathbf{H}_{11}\mathbf{Q}_1(\mathbf{U}_1+\mathbf{V}_2) + \mathbf{H}_{21}\mathbf{Q}_2\mathbf{U}_2 \tag{33}$$

$$= \begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1 & \mathbf{H}_{11}\mathbf{Q}_1 & \mathbf{H}_{21}\mathbf{Q}_2\end{bmatrix}\begin{bmatrix}\mathbf{V}_1\\ \mathbf{U}_1+\mathbf{V}_2\\ \mathbf{U}_2\end{bmatrix} \tag{34}$$

In order to decode the $\mathbf{Y}_i$ using a zero forcing receiver, the total dimensions $3(2M-N)$ should be at most N. This holds true since $\frac{M}{N} \leq \frac{2}{3}$. Since, each secure signal is aligned with the cooperative jamming signal from the other user, the leakage rate is upper bounded by a constant, and hence, is secure from an s.d.o.f. perspective.

2) $\frac{2}{3} < \frac{M}{N} \leq 1$: In this regime, we combine the achievable scheme of the previous regime with the achievable scheme of the basic 2×2 system (or the SISO system). Generate the $\mathbf{V}_i = \begin{bmatrix}\mathbf{V}_i^{(1)}\\ \mathbf{V}_i^{(2)}\end{bmatrix}$ and $\mathbf{U}_i = \begin{bmatrix}\mathbf{U}_i^{(1)}\\ \mathbf{U}_i^{(2)}\end{bmatrix}$, where $\mathbf{V}_i^{(1)}, \mathbf{U}_i^{(1)}$ are Gaussian signals of size of $\lfloor\frac{N}{3}\rfloor$ corresponding to the part that can be protected using spatial alignment only without any real interference alignment. The vectors $\mathbf{V}_i^{(2)}, \mathbf{U}_i^{(2)}$ are chosen from PAM constellation $C(a,Q)$. These vectors are of size $N \bmod 3$ which is either 1 or 2. This separation effectively reduces the problem into designing spatial alignment precoders as previous regime and the basic 2×2 system (or the SISO system). Considering the case of $N \bmod 3 = 2$, and user 1, without loss of generality, the transmitted signals are given by:

$$\mathbf{X}_1 = \mathbf{P}_1\begin{bmatrix}v_{1,1}^{(1)}\\ v_{1,2}^{(1)}\\ \vdots\\ v_{1,\lfloor\frac{N}{3}\rfloor}^{(1)}\\ \mathbf{t}_2^T\mathbf{v}_{11}^{(2)}\\ \mathbf{t}_2^T\mathbf{v}_{12}^{(2)}\end{bmatrix} + \mathbf{Q}_1\begin{bmatrix}u_{1,1}^{(1)}\\ u_{1,2}^{(1)}\\ \vdots\\ u_{1,\lfloor\frac{N}{3}\rfloor}^{(1)}\\ \mathbf{t}_1^T\mathbf{u}_{11}^{(2)}\\ \mathbf{t}_1^T\mathbf{u}_{12}^{(2)}\end{bmatrix} \tag{35}$$

where $\mathbf{P}_i$ and $\mathbf{Q}_i$ can be designed as in (32). This alignment is possible if $2M - N \geq \lfloor\frac{N}{3}\rfloor + N \bmod 3$ which implies that $\frac{M}{N} \geq \frac{2}{3} + \frac{N \bmod 3}{3N}$ which always holds in this regime. Partition $\mathbf{P}_i = \begin{bmatrix}\mathbf{P}_{i_{N\times\lfloor\frac{N}{3}\rfloor}}^{(1)} & \mathbf{P}_{i_{N\times N \bmod 3}}^{(2)}\end{bmatrix}$ and similarly for $\mathbf{Q}_i$. Then,

$$\mathbf{Y}_1 = \begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1^{(1)} & \mathbf{H}_{11}\mathbf{Q}_1^{(1)} & \mathbf{H}_{21}\mathbf{Q}_2^{(1)}\end{bmatrix}\begin{bmatrix}\mathbf{V}_1^{(1)}\\ \mathbf{V}_2^{(1)}+\mathbf{U}_1^{(1)}\\ \mathbf{U}_2^{(1)}\end{bmatrix} + \begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1^{(2)} & \mathbf{H}_{11}\mathbf{Q}_1^{(2)} & \mathbf{H}_{21}\mathbf{Q}_2^{(2)}\end{bmatrix}\begin{bmatrix}\mathbf{V}_1^{(2)}\\ \mathbf{V}_2^{(2)}+\mathbf{U}_1^{(2)}\\ \mathbf{U}_2^{(2)}\end{bmatrix} \tag{36}$$

Define matrix $\mathbf{F}_1 = \begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1^{(1)} & \mathbf{H}_{11}\mathbf{Q}_1^{(1)} & \mathbf{H}_{21}\mathbf{Q}_2^{(1)}\end{bmatrix}$, which is a $\mathbb{R}^{N\times 3\lfloor\frac{N}{3}\rfloor}$ matrix. We null out the effect of the first components from $\mathbf{Y}_1$ by multiplying with the nulling matrix $\mathbf{Z}_1^T \in \mathbb{R}^{N \bmod 3 \times N}$ such that $\mathbf{Z}_1 = \left(\mathbf{F}_1^T\right)^\perp$, and $\tilde{\mathbf{Y}}_1 = \mathbf{Z}_1^T\mathbf{Y}_1$:

$$\tilde{\mathbf{Y}}_1 = \begin{bmatrix}\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{P}_1^{(2)} & \mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)} & \mathbf{Z}_1^T\mathbf{H}_{21}\mathbf{Q}_2^{(2)}\end{bmatrix}\begin{bmatrix}\mathbf{V}_1^{(2)}\\ \mathbf{V}_2^{(2)}+\mathbf{U}_1^{(2)}\\ \mathbf{U}_2^{(2)}\end{bmatrix} \tag{37}$$

Furthermore, we orthogonalize $\mathbf{V}_2^{(2)} + \mathbf{U}_1^{(2)}$ components by multiplying with $(\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)})^{-1}$. Hence,

$$\tilde{\tilde{\mathbf{Y}}}_1 = (\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)})^{-1}\tilde{\mathbf{Y}}_1 \tag{38}$$

$$= \mathbf{A}\mathbf{V}_1^{(2)} + (\mathbf{V}_2^{(2)} + \mathbf{U}_1^{(2)}) + \mathbf{B}\mathbf{U}_2^{(2)} \tag{39}$$

where $\mathbf{A} = (\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)})^{-1}\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{P}_1^{(2)}$ and $\mathbf{B} = (\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)})^{-1}\mathbf{Z}_1^T\mathbf{H}_{21}\mathbf{Q}_2^{(2)}$, where $\mathbf{A}, \mathbf{B}$ are now $N \bmod 3 \times$

$N \bmod 3$ matrices. By designing $\mathbf{t}_i$ as in the 2×2 system, $\mathbf{V}_1^{(2)}$ and $\mathbf{U}_2^{(2)}$ can be decoded without error. Cancelling them from $\mathbf{Y}_1$, we have:

$$\bar{\mathbf{Y}}_1=\begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1^{(1)} & \mathbf{H}_{11}\mathbf{Q}_1^{(1)} & \mathbf{H}_{21}\mathbf{Q}_2^{(1)} & \mathbf{H}_{11}\mathbf{Q}_1^{(2)}\end{bmatrix}\begin{bmatrix}\mathbf{V}_1^{(1)}\\ \mathbf{V}_2^{(1)}+\mathbf{U}_1^{(1)}\\ \mathbf{U}_2^{(1)}\\ \mathbf{V}_2^{(2)}+\mathbf{U}_1^{(2)}\end{bmatrix} \tag{40}$$

To check the decodability, the total number of dimensions is $3\lfloor\frac{N}{3}\rfloor+N \bmod 3 = N$, and hence, decodable. Thus, each user achieves $\lfloor\frac{N}{3}\rfloor+\frac{N \bmod 3}{3}=\frac{N}{3}$ with total s.d.o.f. $d_s \geq \frac{2N}{3}$.

B. For $M \geq N$

For $M > N$, we have two upper bounds. If $1 < \frac{M}{N} < 2$, we have the upper bound $\frac{4M-2N}{3}$, and if $\frac{M}{N} \geq 2$, we have the upper bound $2N$.

1) $1 < \frac{M}{N} < 2$: In this regime, a null space is available for each cross channel matrix. Thus, each user sends $M-N$ signals in the null space of the other user, and use the rest of the antennas as a square system, i.e., the achievable scheme combines spatial and asymptotic real interference alignment in addition to null space transmission. To separate the square system components from contaminating the null space components, we further precode the square system. Let $\mathbf{H}_{11}^{(1)}$, $\mathbf{H}_{12}^{(1)}$ be the $\mathbb{R}^{(M-N)\times M}$ channel matrices to the first $M-N$ antennas at the receivers. The transmitted signals are:

$$\mathbf{X}_1 = \mathbf{H}_{12}^{\perp}\mathbf{V}_{10} + \begin{bmatrix}\mathbf{H}_{11}^{(1)}\\ \mathbf{H}_{12}^{(1)}\end{bmatrix}^{\perp}\left(\mathbf{P}_1\begin{bmatrix}v_{1,1}^{(1)}\\ v_{1,2}^{(1)}\\ \vdots\\ v_{1,\lfloor\frac{\tilde{N}}{3}\rfloor}^{(1)}\\ \mathbf{t}_2^T\mathbf{v}_{11}^{(2)}\\ \mathbf{t}_2^T\mathbf{v}_{12}^{(2)}\end{bmatrix}+\mathbf{Q}_1\begin{bmatrix}u_{1,1}^{(1)}\\ u_{1,2}^{(1)}\\ \vdots\\ u_{1,\lfloor\frac{\tilde{N}}{3}\rfloor}^{(1)}\\ \mathbf{t}_1^T\mathbf{u}_{11}^{(2)}\\ \mathbf{t}_1^T\mathbf{u}_{12}^{(2)}\end{bmatrix}\right) \tag{41}$$

where $\tilde{N} = 2N-M$. This precoding separates the first $M-N$ antennas at each receiver from the square system signals. This leaves $\mathbf{V}_{i0}$ to be reliably received via zero forcing. The $\mathbf{H}_{11}\begin{bmatrix}\mathbf{H}_{11}^{(1)}\\ \mathbf{H}_{12}^{(1)}\end{bmatrix}^{\perp}$ has dimensions of $N\times(2N-M)$. Ignoring the first $M-N$ antennas at the receiver, the remaining system is $(2N-M)\times(2N-M)$, which is a square system as presented in the previous section. By considering the first $M-N$ antennas, $\mathbf{Y}_1^{(1)} = \mathbf{H}_{11}\mathbf{H}_{12}^{\perp}\mathbf{V}_{10}$. Thus, we decode $\hat{\mathbf{V}}_{10} = (\mathbf{H}_{11}\mathbf{H}_{12}^{\perp})^{\dagger}\mathbf{Y}_1^{(1)}$. Cancelling $\mathbf{V}_{10}$ from $\mathbf{Y}_1$, we are left with the square system only. The dimension sets and spatial alignment matrices can be constructed similar to (32) by defining $\bar{\mathbf{H}}_{11} = \mathbf{H}_{11}^{(2)}\begin{bmatrix}\mathbf{H}_{11}^{(1)}\\ \mathbf{H}_{12}^{(1)}\end{bmatrix}^{\perp}$, and similarly, $\bar{\mathbf{H}}_{21} = \mathbf{H}_{21}^{(2)}\begin{bmatrix}\mathbf{H}_{21}^{(1)}\\ \mathbf{H}_{22}^{(1)}\end{bmatrix}^{\perp}$, $\bar{\mathbf{H}}_{12} = \mathbf{H}_{12}^{(2)}\begin{bmatrix}\mathbf{H}_{11}^{(1)}\\ \mathbf{H}_{12}^{(1)}\end{bmatrix}^{\perp}$ and $\bar{\mathbf{H}}_{22} = \mathbf{H}_{22}^{(2)}\begin{bmatrix}\mathbf{H}_{21}^{(1)}\\ \mathbf{H}_{22}^{(1)}\end{bmatrix}^{\perp}$. We can now define the dimension sets on $\bar{\mathbf{H}}_{ij}$ as in the previous section and the asymptotic alignment remains the same.

2) $\frac{M}{N} \geq 2$: In this case, since $M \geq 2N$, each cross channel $\mathbf{H}_{12}$, $\mathbf{H}_{21}$ has $M-N$ null space components since $M-N \geq N$. Each user transmits N secure Gaussian signal components in the null space of the other receiver's channel, i.e., $\mathbf{V}_i = [v_{i_1}\, v_{i_2} \ldots v_{i_N}\, \mathbf{0}_{M-2N}^T]^T$. Thus, the transmitted signals are:

$$\mathbf{X}_1 = \mathbf{H}_{12}^{\perp}\mathbf{V}_1, \quad \mathbf{X}_2 = \mathbf{H}_{21}^{\perp}\mathbf{V}_2 \tag{42}$$

The receiver can perform pseudo-inverse to decode $\mathbf{V}_i$, i.e.,

$$\hat{\mathbf{V}}_1 = (\mathbf{H}_{11}\mathbf{H}_{12}^{\perp})^{\dagger}\mathbf{Y}_1, \quad \hat{\mathbf{V}}_2 = (\mathbf{H}_{22}\mathbf{H}_{21}^{\perp})^{\dagger}\mathbf{Y}_2 \tag{43}$$

These signals are invisible to the other receiver, and are secure.

VII. Conclusions

We determined the exact sum s.d.o.f. of a two-user $M \times N$ MIMO ICCM. For the converse proof, we combined three distinct upper bounds: the cooperative upper bound which treats ICCM as a BCCM; the upper bounding technique that uses vectorized versions of secrecy penalty and role of a helper lemmas; and the IC upper bound without any secrecy constraints. These upper bounds give a sum s.d.o.f. that is an integer multiple of $1/3$ in all cases. For achievability, if the sum s.d.o.f. is an integer (fractional part is zero) then there is no need for real interference alignment; spatial alignment suffices. If the fractional part is $1/3$, then after spatial alignment, real alignment in a single dimension is needed. For the case where the fraction is $2/3$, we developed a new novel achievable scheme for the basic 2×2 MIMO ICCM. This scheme together with its SISO counter part are central for achievable schemes for general M and N. The 2×2 scheme combines spatial alignment for secrecy and asymptotic real interference alignment for decodability.

References

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

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

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

[4] J. Xie and S. Ulukus. Secure degrees of freedom regions of multiple access and interference channels: The polytope structure. *IEEE Trans. on Info. Theory*. To appear. Also available at arXiv:1404.7478.

[5] A. S. Motahari, S. O. Gharan, M.-A. Maddah-Ali, and A. K. Khandani. Real interference alignment: Exploiting the potential of single antenna systems. *IEEE Trans. on Info. Theory*. Submitted. Also available at arXiv:0908.2282.

[6] 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*, June 2015.

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

[8] S. A. Jafar and M. J. Fakhereddin. Degrees of freedom for the MIMO interference channel. *IEEE Trans. on Info. Theory*, 53(7):2637–2642, July 2007.

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