Secure Degrees of Freedom Region of Static and Time-Varying Gaussian MIMO Interference Channel

Karim Banawan, *Student Member, IEEE*, and Sennur Ulukus, *Fellow, IEEE*

***Abstract*— We consider the two-user multiple-input multiple-output (MIMO) interference channel with confidential messages (ICCM). We determine the exact secure degrees of freedom (s.d.o.f.) region 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 interference channel with no secrecy constraints, and vector extensions of the secrecy penalty and role of a helper lemmas. For the achievability, we first show that the s.d.o.f. region is a four-vertex polytope. For the sum s.d.o.f. point, 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. We achieve the other non-trivial extreme polytope points by employing one of the transmitters as a deaf helper for assisting the secure transmission of the other user. We present simplified achievable schemes for the special case of time-varying MIMO ICCM. The achievable schemes, in this case, make use of the time-varying nature of the channel to construct vector-space alignment counterpart of the real interference alignment used in the static channel case.**

***Index Terms*— MIMO interference channel, secure degrees of freedom, confidential messages, interference alignment, static, time-varying.**

I. Introduction

PHYSICAL layer security provides unconditional and provable security schemes that are quantifiable in terms of information-theoretic quantities and rates [1]. Wyner [2] introduced the canonical wiretap channel model, which consists of a transmitter, a legitimate receiver and an eavesdropper, and showed the feasibility of attaining a positive secrecy rate in his degraded channel model. Csiszar and Korner [3] generalized Wyner's result to the case of non-degraded channels. Leung-Yan-Cheong and Hellman [4] extended these results to the Gaussian channel. The physical layer security framework is then extended to various multiuser settings such as: the multiple access wiretap channel (MAC-WT) [5], broadcast channel with confidential messages (BCCM) [6]–[10], interference channel with confidential messages (ICCM) [6], multi-receiver wiretap channels [11], [12], and relay-eavesdropper channels [13]. The secure degrees of freedom (s.d.o.f.) have been considered in the literature as a first order approximation of the secure rates (the pre-log factor of the secure rate) in many multiuser channel models, such as: helper wiretap channel [14], [15], multiple-access wiretap channel [14], [16]–[18], interference channel [14], [18]–[22], X-channel [23], [24], half-duplex relay channel [25], compound wiretap channel [26], diamond channel [27], multiuser channel models under imperfect CSIT [28]–[32].

In this work, we consider the two-user MIMO ICCM [6], where two users wish to send messages to their respective receivers reliably, while keeping them secure from the unintended receiver in the information-theoretic sense. The secrecy capacity region of the ICCM is unknown today. In fact, the capacity region of the IC without secrecy constraints is known only within a constant gap [33]. Most of the current work concentrates on the asymptotic behavior of the secrecy capacity at high SNR in terms of s.d.o.f. The exact *sum* s.d.o.f. [14], [22] and the entire s.d.o.f. *region* [18] of the single-input single-output (SISO) ICCM are known for an arbitrary number of transmitters and receivers. In this paper, we determine the *exact* s.d.o.f. *region* 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 [14] determines the exact s.d.o.f. of several SISO one-hop networks, including the wiretap channel with helpers, MAC-WT, BCCM, and ICCM. For achievability, [14] proposes real interference alignment [34] based achievable schemes that use structured codes in the form of pulse amplitude modulation (PAM). Focusing on the two-user SISO ICCM in [14], 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. This scheme results in $1/3$ s.d.o.f. for each user. For the converse, [14] 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 [22] generalizes the sum s.d.o.f. result of [14] to the case of K-users. The work in [22] shows that in order to achieve real interference alignment at multiple receivers as in the case of the K-user interference channel, *asymptotic* real interference alignment is needed. [18] generalizes [14], [22] to determine the entire

Manuscript received April 27, 2017; revised March 4, 2018; accepted May 11, 2018. Date of publication May 22, 2018; date of current version December 19, 2018. This work was supported by NSF Grants CNS 13-14733, CCF 14-22111, CCF 14-22129, and CNS 15-26608. This paper was presented in part at the 2015 Asilomar Conference.

The authors are with the Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park, MD 20742 USA (e-mail: kbanawan@umd.edu; ulukus@umd.edu).

Communicated by V. M. Prabhakaran, Associate Editor for Shannon Theory.

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

Digital Object Identifier 10.1109/TIT.2018.2839658

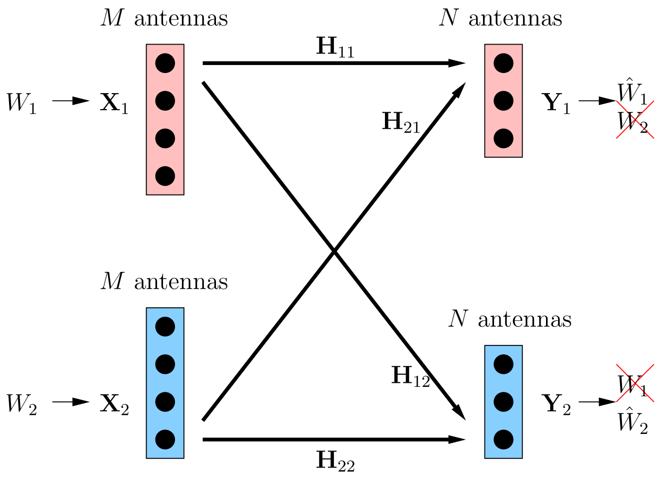


Fig. 1. Two-user MIMO ICCM.

s.d.o.f. region; [18] shows that the s.d.o.f. region has a general polytope structure and the achievability of the extreme points of this polytope region is sufficient to characterize the entire s.d.o.f. region.

Reference [15] extends the result for the wiretap channel with helpers in [14] to the case of MIMO nodes for the special case of a single helper. To that end, [15] extends the role of a helper lemma of [14] 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. Reference [15] 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 [14] is used. Since the s.d.o.f. in the case of a MIMO wiretap channel with a helper is an integer multiple of $1/2$, the strategy of projecting onto a single dimension and using a SISO achievable scheme as in [14] is sufficient.

In this paper, we extend the s.d.o.f. results for the ICCM in [14], [18], and [22] to the case of MIMO nodes, for the special case of a two-user system with an equal number of antennas at both transmitters (M) and both receivers (N). We first focus on the optimal achievability schemes for the sum s.d.o.f. point. 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, $1/3$, or $2/3$. If it is $1/3$, a projection onto a single SISO dimension as in [15] is sufficient. In this SISO dimension, we use real interference alignment scheme of [14] 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 [14] in individual dimensions. Instead, we use a spatial interference alignment scheme [35] to ensure that the leakage is negligible in the s.d.o.f. sense, and an asymptotic real interference alignment scheme [22] to minimize the required number of irrational dimensions at each antenna for decodability. The use of asymptotic alignment ensures that all antenna observations are used efficiently. Any other antenna configuration (any M and N) can be reduced to either a 1×1 ICCM (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 (whenever the number of transmit antennas is larger than the number of receive antennas) and spatial alignment.

We develop a matching converse by using three distinct outer bounds. The first upper bound is the cooperative bound, in which we allow cooperative stochastic encoding among the two users. This effectively transforms the ICCM channel into a BCCM channel, whose upper bound appears in [29]. The second upper bound uses the vectorized version of the upper bounding technique developed in [14] using the secrecy penalty and role of a helper lemmas; see also [15]. The idea of this upper bound is to calculate the secrecy penalty in terms of channel inputs and outputs, while upper bounding the differential entropy of the channel inputs. The third upper bound is the decodability upper bound developed in [36] for the IC without secrecy constraints. The intersection of these three upper bounds gives a tight upper bound for any number of antennas.

To characterize the complete s.d.o.f. region, we first prove that the region is a four-vertex polytope in general as in [18]. The non-trivial extreme points are the sum s.d.o.f. point and the two symmetric maximum individual s.d.o.f. points. We note that the s.d.o.f. region becomes a square if $\frac{N}{2} \leq M \leq \frac{2N}{3}$ or $M \geq 2N$, which implies the feasibility of simultaneous secure transmission with a full s.d.o.f. in these regimes. For other regimes, the s.d.o.f. region is a non-square polytope, since the sum s.d.o.f. point and the maximum individual s.d.o.f. points evolve differently with the number of transmit antennas M; more specifically, the sum s.d.o.f. increases linearly with a slope that is a multiple of $1/3$, in contrast to the maximum individual s.d.o.f. that grows with a slope that is a multiple of $1/2$. We derive the optimal achievable schemes for extreme points of this polytope for all antenna configuration regimes. After establishing the achievable schemes for the non-trivial points of the polytope, the rest of the region is obtained via time-sharing.

Finally, we specialize the problem to the case of time-varying ICCM. We develop simpler achievable schemes that depend on repeating the transmitted symbols over multiple channel uses. This effectively replaces the complicated asymptotic real interference alignment scheme developed for general static channels, enables a simpler vector space alignment solution, and exploits the time-diversity inherent in time-varying ICCM by joint stochastic encoding across different channel realizations.

II. System Model

We consider a two-user symmetric Gaussian MIMO ICCM. Each transmitter has M transmit antennas, and each receiver has N receive antennas. The input-output relationships of a two-user MIMO ICCM (see Fig. 1) are:

$$\mathbf{Y}_1(t) = \mathbf{H}_{11}(t)\mathbf{X}_1(t) + \mathbf{H}_{21}(t)\mathbf{X}_2(t) + \mathbf{N}_1(t) \qquad (1)$$

$$\mathbf{Y}_2(t) = \mathbf{H}_{12}(t)\mathbf{X}_1(t) + \mathbf{H}_{22}(t)\mathbf{X}_2(t) + \mathbf{N}_2(t) \qquad (2)$$

where $\mathbf{H}_{ij}(t) \in \mathbb{R}^{N\times M}$ is the channel gain matrix from transmitter i to receiver j (where $i, j \in \{1, 2\}$) at channel use t. We call the ICCM *static*, if $\mathbf{H}_{ij}(t) = \mathbf{H}_{ij}$ for all channel uses t, $\forall i, j$. The ICCM is *time-varying*, if $\mathbf{H}_{ij}(t)$ takes an independent realization at every channel use t, $\forall i, j$. We assume that $\mathbf{H}_{ij}(t)$ is picked from a continuous distribution. Hence, $\mathbf{H}_{ij}(t)$ admits rationally independent elements with probability 1. Furthermore, any finite collection of the channel gains are linearly independent with probability[1] 1. $\mathbf{X}_i(t) \in \mathbb{R}^M$ is the channel input of transmitter i at channel use t, $\mathbf{Y}_i(t) \in \mathbb{R}^N$ is the channel output of receiver i at channel use t, and $\mathbf{N}_i(t) \in \mathbb{R}^N$ is i.i.d. Gaussian noise vector with a finite variance at receiver i.

Transmitter $i \in \{1, 2\}$ sends a message W_i chosen uniformly from a message set $\mathcal{W}_i$ by encoding it into an n-letter channel input $\mathbf{X}_i^n(t)$. The message W_i is to be conveyed reliably to receiver i and to be kept secret from receiver j, where $j \neq i$. Transmitter i performs stochastic encoding f_i over n channel uses $f_i : \mathcal{W}_i \to \mathbf{X}_i^n(t)$ such that for any $\epsilon > 0$, the following reliability and security constraints are satisfied:

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

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

where $\hat{W}_i$ is the estimate of W_i at receiver i. The channel inputs are subject to average power constraints $\mathrm{tr}(\mathbb{E}[\mathbf{X}_i(t)\mathbf{X}_i(t)^T]) \leq P$, $i = 1, 2$. The rate of user i is $R_i = \frac{1}{n}\log|\mathcal{W}_i|$. The s.d.o.f. d_i of user i is:

$$d_i = \lim_{P\to\infty} \frac{R_i}{\frac{1}{2}\log P} \tag{5}$$

The sum s.d.o.f. d_s is given by $d_s = d_1 + d_2$.

III. Preliminaries

In this section, we review the real interference alignment and spatial alignment techniques as they are the main ingredients of our achievable scheme. In this work, we combine both techniques for MIMO ICCM with static channels.

A. Real Interference Alignment

The real interference alignment technique, which is introduced in [34] and employed in [14] for achieving the s.d.o.f. for one-hop networks, relies on transmitting multiple data streams of PAM signals. Specifically, let $\{b_i\}_{i=1}^L$ be a sequence of L symbols. The symbol b_i is picked from PAM constellation $C(a, Q)$, where a is the separation between any two symbols in the constellation set and the number of symbols in the constellation set is given by $2Q + 1$, i.e., $C(a, Q) = a\{-Q, -Q+1, \cdots, Q-1, Q\}$. Now, consider transmitting these L symbols simultaneously in the form of a linear combination,

$$x = \sum_{i=1}^{L} \alpha_i b_i \tag{6}$$

where $\{\alpha_i : i = 1, \cdots, L\}$ are *rationally independent* real numbers. The rational independence means that if $\sum_{i=1}^{L} \alpha_i q_i = 0$ for some $q_1, \cdots, q_L$ which are rational numbers, then $q_i = 0$ for all i.

Although the signal x is a mixture of $\{b_i\}_{i=1}^L$, these symbols lie in separate rational dimensions if we choose,

$$Q = P^{\frac{1-\delta}{2(L+\delta)}}, \quad a = \gamma \frac{P^{\frac{1}{2}}}{Q} \tag{7}$$

for some $\delta > 0$, a positive constant γ which is independent of P that is chosen to satisfy the power constraint [34]. In this case, the constellation observed at the receiver side consists of $(2Q+1)^L$ points and the probability of error can be upper bounded $P_e \leq \exp(-\eta_\gamma P^\delta)$. To summarize: by careful choice of $C(a, Q)$ (e.g., by choosing the number of points as a function of L as in (7)), one can send L separable data streams that satisfy the average power and the reliability constraints. This is done by creating and exploiting *rational dimensions*.

This technique can be effectively used for security as in [14]. To achieve this, the transmitted signals in general consist of two components, namely, the secure signal V, and the cooperative jamming signal U. The cooperative jamming component U_i from transmitter i is utilized to satisfy the security constraint of transmitter j by being aligned with V_j in the same rational dimension. This can be done by scaling both U_i and V_j by real coefficients such that their scaling is the same at the receiver after passing through the channel. More specifically, the ith transmitter sends $X_i = \alpha_i U_i$ and the jth transmitter sends $X_j = \alpha_j V_j$, such that $\alpha_i h_{ij} = \alpha_j h_{jj}$, where h_{ij} is the channel gain from transmitter i to receiver j and h_{jj} is the channel gain from transmitter j to receiver j. This satisfies the security at the jth receiver as the received signal will have a component $\alpha_j h_{jj}(U_i + V_j)$, i.e., the secure signal and the cooperative jamming signal lie in the same rational dimension and hence the leakage is upper bounded by a constant.

B. Spatial Alignment

The spatial alignment technique, introduced in [35], can be used for security as well if the system is equipped by multiple antennas. Spatial alignment does not require a specific signaling scheme, i.e., it does not require transmitting PAM signals as in the real interference alignment scheme, instead Gaussian signaling can be used. The spatial alignment exploits the *spatial dimensions* offered by the multiple antennas in contrast to the *rational dimensions* in the real interference alignment scheme.

To achieve this, the ith transmitter transmits precoded version of the cooperative jamming signal $\mathbf{U}_i$ by transmitting $\mathbf{X}_i = \mathbf{Q}_i\mathbf{U}_i$, where $\mathbf{Q}_i$ is a precoding matrix for the cooperative jamming components from the ith transmitter. Furthermore, the jth transmitter sends $\mathbf{X}_j = \mathbf{P}_j\mathbf{V}_j$, where $\mathbf{P}_j$ is the precoding matrix for the secure signal component from the jth transmitter. This is achievable since both transmitters are equipped by multiple transmit antennas. By ensuring that $\mathbf{Q}_i\mathbf{H}_{ij} = \mathbf{P}_j\mathbf{H}_{jj}$, both signal components are aligned in the same *spatial dimension* at the jth receiver, i.e., the received

[1] In the exposition of the results, the phrase "for almost all" refers to the rational/linear independence, which occurs with probability 1.

signal has a component $\mathbf{P}_j\mathbf{H}_{jj}(\mathbf{U}_i + \mathbf{V}_j)$. This satisfies the security constraint as well.

Note that in order to ensure reliable decoding at the receiver by a zero forcing decoder, the total number of spatial dimensions spanned by the signal components must be at most N (the number of receive antennas). This is parallel to choosing Q in the real interference alignment scheme. Furthermore, this precoding idea can be extended as in [35] for time-varying SISO channels by *symbol extension*, i.e., completing the transmission over multiple time slots and dealing with the transmitted symbols across time as a spatial vector. In this case, the alignment technique exploits the *time dimension*.

C. Comparison of the Two Alignment Techniques

We note that the main strength of the real interference alignment technique is that it creates a potential of performing interference alignment even for SISO channels which do not enjoy time-varying diversity. This technique requires rational independence of the channel coefficients. However, the decoding procedure of this scheme is generally more complex than spatial alignment that uses simple zero-forcing decoder.

On the other hand, the spatial alignment technique requires either the presence of multiple antennas and/or time-varying channels. This hinders the usage of spatial alignment for static channels despite its simplicity.

IV. Main Results and Discussions

The first result of this paper characterizes the sum s.d.o.f. d_s of the two-user $M \times N$ MIMO ICCM for arbitrary M and N.

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

$$d_s = \begin{cases} \min\{\frac{2N}{3}, [4M-2N]^+\}, & M \leq N \\ \min\{2N, \frac{4M-2N}{3}\}, & M \geq N \end{cases} \tag{8}$$

for almost all channel gains.

Remark 1: For a fixed number of receive antennas N, the sum s.d.o.f. d_s is a piece-wise non-decreasing function of the number of transmitting antennas M. d_s in (8) consists of five regimes that can be written explicitly as,

$$d_s = \begin{cases} 0, & M \leq \frac{N}{2} \\ 4M-2N, & \frac{N}{2} \leq M \leq \frac{2N}{3} \\ \frac{2N}{3}, & \frac{2N}{3} \leq M \leq N \\ \frac{4M-2N}{3}, & N \leq M \leq 2N \\ 2N, & M \geq 2N \end{cases} \tag{9}$$

i.e., d_s increases linearly with M if $\frac{N}{2} \leq M \leq \frac{2N}{3}$ with slope 4. Then, d_s becomes a constant value of $\frac{2N}{3}$ in the regime $\frac{2N}{3} \leq M \leq N$. Next, d_s increases linearly again with slope $\frac{4}{3}$ until it hits $M = 2N$ and continues as $2N$ afterwards. The sum s.d.o.f. as a function of M for an 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 [14].

Remark 2: The term "for almost all channel gains" in Theorem 1 refers to the fact that our achievable schemes for the static ICCM depends on real interference alignment, which necessitates that the channel gains are rationally independent. Since the channel gains are assumed to be drawn randomly from a continuous distribution over $\mathbb{R}^{N\times M}$, the achievable schemes are feasible for almost all channel gains. The same comment holds true for the time-varying ICCM, as the achievable schemes, in this case, assume linear independence of channel gains.

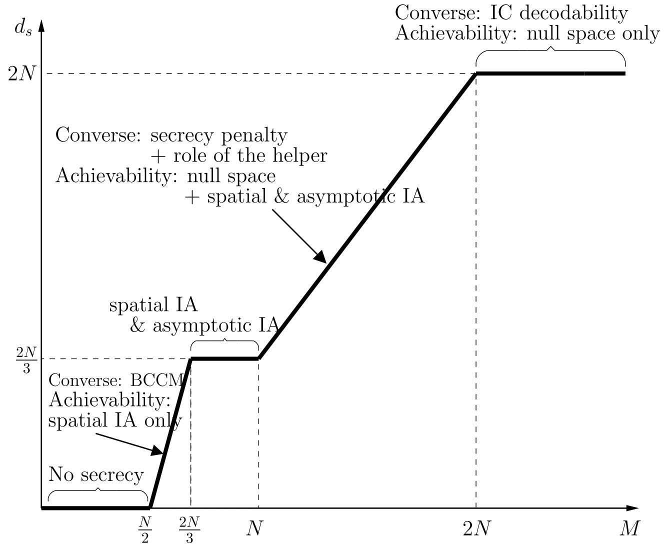


Fig. 2. Sum s.d.o.f. of $M \times N$ two-user ICCM for a given N.

Remark 3: The sum s.d.o.f. in the regime $\frac{N}{2} \leq M \leq \frac{2N}{3}$ coincides with the sum s.d.o.f. of the MIMO BCCM with the transmitter having $2M$ antennas. This implies that, in this regime, there is no loss in the sum s.d.o.f. due to independent coding of the users with respect to the sum s.d.o.f. obtained if cooperation (joint encoding) is allowed.

Remark 4: The sum s.d.o.f. in the regime $\frac{2N}{3} \leq M \leq N$ is constant. This implies that there is no gain in the sum s.d.o.f. that can be obtained by increasing the number of transmit antennas in this regime.

Remark 5: The sum s.d.o.f. in the regime $M \geq 2N$ coincides with the sum degrees of freedom (d.o.f.) of the IC with no security constraints. This implies that there is no loss in the sum s.d.o.f. due to enforcing the security constraint, i.e., we achieve security for free in this regime.

The second result characterizes the entire s.d.o.f. region for the two-user $M \times N$ ICCM.

Theorem 2: The s.d.o.f. region of the two-user $M\times N$ ICCM is given by the set of all pairs (d_1, d_2) that lie in the four-vertex polytope, which is defined as

$$\mathcal{C} = \left\{(d_1, d_2) \in \text{conv}\left\{(0,0), (d_m, 0), (0, d_m), \left(\frac{d_s}{2}, \frac{d_s}{2}\right)\right\}\right\} \tag{10}$$

where conv *denotes the convex hull, and d_m is the maximum individual s.d.o.f., which is given by,*

$$d_m = \begin{cases} \min\{\frac{N}{2}, [2M-N]^+\}, & M \leq N \\ \min\{N, \frac{2M-N}{2}\}, & M \geq N \end{cases} \tag{11}$$

$$\mathcal{C}=\begin{cases}\{(d_1,d_2):d_1=0,\ d_2=0\}, & M\le\frac{N}{2}\\ \{(d_1,d_2):d_1\le 2M-N,\ d_2\le 2M-N,\ d_1\ge 0,\ d_2\ge 0\}, & \frac{N}{2}\le M\le\frac{2N}{3}\\ \{(d_1,d_2):Nd_i+(6M-4N)d_j\le N(2M-N),\ d_i\ge 0,\ i,\ j=1,2\}, & \frac{2N}{3}\le M\le\frac{3N}{4}\\ \{(d_1,d_2):d_1+2d_2\le N,\ 2d_1+d_2\le N,\ d_1\ge 0,\ d_2\ge 0\}, & \frac{3N}{4}\le M\le N\\ \{(d_1,d_2):d_1+2d_2\le 2M-N,\ 2d_1+d_2\le 2M-N,\ d_1\ge 0,\ d_2\ge 0\}, & N\le M\le\frac{3N}{2}\\ \{(d_1,d_2):(2M-N)d_i+(4N-2M)d_j\le N(2M-N),\ d_i\ge 0,\ i,j=1,2\}, & \frac{3N}{2}\le M\le 2N\\ \{(d_1,d_2):d_1\le N,\ d_2\le N\ d_1\ge 0,\ d_2\ge 0\}, & M\ge 2N\end{cases}\tag{12}$$

and d_s is defined as in (8). The result holds for almost all channel gains.

Remark 6: The s.d.o.f. region can be written in an explicit form as $\mathcal{C}$ in (12)*, as shown at the top of this page, for almost all channel gains.*

Remark 7: The maximum individual s.d.o.f. of each user d_m follows a pattern similar to the sum s.d.o.f. in Remark 1. d_m coincides with the s.d.o.f. of the MIMO wiretap channel with $2M$ antennas at the transmitter and N receive antennas for $\frac{N}{2}\le M\le\frac{3N}{4}$. Then, d_m is constant at $\frac{N}{2}$ for the regime $\frac{3N}{4}\le M\le N$. Next, d_m increases linearly with M with slope 1 until $M=\frac{3N}{2}$. The maximum individual s.d.o.f. is constant at N afterwards, which coincides with the maximum individual d.o.f. of MIMO channel with N receive antennas with no security constraints.

Remark 8: From Remarks 1 and 7, we can track the evolution of the s.d.o.f. region by noting the evolution of the extreme points of the corresponding polytope as in Fig. 3. We start with a square region with $d_m=2M-N$, this region increases in size while keeping its square shape with the increase of M until $M=\frac{2N}{3}$. Starting from this point, we cannot support a sum s.d.o.f. larger than $\frac{2N}{3}$. Consequently, the sum s.d.o.f. point is kept constant, while the maximum individual s.d.o.f. points can still increase and the s.d.o.f. region is no longer a square region. This continues until $M=\frac{3N}{4}$, then the maximum s.d.o.f. points are kept constant to $\frac{N}{2}$. This implies that the s.d.o.f. region does not grow in the regime $\frac{3N}{4}\le M\le N$. The s.d.o.f. region starts increasing in size again from $M=N$. The maximum individual s.d.o.f. points increase linearly with slope 1*, while, the sum s.d.o.f. point increases with slope $\frac{2}{3}$. Since slopes are different, the maximum individual s.d.o.f. point hits the N bound first at $M=\frac{3N}{2}$, while the sum s.d.o.f. point hits this bound at $M=2N$ and we are back to a square region again.*

Remark 9: For the regimes $\frac{N}{2}\le M\le\frac{2N}{3}$ and $M\ge 2N$, the s.d.o.f. region is a square, which implies that both users can transmit with their corresponding maximum s.d.o.f. without sacrificing from their individual s.d.o.f.

V. Outer 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. region of this BCCM is a square whose corner points are $(\min\{[2M-N]^+,N\},0)$, $(\min\{[2M-N]^+,N\},\min\{[2M-N]^+,N\})$, $(0,\min\{[2M-N]^+,N\})$ [29]. Hence, the individual s.d.o.f. of the two users is upper bounded by:

$$d_i\le\min\{N,[2M-N]^+\},\quad i=1,2\tag{13}$$

and the sum s.d.o.f. is upper bounded by:

$$d_s\le 2\min\{N,[2M-N]^+\}=\min\{2N,[4M-2N]^+\}\tag{14}$$

Therefore, for $M<N$, the s.d.o.f. region of the MIMO ICCM, $\mathcal{C}$, is upper bounded by the region $\{(d_1,d_2):d_i\ge 0,\ d_i\le 2M-N\}$.

B. For $M\ge N$

We have two distinct upper bounds for the MIMO ICCM when $M\ge N$. From the sum d.o.f. of the two-user IC with no secrecy constraints, $\tilde{d}$, we have the following bound [36]:

$$\begin{aligned}d_s\le\tilde{d}&=\min\{M_1+M_2,N_1+N_2,\max\{M_1,N_2\},\\&\qquad\max\{M_2,N_1\}\}&(15)\\&=\min\{2M,2N,\max\{M,N\}\}&(16)\\&=\min\{2N,M\}&(17)\end{aligned}$$

The above upper bound corresponds to the decodability of IC without secrecy constraints. In addition, for the individual s.d.o.f. d_m, we have $d_m\le N$ if $M\ge N$ from the single-user MIMO channel.

In order to derive an upper bound using the secrecy constraints, we follow the techniques in [14] and [15]. From the *secrecy penalty lemma* in [14], we have:

$$nR_i\le h(\tilde{\mathbf{X}}_1^n)+h(\tilde{\mathbf{X}}_2^n)-h(\mathbf{Y}_j^n)+nc_1\tag{18}$$

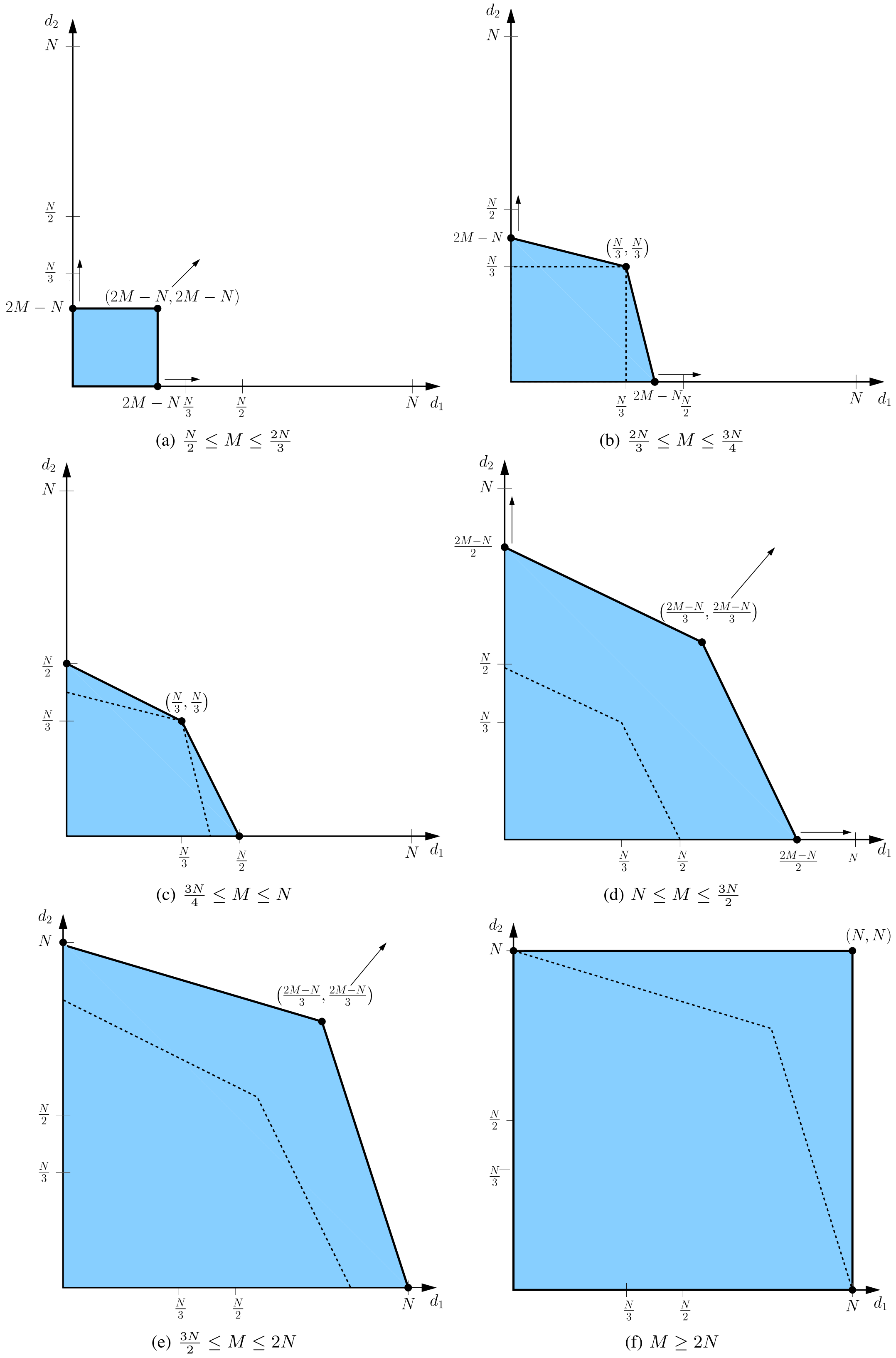
where $i\ne j$, and $\tilde{\mathbf{X}}_i^n=\mathbf{X}_i^n+\tilde{\mathbf{N}}_i^n$ is a finite-variance Gaussian perturbed channel input; here small Gaussian perturbation is introduced in order to avoid mixing continuous and discrete entropies, see [14]. In addition, we have the following vectorized version of the *role of a helper lemma* of [14] (see also [15]).

Lemma 1 (MIMO Role of a Helper Lemma): For $M\ge N$, reliable decoding of the jth transmitter at the ith receiver, $i\ne j$, is guaranteed if the perturbed channel input $\tilde{\mathbf{X}}_i^n$ satisfies

$$h(\tilde{\mathbf{X}}_i^n)\le h(\tilde{\mathbf{X}}_i^{n(2)})+h(\mathbf{Y}_j^n)-nR_j+nc_2,\quad i\ne j\tag{19}$$

where $\tilde{\mathbf{X}}_i^{n(2)}=[\tilde{X}_i^n(N+1)\ \ \tilde{X}_i^n(N+2)\ \ \dots\ \ \tilde{X}_i^n(M)]$.

Remark 10: $\tilde{\mathbf{X}}_i^{n(1)}=[\tilde{X}_i^n(1)\ \ \tilde{X}_i^n(2)\ \ \dots\ \ \tilde{X}_i^n(N)]$ represents the first N (perturbed) antenna inputs, and



(a) $\frac{N}{2} \leq M \leq \frac{2N}{3}$

(b) $\frac{2N}{3} \leq M \leq \frac{3N}{4}$

(c) $\frac{3N}{4} \leq M \leq N$

(d) $N \leq M \leq \frac{3N}{2}$

(e) $\frac{3N}{2} \leq M \leq 2N$

(f) $M \geq 2N$

Fig. 3. Evolution of the s.d.o.f. region with M for a fixed N. The dashed lines in each sub-figure correspond to the rate region in the previous regime for better viewing of how the region evolves.

$\tilde{\mathbf{X}}_i^{n(2)} = [\tilde{X}_i^n(N+1) \ \ \tilde{X}_i^n(N+2) \ \ \dots \ \ \tilde{X}_i^n(M)]$ *represents the* $M-N$ *extra (perturbed) antenna inputs that can be used for null space transmission. Note that, here we have* $M \geq N$, *therefore,* $\tilde{\mathbf{X}}_i^{n(2)}$ *is well-defined. We note also that intuitively we should separate the upper bounding of differential entropies of* $\tilde{\mathbf{X}}_i^{n(1)}$ *and* $\tilde{\mathbf{X}}_i^{n(2)}$ *because the null space components do not* *hurt the other receiver (in fact, they are invisible to the other receiver) as* $\tilde{\mathbf{X}}_i^{n^{(1)}}$ *components do. Consequently, we upper bound the differential entropy of these components directly using Gaussian entropy bounds.*

Proof: Let $\tilde{\mathbf{X}}_i^n = [\tilde{\mathbf{X}}_i^{n^{(1)}} \tilde{\mathbf{X}}_i^{n^{(2)}}]$. Using Fano's inequality, the rate of user j, where $j \neq i$, is upper bounded by

$$\begin{aligned} nR_j &\leq I(\mathbf{X}_j^n; \mathbf{Y}_j^n) + nc_3 && (20)\\ &= h(\mathbf{Y}_j^n) - h(\mathbf{Y}_j^n|\mathbf{X}_j^n) + nc_3 && (21)\\ &\leq h(\mathbf{Y}_j^n) - h(\mathbf{Y}_j^n|\mathbf{X}_j^n, \tilde{\mathbf{X}}_i^{n^{(2)}}) + nc_3 && (22)\\ &= h(\mathbf{Y}_j^n) - h(\mathbf{H}_{jj}\mathbf{X}_j^n + \mathbf{H}_{ij}^{(1)}\mathbf{X}_i^{n^{(1)}} + \mathbf{H}_{ij}^{(2)}\mathbf{X}_i^{n^{(2)}} \\ &\qquad + \mathbf{N}_j^n|\mathbf{X}_j^n, \tilde{\mathbf{X}}_i^{n^{(2)}}) + nc_3 && (23)\\ &\leq h(\mathbf{Y}_j^n) - h(\mathbf{H}_{ij}^{(1)}\tilde{\mathbf{X}}_i^{n^{(1)}} + \mathbf{H}_{ij}^{(2)}\tilde{\mathbf{X}}_i^{n^{(2)}}|\mathbf{X}_j^n, \tilde{\mathbf{X}}_i^{n^{(2)}}) + nc_3 \\ & && (24)\\ &= h(\mathbf{Y}_j^n) - h(\tilde{\mathbf{X}}_i^{n^{(1)}}|\tilde{\mathbf{X}}_i^{n^{(2)}}) + nc_2 && (25) \end{aligned}$$

where $\tilde{\mathbf{X}}_i^n = \mathbf{X}_i^n + \tilde{\mathbf{N}}_i^n$ such that $\tilde{\mathbf{N}}_i^n \sim \mathcal{N}(\mathbf{0}, \rho_i\mathbf{I}_M)$, where $\rho_i < \min_j \frac{1}{||\mathbf{H}_{ij}||^2}$. (24) follows from considering a stochastically equivalent version of $\mathbf{Y}_j$ given by $\tilde{\mathbf{Y}}_j = \mathbf{H}_{jj}\mathbf{X}_j + \mathbf{H}_{ij}\tilde{\mathbf{X}}_i + \bar{\mathbf{N}}_j$, where $\bar{\mathbf{N}}_j \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_M - \rho_i\mathbf{H}_{ij}\mathbf{H}_{ij}^T)$, hence $h(\mathbf{H}_{jj}\mathbf{X}_j^n + \mathbf{H}_{ij}^{(1)}\mathbf{X}_i^{n^{(1)}} + \mathbf{H}_{ij}^{(2)}\mathbf{X}_i^{n^{(2)}} + \mathbf{N}_j|\mathbf{X}_j^n, \tilde{\mathbf{X}}_i^{n^{(2)}}) \geq h(\mathbf{H}_{jj}\mathbf{X}_j^n + \mathbf{H}_{ij}^{(1)}\tilde{\mathbf{X}}_i^{n^{(1)}} + \mathbf{H}_{ij}^{(2)}\tilde{\mathbf{X}}_i^{n^{(2)}}|\mathbf{X}_j^n, \tilde{\mathbf{X}}_i^{n^{(2)}})$. (25) follows from the scaling property of the differential entropy which results in an additional constant that does not depend on P. Hence, the conditional entropy of the ith user's channel input is upper bounded by

$$h(\tilde{\mathbf{X}}_i^{n^{(1)}}|\tilde{\mathbf{X}}_i^{n^{(2)}}) \leq h(\mathbf{Y}_j^n) - nR_j + nc_2 \tag{26}$$

By applying chain rule for users' inputs $h(\tilde{\mathbf{X}}_i^n) = h(\tilde{\mathbf{X}}_i^{n^{(2)}}) + h(\tilde{\mathbf{X}}_i^{n^{(1)}}|\tilde{\mathbf{X}}_i^{n^{(2)}})$, we have (19). ■

By applying the secrecy penalty and MIMO role of a helper lemmas in (18), (19) for user 1, we have the following upper bound

$$nR_1 \leq h(\tilde{\mathbf{X}}_1^{n^{(2)}}) + h(\tilde{\mathbf{X}}_2^{n^{(2)}}) + h(\mathbf{Y}_1^n) - nR_1 - nR_2 + nc_4 \tag{27}$$

which is equivalent to

$$n(2R_1 + R_2) \leq h(\tilde{\mathbf{X}}_1^{n^{(2)}}) + h(\tilde{\mathbf{X}}_2^{n^{(2)}}) + h(\mathbf{Y}_1^n) + nc_4 \tag{28}$$

Using the fact that Gaussian random variables maximize the differential entropy, we obtain:

$$\begin{aligned} n(2R_1 + R_2) &\leq h(\tilde{\mathbf{X}}_1^{n^{(2)}}) + h(\tilde{\mathbf{X}}_2^{n^{(2)}}) + h(\mathbf{Y}_1^n) + nc_4 && (29)\\ &\leq (M - N) \cdot \frac{n}{2}\log P + (M - N) \cdot \frac{n}{2}\log P \\ &\quad + N \cdot \frac{n}{2}\log P + nc_5 && (30)\\ &= (2M - N) \cdot \frac{n}{2}\log P + nc_5 && (31) \end{aligned}$$

Dividing by n yields,

$$2R_1 + R_2 \leq (2M - N) \cdot \frac{1}{2}\log P + c_5 \tag{32}$$

and by dividing by $\frac{1}{2}\log P$ and taking the limit as $P \to \infty$, we obtain:

$$2d_1 + d_2 \leq 2M - N \tag{33}$$

By symmetry, we obtain the following upper bound by writing the secrecy penalty and role of a helper lemmas for user 2

$$d_1 + 2d_2 \leq 2M - N \tag{34}$$

Also, adding (33) and (34), we obtain the following upper bound on the sum s.d.o.f. d_s

$$d_1 + d_2 \leq \frac{4M - 2N}{3} \tag{35}$$

Consequently, the s.d.o.f. region $\mathcal{C}$ is upper bounded by the region $\{(d_1, d_2) : d_i + 2d_j \leq 2M - N,\ d_i \geq 0,\ \ i, j = 1, 2, j \neq i\}$ for $M \geq N$.

Focusing on the sum s.d.o.f., from (35) and (17) we have the upper bound on the sum s.d.o.f. as

$$d_s \leq \min\left\{\frac{4M - 2N}{3}, M, 2N\right\} \tag{36}$$

If the first term in the upper bound is not active, then $M \leq \frac{4M-2N}{3}$ or $2N \leq \frac{4M-2N}{3}$, which both lead to $M \geq 2N$ and hence the M term in the upper bound is never active, and the sum s.d.o.f. upper bound is

$$d_s \leq \min\left\{\frac{4M - 2N}{3}, 2N\right\} \tag{37}$$

Focusing on the maximum individual s.d.o.f. points, from (33) and (34), we have $d_m \leq \frac{2M-N}{2}$. Including the maximum d.o.f. upper bound for the MIMO channel, we have

$$d_m \leq \min\left\{\frac{2M - N}{2}, N\right\} \tag{38}$$

C. Combining Both Bounds

First, we note that since the outer bounds in (13)-(14) and (36)-(37) define a bounded polyhedron in $\mathbb{R}^2$, the outer bounds form a polytope as in [18]. Thus, it is sufficient to characterize upper bounds for its extreme points.

Now, 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, $d_s \leq \frac{2N}{3}$ corresponding to the case of $M = N$ for both the sum s.d.o.f. point and the maximum individual s.d.o.f. point. For the sum s.d.o.f. point, the upper bound in (35) is $\frac{2N}{3}$ for the case $M = N$. Combining the bounds (14) and $d_s \leq \frac{2N}{3}$, we have $d_s \leq \min\{\frac{2N}{3}, 4M - 2N\}$ for $M \leq N$. Consequently, the upper bound for the sum s.d.o.f. of the ICCM for any arbitrary M and N is,

$$d_s = \begin{cases} \min\{\frac{2N}{3}, [4M - 2N]^+\}, & M \leq N \\ \min\{2N, \frac{4M-2N}{3}\}, & M \geq N \end{cases} \tag{39}$$

Similarly, for the maximum individual s.d.o.f. point, the upper bound in (38) for the case $M = N$ is $\frac{N}{2}$. Hence, combining this with (13), $d_m \leq \min\{\frac{N}{2}, [2M - N]^+\}$ for $M \leq N$. Consequently, the maximum individual s.d.o.f. of the ICCM for any arbitrary M and N is,

$$d_m = \begin{cases} \min\{\frac{N}{2}, [2M - N]^+\}, & M \leq N \\ \min\{N, \frac{2M-N}{2}\}, & M \geq N \end{cases} \tag{40}$$

Since the problem is symmetric with respect to the two users, there exists a symmetric sum s.d.o.f. point $\left(\frac{d_s}{2}, \frac{d_s}{2}\right)$ and two maximum individual s.d.o.f. points $(0, d_m)$, $(d_m, 0)$.

VI. Achievable Scheme for Sum s.d.o.f. of the 2 × 2 ICCM for Static Channels

In this section, we develop optimal achievable schemes to match the presented upper bounds. First, we focus on the sum s.d.o.f. point $\left(\frac{d_s}{2}, \frac{d_s}{2}\right)$ for the case of static channels, i.e., $\mathbf{H}_{ij}(t) = \mathbf{H}_{ij}, \ \forall t$. We start by proposing a novel achievable scheme for the 2×2 ICCM system using asymptotic real interference alignment. Then, we build on this achievable scheme to obtain achievable schemes for any M, N by combining spatial alignment and exploiting the null space (whenever possible, i.e., $M > N$) with the 2×2 scheme. Real interference alignment is not needed in regimes that correspond to integer s.d.o.f., i.e., it suffices to use Gaussian codebooks along with spatial alignment and/or null space transmission in these cases. To carry out the secure rate calculation, we use the following result from [6] which states that the following secure rates are achievable for the ICCM[2]:

$$R_1 \leq I(\mathbf{V}_1; \mathbf{Y}_1) - I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2) \tag{41}$$

$$R_2 \leq I(\mathbf{V}_2; \mathbf{Y}_2) - I(\mathbf{V}_2; \mathbf{Y}_1|\mathbf{V}_1) \tag{42}$$

A. Basic System: 2 × 2 MIMO ICCM

The basic building blocks of all achievable schemes for the sum s.d.o.f. point when the channel is static 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 [14]. In this section, we give an achievable scheme for the 2×2 MIMO ICCM. The achievable scheme for the 2×2 system combines spatial alignment with asymptotic real interference alignment. To use asymptotic real interference alignment, the secure signal $\mathbf{V}_i$ and the cooperative jamming signal $\mathbf{U}_i$ are constructed as a linear combination of structured signals picked from PAM constellation $C(a, Q)$ with proper parameters that will be identified shortly. The transmitted signals are:

$$\mathbf{X}_1 = \mathbf{H}_{12}^{-1}\mathbf{V}_1 + \mathbf{H}_{11}^{-1}\mathbf{U}_1 \tag{43}$$

$$\mathbf{X}_2 = \mathbf{H}_{21}^{-1}\mathbf{V}_2 + \mathbf{H}_{22}^{-1}\mathbf{U}_2 \tag{44}$$

The received signals are:

$$\begin{aligned}\mathbf{Y}_1 &= \mathbf{H}_{11}\mathbf{H}_{12}^{-1}\mathbf{V}_1 + (\mathbf{U}_1 + \mathbf{V}_2) + \mathbf{H}_{21}\mathbf{H}_{22}^{-1}\mathbf{U}_2 + \mathbf{N}_1\\ &= \mathbf{A}\mathbf{V}_1 + (\mathbf{U}_1 + \mathbf{V}_2) + \mathbf{B}\mathbf{U}_2 + \mathbf{N}_1\end{aligned} \tag{45}$$

and

$$\begin{aligned}\mathbf{Y}_2 &= (\mathbf{V}_1 + \mathbf{U}_2) + \mathbf{H}_{12}\mathbf{H}_{11}^{-1}\mathbf{U}_1 + \mathbf{H}_{22}\mathbf{H}_{21}^{-1}\mathbf{V}_2 + \mathbf{N}_2\\ &= (\mathbf{V}_1 + \mathbf{U}_2) + \bar{\mathbf{B}}\mathbf{U}_1 + \bar{\mathbf{A}}\mathbf{V}_2 + \mathbf{N}_2\end{aligned} \tag{46}$$

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 in order to decode $\mathbf{V}_i$ with arbitrary small probability of error. However, this wastes the observation space of the second antenna and achieves an s.d.o.f. of $2/5$ from only one antenna.

To see this, let a_{ij}, $i, j \in \{1, 2\}$ be the (i, j)th element of matrix $\mathbf{A}$, and similarly for the other matrices $\mathbf{B}, \bar{\mathbf{A}} = \mathbf{H}_{22}\mathbf{H}_{21}^{-1}, \bar{\mathbf{B}} = \mathbf{H}_{12}\mathbf{H}_{11}^{-1}$. Then, the received signal at receiver 1 is

$$\mathbf{Y}_1 = \begin{bmatrix} a_{11}v_{11} + a_{12}v_{12} + (u_{11} + v_{21}) + b_{11}u_{21} + b_{12}u_{22} \\ a_{21}v_{11} + a_{22}v_{12} + (u_{12} + v_{22}) + b_{21}u_{21} + b_{22}u_{22} \end{bmatrix} + \mathbf{N}_1 \tag{47}$$

where $\mathbf{V}_1 = [v_{11} \ v_{12}]^T, \mathbf{U}_2 = [u_{21} \ u_{22}]^T$. The scaling factors $\{a_{ij}\}_{i,j=1,2}$, $\{b_{ij}\}_{i,j=1,2}$, and 1 are rationally independent almost surely. Thus, in order to decode v_{11}, v_{12} with arbitrarily small probability of error using exact real interference alignment as in [14] and [34], we need to construct at least 5 irrational dimensions. We note also that from antenna 2, the same symbols v_{11}, v_{12} can be decoded. Hence, by using exact real interference alignment, we exploit the observation of the first antenna only, as the second antenna does not give any new information. Consequently, from the first antenna, we achieve an s.d.o.f. of $2/5$, as 2 components of the secure signal can be decoded out of the 5 irrational dimensions needed for correct decoding. To minimize the required irrational dimensions, we need to leave one of v_{11} or v_{12} to be in a separate irrational dimension at each antenna, while the other component is aligned with u_{21}, u_{22}. This type of alignment can be done asymptotically by breaking $\{v_{ij}\}_{i,j=1,2}$, $\{u_{ij}\}_{i,j=1,2}$ into sufficiently large number of components. Hence, for the first antenna, the components of signal v_{11} are in separate irrational dimensions that cover $1/3$ of the total dimensions, and the signal components of $(u_{11}+v_{21})$ cover $1/3$ of the total dimensions, while the signal components of v_{12}, u_{21}, u_{22} are asymptotically aligned together and cover slightly larger than $1/3$ of the total irrational dimensions. Consequently, user 1 can achieve $1/3$ s.d.o.f. from the first antenna. A similar argument holds for the second antenna with switching the roles of v_{11} and v_{12}. This scheme is illustrated in Fig. 4.

We begin discussing the details of the asymptotic real interference alignment [22] by defining sets of irrational dimensions T_i

$$T_1 = \left\{ \prod_{i,j=1, i\neq j}^{2} \bar{a}_{ij}^{r_{ij}} \prod_{i,j=1}^{2} \bar{b}_{ij}^{s_{ij}} : r_{ij}, s_{ij} = 1, \dots, m \right\} \tag{48}$$

$$T_2 = \left\{ \prod_{i,j=1, i\neq j}^{2} a_{ij}^{r_{ij}} \prod_{i,j=1}^{2} b_{ij}^{s_{ij}} : r_{ij}, s_{ij} = 1, \dots, m \right\} \tag{49}$$

[2] Interestingly, the rate region in (41) and (42) is also achievable under the strong security constraint as shown in [37, Th. 1] and [38, Remark 1]. This implies that our s.d.o.f. region is in fact valid if we changed the security constraint to the strong security constraint, i.e., $I(W_i; \mathbf{Y}_j^n) \leq \epsilon$, for $i, j \in \{1, 2\}$ without normalization with n. Note that any scheme that achieves the strong security constraint is a valid achievable scheme under the weak security constraint as well.

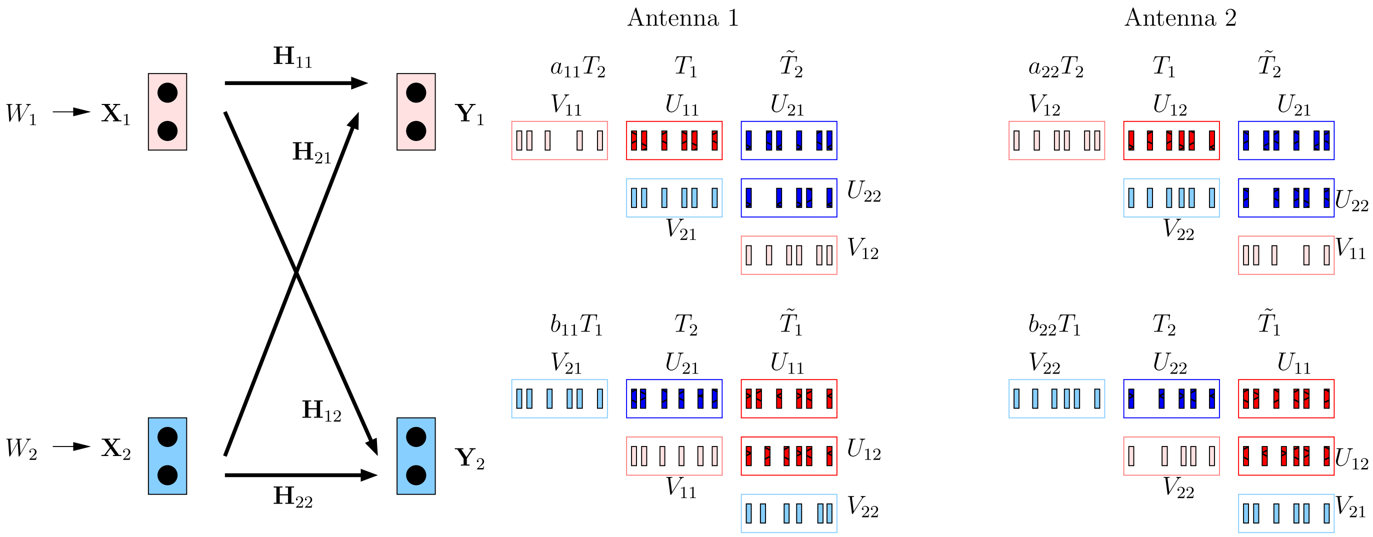


Fig. 4. Illustration of asymptotic real interference alignment for the 2 × 2 system.

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 (which is also the length of the $\mathbf{t}_i$ vector) is given by

$$M_T = |T_i| = m^6, \quad i = 1, 2 \tag{50}$$

We note that T_i set does not contain the gains $a_{ii}, \bar{a}_{ii}$ and hence multiplying by these channel gains 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

$$\tilde{T}_1 = \left\{ \prod_{i,j=1, i \neq j}^{2} \bar{a}_{ij}^{r_{ij}} \prod_{i,j=1}^{2} \bar{b}_{ij}^{s_{ij}} : r_{ij}, s_{ij} = 1, \dots, m+1 \right\} \tag{51}$$

$$\tilde{T}_2 = \left\{ \prod_{i,j=1, i \neq j}^{2} a_{ij}^{r_{ij}} \prod_{i,j=1}^{2} b_{ij}^{s_{ij}} : r_{ij}, s_{ij} = 1, \dots, m+1 \right\} \tag{52}$$

with cardinality of

$$M_R = |\tilde{T}_i| = (m+1)^6, \quad i = 1, 2 \tag{53}$$

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 combinations of M_T PAM signals $\mathbf{v}_{ij} = [v_{ij1}\ v_{ij2} \cdots v_{ijM_T}]^T$ representing secure signal components of user i from antenna j. Generate $\mathbf{u}_i = [u_{ij1} u_{ij2} \cdots u_{ijM_T}]^T$ as cooperative jamming signal as follows

$$\mathbf{V}_1 = \begin{bmatrix} \mathbf{t}_2^T \mathbf{v}_{11} \\ \mathbf{t}_2^T \mathbf{v}_{12} \end{bmatrix}, \quad \mathbf{U}_1 = \begin{bmatrix} \mathbf{t}_1^T \mathbf{u}_{11} \\ \mathbf{t}_1^T \mathbf{u}_{12} \end{bmatrix} \tag{54}$$

$$\mathbf{V}_2 = \begin{bmatrix} \mathbf{t}_1^T \mathbf{v}_{21} \\ \mathbf{t}_1^T \mathbf{v}_{22} \end{bmatrix}, \quad \mathbf{U}_2 = \begin{bmatrix} \mathbf{t}_2^T \mathbf{v}_{21} \\ \mathbf{t}_2^T \mathbf{v}_{22} \end{bmatrix} \tag{55}$$

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 is $\mathbf{Y}_1 = \underline{\mathbf{Y}}_1 + \mathbf{N}_1$ where $\underline{\mathbf{Y}}_1$ is equal to,

$$\begin{bmatrix} a_{11}\mathbf{t}_2^T \mathbf{v}_{11} + \mathbf{t}_1^T(\mathbf{u}_{11} + \mathbf{v}_{21}) + \mathbf{t}_2^T(a_{12}\mathbf{v}_{12} + b_{11}\mathbf{u}_{21} + b_{12}\mathbf{u}_{22}) \\ a_{22}\mathbf{t}_2^T \mathbf{v}_{12} + \mathbf{t}_1^T(\mathbf{u}_{12} + \mathbf{v}_{22}) + \mathbf{t}_2^T(a_{21}\mathbf{v}_{11} + b_{21}\mathbf{u}_{21} + b_{22}\mathbf{u}_{22}) \end{bmatrix} \tag{56}$$

Lemma 2: The sum s.d.o.f. of $\frac{4}{3}$ is achievable using the combination of asymptotic alignment and spatial alignment shown in this section with signals picked from PAM constellation $C(a, Q)$ with $Q = P^{\frac{1-\delta}{2(M_\Sigma + \delta)}}$, $a = \gamma \frac{P^{\frac{1}{2}}}{Q}$, where $M_\Sigma = 2m^6 + (m+1)^6$ for arbitrarily large integer m, and any $\delta > 0$.

Remark 11: From (56), 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 [14]. 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 $\tilde{T}_2$. 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.

Proof: The total number of dimensions at antenna 1 (and similarly antenna 2) needed in this case is

$$M_\Sigma = |a_{11}T_2 \cup T_1 \cup \tilde{T}_2| = 2m^6 + (m+1)^6 \tag{57}$$

By choosing the parameters of the PAM constellation as

$$Q = P^{\frac{1-\delta}{2(M_\Sigma + \delta)}}, \qquad a = \gamma \frac{P^{\frac{1}{2}}}{Q} \tag{58}$$

the average power constraint is satisfied, and the probability of error can be made arbitrarily small as $P \to \infty$ as in [14] and [34]. We can also decode $\mathbf{U}_2$ perfectly at receiver 1 after decoding $\mathbf{V}_1$. By subtracting $\mathbf{V}_1$ from $\mathbf{Y}_1$, we have

$$\mathbf{Y}_1' = (\mathbf{U}_1 + \mathbf{V}_2) + \mathbf{B}\mathbf{U}_2 + \mathbf{N}_1 \tag{59}$$

By filtering the received observations using $\mathbf{C} = \mathbf{B}^{-1}$, we have

$$\mathbf{Y}_1'' = \mathbf{B}^{-1}(\mathbf{U}_1 + \mathbf{V}_2) + \mathbf{U}_2 + \mathbf{N}_1'' \tag{60}$$

$$= \begin{bmatrix} c_{11}\mathbf{t}_1^T(\mathbf{u}_{11} + \mathbf{v}_{21}) + c_{12}\mathbf{t}_1^T(\mathbf{u}_{12} + \mathbf{v}_{22}) + \mathbf{t}_2^T\mathbf{u}_{21} \\ c_{21}\mathbf{t}_1^T(\mathbf{u}_{11} + \mathbf{v}_{21}) + c_{22}\mathbf{t}_1^T(\mathbf{u}_{12} + \mathbf{v}_{22}) + \mathbf{t}_2^T\mathbf{u}_{22} \end{bmatrix} + \mathbf{N}_1'' \tag{61}$$

where $\mathbf{N}_1'' = \mathbf{B}^{-1}\mathbf{N}_1$. Since no specific alignment procedure has been designed for the $\mathbf{C}$ matrix, all these signals are received in separate irrational dimensions. The total required dimensions in this case is $3M_T = 3m^6 < M_\Sigma$, and hence decodable.

Now, we evaluate the rates in (41) focusing on user 1. Using the parameters chosen in (58), $\mathbf{V}_1$ is received with asymptotically vanishing probability of error. Consequently, the first term of (41) can be lower bounded using data processing and Fano's inequality as

$$I(\mathbf{V}_1; \mathbf{Y}_1) \geq I(\mathbf{V}_1; \hat{\mathbf{V}}_1) \tag{62}$$

$$= H(\mathbf{V}_1) - H(\mathbf{V}_1 | \hat{\mathbf{V}}_1) \tag{63}$$

$$\geq (1 - P_e)\log(2Q + 1)^{2M_T} - 1 \tag{64}$$

$$= (1 - P_e)\frac{2M_T(1-\delta)}{M_\Sigma + \delta} \cdot \frac{1}{2}\log P + o(\log P) \tag{65}$$

We can upper bound the leakage as

$$I(\mathbf{V}_1; \mathbf{Y}_2 | \mathbf{V}_2)$$

$$\leq I(\mathbf{V}_1; (\mathbf{V}_1 + \mathbf{U}_2) + \bar{\mathbf{B}}\mathbf{U}_1 + \bar{\mathbf{A}}\mathbf{V}_2 | \mathbf{V}_2) \tag{66}$$

$$= H((\mathbf{V}_1 + \mathbf{U}_2) + \bar{\mathbf{B}}\mathbf{U}_1) - H(\mathbf{U}_2 + \bar{\mathbf{B}}\mathbf{U}_1) \tag{67}$$

The first term in (67) can be upper bounded by

$$H(\mathbf{V}_1 + \mathbf{U}_2) + \bar{\mathbf{B}}\mathbf{U}_1)$$

$$= H(\bar{\mathbf{B}}^{-1}(\mathbf{V}_1 + \mathbf{U}_2) + \mathbf{U}_1) \tag{68}$$

$$= H\left(\begin{bmatrix} \bar{c}_{11}\mathbf{t}_2^T(\mathbf{u}_{21}+\mathbf{v}_{11}) + \bar{c}_{12}\mathbf{t}_2^T(\mathbf{u}_{22}+\mathbf{v}_{12}) + \mathbf{t}_1^T\mathbf{u}_{11} \\ \bar{c}_{21}\mathbf{t}_2^T(\mathbf{u}_{21}+\mathbf{v}_{11}) + \bar{c}_{22}\mathbf{t}_2^T(\mathbf{u}_{22}+\mathbf{v}_{12}) + \mathbf{t}_1^T\mathbf{u}_{12} \end{bmatrix}\right) \tag{69}$$

$$= H\left(\begin{bmatrix} \mathbf{V}_1 + \mathbf{U}_2 \\ \mathbf{U}_1 \end{bmatrix}\right) \tag{70}$$

$$= \log\left((4Q + 1)^{2M_T}(2Q + 1)^{2M_T}\right) \tag{71}$$

where $\bar{\mathbf{C}} = \bar{\mathbf{B}}^{-1}$, (68) holds since $\bar{\mathbf{C}}$ is invertible, and (70) follows from the fact that all signal components lie in different irrational dimensions with a total number of dimensions of $3M_T < M_\Sigma$, which in turn makes these signals decodable for large enough P. Thus, the transformation $\begin{bmatrix}\bar{\mathbf{B}}^{-1} & \mathbf{I}\end{bmatrix}$ is invertible. Similarly, the second term in (67) which solely contains cooperative jamming signals, is

$$H(\mathbf{U}_2 + \bar{\mathbf{B}}\mathbf{U}_1) = H\left(\begin{bmatrix} \mathbf{U}_2 \\ \mathbf{U}_1 \end{bmatrix}\right) = \log\left((2Q + 1)^{4M_T}\right) \tag{72}$$

Then, the leakage in (67) is upper bounded by

$$I(\mathbf{V}_1; \mathbf{Y}_2 | \mathbf{V}_2) \leq \log\left(\frac{4Q + 1}{2Q + 1}\right)^{2M_T} \tag{73}$$

$$\leq 2M_T + o(\log P) \tag{74}$$

Therefore, user 1's rate is lower bounded by

$$R_1 \geq I(\mathbf{V}_1; \mathbf{Y}_1) - I(\mathbf{V}_1; \mathbf{Y}_2 | \mathbf{V}_2) \tag{75}$$

$$= 2M_T\left((1 - P_e)\frac{(1 - \delta)}{M_\Sigma + \delta} \cdot \frac{1}{2}\log P - 1\right) + o(\log P) \tag{76}$$

By normalizing by $\frac{1}{2}\log P$ and taking $P \to \infty$,

$$d_1 \geq \frac{2M_T(1 - \delta)}{M_\Sigma + \delta} \tag{77}$$

$$= \frac{2m^6(1 - \delta)}{2m^6 + (m + 1)^6 + \delta} \tag{78}$$

$$\geq \frac{2(1 - \delta)}{2 + \left(1 + \frac{1}{m}\right)^6 + \delta} \tag{79}$$

As $m \to \infty$ and $\delta \to 0$, the achievable s.d.o.f is 2/3 for each user, and hence the sum s.d.o.f. is $\frac{4}{3}$. ∎

Remark 12: We note that for the SISO system, we do not need any asymptotic alignment. By specializing the spatial alignment presented here to the SISO case, i.e.,

$$X_1 = \frac{1}{h_{12}}V_1 + \frac{1}{h_{11}}U_1 \tag{80}$$

$$X_2 = \frac{1}{h_{21}}V_2 + \frac{1}{h_{22}}U_2 \tag{81}$$

we see that the received signals fit exactly into 3 irrational dimensions. Hence, 1/3 s.d.o.f. per user is achievable as in [14]. Therefore, we focus our attention to the presentation of achievable schemes for the cases that result in a 2 × 2 system, since the SISO case can be obtained as a special case of the 2 × 2 achievable scheme by ignoring the asymptotic alignment step and replacing with an exact real interference alignment step.

VII. Achievable Scheme for Sum s.d.o.f. of the $M \times N$ MIMO ICCM

A. $\frac{N}{2} \leq M \leq \frac{2N}{3}$

In this case, the sum s.d.o.f. is an integer. Hence, we use Gaussian codebooks for transmission of the secure signal $\mathbf{V}_i$ and the 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 signal of the other user.

1) Transmitted Signals: Each user transmits a Gaussian secure signal $\mathbf{V}_i$, and a Gaussian cooperative jamming signal $\mathbf{U}_i$. The signals $\mathbf{V}_i, \mathbf{U}_i \sim \mathcal{N}(\mathbf{0}, \eta_1 \; P\mathbf{I}_{2M-N})$ are of $2M - N$ dimensions, and independent from each other, where η_1 is a constant, which is chosen to satisfy the power constraint. Let $\mathbf{P}_i, \mathbf{Q}_i \in \mathbb{R}^{M\times(2M-N)}$ be the precoding matrices for $\mathbf{V}_i$, $\mathbf{U}_i$, respectively. Then, the transmitted signals are,

$$\mathbf{X}_1 = \mathbf{P}_1\mathbf{V}_1 + \mathbf{Q}_1\mathbf{U}_1 \tag{82}$$

$$\mathbf{X}_2 = \mathbf{P}_2\mathbf{V}_2 + \mathbf{Q}_2\mathbf{U}_2 \tag{83}$$

The received signals in this case are:

$$\begin{aligned} \mathbf{Y}_1 &= \mathbf{H}_{11}\mathbf{P}_1\mathbf{V}_1 + (\mathbf{H}_{11}\mathbf{Q}_1\mathbf{U}_1 + \mathbf{H}_{21}\mathbf{P}_2\mathbf{V}_2) \\ &\quad + \mathbf{H}_{21}\mathbf{Q}_2\mathbf{U}_2 + \mathbf{N}_1 \\ \mathbf{Y}_2 &= (\mathbf{H}_{12}\mathbf{P}_1\mathbf{V}_1 + \mathbf{H}_{22}\mathbf{Q}_2\mathbf{U}_2) + \mathbf{H}_{12}\mathbf{Q}_1\mathbf{U}_1 \\ &\quad + \mathbf{H}_{22}\mathbf{P}_2\mathbf{V}_2 + \mathbf{N}_2 \end{aligned} \tag{84}$$

We choose the precoding matrices $\mathbf{P}_i, \mathbf{Q}_i$ such that they satisfy the following alignment equations

$$\text{span}\{\mathbf{H}_{21}\mathbf{P}_2\} \subseteq \text{span}\{\mathbf{H}_{11}\mathbf{Q}_1\} \tag{85}$$

$$\text{span}\{\mathbf{H}_{12}\mathbf{P}_1\} \subseteq \text{span}\{\mathbf{H}_{22}\mathbf{Q}_2\} \tag{86}$$

2) Feasibility of Alignment: The alignment can be achieved by choosing $\mathbf{P}_i,\ \mathbf{Q}_i$ such that

$$\begin{bmatrix}\mathbf{H}_{11} & -\mathbf{H}_{21}\end{bmatrix}\begin{bmatrix}\mathbf{Q}_1\\ \mathbf{P}_2\end{bmatrix} = \mathbf{0} \tag{87}$$

$$\begin{bmatrix}\mathbf{H}_{12} & -\mathbf{H}_{22}\end{bmatrix}\begin{bmatrix}\mathbf{P}_1\\ \mathbf{Q}_2\end{bmatrix} = \mathbf{0} \tag{88}$$

i.e., by choosing $\mathbf{P}_i, \mathbf{Q}_i$ to be in the null space of the combined channel of the two users. Note that $\begin{bmatrix}\mathbf{H}_{11} & -\mathbf{H}_{21}\end{bmatrix}$ is an $\mathbb{R}^{N\times 2M}$ matrix. Hence, the null space of this matrix, $\begin{bmatrix}\mathbf{H}_{11} & -\mathbf{H}_{21}\end{bmatrix}^{\perp}$, is an $\mathbb{R}^{2M\times 2M-N}$ matrix. Thus, choosing $\mathbf{P}_i, \mathbf{Q}_i$ as $\mathbb{R}^{M\times 2M-N}$ is feasible.

3) Decodability: By this alignment scheme, we have

$$\mathbf{Y}_1 = \mathbf{H}_{11}\mathbf{P}_1\mathbf{V}_1 + \mathbf{H}_{11}\mathbf{Q}_1(\mathbf{U}_1+\mathbf{V}_2) + \mathbf{H}_{21}\mathbf{Q}_2\mathbf{U}_2 + \mathbf{N}_1 \tag{89}$$

$$= \begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1 & \mathbf{H}_{11}\mathbf{Q}_1 & \mathbf{H}_{21}\mathbf{Q}_2\end{bmatrix}\begin{bmatrix}\mathbf{V}_1\\ \mathbf{U}_1+\mathbf{V}_2\\ \mathbf{U}_2\end{bmatrix} + \mathbf{N}_1 \tag{90}$$

Similarly, for receiver 2, we have

$$\mathbf{Y}_2 = \begin{bmatrix}\mathbf{H}_{22}\mathbf{Q}_2 & \mathbf{H}_{12}\mathbf{Q}_1 & \mathbf{H}_{22}\mathbf{P}_2\end{bmatrix}\begin{bmatrix}\mathbf{V}_1+\mathbf{U}_2\\ \mathbf{U}_1\\ \mathbf{V}_2\end{bmatrix} + \mathbf{N}_2 \tag{91}$$

In order to decode $\mathbf{Y}_i$ using a zero forcing receiver, the total dimensions $3(2M-N)$ should be at most N. This holds true since $\frac{M}{N} \leq \frac{2}{3}$. Thus, we can decode $\mathbf{V}_1$ using zero forcing as

$$\begin{bmatrix}\mathbf{V}_1\\ \mathbf{U}_1+\mathbf{V}_2\\ \mathbf{U}_2\end{bmatrix} = \begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1\ \mathbf{H}_{11}\mathbf{Q}_1\ \mathbf{H}_{21}\mathbf{Q}_2\end{bmatrix}^{\dagger}\mathbf{Y}_1 \tag{92}$$

where $(.)^{\dagger}$ is the pseudo-inverse of a matrix.

4) Security: Since each secure signal is aligned with a cooperative jamming signal from the other user, the leakage rate is upper bounded by a constant, and hence the system is secure from the s.d.o.f. perspective, i.e., for user 1 without loss of generality, using Fano's and data processing inequality,

$$R_1 \geq I(\mathbf{V}_1;\mathbf{Y}_1) - I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2) \tag{93}$$

$$\geq I(\mathbf{V}_1;\hat{\mathbf{V}}_1) - h(\mathbf{Y}_2|\mathbf{V}_2) + h(\mathbf{Y}_2|\mathbf{V}_1,\mathbf{V}_2) \tag{94}$$

$$\begin{aligned}&\geq h(\mathbf{V}_1) - h(\mathbf{V}_1|\hat{\mathbf{V}}_1)\\ &\quad - h\left(\begin{bmatrix}\mathbf{H}_{22}\mathbf{Q}_2\ \mathbf{H}_{12}\mathbf{Q}_1\end{bmatrix}\begin{bmatrix}\mathbf{V}_1+\mathbf{U}_2\\ \mathbf{U}_1\end{bmatrix}\right)\\ &\quad + h\left(\begin{bmatrix}\mathbf{H}_{12}\mathbf{Q}_1\ \mathbf{H}_{22}\mathbf{P}_2\end{bmatrix}\begin{bmatrix}\mathbf{U}_2\\ \mathbf{U}_1\end{bmatrix}\right)\end{aligned} \tag{95}$$

$$\begin{aligned}&\geq (1-P_e)(2M-N)\cdot\frac{1}{2}\log P - h\left(\begin{bmatrix}\mathbf{V}_1+\mathbf{U}_2\\ \mathbf{U}_1\end{bmatrix}\right)\\ &\quad + h\left(\begin{bmatrix}\mathbf{U}_2\\ \mathbf{U}_1\end{bmatrix}\right) + o(\log P)\end{aligned} \tag{96}$$

$$\begin{aligned}&= (1-P_e)(2M-N)\cdot\frac{1}{2}\log P - 2(2M-N)\cdot\frac{1}{2}\log P\\ &\quad + 2(2M-N)\cdot\frac{2}{2}\log P + o(\log P)\end{aligned} \tag{97}$$

By dividing by $\frac{1}{2}\log P$ and taking $P\to\infty$, the $P_e\to 0$ and hence $d_1 \geq 2M-N$.

B. $\frac{2N}{3} \leq M \leq N$

In this regime, we combine the achievable scheme of the previous regime with the achievable scheme of the basic 2×2 system (or the 1×1 SISO system).

1) Transmitted Signals: Let $\mathbf{V}_i = \begin{bmatrix}\mathbf{V}_i^{(1)}\\ \mathbf{V}_i^{(2)}\end{bmatrix}$ and $\mathbf{U}_i = \begin{bmatrix}\mathbf{U}_i^{(1)}\\ \mathbf{U}_i^{(2)}\end{bmatrix}$. $\mathbf{V}_i^{(1)}, \mathbf{U}_i^{(1)} \sim \mathcal{N}(\mathbf{0}, \eta_2\ P\mathbf{I}_{\lfloor\frac{N}{3}\rfloor})$ are Gaussian signals of size $\lfloor\frac{N}{3}\rfloor$. $\mathbf{V}_i^{(1)}, \mathbf{U}_i^{(1)}$ correspond 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 structured signals of size $N \bmod 3$ which is either 1 or 2. $\mathbf{V}_i^{(2)}, \mathbf{U}_i^{(2)}$ are picked from PAM constellation $C(a, Q)$, with proper parameters. This separation effectively reduces the problem into designing spatial alignment precoders as in the previous regime and the basic 2×2 system (or the 1×1 SISO system). We consider the case of $N \bmod 3 = 2$, without loss of generality. Let $\mathbf{P}_i,\ \mathbf{Q}_i$ be precoding matrices in $\mathbb{R}^{M\times(\lfloor\frac{N}{3}\rfloor+N \bmod 3)}$, then the transmitted signals are

$$\mathbf{X}_1 = \mathbf{P}_1\begin{bmatrix}v_{1,1}^{(1)}\\ v_{1,2}^{(1)}\\ \vdots\\ v_{1,\lfloor\frac{N}{3}\rfloor}^{(1)}\\ \mathbf{t}_2^T\mathbf{v}_{11}^{(2)}\\ \mathbf{t}_2^T\mathbf{v}_{12}^{(2)}\end{bmatrix} + \mathbf{Q}_1\begin{bmatrix}u_{1,1}^{(1)}\\ u_{1,2}^{(1)}\\ \vdots\\ u_{1,\lfloor\frac{N}{3}\rfloor}^{(1)}\\ \mathbf{t}_1^T\mathbf{u}_{11}^{(2)}\\ \mathbf{t}_1^T\mathbf{u}_{12}^{(2)}\end{bmatrix} \tag{98}$$

$$\mathbf{X}_2 = \mathbf{P}_2\begin{bmatrix}v_{2,1}^{(1)}\\ v_{2,2}^{(1)}\\ \vdots\\ v_{2,\lfloor\frac{N}{3}\rfloor}^{(1)}\\ \mathbf{t}_1^T\mathbf{v}_{21}^{(2)}\\ \mathbf{t}_1^T\mathbf{v}_{22}^{(2)}\end{bmatrix} + \mathbf{Q}_2\begin{bmatrix}u_{2,1}^{(1)}\\ u_{2,2}^{(1)}\\ \vdots\\ u_{2,\lfloor\frac{N}{3}\rfloor}^{(1)}\\ \mathbf{t}_2^T\mathbf{u}_{21}^{(2)}\\ \mathbf{t}_2^T\mathbf{u}_{22}^{(2)}\end{bmatrix} \tag{99}$$

where $\mathbf{P}_i, \mathbf{Q}_i$ are designed using (87), (88).

2) Feasibility of Alignment: Similar to the previous section, this alignment is possible if the null space of the combined channel $\begin{bmatrix}\mathbf{H}_{11} & -\mathbf{H}_{21}\end{bmatrix}^{\perp}$ has dimension $2M-N \geq \lfloor\frac{N}{3}\rfloor + N \bmod 3$, which implies that $\frac{M}{N} \geq \frac{2}{3} + \frac{N \bmod 3}{3N}$. This condition always holds in this regime.

3) Decodability: 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, the received signal at receiver 1 is

$$\begin{aligned}\mathbf{Y}_1 &= \begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1^{(1)} & \mathbf{H}_{11}\mathbf{Q}_1^{(1)} & \mathbf{H}_{21}\mathbf{Q}_2^{(1)}\end{bmatrix}\begin{bmatrix}\mathbf{V}_1^{(1)}\\ \mathbf{V}_2^{(1)}+\mathbf{U}_1^{(1)}\\ \mathbf{U}_2^{(1)}\end{bmatrix}\\ &\quad + \begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1^{(2)}\ \ \mathbf{H}_{11}\mathbf{Q}_1^{(2)}\mathbf{H}_{21}\mathbf{Q}_2^{(2)}\end{bmatrix}\begin{bmatrix}\mathbf{V}_1^{(2)}\\ \mathbf{V}_2^{(2)}+\mathbf{U}_1^{(2)}\\ \mathbf{U}_2^{(2)}\end{bmatrix} + \mathbf{N}_1\end{aligned} \tag{100}$$

Define matrix $\mathbf{F}_1 = \left[\mathbf{H}_{11}\mathbf{P}_1^{(1)}\ \mathbf{H}_{11}\mathbf{Q}_1^{(1)}\ \mathbf{H}_{21}\mathbf{Q}_2^{(1)}\right]$ as an $\mathbb{R}^{N\times 3\lfloor \frac{N}{3}\rfloor}$ matrix. We null out the effect of the first components from $\mathbf{Y}_1$ by multiplying by the nulling matrix $\mathbf{Z}_1^T$, which is defined as the right null space of $\mathbf{F}_1$

$$\mathbf{Z}_1 = \left(\mathbf{F}_1^T\right)^{\perp} \tag{101}$$

The nulling matrix $\mathbf{Z}_1^T$ is $\mathbb{R}^{N \bmod 3\times N}$. Then, the filtered observation is

$$\begin{align}\tilde{\mathbf{Y}}_1 &= \mathbf{Z}_1^T\mathbf{Y}_1 \tag{102}\\ &= \left[\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{P}_1^{(2)}\ \ \mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)}\ \ \mathbf{Z}_1^T\mathbf{H}_{21}\mathbf{Q}_2^{(2)}\right]\begin{bmatrix}\mathbf{V}_1^{(2)}\\ \mathbf{V}_2^{(2)}+\mathbf{U}_1^{(2)}\\ \mathbf{U}_2^{(2)}\end{bmatrix}\nonumber\\ &\quad+\tilde{\mathbf{N}}_1 \tag{103}\end{align}$$

where $\tilde{\mathbf{N}}_1 = \mathbf{Z}_1^T\mathbf{N}_1$. Orthogonalize $\mathbf{V}_2^{(2)}+\mathbf{U}_1^{(2)}$ components by multiplying by $(\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)})^{-1}$,

$$\begin{align}\tilde{\tilde{\mathbf{Y}}}_1 &= (\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)})^{-1}\tilde{\mathbf{Y}}_1 \tag{104}\\ &= \mathbf{A}\mathbf{V}_1^{(2)} + (\mathbf{V}_2^{(2)}+\mathbf{U}_1^{(2)}) + \mathbf{B}\mathbf{U}_2^{(2)} + \tilde{\tilde{\mathbf{N}}}_1 \tag{105}\end{align}$$

where $\mathbf{A} = (\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)})^{-1}\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{P}_1^{(2)}$, $\mathbf{B} = (\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)})^{-1}\mathbf{Z}_1^T\mathbf{H}_{21}\mathbf{Q}_2^{(2)}$, and $\tilde{\tilde{\mathbf{N}}}_1 = (\mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{Q}_1^{(2)})^{-1}\tilde{\mathbf{N}}_1$. $\mathbf{A}$, $\mathbf{B}$ are now $N \bmod 3 \times N \bmod 3$ matrices. By designing $\mathbf{t}_i$ as in the 2×2 system, $\mathbf{V}_1^{(2)}, \mathbf{U}_2^{(2)}$ are decoded without error. Cancelling them from $\mathbf{Y}_1$, we have

$$\begin{align}\bar{\mathbf{Y}}_1 &= \left[\mathbf{H}_{11}\mathbf{P}_1^{(1)}\ \ \mathbf{H}_{11}\mathbf{Q}_1^{(1)}\ \ \mathbf{H}_{21}\mathbf{Q}_2^{(1)}\ \ \mathbf{H}_{11}\mathbf{Q}_1^{(2)}\right]\begin{bmatrix}\mathbf{V}_1^{(1)}\\ \mathbf{V}_2^{(1)}+\mathbf{U}_1^{(1)}\\ \mathbf{U}_2^{(1)}\\ \mathbf{V}_2^{(2)}+\mathbf{U}_1^{(2)}\end{bmatrix}\nonumber\\ &\quad+\mathbf{N}_1 \tag{106}\end{align}$$

To check the decodability, the total number of dimensions is $3\lfloor\frac{N}{3}\rfloor + N \bmod 3 = N$, and hence signals are decodable by a zero-forcing receiver as in the previous section.

4) Security: Similar to the analysis in the previous sections, the secure signals of user 2 at receiver 1 are exactly aligned with the cooperative jamming signals of user 1. Consequently, the leakage rate is bounded by a constant, and each user achieves an s.d.o.f. of $\lfloor\frac{N}{3}\rfloor + \frac{N \bmod 3}{3} = \frac{N}{3}$ with a total s.d.o.f. $d_s \geq \frac{2N}{3}$.

C. $N \leq\ M \leq 2N$

In this regime, we note the availability of a null space for each cross-channel matrix. Consequently, the achievable scheme combines null space transmission with the achievable scheme of the square system $M = N$, which includes spatial and asymptotic real interference alignment. The upper bound suggests that each user sends $M-N$ signals in the null space of the other user, so that they become invisible, and use the rest of the antennas as a square system of dimension $2N-M$ (recall that $d_s \leq \frac{2(2M-N)}{3} = 2(M-N)+2\frac{2N-M}{3}$). To separate the square system components from contaminating the null space components, we further precode the signals of the square system.

1) Transmitted Signals: Generate $\mathbf{V}_{i0} \sim \mathcal{N}(\mathbf{0}, \eta_3\ P\mathbf{I}_{M-N})$ as Gaussian secure signals of size $M-N$ that are transmitted through the null space of the cross-channel to the jth receiver. $\mathbf{V}_i^{(1)}, \mathbf{U}_i^{(1)} \sim \mathcal{N}(\mathbf{0}, \eta_4\ P\mathbf{I}_{\lfloor\frac{2N-M}{3}\rfloor})$ are Gaussian secure signals and Gaussian cooperative jamming signals, respectively, both of size $\lfloor\frac{2N-M}{3}\rfloor$. $\mathbf{v}_{ij}, \mathbf{u}_{ij}$ are structured PAM signals weighted with vectors $\mathbf{t}_i$, which will be defined later. Let $\mathbf{H}_{11}^{(1)}, \mathbf{H}_{12}^{(1)}, \mathbf{H}_{22}^{(1)}, \mathbf{H}_{21}^{(1)}$ are the $\mathbb{R}^{(M-N)\times M}$ channel matrices to the first $M-N$ antennas at the receivers. Therefore, the transmitted signals are

$$\mathbf{X}_1 = \mathbf{H}_{12}^{\perp}\mathbf{V}_{10} + \begin{bmatrix}\mathbf{H}_{11}^{(1)}\\ \mathbf{H}_{12}^{(1)}\end{bmatrix}^{\perp}\left(\mathbf{P}_1\begin{bmatrix}v_{1,1}^{(1)}\\ v_{1,2}^{(1)}\\ \vdots\\ v_{1,\lfloor\frac{\tilde{N}}{3}\rfloor}^{(1)}\\ \mathbf{t}_2^T\mathbf{v}_{11}^{(2)}\\ \mathbf{t}_2^T\mathbf{v}_{12}^{(2)}\end{bmatrix} + \mathbf{Q}_1\begin{bmatrix}u_{1,1}^{(1)}\\ u_{1,2}^{(1)}\\ \vdots\\ u_{1,\lfloor\frac{\tilde{N}}{3}\rfloor}^{(1)}\\ \mathbf{t}_1^T\mathbf{u}_{11}^{(2)}\\ \mathbf{t}_1^T\mathbf{u}_{12}^{(2)}\end{bmatrix}\right) \tag{107}$$

$$\mathbf{X}_2 = \mathbf{H}_{21}^{\perp}\mathbf{V}_{20} + \begin{bmatrix}\mathbf{H}_{21}^{(1)}\\ \mathbf{H}_{22}^{(1)}\end{bmatrix}^{\perp}\left(\mathbf{P}_2\begin{bmatrix}v_{2,1}^{(1)}\\ v_{2,2}^{(1)}\\ \vdots\\ v_{2,\lfloor\frac{\tilde{N}}{3}\rfloor}^{(1)}\\ \mathbf{t}_1^T\mathbf{v}_{21}^{(2)}\\ \mathbf{t}_1^T\mathbf{v}_{22}^{(2)}\end{bmatrix} + \mathbf{Q}_2\begin{bmatrix}u_{2,1}^{(1)}\\ u_{2,2}^{(1)}\\ \vdots\\ u_{2,\lfloor\frac{\tilde{N}}{3}\rfloor}^{(1)}\\ \mathbf{t}_2^T\mathbf{u}_{21}^{(2)}\\ \mathbf{t}_2^T\mathbf{u}_{22}^{(2)}\end{bmatrix}\right) \tag{108}$$

where $\tilde{N} = 2N-M$. This precoding separates the first $M-N$ antennas at each receiver from the square system signals. This leaves the $\mathbf{V}_{i0}$ vectors to be reliably received via zero-forcing processing.

2) Decodability and Security: We focus on receiver 1 without loss of generality. $\mathbf{H}_{11}\begin{bmatrix}\mathbf{H}_{11}^{(1)}\\ \mathbf{H}_{12}^{(1)}\end{bmatrix}^{\perp}$ has the dimension 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, $\mathbf{Y}_1^{(1)} = \mathbf{H}_{11}\mathbf{H}_{12}^{\perp}\mathbf{V}_{10} + \mathbf{N}_1^{(1)}$. Consequently, we can 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 a square system only. Note that the dimensions set and spatial alignment matrices can be constructed in a similar manner 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 $\bar{\mathbf{H}}_{22} = \mathbf{H}_{22}^{(2)}\begin{bmatrix}\mathbf{H}_{21}^{(1)}\\ \mathbf{H}_{22}^{(1)}\end{bmatrix}^{\perp}$. Then the spatial alignment matrices are designed such that

$$\begin{bmatrix}\bar{\mathbf{H}}_{11} & -\bar{\mathbf{H}}_{21}\end{bmatrix}\begin{bmatrix}\mathbf{Q}_1\\ \mathbf{P}_2\end{bmatrix} = \mathbf{0} \tag{109}$$

$$\begin{bmatrix}\bar{\mathbf{H}}_{12} & -\bar{\mathbf{H}}_{22}\end{bmatrix}\begin{bmatrix}\mathbf{P}_1\\ \mathbf{Q}_2\end{bmatrix} = \mathbf{0} \tag{110}$$

We can now define the dimensions sets on $\bar{\mathbf{H}}_{11}, \bar{\mathbf{H}}_{12}, \bar{\mathbf{H}}_{21}, \bar{\mathbf{H}}_{22}$ as in the previous section. Thus, the alignment process, and the secrecy analysis remain the same as the square system analysis.

D. $M \geq 2N$

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 only. Let $\mathbf{V}_i = [v_{i_1}\, v_{i_2} \dots v_{i_N} \quad \mathbf{0}^T_{M-2N}]^T = [\bar{\mathbf{V}}_i \quad \mathbf{0}^T_{M-2N}]^T$ be the transmitted Gaussian signal for user i, where $\bar{\mathbf{V}}_i \sim \mathcal{N}(\mathbf{0}, \eta_4\ P\mathbf{I}_N)$. Thus, the transmitted signals are:

$$\mathbf{X}_1 = \mathbf{H}_{12}^{\perp}\mathbf{V}_1 \tag{111}$$

$$\mathbf{X}_2 = \mathbf{H}_{21}^{\perp}\mathbf{V}_2 \tag{112}$$

Since the channel gains are drawn from a continuous distribution, $\mathbf{H}_{11}\mathbf{H}_{12}^{\perp}$ and $\mathbf{H}_{22}\mathbf{H}_{21}^{\perp}$ are full rank almost surely. Hence, the receiver performs zero-forcing to decode $\mathbf{V}_i$, i.e.,

$$\hat{\mathbf{V}}_1 = (\mathbf{H}_{11}\mathbf{H}_{12}^{\perp})^{\dagger}\mathbf{Y}_1 \tag{113}$$

$$\hat{\mathbf{V}}_2 = (\mathbf{H}_{22}\mathbf{H}_{21}^{\perp})^{\dagger}\mathbf{Y}_2 \tag{114}$$

At high SNR, the probability of error can be made arbitrarily small. These signals are invisible to the other receiver, i.e., transmitted in perfect security.

VIII. The Entire s.d.o.f. Region for the $M \times N$ ICCM

In this section, we derive the optimal achievable schemes for the entire region of the $M \times N$ ICCM. From the converse proof, we note that the s.d.o.f. region is a four-vertex polytope for any M, N. The non-trivial points of the polytope are the sum s.d.o.f. point and the two symmetric maximum individual s.d.o.f. points. Thus, in this section, we concentrate on characterizing achievable schemes for one of the maximum individual s.d.o.f. points only. Since the s.d.o.f. region is naturally a square region for $\frac{N}{2} \leq M \leq \frac{2N}{3}$ and $M \geq 2N$, the problem of characterizing the entire s.d.o.f. region reduces to finding the optimal achievable schemes for the maximum individual s.d.o.f. points for $\frac{2N}{3} \leq M \leq 2N$. Any other point that belongs to the s.d.o.f. region can be achieved by time-sharing. In the following, we consider the achievability of the $(d_m, 0)$ point, without loss of generality. We present these schemes in a concise way because these points can be mapped to the achievable schemes of the MIMO wiretap channel with a helper in [15]. The idea in all these schemes is to let user 2 sacrifice his own s.d.o.f. and send only cooperative jamming signals to jam its own receiver, i.e., it acts as a pure helper.

A. For $\frac{2N}{3} \leq M \leq \frac{3N}{4}$

In this case user 1 sends Gaussian secure signal $\mathbf{V}_1$ of dimension $2M - N$, while user 2 sends pure Gaussian cooperative jamming signal $\mathbf{U}_1$ of the same dimension, i.e., the transmitted signals are

$$\mathbf{X}_1 = \mathbf{P}_1\mathbf{V}_1 \tag{115}$$

$$\mathbf{X}_2 = \mathbf{Q}_2\mathbf{U}_2 \tag{116}$$

Then, the received signals are

$$\mathbf{Y}_1 = \mathbf{H}_{11}\mathbf{P}_1\mathbf{V}_1 + \mathbf{H}_{21}\mathbf{Q}_2\mathbf{U}_2 + \mathbf{N}_1 \tag{117}$$

$$\mathbf{Y}_2 = \mathbf{H}_{12}\mathbf{P}_1\mathbf{V}_1 + \mathbf{H}_{22}\mathbf{Q}_2\mathbf{U}_2 + \mathbf{N}_2 \tag{118}$$

To ensure security, we align the cooperative jamming of user 2 with the secure signal of user 1 at receiver 2 by designing $\mathbf{P}_1$, $\mathbf{Q}_2$ such that

$$\begin{bmatrix}\mathbf{H}_{12} & -\mathbf{H}_{22}\end{bmatrix}\begin{bmatrix}\mathbf{P}_1 \\ \mathbf{Q}_2\end{bmatrix} = \mathbf{0} \tag{119}$$

Since the null space of the matrix $\begin{bmatrix}\mathbf{H}_{12} & -\mathbf{H}_{22}\end{bmatrix}$ has dimension $2M \times (2M - N)$, this alignment is feasible. The decodability is performed via zero-forcing, if the total dimensions $2(2M - N) \leq N$, which is true for $M \leq \frac{3N}{4}$. The leakage rate is upper bounded by a constant as shown in previous sections, hence, the scheme is secure in the s.d.o.f. sense. Consequently, $d_m = 2M - N$ is achievable.

B. For $\frac{3N}{4} \leq M \leq N$

We combine the previous achievable scheme with the exact real interference alignment. The signals compose of Gaussian components $\mathbf{V}_1^{(1)}, \mathbf{U}_2^{(1)}$ of dimension $\lfloor \frac{N}{2} \rfloor$ and structured components $v_1^{(2)}, u_2^{(2)}$ of dimension $N \bmod 2 = 0$ or 1 picked from PAM constellation $C(a, Q)$ with $Q = P^{\frac{1-\delta}{2(2+\delta)}}$, $a = \gamma \frac{P^{\frac{1}{2}}}{Q}$. The transmitted signals are

$$\mathbf{X}_1 = \mathbf{P}_1\begin{bmatrix}\mathbf{V}_1^{(1)} \\ v_1^{(2)}\end{bmatrix}, \quad \mathbf{X}_2 = \mathbf{Q}_2\begin{bmatrix}\mathbf{U}_2^{(1)} \\ u_2^{(2)}\end{bmatrix} \tag{120}$$

Note that the PAM component is ignored if N is even. By using the same $\mathbf{P}_1, \mathbf{Q}_2$ as in the previous section, the transmission is secure from user 2. This alignment is feasible, because the null space dimension $2M - N \geq \lfloor \frac{N}{2} \rfloor + N \bmod 2$ for an integer M that satisfies $\frac{3N}{4} \leq M \leq N$. The received signal at receiver 1 is

$$\begin{aligned}\mathbf{Y}_1 = &\begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1^{(1)} \ \mathbf{H}_{21}\mathbf{Q}_2^{(1)}\end{bmatrix}\begin{bmatrix}\mathbf{V}_1^{(1)} \\ \mathbf{U}_2^{(1)}\end{bmatrix} + \mathbf{H}_{11}\mathbf{P}_1^{(2)}v_1^{(2)} \\ &+ \mathbf{H}_{21}\mathbf{Q}_2^{(2)}u_2^{(2)} + \mathbf{N}_1\end{aligned} \tag{121}$$

where $\mathbf{P}_1 = [\mathbf{P}^{(1)}_{1_{M\times\lfloor \frac{N}{2}\rfloor}} \quad \mathbf{P}^{(2)}_{1_{M\times N \bmod 2}}]$ and similarly for $\mathbf{Q}_2$. By defining $\mathbf{F}_1 = \begin{bmatrix}\mathbf{H}_{11}\mathbf{P}_1^{(1)} \ \mathbf{H}_{21}\mathbf{Q}_2^{(1)}\end{bmatrix}$ and multiplying by the right null space of this matrix, i.e., by multiplying by $\mathbf{Z}_1^T = \left((\mathbf{F}_1^T)^{\perp}\right)^T$, we have

$$\tilde{y}_1 = \mathbf{Z}_1^T\mathbf{H}_{11}\mathbf{P}_1^{(2)}v_1^{(2)} + \mathbf{Z}_1^T\mathbf{H}_{21}\mathbf{Q}_2^{(2)}u_2^{(2)} + \tilde{\mathbf{N}}_1 \tag{122}$$

where $\tilde{\mathbf{N}}_1 = \mathbf{Z}^T\mathbf{N}_1$. Note that this is a SISO system. Therefore, with the choice of $Q = P^{\frac{1-\delta}{2(2+\delta)}}, a = \gamma \frac{P^{\frac{1}{2}}}{Q}$, the $v_1^{(2)}, u_2^{(2)}$, signals are both decodable, because they lie in rationally independent dimensions almost surely. By cancelling these components from $\mathbf{Y}_1$, we are left with $2\lfloor \frac{N}{2} \rfloor \leq N$ signals, which can be decoded using a zero-forcing receiver. Consequently, $d_m = \frac{N}{2}$ is achievable.

C. For $N \leq M \leq \frac{3N}{2}$

In this case, user 1 can exploit the null space of $\mathbf{H}_{12}$ to send $M-N$ Gaussian secure signal components. Similarly, user 2 can generate $M-N$ Gaussian cooperative jamming components that are invisible to receiver 1 if transmitted in the null space of $\mathbf{H}_{21}$. Therefore, user 1 sends four signal components, $\mathbf{V}_{10}$ is the Gaussian secure signal that can be transmitted in the null space of dimension $M-N$, $\mathbf{V}_{11}$ is the Gaussian secure signal that can be protected using the invisible cooperative jamming components of user 2 of dimension $M-N$, $\mathbf{V}_{12}^{(1)}$ is Gaussian secure signal of dimension $\lfloor \frac{3N-2M}{2} \rfloor$ and $v_{12}^{(2)}$ which is a structured secure signal of dimension $N \bmod 2$ picked from PAM constellation $C(a, Q)$ with the same parameters as in the previous section. Similarly, user 2 transmits cooperative jamming signal $\mathbf{U}_{11}$ of dimension $M-N$ and is sent in the null space of receiver 1, $\mathbf{U}_{12}^{(1)}$ Gaussian of dimension $\lfloor \frac{3N-2M}{2} \rfloor$ and a structured component $u_{12}^{(2)}$ of dimension $N \bmod 2$. The transmitted signals are,

$$\mathbf{X}_1 = \mathbf{H}_{12}^{\perp}\mathbf{V}_{10} + \mathbf{P}_{11}\mathbf{V}_{11} + \mathbf{P}_{12}\begin{bmatrix} \mathbf{V}_{12}^{(1)} \\ v_{12}^{(2)} \end{bmatrix} \tag{123}$$

$$\mathbf{X}_2 = \mathbf{H}_{21}^{\perp}\mathbf{Q}_{21}\mathbf{U}_{11} + \mathbf{Q}_{22}\begin{bmatrix} \mathbf{U}_{12}^{(1)} \\ u_{12}^{(2)} \end{bmatrix} \tag{124}$$

By forcing, $\mathbf{H}_{12}\mathbf{P}_{11} = \mathbf{H}_{22}\mathbf{H}_{21}^{\perp}\mathbf{Q}_{21}$ and $\mathbf{H}_{12}\mathbf{P}_{12} = \mathbf{H}_{22}\mathbf{Q}_{22}$, the scheme is secure in the s.d.o.f. sense. Then, the received signals are,

$$\begin{aligned} \mathbf{Y}_1 &= \mathbf{H}_{11}\mathbf{H}_{12}^{\perp}\mathbf{V}_{10} + \mathbf{H}_{11}\mathbf{P}_{11}\mathbf{V}_{11} + \mathbf{H}_{11}\mathbf{P}_{12}\begin{bmatrix} \mathbf{V}_{12}^{(1)} \\ v_{12}^{(2)} \end{bmatrix} \\ &\quad + \mathbf{H}_{21}\mathbf{Q}_{22}\begin{bmatrix} \mathbf{U}_{12}^{(1)} \\ u_{12}^{(2)} \end{bmatrix} + \mathbf{N}_1 \end{aligned} \tag{125}$$

$$\begin{aligned} \mathbf{Y}_2 &= \mathbf{H}_{22}\mathbf{H}_{21}^{\perp}\mathbf{Q}_{21}(\mathbf{V}_{11} + \mathbf{U}_{11}) \\ &\quad + \mathbf{H}_{22}\mathbf{Q}_{22}\begin{bmatrix} \mathbf{V}_{12}^{(1)} + \mathbf{U}_{12}^{(1)} \\ v_{12}^{(2)} + u_{12}^{(2)} \end{bmatrix} + \mathbf{N}_2 \end{aligned} \tag{126}$$

This alignment can be designed by choosing $\mathbf{P}_{1i}, \mathbf{Q}_{2i}, i = 1, 2$ such that

$$\begin{bmatrix} \mathbf{H}_{12} & -\mathbf{H}_{22}\mathbf{H}_{21}^{\perp} \end{bmatrix}\begin{bmatrix} \mathbf{P}_{11} \\ \mathbf{Q}_{21} \end{bmatrix} = \mathbf{0} \tag{127}$$

$$\begin{bmatrix} \mathbf{H}_{12} & -\mathbf{H}_{22} \end{bmatrix}\begin{bmatrix} \mathbf{P}_{12} \\ \mathbf{Q}_{22} \end{bmatrix} = \mathbf{0} \tag{128}$$

This alignment is feasible if the null space of $\begin{bmatrix} \mathbf{H}_{12} & -\mathbf{H}_{22}\mathbf{H}_{21}^{\perp} \end{bmatrix}$, which has a dimension of $2(M-N)$ is at least accommodating $\mathbf{V}_{11}$ of $M-N$ dimension, i.e., $2(M-N) \geq M-N$. The null space of $\begin{bmatrix} \mathbf{H}_{21} & -\mathbf{H}_{22} \end{bmatrix}$ is also accommodating $\mathbf{V}_{12}$, i.e., $2M - N \geq \lfloor \frac{3N-2M}{2} \rfloor + N \bmod 2$. Both conditions hold true if $M \geq N$. Considering the decodability, we write the received signal at receiver 1 as

$$\begin{aligned} \mathbf{Y}_1 &= \begin{bmatrix} \mathbf{H}_{11}\mathbf{H}_{12}^{\perp} & \mathbf{H}_{11}\mathbf{P}_{11} & \mathbf{H}_{11}\mathbf{P}_{12}^{(1)} & \mathbf{H}_{21}\mathbf{Q}_{22}^{(2)} \end{bmatrix}\begin{bmatrix} \mathbf{V}_{10} \\ \mathbf{V}_{11} \\ \mathbf{V}_{12}^{(1)} \\ \mathbf{U}_{12}^{(1)} \end{bmatrix} \\ &\quad + \mathbf{H}_{11}\mathbf{P}_{12}^{(2)}v_{12}^{(2)} + \mathbf{H}_{21}\mathbf{Q}_{22}^{(2)}u_{12}^{(2)} + \mathbf{N}_1 \end{aligned} \tag{129}$$

By defining $\mathbf{F}_1 = \begin{bmatrix} \mathbf{H}_{11}\mathbf{H}_{12}^{\perp} & \mathbf{H}_{11}\mathbf{P}_{11} & \mathbf{H}_{11}\mathbf{P}_{12}^{(1)} & \mathbf{H}_{21}\mathbf{Q}_{22}^{(2)} \end{bmatrix}$, we can null out the effect of its symbols by multiplying with the right null space of $\mathbf{F}_1$. This is feasible because $\mathbf{F}_1 \in \mathbb{R}^{N \times 2(M-N)+2\lfloor \frac{3N-2M}{2} \rfloor}$ which has right null space of dimension $N \bmod 2 \times N$. Hence, we are left with $\mathbf{Y}_1^{(2)} = \mathbf{Z}_1^T(\mathbf{H}_{11}\mathbf{P}_{12}^{(2)}v_{12}^{(2)} + \mathbf{H}_{21}\mathbf{Q}_{22}^{(2)}u_{12}^{(2)}) + \tilde{n}_1$. Since, $v_{12}^{(2)}$, $u_{12}^{(2)}$ are picked from structured signals with proper a, Q, these signals are decodable. By cancelling these signals from $\mathbf{Y}_1$ and applying zero-forcing, the rest of the components are also decodable. Consequently, user 1 can transmit $2(M-N) + \lfloor \frac{3N-2M}{2} \rfloor + N \bmod 2$ secure signal components and hence $d_m = \frac{2M-N}{2}$ is achievable.

D. For $\frac{3N}{2} \leq M \leq 2N$

In this case, user 1 can send $\mathbf{V}_{10}$ Gaussian secure signal of dimension $M-N$ in the null space of cross channel to receiver 2. Therefore, these components are invisible at receiver 2, i.e., perfectly secure. User 2 can send $\mathbf{U}_2$ Gaussian cooperative jamming signals of size $2N-M$ in the null space of the cross channel to receiver 1. These signals ensure the security of signals $\mathbf{V}_1$ of user 1 and at the same time are invisible to receiver 1, and hence leave the space for decodability of the secure signals only. The transmitted signals are

$$\mathbf{X}_1 = \mathbf{H}_{12}^{\perp}\mathbf{V}_{10} + \mathbf{P}_1\mathbf{V}_1 \tag{130}$$

$$\mathbf{X}_2 = \mathbf{H}_{21}^{\perp}\mathbf{Q}_2\mathbf{U}_2 \tag{131}$$

The received signals are

$$\mathbf{Y}_1 = \mathbf{H}_{11}\mathbf{H}_{12}^{\perp}\mathbf{V}_{10} + \mathbf{H}_{11}\mathbf{P}_1\mathbf{V}_1 + \mathbf{N}_1 \tag{132}$$

$$\mathbf{Y}_2 = \mathbf{H}_{12}\mathbf{P}_1\mathbf{V}_1 + \mathbf{H}_{22}\mathbf{H}_{21}^{\perp}\mathbf{Q}_2\mathbf{U}_2 + \mathbf{N}_2 \tag{133}$$

By designing $\mathbf{P}_1 \in \mathbb{R}^{M \times 2N-M}$, $\mathbf{Q}_2 \in \mathbb{R}^{M-N \times 2N-M}$ such that

$$\begin{bmatrix} \mathbf{H}_{12} & -\mathbf{H}_{22}\mathbf{H}_{21}^{\perp} \end{bmatrix}\begin{bmatrix} \mathbf{P}_1 \\ \mathbf{Q}_2 \end{bmatrix} = \mathbf{0} \tag{134}$$

The leakage rate of $\mathbf{V}_1$ can be upper bounded by a constant, and hence, secure in the s.d.o.f. sense. This alignment is feasible as long as the null space of user 2 dimension $M-N$ is at least as the dimension of $\mathbf{V}_1$, i.e., $M-N \geq 2N-M$. We have also the condition from the precoder design that the null space of $\begin{bmatrix} \mathbf{H}_{12} & -\mathbf{H}_{22}\mathbf{H}_{21}^{\perp} \end{bmatrix}$ columns (which is $2(M-N)$) should be larger than $2N-M$ which both hold true if $M \geq \frac{3N}{2}$. For the decodability, the number of dimensions at receiver 1 is N and hence decodable using a zero-forcing receiver. Consequently, $d_m = N$ is achievable.

IX. Special Case: Time-Varying $M \times N$ ICCM

In this section, we consider the special case of time-varying channels. The converse proofs do not change if we change the setting to time-varying channels. Any achievable scheme for the static channel is a valid achievable scheme for the time-varying setting. However, we can use channel variations to simplify the achievable schemes via symbol extension as in [35]. By symbol repetition and coding across multiple channel uses, we can obtain fractional s.d.o.f. in a simpler way. The symbol extension (repetition) replaces the complex real interference alignment (exact or asymptotic) with simplified encoding and decoding schemes. Since symbol extension is used to replace real interference alignment in regimes that have fractional s.d.o.f., it suffices to develop achievable schemes for the sum s.d.o.f. point in the $\frac{2N}{3} \leq M \leq 2N$ regime and the maximum individual s.d.o.f. point for the $\frac{3N}{4} \leq M \leq \frac{3N}{2}$ regime because the remaining points achieve integer s.d.o.f. and do not use real interference alignment for achievability.

A. Sum s.d.o.f. Point for $\frac{2N}{3} \leq M \leq N$

The users send N secure signal components over 3 channel uses. We call the secure signal $\mathbf{V}_i^{(1)}(t)$ as *time-varying*, if for every channel use $t = 1, 2, 3$, $\mathbf{V}_i^{(1)}(t)$ takes an independent realization from an underlying Gaussian distribution. We call the secure signal $\mathbf{V}_i^{(2)}$ as *fixed*, if for every channel use t, the same realization is transmitted (repeated), i.e., $\mathbf{V}_i^{(2)}(t) = \mathbf{V}_i^{(2)}$, $t = 1, 2, 3$. Each user divides its transmitted secure signals $\mathbf{V}_i$ into two parts. The first part is time-varying $\mathbf{V}_i^{(1)}(t)$, which is a Gaussian vector of dimension $\lfloor \frac{N}{3} \rfloor$. This vector takes new symbols at each channel use t. The second part $\mathbf{V}_i^{(2)}$ is fixed, which is a Gaussian vector of dimension $N \bmod 3$. This vector is repeated over channel uses $t = 1, 2, 3$. Similarly, each user sends cooperative jamming signal $\mathbf{U}_i$ with the same structure. The transmitted signals are

$$\mathbf{X}_1(t) = \mathbf{P}_1(t) \begin{bmatrix} \mathbf{V}_1^{(1)}(t) \\ \mathbf{V}_1^{(2)} \end{bmatrix} + \mathbf{Q}_1(t) \begin{bmatrix} \mathbf{U}_1^{(1)}(t) \\ \mathbf{U}_1^{(2)} \end{bmatrix} \tag{135}$$

$$\mathbf{X}_2(t) = \mathbf{P}_2(t) \begin{bmatrix} \mathbf{V}_2^{(1)}(t) \\ \mathbf{V}_2^{(2)} \end{bmatrix} + \mathbf{Q}_2(t) \begin{bmatrix} \mathbf{U}_2^{(1)}(t) \\ \mathbf{U}_2^{(2)} \end{bmatrix} \tag{136}$$

where $t = 1, 2, 3$. The precoding matrices vary with t and are designed for every t such that

$$\begin{bmatrix} \mathbf{H}_{11}(t) & -\mathbf{H}_{21}(t) \end{bmatrix} \begin{bmatrix} \mathbf{Q}_1(t) \\ \mathbf{P}_2(t) \end{bmatrix} = \mathbf{0} \tag{137}$$

$$\begin{bmatrix} \mathbf{H}_{12}(t) & -\mathbf{H}_{22}(t) \end{bmatrix} \begin{bmatrix} \mathbf{P}_1(t) \\ \mathbf{Q}_2(t) \end{bmatrix} = \mathbf{0} \tag{138}$$

This alignment is feasible, since $2M - N \geq \lfloor \frac{N}{3} \rfloor + N \bmod 3$ in this regime. Then, the received signal at receiver 1 in this case is

$$\begin{aligned} \mathbf{Y}_1(t) = \mathbf{H}_{11}(t)\mathbf{P}_1(t) &\begin{bmatrix} \mathbf{V}_1^{(1)}(t) \\ \mathbf{V}_1^{(2)} \end{bmatrix} \\ + \mathbf{H}_{11}(t)\mathbf{Q}_1(t) &\begin{bmatrix} \mathbf{U}_1^{(1)}(t) + \mathbf{V}_2^{(1)}(t) \\ \mathbf{U}_1^{(2)} + \mathbf{V}_2^{(2)} \end{bmatrix} \\ + \mathbf{H}_{21}(t)\mathbf{Q}_2(t) &\begin{bmatrix} \mathbf{U}_2^{(1)}(t) \\ \mathbf{U}_2^{(2)} \end{bmatrix} + \mathbf{N}_1(t) \end{aligned} \tag{139}$$

for $t = 1, 2, 3$. By observing $\mathbf{Y}_1(t)$ over the 3 channel uses we can form a linear system with $3N$ unknowns and $3N$ equations. The unknowns are $\mathbf{V}_1^{(1)}(t)$, $\mathbf{U}_1^{(1)}(t)+\mathbf{V}_1^{(1)}(t)$, $\mathbf{U}_2^{(1)}(t)$, $t = 1, 2, 3$, each of dimension $3\lfloor \frac{N}{3} \rfloor$ over the 3 channel uses. $\mathbf{V}_1^{(2)}$, $\mathbf{U}_1^{(2)} + \mathbf{V}_2^{(2)}$, $\mathbf{U}_2^{(2)}$ of dimension of $N \bmod 3$ each. Hence, the total number of unknowns are $3\left(3\lfloor \frac{N}{3} \rfloor + N \bmod 3\right) = 3N$. Since receiver has N antennas, and realizations of channels are independently time-varying, the receiver has $3N$ independent observations almost surely over the 3 channel uses. Using zero-forcing we can decode these unknowns with arbitrarily small probability of error. Each secure signal component of user 2 is aligned with one cooperative jamming signal component from user 1, hence the scheme is secure. Now, since each user transmits $3\lfloor \frac{N}{3} \rfloor + N \bmod 3$ over 3 channel uses, $d_s = \frac{2N}{3}$ is achievable.

B. Sum s.d.o.f. Point for $N \leq M \leq 2N$

In this case, the users make use of the null spaces to send their time-varying secure signals. Specifically, each user transmits a time-varying $\mathbf{V}_{i0}(t)$, $t = 1, 2, 3$ Gaussian secure signal of dimension $M - N$. Each user transmits a fixed $\mathbf{V}_i$ Gaussian secure signal of dimension $2N - M$, and a fixed $\mathbf{U}_i$ Gaussian cooperative jamming signal. We restrict the first $M - N$ antennas at the receiver for decoding of the time-varying symbols and the rest of the antennas for the fixed symbols. To do this restriction, we precode the transmitted signals as

$$\mathbf{X}_1(t) = \mathbf{H}_{12}(t)^{\perp}\mathbf{V}_{10}(t) + \begin{bmatrix} \mathbf{H}_{11}^{(1)}(t) \\ \mathbf{H}_{12}^{(1)}(t) \end{bmatrix}^{\perp} (\mathbf{P}_1(t)\mathbf{V}_1 + \mathbf{Q}_1(t)\mathbf{U}_1) \tag{140}$$

$$\mathbf{X}_2(t) = \mathbf{H}_{21}(t)^{\perp}\mathbf{V}_{20}(t) + \begin{bmatrix} \mathbf{H}_{21}^{(1)}(t) \\ \mathbf{H}_{22}^{(1)}(t) \end{bmatrix}^{\perp} (\mathbf{P}_2(t)\mathbf{V}_2 + \mathbf{Q}_2(t)\mathbf{U}_2) \tag{141}$$

where $\mathbf{H}_{ij}^{(1)}(t)$, $\mathbf{H}_{ij}^{(2)}(t)$ correspond to the channel matrix from the ith user to the first $M - N$ antennas, and the rest of the $2N - M$ antennas at receiver j, respectively. Focusing on the first $M - N$ antennas of user 1, without loss of generality. The $\mathbf{Y}_1^{(1)}(t) = \mathbf{H}_{11}^{(1)}(t)\mathbf{H}_{12}(t)^{\perp}\mathbf{V}_{10}(t) + \mathbf{N}_1^{(1)}(t)$. Then, using zero-forcing, the signal $\mathbf{V}_{10}(t)$, $t = 1, 2, 3$ is decodable. After decoding $\mathbf{V}_{10}(t)$, we cancel it from $\mathbf{Y}_1(t)$. By defining $\bar{\mathbf{H}}_{11}(t) = \mathbf{H}_{11}^{(2)}(t) \begin{bmatrix} \mathbf{H}_{11}^{(1)}(t) \\ \mathbf{H}_{12}^{(1)}(t) \end{bmatrix}^{\perp}$, and similarly, $\bar{\mathbf{H}}_{21}(t) = \mathbf{H}_{21}^{(2)}(t) \begin{bmatrix} \mathbf{H}_{21}^{(1)}(t) \\ \mathbf{H}_{22}^{(1)}(t) \end{bmatrix}^{\perp}$, $\bar{\mathbf{H}}_{12}(t) = \mathbf{H}_{12}^{(2)}(t) \begin{bmatrix} \mathbf{H}_{11}^{(1)}(t) \\ \mathbf{H}_{12}^{(1)}(t) \end{bmatrix}^{\perp}$ and $\bar{\mathbf{H}}_{22}(t) = \mathbf{H}_{22}^{(2)}(t) \begin{bmatrix} \mathbf{H}_{21}^{(1)}(t) \\ \mathbf{H}_{22}^{(1)}(t) \end{bmatrix}^{\perp}$, the received signals after cancelling $\mathbf{V}_{10}$ at the second $2N - M$ antennas are

$$\begin{aligned} \mathbf{Y}_1^{(2)}(t) &= (\bar{\mathbf{H}}_{11}(t)\mathbf{Q}_1(t)\mathbf{U}_1 + \bar{\mathbf{H}}_{21}(t)\mathbf{P}_2\mathbf{V}_2) \\ &\quad + \bar{\mathbf{H}}_{11}(t)\mathbf{P}_1(t)\mathbf{V}_1 + \bar{\mathbf{H}}_{21}(t)\mathbf{Q}_2(t)\mathbf{U}_2 + \mathbf{N}_1(t) \end{aligned} \tag{142}$$

$$\begin{aligned} \mathbf{Y}_2^{(2)}(t) &= (\bar{\mathbf{H}}_{12}(t)\mathbf{P}_1(t)\mathbf{V}_1 + \bar{\mathbf{H}}_{22}(t)\mathbf{Q}_2(t)\mathbf{U}_2) \\ &\quad + \bar{\mathbf{H}}_{22}(t)\mathbf{P}_2(t)\mathbf{V}_2 + \bar{\mathbf{H}}_{12}(t)\mathbf{Q}_1\mathbf{U}_1 + \mathbf{N}_2(t) \end{aligned} \tag{143}$$

Note that $\bar{\mathbf{H}}_{ij}(t)$ is a square matrix $\forall i, j$. By choosing the precoding matrices as

$$\mathbf{P}_1(t) = \bar{\mathbf{H}}_{12}(t)^{-1}, \quad \mathbf{Q}_1(t) = \bar{\mathbf{H}}_{11}(t)^{-1} \tag{144}$$

$$\mathbf{P}_2(t) = \bar{\mathbf{H}}_{21}(t)^{-1}, \quad \mathbf{Q}_2(t) = \bar{\mathbf{H}}_{22}(t)^{-1} \tag{145}$$

the received signals become

$$\begin{aligned}\mathbf{Y}_1^{(2)}(t) &= \bar{\mathbf{H}}_{11}(t)\bar{\mathbf{H}}_{12}(t)^{-1}\mathbf{V}_1 + (\mathbf{U}_1 + \mathbf{V}_2)\\ &\quad + \bar{\mathbf{H}}_{21}(t)\bar{\mathbf{H}}_{22}(t)^{-1}\mathbf{U}_2 + \mathbf{N}_1(t) \qquad (146)\\ \mathbf{Y}_2^{(2)}(t) &= (\mathbf{V}_1 + \mathbf{U}_2) + \bar{\mathbf{H}}_{22}(t)\bar{\mathbf{H}}_{21}(t)^{-1}\mathbf{V}_2\\ &\quad + \bar{\mathbf{H}}_{12}(t)\bar{\mathbf{H}}_{11}(t)^{-1}\mathbf{U}_1 + \mathbf{N}_2(t) \qquad (147)\end{aligned}$$

Hence, the scheme is secure. $\mathbf{Y}_i^{(2)}(t)$, $t = 1, 2, 3$ correspond to $3(2N - M)$ independent observations, and we have $\mathbf{V}_1$, $\mathbf{V}_2 + \mathbf{U}_1$, $\mathbf{U}_2$ unknowns of $2N - M$ each. Consequently, we can form $3(2N-M) \times 3(2N-M)$ square linear system with unique solution using zero-forcing receiver. Therefore, each user transmits $3(M - N)$ time-varying symbols and $(2N - M)$ fixed symbols over 3 channel uses, then $d_s = 2\frac{3(M-N)+2N-M}{3} = \frac{2(2M-N)}{3}$ is achievable.

C. Maximum Individual s.d.o.f. Point for $\frac{3N}{4} \leq M \leq N$

User 1 transmits a time-varying vector $\mathbf{V}_1^{(1)}(t)$, $t = 1, 2$ Gaussian secure signals of dimension $\lfloor \frac{N}{2} \rfloor$ and a fixed vector $\mathbf{V}_1^{(2)}$ Gaussian secure signal of dimension $N \bmod 2$. The fixed vector is repeated over 2 channel uses. User 2 transmits signals with the same structure for cooperative jamming signalling. The transmitted signals are

$$\mathbf{X}_1(t) = \mathbf{P}_1(t)\begin{bmatrix}\mathbf{V}_1^{(1)}(t)\\ v_1^{(2)}\end{bmatrix} \qquad (148)$$

$$\mathbf{X}_2(t) = \mathbf{Q}_2(t)\begin{bmatrix}\mathbf{U}_2^{(1)}(t)\\ u_2^{(2)}\end{bmatrix} \qquad (149)$$

where $\mathbf{P}_1(t)$, $\mathbf{Q}_2(t)$ satisfy

$$\begin{bmatrix}\mathbf{H}_{12}(t) & -\mathbf{H}_{22}(t)\end{bmatrix}\begin{bmatrix}\mathbf{P}_1(t)\\ \mathbf{Q}_2(t)\end{bmatrix} = \mathbf{0} \qquad (150)$$

where $t = 1, 2$. This alignment is feasible, since $2M - N \geq \lfloor \frac{N}{2} \rfloor + N \bmod 2$ in this regime Hence, the received signals are

$$\begin{aligned}\mathbf{Y}_1(t) &= \mathbf{H}_{11}(t)\mathbf{P}_1(t)\begin{bmatrix}\mathbf{V}_1^{(1)}(t)\\ v_1^{(2)}\end{bmatrix}\\ &\quad + \mathbf{H}_{21}(t)\mathbf{Q}_2(t)\begin{bmatrix}\mathbf{U}_2^{(1)}(t)\\ u_2^{(2)}\end{bmatrix} + \mathbf{N}_1(t) \qquad (151)\\ \mathbf{Y}_2(t) &= \mathbf{H}_{11}(t)\mathbf{P}_1(t)\begin{bmatrix}\mathbf{U}_2^{(1)}(t) + \mathbf{V}_1^{(1)}(t)\\ u_2^{(2)} + v_1^{(2)}\end{bmatrix} + \mathbf{N}_2(t) \qquad (152)\end{aligned}$$

which implies that the scheme is secure. For decodability, we note that $\mathbf{Y}_1(t)$, $t = 1, 2$ has $2N$ independent observations. The unknowns are $\mathbf{V}_1^{(1)}(t)$, $\mathbf{U}_2^{(1)}(t)$, $t = 1, 2$ with $2\lfloor \frac{N}{2} \rfloor$ dimension each and $\mathbf{V}_1^{(2)}$, $\mathbf{U}_2^{(2)}$ of $N \bmod 2$ dimension each. Hence, the total number of unknowns is $2\left(2\lfloor \frac{N}{2} \rfloor + N \bmod 2\right) = 2N$. Therefore, using this achievable scheme, and observing $\mathbf{Y}_1(t)$ for 2 channel uses, we have $2N$ independent observations. Hence, we can form $2N \times 2N$ independent linear system of equations and hence unknowns are decodable. Therefore, user 1 transmits $2\lfloor \frac{N}{2} \rfloor$ time-varying symbols and Nmod2 fixed symbol over 2 channel uses and hence $d_m = \frac{2\lfloor \frac{N}{2} \rfloor + N \bmod 2}{2} = \frac{N}{2}$ is achievable.

D. Maximum Individual s.d.o.f. Point for $N \leq M \leq \frac{3N}{2}$

The same scheme presented for static channels can be used here by replacing the structured signals $v_{12}^{(2)}$, $u_{12}^{(2)}$ by fixed Gaussian signals, which are repeated across 2 channel uses. Hence, the transmitted signals are

$$\begin{aligned}\mathbf{X}_1(t) &= \mathbf{H}_{12}(t)^{\perp}\mathbf{V}_{10}(t) + \mathbf{P}_{11}(t)\mathbf{V}_{11}(t)\\ &\quad + \mathbf{P}_{12}(t)\begin{bmatrix}\mathbf{V}_{12}^{(1)}(t)\\ v_{12}^{(2)}\end{bmatrix} \qquad (153)\end{aligned}$$

$$\mathbf{X}_2(t) = \mathbf{H}_{21}(t)^{\perp}\mathbf{Q}_{21}(t)\mathbf{U}_{11}(t) + \mathbf{Q}_{22}(t)\begin{bmatrix}\mathbf{U}_{12}^{(1)}(t)\\ u_{12}^{(2)}\end{bmatrix} \qquad (154)$$

By applying the same alignment procedure, i.e., designing $\mathbf{P}_{1i}$, $\mathbf{Q}_{2i}$, $i = 1, 2$ such that

$$\begin{bmatrix}\mathbf{H}_{12}(t) & -\mathbf{H}_{22}(t)\mathbf{H}_{21}(t)^{\perp}\end{bmatrix}\begin{bmatrix}\mathbf{P}_{11}(t)\\ \mathbf{Q}_{21}(t)\end{bmatrix} = \mathbf{0} \qquad (155)$$

$$\begin{bmatrix}\mathbf{H}_{12}(t) & -\mathbf{H}_{22}(t)\end{bmatrix}\begin{bmatrix}\mathbf{P}_{12}(t)\\ \mathbf{Q}_{22}(t)\end{bmatrix} = \mathbf{0} \qquad (156)$$

where $t = 1, 2$, the scheme is secure. The received signal is

$$\begin{aligned}\mathbf{Y}_1(t) &= \mathbf{H}_{11}(t)\mathbf{H}_{12}(t)^{\perp}\mathbf{V}_{10}(t) + \mathbf{H}_{11}(t)\mathbf{P}_{11}(t)\mathbf{V}_{11}(t)\\ &\quad + \mathbf{H}_{11}(t)\mathbf{P}_{12}(t)\begin{bmatrix}\mathbf{V}_{12}^{(1)}(t)\\ v_{12}^{(2)}\end{bmatrix}\\ &\quad + \mathbf{H}_{21}(t)\mathbf{Q}_{22}(t)\begin{bmatrix}\mathbf{U}_{12}^{(1)}(t)\\ u_{12}^{(2)}\end{bmatrix} + \mathbf{N}_1(t) \qquad (157)\end{aligned}$$

Then, $\mathbf{Y}_1(t)$, $t = 1, 2$ correspond to $2N$ unknowns by $2N$ equations. Using transmission over 2 channel uses, the receiver has $2N$ independent observations. We have $\mathbf{V}_{10}(t)$, $\mathbf{V}_{11}(t)$, $t = 1, 2$ each with $2(M - N)$ dimensions, $\mathbf{V}_{12}^{(1)}(t)$, $\mathbf{V}_{12}^{(1)}(t)$, $t = 1, 2$ each with $2\lfloor \frac{3N-2M}{2} \rfloor$ dimensions and $v_{12}^{(2)}$, $u_{12}^{(2)}$ with $(3N - 2M) \bmod 2$ dimensions. Consequently, the total number of unknowns is $2\left(2(M - N) + 2\lfloor \frac{3N-2M}{2} \rfloor + (3N - 2M) \bmod 2\right) = 2N$. Hence, we constructed a $2N \times 2N$ system, where symbols are decodable over 2 channel uses, and $d_m = N$ is achievable.

X. Conclusion

We determined the exact s.d.o.f. region of a two-user $M \times N$ MIMO ICCM for any arbitrary symmetric antenna configuration. For the converse proof, we showed that the cooperative bound which results in a two-user BCCM system is tight if $M \leq \frac{2N}{3}$. We also constructed another outer bound that uses vectorized versions of the secrecy penalty and role of a helper lemmas. We used these outer bounds together with the IC without secrecy constraints to determine the entire s.d.o.f. region for any M, N.

For the achievability, we showed that the s.d.o.f. region is a four-vertex polytope. Focusing on the sum s.d.o.f. point, 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 novel achievable scheme for the basic 2×2 MIMO ICCM. This scheme together with its SISO counterpart are central for achievable schemes for general M and N. The 2×2 scheme combines spatial alignment, which ensures that secure signals and cooperative jamming signals lie in the same rational dimension irrespective of the joint MIMO processing used at the receiver, and asymptotic real interference alignment to minimize the required dimensions needed for decodability and ensuring that observations of all receiving antennas are exploited. We showed the achievability of the other non-trivial polytope points by forcing one of the users to act as a cooperative jammer (helper) that jams its own receiver.

Interestingly, we showed that the s.d.o.f. region starts as a square region if $M \leq \frac{2N}{3}$, then it takes the shape of an irregular polytope until it returns back to a square region when the number of transmit antennas is at least twice the number of receiving antennas. We showed that if the ICCM channel is time-varying, the achievable schemes can be simplified by using vector space alignment via symbol extension over multiple channel uses instead of real interference alignment that is necessary for static channels.

References

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. TIT-24, no. 3, pp. 339–348, May 1978.

[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. TIT-24, no. 4, pp. 451–456, Jul. 1978.

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

[6] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[7] H.-F. Chong and Y.-C. Liang, "Secrecy capacity region of a class of two-user Gaussian MIMO BC with degraded message sets," in *Proc. IEEE ISIT*, Jul. 2013, pp. 2009–2013.

[8] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[9] A. Khina, Y. Kochman, and A. Khisti, "The confidential MIMO broadcast capacity: A simple derivation," in *Proc. IEEE ISIT*, Jun. 2015, pp. 1981–1985.

[10] Z. Goldfeld and H. Permuter. (2016). "MIMO Gaussian broadcast channels with common, private and confidential messages." [Online]. Available: https://arxiv.org/abs/1608.06057

[11] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[12] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[13] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

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

[15] M. Nafea and A. Yener, "Secure degrees of freedom for the MIMO wire-tap channel with a multi-antenna cooperative jammer," *IEEE Trans. Inf. Theory*, vol. 63, no. 11, pp. 7420–7441, Nov. 2017.

[16] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. (2010). "On the secure degrees-of-freedom of the multiple-access-channel." [Online]. Available: https://arxiv.org/abs/1003.0729

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

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

[19] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the K-user Gaussian interference channel," in *Proc. IEEE ISIT*, Jul. 2008, pp. 384–388.

[20] X. He and A. Yener, "K-user interference channels: Achievable secrecy rate and degrees of freedom," in *Proc. IEEE ITW*, Jun. 2009, pp. 336–340.

[21] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling," in *Proc. IEEE Globecomm*, Nov./Dec. 2009, pp. 1–6.

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

[23] T. Gou and S. A. Jafar, "On the secure degrees of freedom of wireless X networks," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 826–833.

[24] Z. Wang, M. Xiao, M. Skoglund, and H. V. Poor, "Secure degrees of freedom of wireless X networks using artificial noise alignment," *IEEE Trans. Commun.*, vol. 63, no. 7, pp. 2632–2646, Jul. 2015.

[25] T. T. Kim and H. V. Poor, "On the secure degrees of freedom of relaying with half-duplex feedback," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 291–302, Jan. 2011.

[26] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.

[27] S.-H. Lee, W. Zhao, and A. Khisti, "Secure degrees of freedom of the Gaussian diamond-wiretap channel," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 496–508, Jan. 2017.

[28] R. Tandon, S. Mohajer, H. V. Poor, and S. Shamai (Shitz), "Degrees of freedom region of the MIMO interference channel with output feedback and delayed CSIT," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1444–1457, Mar. 2013.

[29] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai (Shitz), "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5244–5256, Sep. 2013.

[30] A. Zaidi, Z. H. Awan, S. Shamai (Shitz), and L. Vandendorpe, "Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSIT," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1760–1774, Nov. 2013.

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

[32] P. Mukherjee, R. Tandon, and S. Ulukus, "Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3823–3853, Jun. 2017.

[33] R. H. Etkin, D. N. C. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5534–5562, Dec. 2008.

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

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

[36] S. A. Jafar and M. J. Fakhereddin, "Degrees of freedom for the MIMO interference channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2637–2642, Jul. 2007.

[37] Z. Wang, R. F. Schaefer, M. Skoglund, H. V. Poor, and M. Xiao, "Strong secrecy for interference channels from channel resolvability," in *Proc. 49th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2015, pp. 559–563.

[38] M. Nafea and A. Yener, "New models for interference and broadcast channels with confidential messages," in *Proc. IEEE ISIT*, Jun. 2017, pp. 1808–1812.

Karim Banawan (S'13) received the B.Sc. and M.Sc. degrees (Highest Hons.) in electrical engineering from Alexandria University, Alexandria, Egypt, in 2008, 2012, respectively, M.Sc. degree in electrical engineering from University of Maryland, College Park, MD, USA in 2017. He is currently pursuing the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, USA. He was the recipient of the Distinguished Dissertation Fellowship from the Department of Electrical and Computer Engineering, at the University of Maryland College Park, for his Ph.D. thesis work. His research interests include information theory, wireless communications, physical layer security and private information retrieval.

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

Dr. Ulukus is a fellow of the IEEE, and a Distinguished Scholar-Teacher of the University of Maryland. She received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, an 2005 NSF CAREER Award, the 2010-2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 ECE George Corcoran Education Award. She is a Distinguished Lecturer of the Infomation Theory Society for 2018-2019. She is on the Editorial Board of the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING since 2016. She was an Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Series on Green Communications and Networking (2015-2016), IEEE TRANSACTIONS ON INFORMATION THEORY (2007-2010), and IEEE TRANSACTIONS ON COMMUNICATIONS (2003-2007). She was a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (2015 and 2008), JOURNAL OF COMMUNICATIONS AND NETWORKS (2012), and IEEE TRANSACTIONS ON INFORMATION THEORY (2011). She was a general TPC co-chair of 2017 IEEE ISIT, 2016 IEEE GLOBECOM, 2014 IEEE PIMRC, and 2011 IEEE CTW.