Improving Wireless Physical Layer Security via Exploiting Co-Channel Interference

Lingxiang Li, Athina P. Petropulu, *Fellow, IEEE*,
Zhi Chen, *Member, IEEE*, and Jun Fang, *Member, IEEE*

Abstract—This paper considers a scenario in which a source-destination pair needs to establish a confidential connection against an external eavesdropper, aided by the interference generated by another source-destination pair that exchanges public messages. The goal is to compute the maximum achievable secrecy degrees of freedom (S.D.o.F) region of a MIMO two-user wiretap network. First, a cooperative secrecy transmission scheme is proposed, whose feasible set is shown to achieve all S.D.o.F. pairs on the S.D.o.F. region boundary. In this way, the determination of the S.D.o.F. region is reduced to a problem of maximizing the S.D.o.F. pair over the proposed transmission scheme. The maximum achievable S.D.o.F. region boundary points are obtained in closed form, and the construction of the precoding matrices achieving the maximum S.D.o.F. region boundary is provided. The obtained analytical expressions clearly show the relation between the maximum achievable S.D.o.F. region and the number of antennas at each terminal.

Index Terms—Physical-layer security, Cooperative communications, Multi-input Multi-output, Secrecy Degrees of Freedom.

I. INTRODUCTION

The area of physical (PHY) layer security has been pioneered by Wyner [1], who introduced the wiretap channel and and the notion of secrecy capacity, i.e., the rate at which the legitimate receiver can correctly decode the source message, while an unauthorized user, often referred to as eavesdropper, obtains no useful information about the source signal. For the classical source-destination-eavesdropper Gaussian wiretap channel, the secrecy capacity is zero when the quality of the legitimate channel is worse than the eavesdropping channel [2]. One way to achieve non-zero secrecy rates in the latter case is to introduce one [3]–[8] or more [9]–[15] external helpers, who transmit artificial noise, thus acting as jammers to the eavesdropper. More complex K-user interference channels (IFC) are considered in [16]–[19], where each user secures its communication from the remaining $K-1$ users by transmitting jamming signals along with its message signal.

From a system design perspective, introducing non-message carrying artificial noise into a network is power inefficient and lowers the overall network throughput. In dense multiuser networks there is ubiquitous co-channel interference (CCI), which, in a cooperative scenario could be designed to effectively act as noise and degrade the eavesdropping channel.

Indeed, there are recent results [19]–[24] on exploiting CCI to enhance secrecy. [19]–[22] consider the scenario of a K-user IFC in which the users wish to establish secure communication against an eavesdropper. Specifically, [19]–[21] consider the single-antenna case and examine the achievable secrecy degrees of freedom by applying interference alignment techniques. The work of [22] considers the multi-antenna case and proposes interference-alignment-based algorithms for the sake of maximizing the achievable secrecy sum rate. In [23], [24], a two-user wiretap interference network is considered, in which only one user needs to establish a confidential connection against an external eavesdropper, and the secrecy rate is increased by exploiting CCI due to the nonconfidential connection. [23], [24] maximize the secrecy transmission rate of the confidential connection subject to a quality of service constraint for the non-confidential connection.

In this paper, we consider a two-user wiretap interference network as in [23], [24], except that, unlike [23], [24], which assume the single input single-output (SISO) case or multiple-input single-output (MISO) case, we address the most general multiple-input multiple-output (MIMO) case, i.e., the case in which each terminal is equipped with multiple antennas. Out network comprises a source destination pair exchanging confidential messages, another pair exchanging public messages, and a passive eavesdropper. Our goal is to exploit the interference generated by the second source destination pair, in order to enhance the secrecy rate performance of the network. We should note that, although the eavesdropper is not interested in the messages of the second pair, for uniformity, we will still refer to the rate of the second pair as secrecy rate. Since determining the exact maximum achievable secrecy rate of a helper-assisted wiretap channel, or of an interference channel is a very difficult problem [3]–[17], we consider the high signal to noise ratio (SNR) behavior of the achievable secrecy rate, i.e., the secrecy degrees of freedom (S.D.o.F.) as an alternative. A similar alternative has also been considered in [19]–[21], [25]–[27]. Our main contributions are summarized below.

1) We propose a cooperative secrecy transmission scheme, in which the message and interference signals lie in different subspaces at the destination of the confidential connection, but are aligned along the same subspace at the eavesdropper. We show that the proposed scheme can achieve all the boundary points of the S.D.o.F. region (see *Proposition 3*). In this way, we reduce the determination of each S.D.o.F. region boundary point

Lingxiang Li, Zhi Chen, and Jun Fang are with the National Key Laboratory of Science and Technology on Communications, UESTC, Chengdu 611731, China (e-mails: lingxiang.li@rutgers.edu; {chenzhi, JunFang}@uestc.edu.cn).

Athina P. Petropulu is with the Department of Electrical and Computer Engineering, Rutgers–The State University of New Jersey, New Brunswick, NJ 08854 USA (e-mail: athinap@rci.rutgers.edu).

to an S.D.o.F. pair maximization problem over our proposed transmission scheme.

2) We determine in closed form the Single-User points, *SU*1 and *SU*2 (see eq. (40) and (41), respectively) corresponding to when only one user communicates information, the strict S.D.o.F. region boundary (see eq. (48)), and the ending points of the strict S.D.o.F. region boundary, *E*1 and *E*2 (see eq. (49) and (58), respectively). Our analytical results fully describe the dependence of the S.D.o.F. region of a MIMO two-user wiretap interference channel on the number of antennas.

3) We derive in closed form the general term formulas for the feasible precoding vector pairs corresponding to the proposed transmission scheme, based on which we construct precoding matrices achieving S.D.o.F. pairs on the S.D.o.F. region boundary (see Table III).

The corner point of our S.D.o.F. region corresponding to zero S.D.o.F for the nonconfidential connection has also been studied in [25]–[27], wherein the maximum achievable S.D.o.F. of a MIMO wiretap channel with a multi-antenna cooperative jammer has been studied. Our corner point result is more general because, unlike [25]–[27] it applies to any number of antennas. It is interesting to note that although we derive the achievable S.D.o.F. from a signal processing point of view, our corner point result matches the S.D.o.F. result of [25]–[27], which is derived from an information theoretic point of view.

The idea of signal subspace alignment is also used in [28]–[31] in the derivation of the D.o.F. of the X channel and the K-user interference channel. Due to the difference in signal models, the motivation and use of subspace alignment is different. In [28]–[31], the authors jointly design the precoding matrices at the sources, which align multiple interference signals into a small subspace at each receiver so that the sum dimension of the interference-free subspaces remaining for the desired signals can be maximized. In our work, we apply subspace alignment for the sake of degrading the eavesdropping channel and our goal is to maximize the dimension difference of the interference-free subspaces that the legitimate receiver and the eavesdropper can see.

The rest of this paper is organized as follows. In Section II, we introduce a mathematical background, i.e., generalized singular value decomposition (GSVD), that provides the basis for the derivations to follow. In Section III, we describe the system model for the MIMO two-user wiretap interference channel and formulate the S.D.o.F. maximization problem. In Section IV, we propose a secrecy cooperative transmission scheme, and prove that its feasible set is sufficient to achieve all S.D.o.F. pairs on the S.D.o.F. region boundary. In Section V, we determine the maximum achievable S.D.o.F. region boundary, and uncover its connection to the number of antennas. In Section VI, we construct the precoding matrices which achieve the S.D.o.F. pair on the boundary. Numerical results are given in Section VII and conclusions are drawn in Section VIII.

Notation: $x \sim \mathcal{CN}(0, \Sigma)$ means x is a random variable following a complex circular Gaussian distribution with mean zero and covariance Σ; $(a)^+ \triangleq \max(a, 0)$; $\lfloor a \rfloor$ denotes the biggest integer which is less or equal to a; $|a|$ is the absolute value of a; $\mathbf{I}$ represents an identity matrix with appropriate size; $\mathbb{C}^{N \times M}$ indicates a $N \times M$ complex matrix set; $\mathbf{A}^T$, $\mathbf{A}^H$, $\text{tr}\{\mathbf{A}\}$, $\text{rank}\{\mathbf{A}\}$, and $|\mathbf{A}|$ stand for the transpose, hermitian transpose, trace, rank and determinant of the matrix $\mathbf{A}$, respectively; $\mathbf{A}(:, j)$ indicates the j-th column of $\mathbf{A}$ while and $\mathbf{A}(:, i : j)$ denotes the columns from i to j of $\mathbf{A}$; $\text{span}(\mathbf{A})$ and $\text{span}(\mathbf{A})^\perp$ are the subspace spanned by the columns of $\mathbf{A}$ and its orthogonal complement, respectively; $\text{null}(\mathbf{A})$ denotes the null space of $\mathbf{A}$; $\text{span}(\mathbf{A})/\text{span}(\mathbf{B}) \triangleq \{\mathbf{x} | \mathbf{x} \in \text{span}(\mathbf{A}), \mathbf{x} \notin \text{span}(\mathbf{B})\}$; $\text{span}(\mathbf{A}) \cap \text{span}(\mathbf{B}) = \mathbf{0}$ means that $\text{span}(\mathbf{A})$ and $\text{span}(\mathbf{B})$ have no intersections; $\dim\{\text{span}(\mathbf{A})\}$ represents the number of dimension of the subspace spanned by the columns of $\mathbf{A}$; $\mathbf{\Gamma}(\mathbf{A})$ denotes the orthonormal basis of $\text{null}(\mathbf{A})$; $\mathbf{A}^\perp$ denotes the orthonormal basis of $\text{null}(\mathbf{A}^H)$.

II. MATHEMATICAL BACKGROUND

Given two full rank matrices $\mathbf{A} \in \mathbb{C}^{N \times M}$ and $\mathbf{B} \in \mathbb{C}^{N \times K}$. The GSVD of $(\mathbf{A}, \mathbf{B})$ [32] returns unitary matrices $\mathbf{\Psi}_1 \in \mathbb{C}^{M \times M}$, $\mathbf{\Psi}_2 \in \mathbb{C}^{K \times K}$ and $\mathbf{\Psi}_0 \in \mathbb{C}^{N \times N}$, non-negative diagonal matrices $\mathbf{D}_1 \in \mathbb{C}^{M \times k}$ and $\mathbf{D}_2 \in \mathbb{C}^{K \times k}$, and a matrix $\mathbf{\Omega} \in \mathbb{C}^{k \times k}$ with $\text{rank}\{\mathbf{\Omega}\} = k$, such that

$$\mathbf{A}^H = \mathbf{\Psi}_1 \mathbf{D}_1 \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0} \end{bmatrix} \mathbf{\Psi}_0^H, \quad (1a)$$

$$\mathbf{B}^H = \mathbf{\Psi}_2 \mathbf{D}_2 \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0} \end{bmatrix} \mathbf{\Psi}_0^H, \quad (1b)$$

with $\mathbf{D}_1 = \begin{bmatrix} \mathbf{I}_r & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Lambda}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}$, $\mathbf{D}_2 = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Lambda}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_p \end{bmatrix}$, where the diagonal entries of $\mathbf{\Lambda}_1 \in \mathbb{R}^{s \times s}$ and $\mathbf{\Lambda}_2 \in \mathbb{R}^{s \times s}$ are greater than 0, and $\mathbf{D}_1^H \mathbf{D}_1 + \mathbf{D}_2^H \mathbf{D}_2 = \mathbf{I}$. It holds that

$$k \triangleq \text{rank}\{[(\mathbf{A}^H)^T, (\mathbf{B}^H)^T]^T\} = \min\{M + K, N\}, \quad (2a)$$

$$p \triangleq \dim\{\text{span}(\mathbf{A})^\perp \cap \text{span}(\mathbf{B})\} = k - \min\{M, N\}, \quad (2b)$$

$$r \triangleq \dim\{\text{span}(\mathbf{A}) \cap \text{span}(\mathbf{B})^\perp\} = k - \min\{K, N\}, \quad (2c)$$

$$s \triangleq \dim\{\text{span}(\mathbf{A}) \cap \text{span}(\mathbf{B})\} = k - p - r$$
$$= (\min\{M, N\} + \min\{K, N\} - N)^+. \quad (2d)$$

Let $\mathbf{X} = \mathbf{\Psi}_0 \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0} \end{bmatrix}^H$ and substitute it into (1a) and (1b). Then, (1a) and (1b) can be respectively rewritten as,

$$\mathbf{A}\mathbf{\Psi}_1 = \mathbf{X}\mathbf{D}_1^H, \quad (3a)$$

$$\mathbf{B}\mathbf{\Psi}_2 = \mathbf{X}\mathbf{D}_2^H. \quad (3b)$$

Let $\mathbf{\Psi}_{11}$, $\mathbf{\Psi}_{12}$ and $\mathbf{\Psi}_{13}$ be the collection of columns $1 : r$, $r + 1 : r + s$, $r + s + 1 : M$ of $\mathbf{\Psi}_1$, respectively, and let $\mathbf{\Psi}_{21}$, $\mathbf{\Psi}_{22}$ and $\mathbf{\Psi}_{23}$ be the collection of columns $1 : K - s - p$, $K - s - p + 1 : K - p$, $K - p + 1 : K$ of $\mathbf{\Psi}_2$, respectively. In addition, let $\mathbf{X}_1$, $\mathbf{X}_2$ and $\mathbf{X}_3$ be the collection of columns $1 : r$, $r + 1 : r + s$, $r + s + 1 : k$ of $\mathbf{X}$, respectively. We can rewrite (3a) and (3b) as $\mathbf{A}\mathbf{\Psi}_{11} = \mathbf{X}_1$, $\mathbf{A}\mathbf{\Psi}_{12} = \mathbf{X}_2\mathbf{\Lambda}_1$, $\mathbf{A}\mathbf{\Psi}_{13} = \mathbf{0}$; $\mathbf{B}\mathbf{\Psi}_{21} = \mathbf{0}$, $\mathbf{B}\mathbf{\Psi}_{22} = \mathbf{X}_2\mathbf{\Lambda}_2$, $\mathbf{B}\mathbf{\Psi}_{23} = \mathbf{X}_3$.

In the rest of the paper we will denote the GSVD decomposition in (3a) and (3b) as

$$\text{GSVD}(\mathbf{A}, \mathbf{B}; N, M, K) = (\mathbf{\Psi}_1, \mathbf{\Psi}_2, \mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \mathbf{X}, k, r, s, p).$$

With the GSVD decomposition, one can decompose the union of $\text{span}(\mathbf{A})$ and $\text{span}(\mathbf{B})$ into three subspaces, i.e., (i)
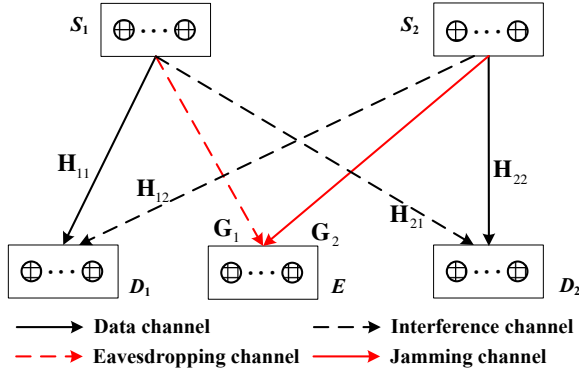
Fig. 1: A MIMO two-user wiretap interference channel

$\mathrm{span}(\mathbf{A}) \cap \mathrm{span}(\mathbf{B})^{\perp}$, which is also the same as $\mathrm{span}(\mathbf{X}_1)$ and has r independent vectors, (ii) $\mathrm{span}(\mathbf{A}) \cap \mathrm{span}(\mathbf{B})$, which is also the same as $\mathrm{span}(\mathbf{X}_2)$ and has s independent vectors, and (iii) $\mathrm{span}(\mathbf{A})^{\perp} \cap \mathrm{span}(\mathbf{B})$, which is also the same as $\mathrm{span}(\mathbf{X}_3)$ and has p independent vectors.

Proposition 1: Consider two full rank matrices $\mathbf{A} \in \mathbb{C}^{N \times M}$ and $\mathbf{B} \in \mathbb{C}^{N \times K}$, and the $\mathrm{GSVD}(\mathbf{A}, \mathbf{B}; N, M, K) = (\mathbf{\Psi}_1, \mathbf{\Psi}_2, \mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \mathbf{X}, k, r, s, p)$.

(i) $\mathbf{A}\mathbf{v} = \mathbf{B}\mathbf{w} \neq \mathbf{0}$ holds true if and only if

$$\mathbf{v} = \mathbf{\Phi}_1 \mathbf{y}_{s1} = \begin{bmatrix} \mathbf{\Psi}_{12}\mathbf{\Lambda}_1^{-1} & \mathbf{\Gamma}(\mathbf{A}) \end{bmatrix} \begin{bmatrix} \mathbf{y}_s \\ \mathbf{y}_1 \end{bmatrix}, \tag{4a}$$

$$\mathbf{w} = \mathbf{\Phi}_2 \mathbf{y}_{s2} = \begin{bmatrix} \mathbf{\Psi}_{22}\mathbf{\Lambda}_2^{-1} & \mathbf{\Gamma}(\mathbf{B}) \end{bmatrix} \begin{bmatrix} \mathbf{y}_s \\ \mathbf{y}_2 \end{bmatrix}, \tag{4b}$$

with $\mathbf{y}_s$ being any nonzero vectors, $\mathbf{y}_{s1}, \mathbf{y}_{s2}, \mathbf{y}_1$ and $\mathbf{y}_2$ being any vectors, with appropriate length.

(ii) The number of linearly independent vectors $\mathbf{v}$ satisfying $\mathbf{A}\mathbf{v} = \mathbf{B}\mathbf{w} \neq \mathbf{0}$ is $s + \dim\{\mathrm{null}(\mathbf{A})\}$.

Proof: See Appendix A. ∎

III. SYSTEM MODEL AND PROBLEM STATEMENT

We consider a MIMO interference network which consists of a wiretap channel S_1-D_1-E and a point-to-point channel S_2-D_2 (see Fig. 1). In a real setting, the former channel would correspond to a source-destination pair that needs to maintain secret communications, while the latter would correspond to a public communication system. While communicating with its intended destination, S_2 acts as a jammer to the external passive eavesdropper E. S_1 and S_2 are equipped with N_s^1, N_s^2 antennas, respectively; D_1, D_2 and E are equipped with N_d^1, N_d^2 and N_e antennas, respectively. Let $\mathbf{s}_1 \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and $\mathbf{s}_2 \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ be the messages transmitted from S_1 and S_2, respectively. Each message is precoded by a matrix before transmission. The signals received at the legitimate receiver D_i can be expressed as

$$\mathbf{y}_d^i = \mathbf{H}_{i1}\mathbf{V}\mathbf{s}_1 + \mathbf{H}_{i2}\mathbf{W}\mathbf{s}_2 + \mathbf{n}_d^i, i = 1, 2, \tag{5}$$

while the signal received at the eavesdropper E can be expressed as

$$\mathbf{y}_e = \mathbf{G}_1\mathbf{V}\mathbf{s}_1 + \mathbf{G}_2\mathbf{W}\mathbf{s}_2 + \mathbf{n}_e. \tag{6}$$

Here, $\mathbf{V} \in \mathbb{C}^{N_s^1 \times K_v}$ and $\mathbf{W} \in \mathbb{C}^{N_s^2 \times K_w}$ are the precoding matrices at S_1 and S_2, respectively; $\mathbf{n}_d^i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and $\mathbf{n}_e \sim$

$\mathcal{CN}(\mathbf{0}, \mathbf{I})$ represent noise at the ith destination D_i and the eavesdropper E, respectively; $\mathbf{H}_{ij} \in \mathbb{C}^{N_d^i \times N_s^j}$, $i, j \in \{1, 2\}$, denotes the channel matrix from S_j to D_i; $\mathbf{G}_j \in \mathbb{C}^{N_e \times N_s^j}$, $j \in \{1, 2\}$, represents the channel matrix from S_j to E.

In this paper, we make the following assumptions:

1) The messages $\mathbf{s}_1$ and $\mathbf{s}_2$ are independent of each other, and independent of the noise vectors $\mathbf{n}_d^i$ and $\mathbf{n}_e$.

2) CCI is treated as noise at each receiver. We assume Gaussian signaling for S_2. Thus the MIMO wiretap channel S_1-D_1-E is Gaussian. For this case, a Gaussian input signal at S_1 is the optimal choice [33], [34].

3) All channel matrices are full rank. Global channel state information (CSI) is available, including the CSI for the eavesdropper. This is possible in situations in which the eavesdropper is an active member of the network, and thus its whereabouts and behavior can be monitored.

The achievable secrecy rate for transmitting the message $\mathbf{s}_1$ and $\mathbf{s}_2$ are respectively given as [35]

$$R_s^1 = (R_d^1 - R_e)^+, \tag{7}$$
$$R_s^2 = R_d^2. \tag{8}$$

where

$$R_d^1 = \log|\mathbf{I} + (\mathbf{I} + \mathbf{H}_{12}\mathbf{Q}_w\mathbf{H}_{12}^H)^{-1}\mathbf{H}_{11}\mathbf{Q}_v\mathbf{H}_{11}^H|, \tag{9a}$$
$$R_d^2 = \log|\mathbf{I} + (\mathbf{I} + \mathbf{H}_{21}\mathbf{Q}_v\mathbf{H}_{21}^H)^{-1}\mathbf{H}_{22}\mathbf{Q}_w\mathbf{H}_{22}^H|, \tag{9b}$$
$$R_e = \log|\mathbf{I} + (\mathbf{I} + \mathbf{G}_2\mathbf{Q}_w\mathbf{G}_2^H)^{-1}\mathbf{G}_1\mathbf{Q}_v\mathbf{G}_1^H|, \tag{9c}$$

with $\mathbf{Q}_v \triangleq \mathbf{V}\mathbf{V}^H$ and $\mathbf{Q}_w \triangleq \mathbf{W}\mathbf{W}^H$ denoting the transmit covariance matrices of S_1 and S_2, respectively.

The *achievable secrecy rate region* is the set of all secrecy rate pairs, i.e., $\mathcal{R} \triangleq \underset{(\mathbf{V}, \mathbf{W}) \in \mathcal{I}}{\cup} (R_s^1, R_s^2)$, where $\mathcal{I} \triangleq \{(\mathbf{V}, \mathbf{W})|\mathrm{tr}\{\mathbf{V}\mathbf{V}^H\} = P, \mathrm{tr}\{\mathbf{W}\mathbf{W}^H\} = P\}$, with P denoting the transmit power budget. Generally, the determination of the outer boundary of $\mathcal{R}$ is a non-convex problem. Next, we study a simpler problem, namely the *achievable secrecy degrees of freedom region*, defined as

$$\mathcal{D} \triangleq \underset{(\mathbf{V}, \mathbf{W}) \in \mathcal{I}}{\cup} (d_s^1, d_s^2), \tag{10}$$

where d_s^i denotes the high SNR behavior of the achievable secrecy rate, i.e.,

$$d_s^i \triangleq \lim_{P \to \infty} \frac{R_s^i}{\log P}, i \in \{1, 2\}. \tag{11}$$

As shown in Fig. 2, the outer boundary of $\mathcal{D}$ consists of the strict S.D.o.F. region boundary (the part between $E1$ and $E2$ in the graph) and the non-strict S.D.o.F. region boundary (the vertical part below $E1$ and the horizontal part up to $E2$ of the graph). The points marked by $SU1$ and $SU2$ correspond to single user S.D.o.F., i.e., when only one user communicates. For an arbitrary point on the strict S.D.o.F. region boundary, it is impossible to improve one S.D.o.F., without decreasing the other. On the other hand, for a point on the non-strict S.D.o.F. region boundary, one S.D.o.F. can be further improved while the other S.D.o.F. remains at the maximum value.

In the following, we will determine the outer boundary of $\mathcal{D}$, and find its connection to the number of antennas. Towards
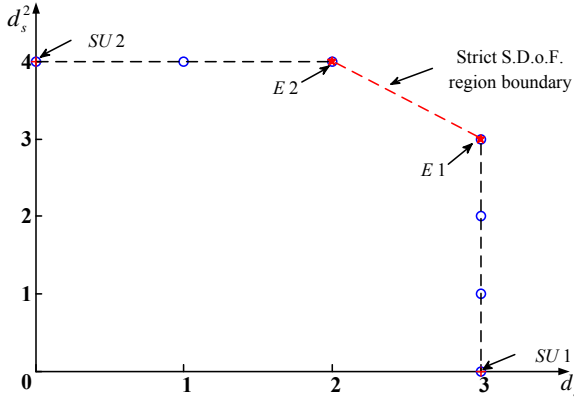
Fig. 2: Achievable S.D.o.F. region boundary

that goal, we first introduce a cooperative transmission scheme. Then, by studying that scheme we determine in closed form the outer boundary of $\mathcal{D}$ and also we construct the precoding matrices which achieve the outer boundary of $\mathcal{D}$.

IV. COOPERATIVE SECRECY TRANSMISSION SCHEME

Proposition 2: For the precoding matrix pair $(\mathbf{V}, \mathbf{W})$, the achieved S.D.o.F. equals

$$d_s^1(\mathbf{V}, \mathbf{W}) = \text{rank}\{\mathbf{H}_{11}\mathbf{V}\} - m(\mathbf{V}, \mathbf{W}) - n(\mathbf{V}, \mathbf{W}), \quad (12a)$$

$$d_s^2(\mathbf{V}, \mathbf{W}) = \dim\{\text{span}(\mathbf{H}_{22}\mathbf{W})/\text{span}(\mathbf{H}_{21}\mathbf{V})\}, \quad (12b)$$

in which $m(\mathbf{V}, \mathbf{W}) \triangleq \dim\{\text{span}(\mathbf{G}_1\mathbf{V})/\text{span}(\mathbf{G}_2\mathbf{W})\}$ and $n(\mathbf{V}, \mathbf{W}) \triangleq \dim\{\text{span}(\mathbf{H}_{12}\mathbf{W}) \cap \text{span}(\mathbf{H}_{11}\mathbf{V})\}$.

Proof: See Appendix B. ∎

According to *Proposition 2*, the achievable S.D.o.F. of S_1-D_1 depends only on the dimension difference of the interference-free subspaces which D_1 and E can see. Motivated by this observation, we propose a transmission scheme in which the subspace spanned by the message signal has no intersection with the subspace spanned by the interference signal at D_1, and belongs to the subspace spanned by the interference signal at E. In this way, D_1 can see an interference-free message signal, such that R_d^1 scales with $\log(P)$, while E can only see a distorted version of the message signal, such that R_e converges to a constant as P approaches to infinity. In other words, the precoding matrix pairs belongs to the set $\bar{\mathcal{I}}$, which is defined as follows:

$$\bar{\mathcal{I}} \triangleq \{(\mathbf{V}, \mathbf{W}) | (\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}_1 \cap \bar{\mathcal{I}}_2 \cap \mathcal{I}\},$$

where

$$\bar{\mathcal{I}}_1 \triangleq \{(\mathbf{V}, \mathbf{W}) | \text{span}(\mathbf{G}_1\mathbf{V}) \subset \text{span}(\mathbf{G}_2\mathbf{W})\}, \quad (13a)$$

$$\bar{\mathcal{I}}_2 \triangleq \{(\mathbf{V}, \mathbf{W}) | \text{span}(\mathbf{H}_{11}\mathbf{V}) \cap \text{span}(\mathbf{H}_{12}\mathbf{W}) = \mathbf{0}\}. \quad (13b)$$

Next, we show that the proposed scheme can achieve all the boundary points of the S.D.o.F. region.

Proposition 3: Let

$$\bar{\mathcal{D}} \triangleq \bigcup_{(\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}} (d_s^1, d_s^2). \quad (14)$$

Then, the outer boundary of $\bar{\mathcal{D}}$ is the same as that of $\mathcal{D}$.

Proof: See Appendix C. ∎

By restricting $(\mathbf{V}, \mathbf{W})$ to lie in $\bar{\mathcal{I}}$, we exclude a large number of precoding matrix pairs in $\mathcal{I}$, which have no contribution to the outer boundary, and thus reduce the number of precoding matrices we need to investigate in determining the outer boundary of the S.D.o.F. region. It turns out that we can reduce the set even further without changing the achievable S.D.o.F. region; this is discussed in the following corollary, where we introduce a new set $\hat{\mathcal{I}}$, which is a subset of $\bar{\mathcal{I}}$.

Corollary 1: Let

$$\hat{\mathcal{D}} \triangleq \bigcup_{(\mathbf{V}, \mathbf{W}) \in \hat{\mathcal{I}}} (d_s^1, d_s^2), \quad (15)$$

where the set of $\hat{\mathcal{I}}$ is defined as follows,

$$\hat{\mathcal{I}} \triangleq \{(\mathbf{V}, \mathbf{W}) | \mathbf{G}_1\mathbf{V} = \mathbf{G}_2\mathbf{W}(:, 1 : K_v), (\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}\}. \quad (16)$$

Then, $\hat{\mathcal{D}} = \bar{\mathcal{D}}$.

Proof: See Appendix D. ∎

Corollary 2: For any given precoding matrix pair $(\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}$, the achieved S.D.o.F. over the wiretap channel S_1-D_1-E is $d_s^1 = \text{rank}(\mathbf{H}_{11}\mathbf{V})$.

Proof: Since $(\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}$, it holds that $\text{span}(\mathbf{G}_1\mathbf{V}) \subset \text{span}(\mathbf{G}_2\mathbf{W})$, which indicates $\lim_{P \to \infty} \frac{R_e}{\log(P)} = 0$. In addition, $\text{span}(\mathbf{H}_{11}\mathbf{V}) \cap \text{span}(\mathbf{H}_{12}\mathbf{W}) = \mathbf{0}$, thus $\lim_{P \to \infty} \frac{R_d^1}{\log(P)} = \text{rank}(\mathbf{H}_{11}\mathbf{V})$. So,

$$d_s^1 = \lim_{P \to \infty} \frac{R_d^1}{\log(P)} - \lim_{P \to \infty} \frac{R_e}{\log(P)} = \text{rank}(\mathbf{H}_{11}\mathbf{V}).$$

This completes the proof. ∎

V. COMPUTATION OF THE S.D.o.F. BOUNDARY

The key idea for computing the S.D.o.F. boundary is to maximize the value of d_s^2 for a fixed value of d_s^1, say $d_s^1 = \hat{d}_s^1$. Based on *Corollary 1*, in order to determine the outer boundary of $\mathcal{D}$, we only need to focus on the set $\hat{\mathcal{I}}$ (see eq. (16)). Further, *Corollary 2* shows that for $(\mathbf{V}, \mathbf{W}) \in \hat{\mathcal{I}}$ the achieved S.D.o.F. is $d_s^1 = \text{rank}\{\mathbf{H}_{11}\mathbf{V}\}$. The problem of interest now is to construct precoding matrices which satisfy $(\mathbf{V}, \mathbf{W}) \in \hat{\mathcal{I}}$, $K_v = \hat{d}_s^1$, and also leave a maximum dimension interference-free subspace for D_2.

For ease of exposition, let $(\mathbf{v}, \mathbf{w})^1$ denote the precoding vector pair. Some observations are in order. First, one can see that when the source message sent by S_1 lies in the null space of the eavesdropping channel, even if the pair S_2-D_2 communicates, their interference cannot degrade any further the eavesdropping channel because the eavesdropper already receives nothing; in those cases we may take $\mathbf{w} = \mathbf{0}$. Second, according to *Corollary 2*, for any precoding matrix pairs $(\mathbf{V}, \mathbf{W}) \in \hat{\mathcal{I}}$, the achieved S.D.o.F. $d_s^1 = \text{rank}\{\mathbf{H}_{11}\mathbf{V}\}$. Thus, a greater value of d_s^1 can be achieved by including more linear independent precoding vector pairs in $(\mathbf{V}, \mathbf{W})$.

---

[1] The precoding vector pairs $(\mathbf{v}, \mathbf{w})$ we consider in the construction of $(\mathbf{V}, \mathbf{W})$ are linear independent of each other.

Third, the maximum number of linear precoding vector pairs is determined by (13b), which requires that

$$\dim\{\text{span}(\mathbf{H}_{11}\mathbf{V})\} + \dim\{\text{span}(\mathbf{H}_{12}\mathbf{W})\} \leq N_d^1. \quad (17)$$

Fourth, the maximum dimension of the interference-free subspace at D_2 depends on whether D_2 experiences interference from S_1. So, in the following subsections, we will divide the set satisfying $\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w}$ into six subsets, according to whether the source message from S_1 lies in the null space of the eavesdropping channel, whether the source message from S_2 has interference on D_1, and whether the source message from S_1 has interference on D_2. Accordingly, we characterize the precoding vector pairs in each subset with the signal dimension triplet (a, b, c), where a and b denote the number of signal dimensions we respectively need at D_1 and S_2, and c denotes the signal dimension penalty at D_2, for obtaining one S.D.o.F. over the wiretap channel S_1-D_1-E. In particular, $a \triangleq \text{rank}\{\mathbf{H}_{11}\mathbf{v}\} + \text{rank}\{\mathbf{H}_{12}\mathbf{w}\}$; $b \triangleq \text{rank}\{\mathbf{w}\}$; $c \triangleq \text{rank}\{\mathbf{H}_{21}\mathbf{v}\}$. Then,

1) if the message signal sent by S_1 spreads within the null space of the eavesdropping channel, the message signal sent from S_1 is secure even without the help of S_2, thus $b = 0$, $a = 1$; otherwise, $b = 1$.
2) if the message signal sent by S_2 interferes with D_1, we need at least two signal dimensions at D_1 in order to tell the message signal sent by S_1 apart from that sent by S_2, which means that $a = 2$; otherwise, $a = 1$.
3) if the message signal sent by S_1 interferes with D_2, the signal dimension penalty at D_2 is one, thus $c = 1$; otherwise, $c = 0$.

Please refer to Table I for the triplet (a, b, c) of the precoding vector pair from each subset. Based on this triplet (a, b, c), in this section, we will analyze the Single-User points $SU1$ and $SU2$, the strict S.D.o.F. region boundary, and the ending points of strict S.D.o.F. region boundary $E1$ and $E2$.

A. Aligned signal subspace decomposition

In this subsection, we divide the set satisfying $\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w}$ into six subsets, i.e., Sub_I,..., Sub_VI, and determine the number of linear independent precoding vector pairs that should be considered in each subset, i.e., d_I,...,d_VI, respectively.

I) *The message signal sent by S_1 spreads within the null space of the eavesdropping channel, and does not interfere with D_2. That is, the precoding vector pairs in Sub_I should satisfy*

$$\mathbf{G}_1\mathbf{v} = \mathbf{0}, \quad (18a)$$
$$\mathbf{H}_{21}\mathbf{v} = \mathbf{0}. \quad (18b)$$

Further, it holds that $\mathbf{G}_2\mathbf{w} = \mathbf{G}_1\mathbf{v} = \mathbf{0}$. The case where $\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} = 0$ and $\mathbf{w} \neq 0$ is not considered here, because even if the pair S_2-D_2 communicates, their interference cannot degrade any further the eavesdropping channel. So we will consider $\mathbf{w} = \mathbf{0}$ for simplicity. Substituting $\mathbf{v} = \mathbf{\Gamma}(\mathbf{G}_1)\mathbf{x}$ into (18b), with $\mathbf{x}$ being any vectors with appropriate length, we arrive at $\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1)\mathbf{x} = \mathbf{0}$, which is equivalent to $\mathbf{x} =$ $\mathbf{\Gamma}(\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1))\mathbf{y}$, with $\mathbf{y}$ being any vectors with appropriate length. Therefore, the formula of $\mathbf{v}$ in Sub_I is

$$\mathbf{v} = \mathbf{\Gamma}(\mathbf{G}_1)\mathbf{\Gamma}(\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1))\mathbf{z}, \quad (19)$$

with $\mathbf{z}$ being any nonzero vectors with appropriate length. In addition, since all the channel matrices are assumed to be full rank, it holds that

$$d_\text{I} \leq \dim\{\text{null}(\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1))\} = (N_s^1 - N_e - N_d^2)^+. \quad (20)$$

II) *The message signal sent by S_1 spreads within the null space of the eavesdropping channel, but does interfere with D_2. That is, the vectors in Sub_II should satisfy*

$$\mathbf{G}_1\mathbf{v} = \mathbf{0}, \quad (21a)$$
$$\mathbf{H}_{21}\mathbf{v} \neq \mathbf{0}. \quad (21b)$$

Here again, we will consider $\mathbf{w} = \mathbf{0}$ for simplicity. On combining (18a)-(18b) with (21a)-(21b), it holds that

$$Sub_\text{I} \cup Sub_\text{II} = \{(\mathbf{v}, \mathbf{w}) | \mathbf{G}_1\mathbf{v} = \mathbf{0}, \mathbf{w} = \mathbf{0}\}. \quad (22)$$

So, the linear independent vectors we can choose from Sub_I and Sub_II should be no greater than $\dim\{\text{null}(\mathbf{G}_1)\}$. That is,

$$d_\text{II} + d_\text{I} \leq (N_s^1 - N_e)^+. \quad (23)$$

III) *The message signal sent by S_1 does not spread within the null space of the eavesdropping channel. The message signals sent by S_1 and S_2 do not interfere with D_2 and D_1, respectively. That is, the precoding vector pairs in Sub_III should satisfy*

$$\mathbf{H}_{12}\mathbf{w} = \mathbf{0}, \quad (24a)$$
$$\mathbf{H}_{21}\mathbf{v} = \mathbf{0}, \quad (24b)$$
$$\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}. \quad (24c)$$

Substituting $\mathbf{v} = \mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{x}$ and $\mathbf{w} = \mathbf{\Gamma}(\mathbf{H}_{12})\mathbf{y}$ into (24c), we arrive at

$$\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{x} = \mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12})\mathbf{y} \neq \mathbf{0}. \quad (25)$$

Consider the decomposition

$$\text{GSVD}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}), \mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12}); N_e, \hat{N}_s^1, \hat{N}_s^2)$$
$$= (\hat{\mathbf{\Psi}}_1, \hat{\mathbf{\Psi}}_2, \hat{\mathbf{\Lambda}}_1, \hat{\mathbf{\Lambda}}_2, \hat{\mathbf{X}}, \hat{k}, \hat{r}, \hat{s}, \hat{p}),$$

where $\hat{N}_s^1 \triangleq (N_s^1 - N_d^2)^+$ and $\hat{N}_s^2 \triangleq (N_s^2 - N_d^1)^+$. Applying *Proposition 1*, we can obtain the number of linearly independent vectors $\mathbf{v}$ satisfying (25), i.e.,

$$\hat{d}_\text{III} \triangleq \hat{s} + \dim\{\text{null}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))\}.$$

Since $\text{null}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21})) = \text{null}(\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1))$, the basis of $\text{null}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))$ also spans the solution space of $\mathbf{v}$ in Sub_I. Thus,

$$d_\text{III} + d_\text{I} \leq \hat{d}_\text{III} = \hat{s} + (N_s^1 - N_e - N_d^2)^+, \quad (26)$$

IV) *The message signal sent by S_1 does not spread within the null space of the eavesdropping channel. The message signal sent by S_2 does not interfere with D_1, but the message*

TABLE I: The triplet (a, b, c) corresponding to the precoding vector pair from each subset and the number of linear independent precoding vector pairs that should be considered in each subset

subsets	(a,b,c)	maximum number of linear independent precoding vector pairs $(\mathbf{v}, \mathbf{w})$
Sub_{I}	$(1,0,0)$	$d_{\mathrm{I}} = (N_s^1 - N_e - N_d^2)^+$
Sub_{II}	$(1,0,1)$	$d_{\mathrm{II}} = \min\{N_d^2, (N_s^1 - N_e)^+\}$
Sub_{III}	$(1,1,0)$	$d_{\mathrm{III}} = (\min\{(N_s^1 - N_d^2)^+, N_e\} + \min\{(N_s^2 - N_d^1)^+, N_e\} - N_e)^+$
Sub_{IV}	$(1,1,1)$	$d_{\mathrm{IV}} = (\min\{N_s^1, N_e\} + \min\{(N_s^2 - N_d^1)^+, N_e\} - N_e)^+ - d_{\mathrm{III}}$
Sub_{V}	$(2,1,0)$	$d_{\mathrm{V}} = (\min\{(N_s^1 - N_d^2)^+, N_e\} + \min\{N_s^2, N_e\} - N_e)^+ - d_{\mathrm{III}}$
Sub_{VI}	$(2,1,1)$	$d_{\mathrm{VI}} = (\min\{N_s^1, N_e\} + \min\{N_s^2, N_e\} - N_e)^+ - (d_{\mathrm{III}} + d_{\mathrm{IV}} + d_{\mathrm{V}})$

signal sent by S_1 interferes with D_2. That is, the precoding vector pairs in Sub_{IV} should satisfy

$$\mathbf{H}_{12}\mathbf{w} = \mathbf{0}, \tag{27a}$$

$$\mathbf{H}_{21}\mathbf{v} \neq \mathbf{0}, \tag{27b}$$

$$\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}. \tag{27c}$$

Substituting $\mathbf{w} = \mathbf{\Gamma}(\mathbf{H}_{12})\mathbf{y}$ into (27c), we get

$$\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12})\mathbf{y} \neq \mathbf{0}. \tag{28}$$

Consider the decomposition

$$\text{GSVD}(\mathbf{G}_1, \mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12}); N_e, N_s^1, \hat{N}_s^2)$$
$$= (\bar{\mathbf{\Psi}}_1, \bar{\mathbf{\Psi}}_2, \bar{\mathbf{\Lambda}}_1, \bar{\mathbf{\Lambda}}_2, \bar{\mathbf{X}}, \bar{k}, \bar{r}, \bar{s}, \bar{p}).$$

Applying *Proposition 1* we can obtain the number of linearly independent vectors $\mathbf{v}$ satisfying (28), i.e.,

$$\hat{d}_{\mathrm{IV}} \triangleq \bar{s} + \dim\{\text{null}(\mathbf{G}_1)\}.$$

On combining (24a)-(24c) with (27a)-(27c), it holds that

$$Sub_{\mathrm{III}} \cup Sub_{\mathrm{IV}} = \{(\mathbf{v}, \mathbf{w}) | \mathbf{H}_{12}\mathbf{w} = \mathbf{0}, \mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}\}$$

In addition, the basis of $\text{null}(\mathbf{G}_1)$ also spans the solution space of $\mathbf{v}$ in $Sub_{\mathrm{I}} \cup Sub_{\mathrm{II}}$. Therefore,

$$d_{\mathrm{IV}} + d_{\mathrm{III}} + d_{\mathrm{II}} + d_{\mathrm{I}} \leq \hat{d}_{\mathrm{IV}} = \bar{s} + (N_s^1 - N_e)^+. \tag{29}$$

V) *The message signal sent by S_1 does not spread within the null space of the eavesdropping channel. The message signal sent by S_2 interferes with D_1, but the message signal sent by S_1 does not interfere with D_2.* That is, the precoding vector pairs in Sub_{V} should satisfy

$$\mathbf{H}_{12}\mathbf{w} \neq \mathbf{0}, \tag{30a}$$

$$\mathbf{H}_{21}\mathbf{v} = \mathbf{0}, \tag{30b}$$

$$\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}. \tag{30c}$$

Substituting $\mathbf{v} = \mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{x}$ into (30c), we obtain

$$\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{x} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}. \tag{31}$$

Consider the decomposition

$$\text{GSVD}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}), \mathbf{G}_2; N_e, \hat{N}_s^1, N_s^2)$$
$$= (\breve{\mathbf{\Psi}}_1, \breve{\mathbf{\Psi}}_2, \breve{\mathbf{\Lambda}}_1, \breve{\mathbf{\Lambda}}_2, \breve{\mathbf{X}}, \breve{k}, \breve{r}, \breve{s}, \breve{p}).$$

Applying *Proposition 1*, we can obtain the number of linearly independent vectors $\mathbf{v}$ satisfying (31), i.e.,

$$\hat{d}_{\mathrm{V}} \triangleq \breve{s} + \dim\{\text{null}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))\}.$$

On combining (24a)-(24c) with (30a)-(30c), it holds that

$$Sub_{\mathrm{III}} \cup Sub_{\mathrm{V}} = \{(\mathbf{v}, \mathbf{w}) | \mathbf{H}_{21}\mathbf{v} = \mathbf{0}, \mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}\}$$

In addition, the basis of $\text{null}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))$ also spans the solution space of $\mathbf{v}$ in Sub_{I}. Therefore,

$$d_{\mathrm{V}} + d_{\mathrm{III}} + d_{\mathrm{I}} \leq \hat{d}_{\mathrm{V}} = \breve{s} + (N_s^1 - N_e - N_d^2)^+. \tag{32}$$

VI) *The message signal sent by S_1 does not spread within the null space of the eavesdropping channel. The message signals sent by S_2 and S_1 interfere with D_1 and D_2, respectively.* That is, the precoding vector pairs in Sub_{VI} should satisfy

$$\mathbf{H}_{12}\mathbf{w} \neq \mathbf{0}, \tag{33a}$$

$$\mathbf{H}_{21}\mathbf{v} \neq \mathbf{0}, \tag{33b}$$

$$\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}. \tag{33c}$$

Consider the decomposition

$$\text{GSVD}(\mathbf{G}_1, \mathbf{G}_2; N_e, N_s^1, N_s^2) = (\tilde{\mathbf{\Psi}}_1, \tilde{\mathbf{\Psi}}_2, \tilde{\mathbf{\Lambda}}_1, \tilde{\mathbf{\Lambda}}_2, \tilde{\mathbf{X}}, \tilde{k}, \tilde{r}, \tilde{s}, \tilde{p}).$$

According to *Proposition 1*, we can obtain the number of linearly independent vectors $\mathbf{v}$ satisfying (33c), i.e.,

$$d_s \triangleq \tilde{s} + \dim\{\text{null}(\mathbf{G}_1)\}.$$

On combining (33a)-(33c) with (24a)-(24c), (27a)-(27c) and (30a)-(30c), it holds that $Sub_{\mathrm{III}} \cup Sub_{\mathrm{IV}} \cup Sub_{\mathrm{V}} \cup Sub_{\mathrm{VI}} = \{(\mathbf{v}, \mathbf{w}) | \mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}\}$. In addition, the basis of $\text{null}(\mathbf{G}_1)$ also spans the solution space of $\mathbf{v}$ in $Sub_{\mathrm{I}} \cup Sub_{\mathrm{II}}$. Thus,

$$d_{\mathrm{VI}} + d_{\mathrm{V}} + d_{\mathrm{IV}} + d_{\mathrm{III}} + d_{\mathrm{II}} + d_{\mathrm{I}} \leq d_s. \tag{34}$$

We should note that with all three variables smaller than the corresponding variables of other triplets, the precoding vector pair from Sub_{I} has the potential to achieve a greater S.D.o.F. than the others, and so it has the highest priority in the construction of $(\mathbf{V}, \mathbf{W})$. Similarly, the precoding vector pair from Sub_{IV} has lower priority than that one from $Sub_{\mathrm{I}} \cup Sub_{\mathrm{II}} \cup Sub_{\mathrm{III}}$; the precoding vector pair from Sub_{V} has lower priority than that one from $Sub_{\mathrm{I}} \cup Sub_{\mathrm{III}}$; and the precoding vector pair from Sub_{VI} has the lowest priority. Therefore, all the equalities in (20), (23), (26), (29), (32) and (34) hold true. As a conclusion, the number of linear independent precoding vector pairs that should be considered in each subset is given in Table I.

Correspondingly, in what follows, we give the formulas of $\mathbf{v}$ and $\mathbf{w}$ we consider in each subset. Combining the formula

of $\mathbf{v}$ in Sub_{I}, i.e., (19), and that one in $Sub_{\mathrm{I}} \cup Sub_{\mathrm{II}}$, i.e., (22), we obtain the one in Sub_{II}, i.e.,

$$\mathbf{v} = \mathbf{\Gamma}(\mathbf{G}_1)\mathbf{\Gamma}^\perp(\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1))\mathbf{z} + \mathbf{\Gamma}(\mathbf{G}_1)\mathbf{\Gamma}(\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1))\mathbf{y}.$$

with $\mathbf{z}$ being any nonzero vectors with appropriate length. Since we want linear independent precoding vectors, the beamforming direction already considered in the set with higher priority, e.g., Sub_{I}, should not be under consideration in other subsets. Thus, the formula of $\mathbf{v}$ in Sub_{II} is

$$\mathbf{v} = \mathbf{\Gamma}(\mathbf{G}_1)\mathbf{\Gamma}^\perp(\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1))\mathbf{z}. \tag{35}$$

Similarly, the formulas of $\mathbf{v}$ and $\mathbf{w}$ in Sub_{III} are, respectively,

$$\mathbf{v} = \hat{\mathbf{\Psi}}_{12}\hat{\mathbf{\Lambda}}_1^{-1}\mathbf{z}, \quad \mathbf{w} = \hat{\mathbf{\Psi}}_{22}\hat{\mathbf{\Lambda}}_2^{-1}\mathbf{z}. \tag{36}$$

The formulas of $\mathbf{v}$ and $\mathbf{w}$ in Sub_{IV} are, respectively,

$$\mathbf{v} = \bar{\mathbf{\Psi}}_{12}\bar{\mathbf{\Lambda}}_1^{-1}\mathbf{z}, \quad \mathbf{w} = \bar{\mathbf{\Psi}}_{22}\bar{\mathbf{\Lambda}}_2^{-1}\mathbf{z}. \tag{37}$$

The formulas of $\mathbf{v}$ and $\mathbf{w}$ in Sub_{V} are, respectively,

$$\mathbf{v} = \breve{\mathbf{\Psi}}_{12}\breve{\mathbf{\Lambda}}_1^{-1}\mathbf{z}, \quad \mathbf{w} = \breve{\mathbf{\Psi}}_{22}\breve{\mathbf{\Lambda}}_2^{-1}\mathbf{z}. \tag{38}$$

And the formulas of $\mathbf{v}$ and $\mathbf{w}$ in Sub_{VI} are, respectively,

$$\mathbf{v} = \tilde{\mathbf{\Psi}}_{12}\tilde{\mathbf{\Lambda}}_1^{-1}\mathbf{z}, \quad \mathbf{w} = \tilde{\mathbf{\Psi}}_{22}\tilde{\mathbf{\Lambda}}_2^{-1}\mathbf{z}. \tag{39}$$

We should note that since $\mathbf{H}_{21}$ is independent of the channels $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{H}_{12}$, for precoding vector pairs in (37) $\mathbf{H}_{21}\mathbf{v} \neq 0$ holds true with probability one. Similar argument also applies in the derivation of the formulas of $\mathbf{v}$ and $\mathbf{w}$ in Sub_{V} and Sub_{VI}.

B. Single-User points $SU1(\bar{d}_s^1, 0)$ and $SU2(0, \bar{d}_s^2)$

A single-user point corresponds to a scenario in which only one source-destination communicates. Let $\bar{d}_s^1$ and $\bar{d}_s^2$ denote the maximum achievable value of d_s^1 and d_s^2, respectively.

1) The single-user point $SU1(\bar{d}_s^1, 0)$: In this case, the pair S_2-D_2 does not communicate, but S_2 still transmits, acting as a cooperative jammer targeting at degrading the eavesdropping channel. In this case, the system model reduces to a wiretap channel with a cooperative jammer. Based on *Corollary 1* and *Corollary 2*, we see that our problem for maximizing d_s^1 is including as more precoding vector pairs as possible in $(\mathbf{V}, \mathbf{W})$. In Table I, we divide the set which satisfies $\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w}$ into six subsets. Due to the requirement in (17), it holds that more precoding vector pairs can be included in $(\mathbf{V}, \mathbf{W})$ by choosing precoding vector pairs from the subsets with smaller a. For example, $a = 1$ for Sub_{IV} while $a = 2$ for Sub_{VI}. We can select at most N_d^1 precoding vector pairs from Sub_{IV}, in which $a = 1$, while we can select only $\lfloor N_d^1/2 \rfloor$ precoding vector pairs from Sub_{VI}, in which $a = 2$. In addition, since the achieved S.D.o.F. is $d_s^1 = \mathrm{rank}\{\mathbf{H}_{11}\mathbf{V}\}$, a greater value of d_s^1 can be achieved with precoding vector pairs from Sub_{IV}. Therefore, in the construction of $(\mathbf{V}, \mathbf{W})$, the precoding vector pairs from the first four subsets have the same priority, and the precoding vector pairs from the last two subsets have the same priority. Moreover, a precoding vector pair from the first four subsets has higher priority than that one from the last two subsets. If $N_d^1 \leq d_{\mathrm{I}} + d_{\mathrm{II}} + d_{\mathrm{III}} + d_{\mathrm{IV}}$, we just select N_d^1 precoding vector pairs from $Sub_{\mathrm{I}} \cup Sub_{\mathrm{II}} \cup$ $Sub_{\mathrm{III}} \cup Sub_{\mathrm{IV}}$; otherwise, we first select all the precoding vector pairs in $Sub_{\mathrm{I}} \cup Sub_{\mathrm{II}} \cup Sub_{\mathrm{III}} \cup Sub_{\mathrm{IV}}$, and then we pick $\lfloor \frac{N_d^1 - (d_{\mathrm{I}} + d_{\mathrm{II}} + d_{\mathrm{III}} + d_{\mathrm{IV}})}{2} \rfloor$ precoding vector pairs from $Sub_{\mathrm{V}} \cup Sub_{\mathrm{VI}}$.

Example 1: Consider the case $(N_s^1, N_d^1, N_e) = (6, 3, 6)$, $(N_s^2, N_d^2) = (6, 6)$. Based on Table I, the maximum number of linear independent precoding vector pairs in each subset is $d_{\mathrm{I}} = 0$, $d_{\mathrm{II}} = 0$, $d_{\mathrm{III}} = 0$, $d_{\mathrm{IV}} = 3$, $d_{\mathrm{V}} = 0$, $d_{\mathrm{VI}} = 3$. Since $N_d^1 = d_{\mathrm{I}} + d_{\mathrm{II}} + d_{\mathrm{III}} + d_{\mathrm{IV}}$, we first select three precoding vector pairs in Sub_{IV}. We cannot pick any more precoding vector pairs without violating (17) since in that case the the remaining signal dimension at D_1 is $N_d^1 - d_{\mathrm{IV}} = 0$. Concluding, we can select a total of 3 precoding vector pairs, and based on *Corollary 2*, $\bar{d}_s^1 = 3$.

Example 2: Consider the case $(N_s^1, N_d^1, N_e) = (6, 5, 5)$, $(N_s^2, N_d^2) = (6, 4)$. Based on Table I we get that $d_{\mathrm{I}} = 0$, $d_{\mathrm{II}} = 1$, $d_{\mathrm{III}} = 0$, $d_{\mathrm{IV}} = 1$, $d_{\mathrm{V}} = 2$, $d_{\mathrm{VI}} = 2$. Since $N_d^1 > d_{\mathrm{I}} + d_{\mathrm{II}} + d_{\mathrm{III}} + d_{\mathrm{IV}}$, we first select all the precoding vector pairs in Sub_{II} and Sub_{IV}, i.e., $(\mathbf{v}_1, \mathbf{w}_1)$, $(\mathbf{v}_2, \mathbf{w}_2)$, with $\mathbf{H}_{12}\mathbf{w}_1 = 0$ and $\mathbf{H}_{12}\mathbf{w}_2 = 0$. From the remaining sets Sub_{V} and Sub_{VI}, we can at most pick one pair, i.e., $(\mathbf{v}_3, \mathbf{w}_3)$. For either Sub_{V} or Sub_{VI}, it holds that $\mathbf{H}_{12}\mathbf{w}_3 \neq 0$. Thus, for $\mathbf{V} = [\mathbf{v}_1 \ \mathbf{v}_2 \ \mathbf{v}_3]$ and $\mathbf{W} = [\mathbf{w}_1 \ \mathbf{w}_2 \ \mathbf{w}_3]$ it holds that $\dim\{\mathrm{span}(\mathbf{H}_{11}\mathbf{V})\} + \dim\{\mathrm{span}(\mathbf{H}_{12}\mathbf{W})\} = 3 + 1 = 4$. If we picked another pair, (17) would be violated. Concluding, we can select a total of 3 precoding vector pairs, and based on *Corollary 2*, $\bar{d}_s^1 = 3$.

Summarizing, the maximum achievable value $\bar{d}_s^1$, i.e.,

$$\bar{d}_s^1 = \min\{d_{a=1} + d_{a=2}^\star, N_d^1\}, \tag{40}$$

where $d_{a=1} = d_{\mathrm{I}} + d_{\mathrm{II}} + d_{\mathrm{III}} + d_{\mathrm{IV}}$, and

$$d_{a=2}^\star = \min\{d_{\mathrm{V}} + d_{\mathrm{VI}}, \lfloor (N_d^1 - d_{a=1})^+/2 \rfloor\}.$$

Remark 1: To gain more insight into $\bar{d}_s^1$, we give Table II which shows the dependence of $\bar{d}_s^1$ on the number of antennas.

2) The single-user point of $SU2(0, \bar{d}_s^2)$: In this case, the wiretap channel S_1-D_1-E does not work. For a point-to-point MIMO user, the maximum achievable degrees of freedom equals $\min\{N_s^2, N_d^2\}$. That is,

$$\bar{d}_s^2 = \min\{N_s^2, N_d^2\}. \tag{41}$$

C. Computation of the strict S.D.o.F. region boundary

The key idea for computing the strict S.D.o.F. boundary is to maximize the value of d_s^2 for a fixed value of d_s^1.

Assume that $\mathbf{V}$ consists of $\hat{d}_s^1$ columns, among which z columns come from a subset for which the message signal sent by S_1 interferes with D_2. Then, D_2 can at most see a $(N_d^2 - z)^+$-dimension interference-free subspace. Thus,

$$\hat{d}_s^2(z) \leq (N_d^2 - z)^+. \tag{42}$$

In addition, it holds that $\hat{d}_s^1 + \dim\{\mathrm{span}(\mathbf{H}_{12}\mathbf{W})\} \leq N_d^1$ due to (17). So,

$$\mathrm{rank}\{\mathbf{W}\} \leq (\max\{N_s^2, N_d^1\} - \hat{d}_s^1)^+. \tag{43}$$

TABLE II: Summary of the closed-form results on $\bar{d}_s^1$

Inequalities on the number of antennas at terminals	$\bar{d}_s^1$
$N_s^1 \geq N_e + N_d^1$	
$N_s^2 \geq N_e + N_d^1$	$\min\{N_s^1, N_d^1\}$
$2N_d^1 + N_e - N_s^2 \leq N_s^1 < N_e + N_d^1$	
$N_d^1 < N_s^2 < N_e + N_d^1$	
$N_d^1 + N_e - N_s^2 < N_s^1 < 2N_d^1 + N_e - N_s^2$	$N_s^1 + N_s^2 - (N_d^1 + N_e) + \min\{s, \lfloor \frac{2N_d^1 + N_e - N_s^1 - N_s^2}{2} \rfloor\}$
$N_d^1 < N_s^2 < N_e + N_d^1$	$s = \min\{N_d^1 + N_e - N_s^2, N_e\} + \min\{N_s^2, N_e\} - N_e$
$N_e < N_s^1 < N_e + N_d^1, N_s^2 \leq N_d^1$	$N_s^1 - N_e + \min\{s, \lfloor \frac{N_d^1 + N_e - N_s^1}{2} \rfloor\}, s = \min\{N_s^2, N_e\}$
$N_s^1 \leq N_d^1 + N_e - N_s^2, N_d^1 < N_s^2 < N_e + N_d^1$	$\min\{s, \lfloor \frac{N_d^1}{2} \rfloor\}$
$N_s^1 \leq N_e, N_s^2 \leq N_d^1$	$s = \min\{N_s^1, N_e\} + \min\{N_s^2, N_e\} - \min\{N_s^1 + N_s^2, N_e\}$

Combining (41), (42) and (43), we get the maximum achievable value of d_s^2, i.e.,

$$\hat{d}_s^2(z) = \min\{N_s^2, (\max\{N_s^2, N_d^1\} - \hat{d}_s^1)^+, (N_d^2 - z)^+\}. \quad (44)$$

Thus, in order to maximize the value of d_s^2, we only need to minimize the value of z.

According to Table I, the minimum value of z without the constraint $d_s^1 = \hat{d}_s^1$ equals $(\hat{d}_s^1 - (d_V + d_I + d_{III}))^+$. Due to the constraint $d_s^1 = \hat{d}_s^1$ and the fact that $a = 2$ in Sub_V, we have limitations on the number of pairs that can be selected from Sub_V. For example, consider the case $d_I + d_{III} = 2$, $d_V = 2$, $N_d^1 = 3$ and $\hat{d}_s^1 = 3$. The minimum value of z without the constraint $d_s^1 = \hat{d}_s^1 = 3$ equals 0, in which case we need at least choose one pair from Sub_V. Noting that (17) should be satisfied for $(\mathbf{V}, \mathbf{W}) \in \hat{\mathcal{I}}$ and $a = 2$ in Sub_V, if we have picked one pair from Sub_V, we can then at most pick one more pair from the first four subsets. Thus, the maximum achievable value of d_s^1 equals 2, which violates the constraint $d_s^1 = 3$. Due to the constraint $d_s^1 = 3$ and the fact that $a = 2$ in Sub_V, we cannot select any pairs from Sub_V, and so the minimum value of z equals to 1.

Let x and y denote the number of columns which come from the first four subsets and the last two subsets, respectively. The maximum allowable value of y under the constraint of $d_s^1 = \hat{d}_s^1$ is

$$y_{\max} \triangleq \max_{x,y} \quad y$$
$$\text{s.t.} \quad x + y = \hat{d}_s^1, \quad (45a)$$
$$x + 2y \leq N_d^1, \quad (45b)$$
$$0 \leq x \leq d_I + d_{II} + d_{III} + d_{IV}, \quad (45c)$$
$$0 \leq y \leq d_V + d_{VI}. \quad (45d)$$

Substituting $x = \hat{d}_s^1 - y$ into (45b), we arrive at $y \leq N_d^1 - \hat{d}_s^1$, which combined with (45c) and (45d) gives

$$y_{\max} = \min\{N_d^1 - \hat{d}_s^1, d_V + d_{VI}, \hat{d}_s^1\}. \quad (46)$$

Thus, we can select at most $\min\{y_{\max}, d_V\}$ precoding vector pairs from Sub_V. Therefore, the minimum value of z is,

$$z_{\min}(\hat{d}_s^1) = (\hat{d}_s^1 - (\min\{y_{\max}, d_V\} + d_I + d_{III}))^+. \quad (47)$$

Substituting (47) into (44), we obtain the maximum value of d_s^2, i.e.,

$$\hat{d}_s^2 = \min\{N_s^2, (\max\{N_s^2, N_d^1\} - \hat{d}_s^1)^+, (N_d^2 - z_{\min}(\hat{d}_s^1))^+\}. \quad (48)$$

Remark 2: For any given values of d_s^1, we can derive a maximum achievable value of d_s^2 based on (48). Finally, the strict S.D.o.F. region boundary can be computed based on the following iteration:
1) Initialize $\hat{d}_s^1 = \bar{d}_s^1$;
2) Compute $\hat{d}_s^2$ with (48);
3) Compare $\hat{d}_s^2$ with $\bar{d}_s^2$. If $\hat{d}_s^2 < \bar{d}_s^2$, let $\hat{d}_s^1 = \hat{d}_s^1 - 1$ and go to 2); otherwise, stop and output all the pairs $(\hat{d}_s^1, \hat{d}_s^2)$.

Example 3: Let us revisit *Example 2*, for which we obtained $\bar{d}_s^1 = 3$ and $\bar{d}_s^2 = 4$, respectively. Initialize $\hat{d}_s^1$ with $\bar{d}_s^1 = 3$. Substituting $\hat{d}_s^1 = 3$ into (48), we obtain $\hat{d}_s^2 = 3$. Since $\hat{d}_s^2 < \bar{d}_s^2$, we continue the iteration. Letting $\hat{d}_s^1 = 2$ and substituting it into (48), we obtain $\hat{d}_s^2 = 4$, which equals $\bar{d}_s^2$. So, we stop the iteration and output all the S.D.o.F. pairs on the strict S.D.o.F. region boundary, i.e., $(\hat{d}_s^1, \hat{d}_s^2) = (3, 3)$ and $(\hat{d}_s^1, \hat{d}_s^2) = (2, 4)$.

D. Ending points of strict S.D.o.F. region boundary $E1(\bar{d}_s^1, \underline{d}_s^2)$ and $E2(\underline{d}_s^1, \bar{d}_s^2)$

As shown in Fig. 2, $E1$ and $E2$ denote the ending points of the strict S.D.o.F. region boundary. In particular, $\underline{d}_s^2$ denotes the maximum achievable value of d_s^2 under the constraint $d_s^1 = \bar{d}_s^1$, and $\underline{d}_s^1$ denotes the maximum achievable value of d_s^1 under the constraint $d_s^2 = \bar{d}_s^2$.

1) The ending point $E1(\bar{d}_s^1, \underline{d}_s^2)$. According to (40), we obtain $\bar{d}_s^1$ which denotes the maximum achievable value of d_s^1. Substituting $\hat{d}_s^1 = \bar{d}_s^1$ into (46)-(48), we arrive at

$$\underline{d}_s^2 = \min\{N_s^2, (\max\{N_s^2, N_d^1\} - \bar{d}_s^1)^+, (N_d^2 - z_{\min}(\bar{d}_s^1))^+\}. \quad (49)$$

2) The ending point $E2(\underline{d}_s^1, \bar{d}_s^2)$. According to the previous analysis on the single-user point of $SU2(0, \bar{d}_s^2)$, we obtain $\bar{d}_s^2 = \min\{N_s^2, N_d^2\}$, which, combined with (44), gives

$$\min\{N_s^2, N_d^2\} \leq \max\{N_s^2, N_d^1\} - \underline{d}_s^1, \quad (50a)$$
$$\min\{N_s^2, N_d^2\} \leq N_d^2 - z. \quad (50b)$$

In the following, we consider two distinct cases.

(i) For the case of $N_s^2 > N_d^2$, (50a) becomes

$$\underline{d}_s^1 \leq \max\{N_s^2, N_d^2\} - N_d^2. \tag{51}$$

Besides, (50b) indicates that $z = 0$, and thus all of the signal steams sent by S_1 should not interfere with D_2. That is, Sub_{II}, Sub_{IV} and Sub_{VI} are not under consideration. Applying (40), we obtain

$$\underline{d}_s^1 \leq \min\{d_{\text{I}} + d_{\text{III}} + \beta^\star, N_d^1\}, \tag{52}$$

where $\beta^\star = \min\{d_{\text{V}}, \lfloor (N_d^1 - d_{\text{I}} - d_{\text{III}})^+/2 \rfloor\}$. Combining (51) and (52), we arrive at

$$\underline{d}_s^1 = \min\{d_{\text{I}} + d_{\text{III}} + \beta^\star, \max\{N_s^2, N_d^1\} - N_d^2, N_d^1\}. \tag{53}$$

(ii) For the case of $N_s^2 \leq N_d^2$, (50a) becomes

$$\underline{d}_s^1 \leq \max\{N_s^2, N_d^1\} - N_s^2, \tag{54}$$

which indicates that $\underline{d}_s^1 = 0$ when $N_s^2 \geq N_d^1$. So, in the following, we only consider the case of $N_s^2 < N_d^1$, where it holds that $d_{\text{III}} = d_{\text{IV}} = 0$. In addition, (50b) indicates that $z \leq N_d^2 - N_s^2$. Therefore, $\xi = \min\{d_{\text{VI}}, (N_d^2 - N_s^2 - d_{\text{II}})^+\} + d_{\text{V}}$, where ξ denotes the maximum number of precoding vector pairs that can be chosen from Sub_{V} and Sub_{VI}. Applying (40), we get

$$\underline{d}_s^1 \leq \min\{d_{\text{I}} + \hat{d}_{\text{II}} + \xi^\star, N_d^1\}, \tag{55}$$

where $\hat{d}_{\text{II}} = \min\{N_d^2 - N_s^2, d_{\text{II}}\}$, and

$$\xi^\star = \min\{\xi, \lfloor (N_d^1 - d_{\text{I}} - \hat{d}_{\text{II}})^+/2 \rfloor\}.$$

Combining (54) and (55), we arrive at

$$\underline{d}_s^1 = \min\{d_{\text{I}} + \hat{d}_{\text{II}} + \xi^\star, \max\{N_s^2, N_d^1\} - N_s^2\}. \tag{57}$$

We should note that this expression also applies to the case of $N_s^2 \geq N_d^1$, where $\underline{d}_s^1 = 0$.

Summarizing the above two cases, we arrive at

$$\underline{d}_s^1 = \begin{cases} \min\{d_{\text{I}} + d_{\text{III}} + \beta^\star, \eta - N_d^2, N_d^1\}, & \text{if } N_s^2 > N_d^2 \\ \min\{d_{\text{I}} + \hat{d}_{\text{II}} + \xi^\star, \eta - N_s^2\}, & \text{if } N_s^2 \leq N_d^2 \end{cases} \tag{58}$$

where $\eta = \max\{N_s^2, N_d^1\}$.

VI. CONSTRUCTION OF PRECODING MATRICES WHICH ACHIEVE THE POINT ON THE S.D.o.F. REGION BOUNDARY

According to Section V. C, by carefully choosing $(\mathbf{v}, \mathbf{w})$ we are able to construct precoding matrix pairs $(\mathbf{V}, \mathbf{W})$ which achieve the S.D.o.F. pairs on the S.D.o.F. region boundary. In particular, by selecting $u = \min\{\hat{d}_s^1, \min\{y_{\max}, d_{\text{V}}\} + d_{\text{I}} + d_{\text{III}}\}$ pairs from $Sub_{\text{o}} = Sub_{\text{I}} \cup Sub_{\text{III}} \cup Sub_{\text{V}}$ and $t = \hat{d}_s^1 - u$ pairs from $Sub_{\text{e}} = Sub_{\text{II}} \cup Sub_{\text{IV}} \cup Sub_{\text{VI}}$, subject to the number of pairs selected from $Sub_{\text{V}} \cup Sub_{\text{VI}}$ being no greater than $y_{\max}$, we have completed the construction of precoding matrices $(\mathbf{V}, \mathbf{W}(:, 1 : K_v)) \in \hat{\mathcal{I}}$. This construction satisfies $d_s^1 = \hat{d}_s^1$ and also leaves a maximum dimension, i.e., $d_s^2 = \hat{d}_s^2$ (see eq. (48)), interference-free subspace for D_2. Further, if $\hat{d}_s^2 \leq \text{rank}(\mathbf{W}(:, 1 : K_v))$, S_2 does not need to add any beamforming vectors, and the S.D.o.F. of $\hat{d}_s^2$ is achieved. In this case, K_w equals the number of nonzero columns of $\mathbf{W}(:, 1 : K_v)$. If $\hat{d}_s^2 > \text{rank}(\mathbf{W}(:, 1 : K_v))$, S_2 can add $\breve{d}_s^2 = \hat{d}_s^2 - \text{rank}(\mathbf{W}(:, 1 : K_v))$ columns to its

---

TABLE III: An algorithm for constructing $(\mathbf{V}, \mathbf{W})$ which achieve $(\hat{d}_s^1, \hat{d}_s^2)$ on the S.D.o.F. region boundary

1. Initialize $u = \min\{\hat{d}_s^1, \min\{y_{\max}, d_{\text{V}}\} + d_{\text{I}} + d_{\text{III}}\}$, $t = \hat{d}_s^1 - u$;

2. $(\mathbf{V}_{\text{o}}, \mathbf{W}_{\text{o}}) \leftarrow$ select u precoding vector pairs from Sub_{o};
3. $(\mathbf{V}_{\text{e}}, \mathbf{W}_{\text{e}}) \leftarrow$ select t precoding vector pairs from Sub_{e};
4. $\mathbf{V} \leftarrow [\mathbf{V}_{\text{o}} \ \mathbf{V}_{\text{e}}]$;
5. $\mathbf{W}_1 \leftarrow [\mathbf{W}_{\text{o}} \ \mathbf{W}_{\text{e}}]$;

6. Let $\breve{d}_s^2 = \hat{d}_s^2 - \text{rank}(\mathbf{W}_1)$;
7. **if** $\breve{d}_s^2 > 0$
8.   Let $\tilde{d}_s^2 = \min\{\breve{d}_s^2, (N_s^2 - N_d^1)^+\}$;
9. $\mathbf{W}_2 \leftarrow \mathbf{A}(:, 1 : \tilde{d}_s^2)$, where $\mathbf{A} = \mathbf{\Gamma}(\mathbf{H}_{12})$;
10.   Do the singular value decomposition (SVD) $\mathbf{H}_{22} = \mathbf{U}\mathbf{S}\mathbf{R}^H$;
11. $\mathbf{W} \leftarrow [\mathbf{W}_1 \ \mathbf{W}_2 \ \mathbf{R}(:, 1 : \breve{d}_s^2 - \tilde{d}_s^2)]$;
12. **else**
13. $\mathbf{W} \leftarrow \mathbf{W}_1$;
14. **end**

15. **Output:** $(\mathbf{V}, \mathbf{W})$.

---

precoding matrix without violating any constraints of $\hat{\mathcal{I}}$ and also achieves an S.D.o.F. of $\hat{d}_s^2$. In particular, by adding the first $\tilde{d}_s^2 = \min\{\breve{d}_s^2, (N_s^2 - N_d^1)^+\}$ columns of $\mathbf{\Gamma}(\mathbf{H}_{12})$ and the first $\breve{d}_s^2 - \tilde{d}_s^2$ columns of $\mathbf{R}$ as the other beamforming vectors at S_2, we complete the construction of the precoding matrices $(\mathbf{V}, \mathbf{W})$. In this case $K_w = \hat{d}_s^2$. Here $\mathbf{R}$ is obtained with the singular value decomposition (SVD) $\mathbf{H}_{22} = \mathbf{U}\mathbf{S}\mathbf{R}^H$. By this SVD the channel $\mathbf{H}_{22}$ is decomposed into several parallel sub-channels, and the first $\breve{d}_s^2 - \tilde{d}_s^2$ columns of $\mathbf{R}$ correspond the ones which are of better channel quality than the others.

Example 4: Let us revisit *Example 3*, in which we obtained an S.D.o.F. pair $(\hat{d}_s^1, \hat{d}_s^2) = (2, 4)$ on the strict S.D.o.F. region boundary. According to Section V. C, at this boundary point, $y_{\max} = 2$ and $z_{\min} = 0$. Since $u = 2$, $d_{\text{I}} = d_{\text{III}} = 0$ and $d_{\text{V}} = 2$, we first select two precoding vector pairs in Sub_{V}, i.e., $(\mathbf{v}_1, \mathbf{w}_1)$ and $(\mathbf{v}_2, \mathbf{w}_2)$, with $\mathbf{H}_{21}\mathbf{v}_1 = 0$, $\mathbf{H}_{21}\mathbf{v}_2 = 0$, $\mathbf{H}_{12}\mathbf{w}_1 \neq 0$ and $\mathbf{H}_{12}\mathbf{w}_2 \neq 0$. From the remaining sets we do not pick any pairs since $t = 0$. So far, we have finished the construction of $\mathbf{V}$ and $\mathbf{W}(:, 1 : K_v)$, i.e., $[\mathbf{v}_1 \ \mathbf{v}_2]$ and $[\mathbf{w}_1 \ \mathbf{w}_2]$. Since $\breve{d}_s^2 = \hat{d}_s^2 - \text{rank}(\mathbf{W}(:, 1 : K_v)) = 2 > 0$, we further add $\tilde{d}_s^2 = \min\{\breve{d}_s^2, (N_s^2 - N_d^1)^+\} = 1$ column of $\mathbf{\Gamma}(\mathbf{H}_{12})$, i.e., $\mathbf{w}_3$, with $\mathbf{H}_{12}\mathbf{w}_3 = 0$, and $\breve{d}_s^2 - \tilde{d}_s^2 = 1$ column of $\mathbf{R}$, i.e., $\mathbf{w}_4$, with $\mathbf{H}_{22}\mathbf{w}_4 \neq 0$, as the other beamforming vectors at S_2. Since $\mathbf{H}_{11}\mathbf{v}_i \neq 0$, $\mathbf{H}_{22}\mathbf{w}_i \neq 0$ and $\mathbf{H}_{12}\mathbf{w}_4 \neq 0$ hold true with probability one, for $\mathbf{V} = [\mathbf{v}_1 \ \mathbf{v}_2]$ and $\mathbf{W} = [\mathbf{w}_1 \ \mathbf{w}_2 \ \mathbf{w}_3 \ \mathbf{w}_4]$ it holds that $\dim\{\text{span}(\mathbf{H}_{11}\mathbf{V})\} + \dim\{\text{span}(\mathbf{H}_{12}\mathbf{W})\} = 2 + 3 = 5$ and $\dim\{\text{span}(\mathbf{H}_{22}\mathbf{W})\} + \dim\{\text{span}(\mathbf{H}_{21}\mathbf{V})\} = 4 + 0 = 4$. Therefore, the S.D.o.F. pair $(\hat{d}_s^1, \hat{d}_s^2) = (2, 4)$ is achieved.

Concluding, an algorithm for constructing $(\mathbf{V}, \mathbf{W})$ is given in TABLE III. Note that the formulas of $\mathbf{v}_i$ and $\mathbf{w}_i$ in Sub_i, $i = \text{I}, \text{II}, \cdots, \text{VI}$, are given in (19), (35), (36), (37), (38) and (39), respectively.

Remark 3: In light of (12a) and (12b) derived in *Proposition 2*, whenever we find a solution $(\mathbf{V}, \mathbf{W})$ achieving the S.D.o.F. pair $(\hat{d}_s^1, \hat{d}_s^2)$ on the S.D.o.F. region boundary, we actually find the solution spaces $\text{span}(\mathbf{V})$ and $\text{span}(\mathbf{W})$, i.e., the precoding matrices $(\mathbf{V}\mathbf{A}, \mathbf{W}\mathbf{B})$ also achieve the S.D.o.F. pair $(\hat{d}_s^1, \hat{d}_s^2)$ on the S.D.o.F. region boundary as long as $\mathbf{A}$ and $\mathbf{B}$ are invertible.
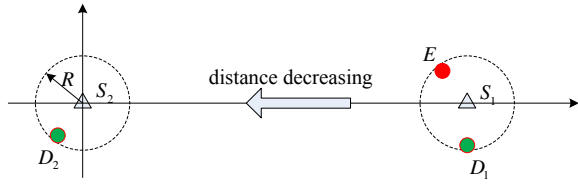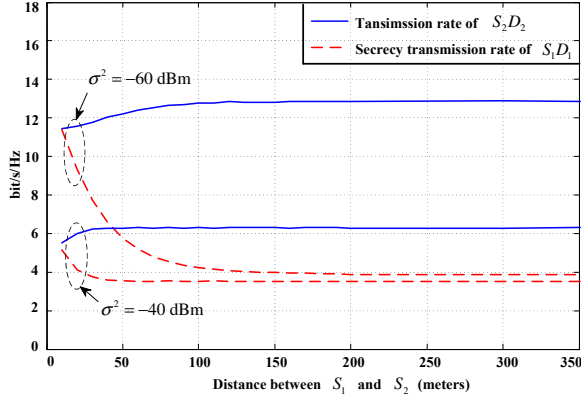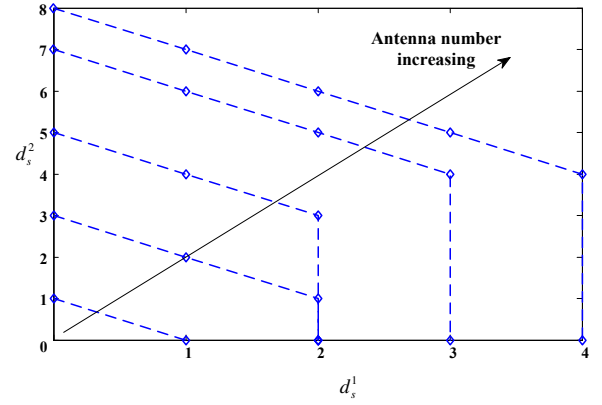
Fig. 3: Model used for numerical experiments

Fig. 4: Achievable rates versus S_1-S_2 distance

Fig. 5: Achievable secrecy degrees of freedom region with an increasing number of antennas at S_2-D_2

Fig. 6: Achievable secrecy rate of S_1-D_1 versus the uncertainty of the eavesdropper's channels α.

VII. NUMERICAL RESULTS

In this section, we give numerical results to validate our theoretical findings. For simplicity, we consider a simple semi-symmetric system model, as illustrated in Fig. 3. In particular, the antenna numbers $N_s^1 = N_d^1 = N_e \triangleq N_1$, and $N_s^2 = N_d^2 \triangleq N_2$. We assume that D_i or E is uniformly distributed on a ring of radius $1 \leq R \leq 10$ (unit: meters) and center located at S_i. The source-destination distances or the source-eavesdropper distance are no greater than the source-source distance. To highlight the effects of distances, the channel between any transmit-receiver antenna pair is modeled by a simple line-of-sight channel model including the path loss effect and a random phase, i.e., $h_{12} = d_{12}^{-c/2} e^{j\theta}$ where d_{12} denotes the distance between the S_2 and D_1, $c = 3.5$ is the path loss exponent, θ is the random phase uniformly distributed within $[0, 2\pi)$. The distances between transmit or receiver antennas at each terminal are assumed to be much smaller than the source-destination distance or the source-eavesdropper distance, so the path losses of different transmit-receiver antenna pairs from the same transmit-receiver link are approximately the same. S_2 is located at a fixed two-dimensional coordinates (0,0) (unit: meters), while S_1 moves from (350,0) to (10,0). The transmitting power of each source is $P = 0$dBm. Results are averaged over one hundred thousand independent channel trials.

Fig. 4 illustrates the achievable secrecy transmission rate of the user S_1-D_1, and also the achievable transmission rate of the user S_2-D_2 for $N_1 = 4$ and $N_2 = 2$. The noise power $\sigma^2 = -60$dBm and $\sigma^2 = -40$dBm are considered, respectively. According to (48), we see that with our proposed cooperative transmission scheme, the S.D.o.F. pair (1,1) can be achieved. We compute the precoding vectors $\mathbf{v}$ and $\mathbf{w}$ according to TABLE III, and compute the achievable transmission rate of each user according to (7) and (8), respectively. It
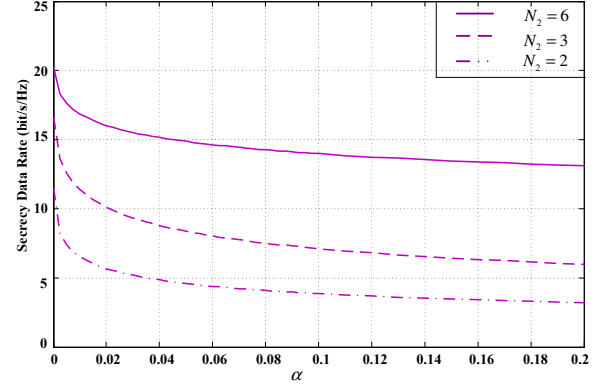
shows that the achievable secrecy transmission rate of S_1-D_1 increases monotonically as S_1 moves close to S_2. In contrast, the achievable transmission rate of S_2-D_2 decreases with the decreasing of the source-source distance. As compared with the decrease in the transmission rate of S_2-D_2, the increase in the secrecy transmission rate of S_1-D_1 is drastic. Therefore, the network performance benefits when the two users get closer.

Fig. 5 illustrates the achievable secrecy degrees of freedom region versus different values of N_2. Here, we set $N_1 = 4$ and let N_2 vary from 1 to 8. We compute the achievable secrecy degrees of freedom region according to (48). As expected, the secrecy degrees of freedom region expands with an increasing N_2. Note that previous work [36] shows that for the classic wiretap channel with no cooperative helpers the condition to achieve a nonzero S.D.o.F. is $N_s^1 \geq N_e + 1$. Here although $N_s^1 = N_e$, by exploiting the co-channel interference an S.D.o.F. of N_s^1 can be achieved.

In practice, while one may have a good estimate of the position of the eavesdropper, an estimate of the phase of the eavesdropper's channels is more difficult to obtain. Since the proposed precoding matrix design highly depends on the eavesdropper's channels, we next examine the secrecy rate performance degradation in the presence of imperfect channel estimate. In Fig. 6, we plot the achievable secrecy rate with imperfect CSI of the eavesdropper's channels. Here, we set $N_1 = 4$ and let N_2 vary from 2 to 6. S_1 and S_2 are located at (10,0) and (0,0), respectively. The noise power $\sigma^2 = -60$dBm.

The channel from S_i ($i = 1, 2$) to E is

$$\mathbf{G}_i = d_{ei}^{-c/2} \left(\frac{1}{\sqrt{1+\alpha}} \bar{\mathbf{G}}_i + \sqrt{\frac{\alpha}{1+\alpha}} \Delta \bar{\mathbf{G}}_i \right), \qquad (59)$$

where α denotes the channel uncertainty. $\bar{\mathbf{G}}_i$ represents the estimated channel part at S_i. The entries of $\bar{\mathbf{G}}_i$ are $e^{j\theta}$ with θ be a random phase uniformly distributed within $[0, 2\pi)$. $\Delta \bar{\mathbf{G}}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ represents the Gaussian error channel matrices. d_{ei} denotes the distance from S_i. According to (48), we see that the S.D.o.F. pairs (1,1), (2,1) and (3,3) can be achieved for the case of $N_2 = 2$, $N_2 = 3$ and $N_2 = 6$, respectively. For these S.D.o.F. pairs, we construct the precoding matrices $\mathbf{V}$ and $\mathbf{W}$ according to TABLE III, subject to power being equally allocated between different signal streams. The achievable secrecy transmission rate is computed according to (7). It can be observed that the achievable secrecy rate drops with the increase of channel uncertainties when the channel uncertainty α is small. Fortunately, when the number of antennas N_2 increases, this secrecy rate performance degradation is smaller. On the other hand, on comparing the secrecy transmission rate of S_1-D_1 for the case $N_2 = 2$ with that in Fig. 4, one can see that the secrecy rate achieved for the case where $\alpha = 0.1$ and S_1-S_2 distance of 10 meters, is almost equal to the secrecy rate achieved for the case where $\alpha = 0$ and S_1-S_2 distance of 150 meters. This suggests that in wiretap interference networks, the secrecy rate degradation due to CSI estimation error can be counteracted by bringing the two users closer together.

VIII. CONCLUSION

We have examined the maximum achievable secrecy degrees of freedoms (S.D.o.F.) region of a MIMO two-user wiretap interference channel, where one user requires confidential connection against an external passive eavesdropper, while the other uses a public connection. We have addressed analytically the S.D.o.F. pair maximization (component-wise). Specifically, we have proposed a cooperative secrecy transmission scheme and proven that its feasible set is sufficient to achieve all the points on the S.D.o.F. region boundary. For the proposed cooperative secrecy transmission scheme, we have obtained analytically the maximum achievable S.D.o.F. region boundary points. We have also constructed the precoding matrices which achieve the S.D.o.F. region boundary. Our results revealed the connection between the maximum achievable S.D.o.F. region and the number of antennas, thus shedding light on how the secrecy rate region behaves for different number of antennas. Numerical results show that the network performance benefits when the two users get closer. This is interesting. It tells us that in wiretap interference networks, the secrecy rate degradation due to CSI estimation error can be counteracted by bringing the two users closer together.

APPENDIX A
PROOF OF *Proposition 1*

In what follows, we prove that $\mathbf{Av} = \mathbf{Bw}$ holds true if and only if $\mathbf{v}$ and $\mathbf{w}$ are given in (4a) and (4b), with $\mathbf{y}_s$, $\mathbf{y}_{s1}$, $\mathbf{y}_{s2}$, $\mathbf{y}_1$ and $\mathbf{y}_2$ being any vectors with appropriate length. With this result, the first conclusion in *Proposition 1* is a

natural extension. According to the GSVD decomposition, $\mathbf{A}\mathbf{\Psi}_{12}\mathbf{\Lambda}_1^{-1} = \mathbf{B}\mathbf{\Psi}_{22}\mathbf{\Lambda}_2^{-1} = \mathbf{X}_2$. Thus, $\mathbf{Av} = \mathbf{Bw}$ holds true if $\mathbf{v}$ and $\mathbf{w}$ are given by (4a) and (4b), respectively. Next, we prove by contradiction that $\mathbf{Av} = \mathbf{Bw}$ holds true only if $\mathbf{v} \in \mathrm{span}(\mathbf{\Phi}_1)$; the argument for $\mathbf{w}$ is similar. Assume that there exists a nonzero vector $\bar{\mathbf{v}} \notin \mathrm{span}(\mathbf{\Phi}_1)$ satisfying $\mathbf{A}\bar{\mathbf{v}} = \mathbf{Bw}$. Then, $\mathbf{A}\bar{\mathbf{v}} \notin \mathrm{span}(\mathbf{A}\mathbf{\Phi}_1)$; otherwise, it holds that $\mathbf{A}\bar{\mathbf{v}} = \mathbf{A}\mathbf{\Phi}_1\mathbf{x}$ which implies $\bar{\mathbf{v}} - \mathbf{\Phi}_1\mathbf{x} = \mathbf{\Gamma}(\mathbf{A})\mathbf{y}_1$, and so $\bar{\mathbf{v}} \in \mathrm{span}(\mathbf{\Phi}_1)$ which contradicts with the assumption. However, $\mathbf{A}\bar{\mathbf{v}} \in \mathrm{span}(\mathbf{X}_2)$ due to $\mathbf{A}\bar{\mathbf{v}} = \mathbf{Bw}$. In addition, by the GSVD, $\mathrm{span}(\mathbf{X}_2) = \mathrm{span}(\mathbf{A}\mathbf{\Phi}_1)$. Thus, $\mathbf{A}\bar{\mathbf{v}} \in \mathrm{span}(\mathbf{A}\mathbf{\Phi}_1)$ and so $\mathbf{A}\bar{\mathbf{v}} \notin \mathrm{span}(\mathbf{A}\mathbf{\Phi}_1)$ is contradicted. This completes the proof of the first conclusion in *Proposition 1*.

According to the GSVD, $\mathbf{A}\mathbf{\Psi}_{13} = \mathbf{0}$. Thus, $\mathrm{span}(\mathbf{\Psi}_{13}) \subset \mathrm{span}(\mathbf{\Gamma}(\mathbf{A}))$. In addition, $\mathrm{rank}(\mathbf{\Psi}_{13}) = M - r - s = M - \min\{M, N\} = (M - N)^+$, which indicates that the linear independent vectors in $\mathrm{span}(\mathbf{\Psi}_{13})$ is the same as that in $\mathrm{span}(\mathbf{\Gamma}(\mathbf{A}))$. So, $\mathrm{span}(\mathbf{\Psi}_{13}) = \mathrm{span}(\mathbf{\Gamma}(\mathbf{A}))$. Since $\mathbf{\Psi}_1$ is an unitary matrix, it holds that $\mathrm{span}(\mathbf{\Psi}_{12}) \cap \mathrm{span}(\mathbf{\Psi}_{13}) = \mathbf{0}$. Therefore, $\mathrm{span}(\mathbf{\Psi}_{12}) \cap \mathrm{span}(\mathbf{\Gamma}(\mathbf{A})) = \mathbf{0}$, which, combined with (4a), indicates that the number of linearly independent vectors $\mathbf{v}$ satisfying $\mathbf{Av} = \mathbf{Bw} \neq \mathbf{0}$ is $s + \dim\{\mathrm{null}(\mathbf{A})\}$. This completes the proof.

APPENDIX B
PROOF OF *Proposition 2*

Given an arbitrary point $(\mathbf{V}, \mathbf{W})$, with $\mathrm{tr}\{\mathbf{Q}_v\} = P$ and $\mathrm{tr}\{\mathbf{Q}_w\} = P$. We can respectively rewrite $\mathbf{Q}_v$ and $\mathbf{Q}_w$ as $\mathbf{Q}_v = P\bar{\mathbf{Q}}_v$ and $\mathbf{Q}_w = P\bar{\mathbf{Q}}_w$, with $\mathrm{tr}\{\bar{\mathbf{Q}}_v\} = \mathrm{tr}\{\bar{\mathbf{Q}}_w\} = 1$. Correspondingly, (9a) can be rewritten as

$$R_d^1 = \log|\mathbf{I} + (\mathbf{I} + P\mathbf{H}_{12}\bar{\mathbf{Q}}_w\mathbf{H}_{12}^H)^{-1}\mathbf{H}_{11}\bar{\mathbf{Q}}_v\mathbf{H}_{11}^H P|. \quad (60)$$

Let $\mathbf{\Theta}_2 = \mathbf{H}_{11}\bar{\mathbf{Q}}_v\mathbf{H}_{11}^H$. Denoting $\mathbf{H}_{12}\bar{\mathbf{Q}}_w\mathbf{H}_{12}^H = [\mathbf{U}_1 \ \mathbf{U}_0] \begin{bmatrix} \mathbf{\Sigma}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{U}_1^H \\ \mathbf{U}_0^H \end{bmatrix}$ as the singular value decomposition (SVD), and substituting it into (60), we obtain

$$R_d^1 = \log|\mathbf{I} + \mathbf{U}_1(\mathbf{I} + P\mathbf{\Sigma}_1)^{-1}\mathbf{U}_1^H \mathbf{\Theta}_2 P + \mathbf{U}_0\mathbf{U}_0^H\mathbf{\Theta}_2 P|$$
$$= \log|\mathbf{I} + \mathbf{U}_1(\frac{\mathbf{I}}{P} + \mathbf{\Sigma}_1)^{-1}\mathbf{U}_1^H\mathbf{\Theta}_2 + \mathbf{U}_0\mathbf{U}_0^H\mathbf{\Theta}_2 P|.$$

Therefore,

$$\lim_{P \to \infty} R_d^1/\log(P)$$
$$= \lim_{P \to \infty} \frac{\log|\mathbf{I} + \mathbf{U}_1(\mathbf{\Sigma}_1)^{-1}\mathbf{U}_1^H\mathbf{\Theta}_2 + \mathbf{U}_0\mathbf{U}_0^H\mathbf{\Theta}_2 P|}{\log(P)}$$
$$= \lim_{P \to \infty} \frac{\log|\mathbf{I} + (\frac{1}{P}\mathbf{U}_1(\mathbf{\Sigma}_1)^{-1}\mathbf{U}_1^H + \mathbf{U}_0\mathbf{U}_0^H)\mathbf{\Theta}_2 P|}{\log(P)}$$
$$= \lim_{P \to \infty} \frac{\log|\mathbf{I} + \mathbf{U}_0\mathbf{U}_0^H\mathbf{H}_{11}\mathbf{V}\mathbf{V}^H\mathbf{H}_{11}^H|}{\log(P)}$$
$$= \mathrm{rank}\{\mathbf{U}_0\mathbf{U}_0^H\mathbf{H}_{11}\mathbf{V}\mathbf{V}^H\mathbf{H}_{11}^H\} \qquad (61)$$
$$= \dim\{\mathrm{span}(\mathbf{H}_{11}\mathbf{V})/\mathrm{span}(\mathbf{H}_{12}\mathbf{W})\} \qquad (62)$$
$$= \mathrm{rank}\{\mathbf{H}_{11}\mathbf{V}\} - \dim\{\mathrm{span}(\mathbf{H}_{11}\mathbf{V}) \cap \mathrm{span}(\mathbf{H}_{12}\mathbf{W})\}. \qquad (63)$$

where (61) comes from the fact that

$$\lim_{P \to \infty} \frac{\log|\mathbf{I} + \mathbf{A}P|}{\log(P)} = \lim_{P \to \infty} \frac{\sum_{i=1}^{t} \log(1 + \lambda_i P)}{\log(P)} = \mathrm{rank}\{\mathbf{A}\},$$

with λ_i and t being the nonzero eigenvalue and the rank of $\mathbf{A}$. (62) comes from the fact that $\mathbf{U}_0\mathbf{U}_0^H$ is the projection matrix of the subspace $\text{span}(\mathbf{H}_{12}\mathbf{W})^\perp$.

Applying similar derivations from (60) to (62) yields

$$\lim_{P\to\infty}\frac{R_d^2}{\log(P)} = \dim\{\text{span}(\mathbf{H}_{22}\mathbf{W})/\text{span}(\mathbf{H}_{21}\mathbf{V})\}, \quad (64)$$

$$\lim_{P\to\infty}\frac{R_e}{\log(P)} = \dim\{\text{span}(\mathbf{G}_1\mathbf{V})/\text{span}(\mathbf{G}_2\mathbf{W})\}. \quad (65)$$

Substituting (63)-(65) into (11), we arrive at (12a) and (12b). This completes the proof.

APPENDIX C
PROOF OF *Proposition 3*

By definition, we have $\bar{\mathcal{D}} \subset \mathcal{D}$. Thus, the boundary of $\bar{\mathcal{D}}$ is included by that of $\mathcal{D}$. In the following, we show that for any given precoding matrices $(\mathbf{V}, \mathbf{W}) \in \mathcal{I}$, we can always find another precoding matrices $(\mathbf{V}', \mathbf{W}') \in \bar{\mathcal{I}}$, which satisfy $d_s^1(\mathbf{V}, \mathbf{W}) \leq d_s^1(\mathbf{V}', \mathbf{W}')$ and $d_s^2(\mathbf{V}, \mathbf{W}) \leq d_s^2(\mathbf{V}', \mathbf{W}')$. So, the boundary of $\mathcal{D}$ is included by that of $\bar{\mathcal{D}}$. Concluding, the outer boundary of $\mathcal{D}$ is the same as that of $\bar{\mathcal{D}}$.

Before proceeding, we first introduce two critical properties on matrix that will be used in the following analyses. That is, for any given matrices $\mathbf{A}$ and $\mathbf{B}$, if $\mathbf{B}$ is invertible, then

$$\text{span}(\mathbf{A}) = \text{span}(\mathbf{AB}), \quad (66)$$

$$\text{rank}\{\mathbf{A}\} = \text{rank}\{\mathbf{AB}\}. \quad (67)$$

In what follows, based on the GSVD decomposition of $(\mathbf{H}_{12}\mathbf{W}, \mathbf{H}_{11}\mathbf{V})$ we first construct a precoding matrix pair $(\hat{\mathbf{V}}, \hat{\mathbf{W}})$, which excludes the intersection subspace of $\text{span}(\mathbf{H}_{12}\mathbf{W})$ and $\text{span}(\mathbf{H}_{11}\mathbf{V})$ without decreasing the achieved S.D.o.F. pair. Further, based on the GSVD decomposition of $(\mathbf{G}_2\hat{\mathbf{W}}, \mathbf{G}_1\hat{\mathbf{V}})$ we construct a precoding matrix pair $(\mathbf{V}', \mathbf{W}')$, which excludes the subspace $\text{span}(\mathbf{G}_{21}\hat{\mathbf{V}})/\text{span}(\mathbf{G}_{22}\hat{\mathbf{W}})$ without decreasing the achieved S.D.o.F. pair. In this way, we finish the construction of the wanted precoding matrix pair.

Consider the decomposition

$$\begin{aligned}\text{GSVD}&(\mathbf{H}_{12}\mathbf{W}, \mathbf{H}_{11}\mathbf{V}; N_d^1, K_w, K_v) \\ &= (\hat{\boldsymbol{\Psi}}_1, \hat{\boldsymbol{\Psi}}_2, \hat{\boldsymbol{\Lambda}}_1, \hat{\boldsymbol{\Lambda}}_2, \hat{\mathbf{X}}, \hat{k}, \hat{r}, \hat{s}, \hat{p}).\end{aligned} \quad (68)$$

Let $\hat{\boldsymbol{\Psi}}_2^0 = [\hat{\boldsymbol{\Psi}}_{21}, \hat{\boldsymbol{\Psi}}_{23}]$. Since $\hat{\boldsymbol{\Psi}}_1$ and $\hat{\boldsymbol{\Psi}}_2$ are invertible, $\hat{\boldsymbol{\Psi}}_1' = [\hat{\boldsymbol{\Psi}}_{11}, \hat{\boldsymbol{\Psi}}_{13}, \hat{\boldsymbol{\Psi}}_{12}]$ and $\hat{\boldsymbol{\Psi}}_2' = [\hat{\boldsymbol{\Psi}}_2^0, \hat{\boldsymbol{\Psi}}_{22}]$ are also invertible. Applying (66) and (67), we have

$$d_s^1(\mathbf{V}, \mathbf{W}) = d_s^1(\mathbf{V}\hat{\boldsymbol{\Psi}}_2', \mathbf{W}\hat{\boldsymbol{\Psi}}_1') \quad (69a)$$

$$= \text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\} - m(\mathbf{V}\hat{\boldsymbol{\Psi}}_2', \mathbf{W}\hat{\boldsymbol{\Psi}}_1') \quad (69b)$$

$$\leq \text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\} - m(\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0, \mathbf{W}\hat{\boldsymbol{\Psi}}_1'), \quad (69c)$$

in which (69b) can be justified with $\text{span}(\mathbf{H}_{12}\mathbf{W}\hat{\boldsymbol{\Psi}}_1') \cap \text{span}(\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2') = \text{span}(\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_{22})$. Besides, (69c) comes from the fact that $m(\mathbf{V}\hat{\boldsymbol{\Psi}}_2', \mathbf{W}\hat{\boldsymbol{\Psi}}_1') \geq m(\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0, \mathbf{W}\hat{\boldsymbol{\Psi}}_1')$. Here $(\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0, \mathbf{W}\hat{\boldsymbol{\Psi}}_1')$ is the precoding matrix pair $(\hat{\mathbf{V}}, \hat{\mathbf{W}})$ we mentioned in the above text.

Consider the decomposition

$$\begin{aligned}\text{GSVD}&(\mathbf{G}_2\mathbf{W}\hat{\boldsymbol{\Psi}}_1', \mathbf{G}_1\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0; N_e, K_w, K_v - \hat{s}) \\ &= (\breve{\boldsymbol{\Psi}}_1, \breve{\boldsymbol{\Psi}}_2, \breve{\boldsymbol{\Lambda}}_1, \breve{\boldsymbol{\Lambda}}_2, \breve{\mathbf{X}}, \breve{k}, \breve{r}, \breve{s}, \breve{p}).\end{aligned} \quad (70)$$

Let $\breve{\boldsymbol{\Psi}}_2^1 = [\breve{\boldsymbol{\Psi}}_{21}, \breve{\boldsymbol{\Psi}}_{22}]$. Since $\breve{\boldsymbol{\Psi}}_1$ and $\breve{\boldsymbol{\Psi}}_2$ are invertible, $\breve{\boldsymbol{\Psi}}_1' = [\breve{\boldsymbol{\Psi}}_{13}, \breve{\boldsymbol{\Psi}}_{11}, \breve{\boldsymbol{\Psi}}_{12}]$ and $\breve{\boldsymbol{\Psi}}_2' = [\breve{\boldsymbol{\Psi}}_{23}, \breve{\boldsymbol{\Psi}}_2^1]$ are also invertible. Applying (66) and (67), we have

$$\text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\} - m(\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0, \mathbf{W}\hat{\boldsymbol{\Psi}}_1')$$

$$= \text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2'\} - m(\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2', \mathbf{W}\hat{\boldsymbol{\Psi}}_1'\breve{\boldsymbol{\Psi}}_1') \quad (71a)$$

$$= \text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2'\} - \text{rank}\{\breve{\boldsymbol{\Psi}}_{23}\} \quad (71b)$$

$$\leq \text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1\}. \quad (71c)$$

Here, since $\text{span}(\mathbf{G}_1\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2')/\text{span}(\mathbf{G}_2\mathbf{W}\hat{\boldsymbol{\Psi}}_1'\breve{\boldsymbol{\Psi}}_1') = \text{span}(\mathbf{G}_1\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_{23}) = \text{rank}\{\breve{\boldsymbol{\Psi}}_{23}\}$, we see that (71b) holds true. Since $\text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_{23}\} \leq \text{rank}\{\breve{\boldsymbol{\Psi}}_{23}\}$ and $\text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2'\} \leq \text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1\} + \text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_{23}\}$, we see that (71c) holds true.

Combining (69a)-(69c) with (71a)-(71c), we arrive at

$$d_s^1(\mathbf{V}, \mathbf{W}) \leq \text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1\}. \quad (72)$$

On the other hand, according to (70), it holds that $m(\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1, \mathbf{W}\hat{\boldsymbol{\Psi}}_1'\breve{\boldsymbol{\Psi}}_1') = 0$, which indicates

$$\text{span}(\mathbf{G}_1\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1) \subset \text{span}(\mathbf{G}_2\mathbf{W}\hat{\boldsymbol{\Psi}}_1'\breve{\boldsymbol{\Psi}}_1'). \quad (73)$$

According to (68), $\text{span}(\mathbf{H}_{12}\mathbf{W}\hat{\boldsymbol{\Psi}}_1') \cap \text{span}(\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0) = \mathbf{0}$, which together with $\text{span}(\mathbf{H}_{12}\mathbf{W}\hat{\boldsymbol{\Psi}}_1') = \text{span}(\mathbf{H}_{12}\mathbf{W}\hat{\boldsymbol{\Psi}}_1'\breve{\boldsymbol{\Psi}}_1')$ and $\text{span}(\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0) \supset \text{span}(\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1)$, implies

$$\text{span}(\mathbf{H}_{12}\mathbf{W}\hat{\boldsymbol{\Psi}}_1'\breve{\boldsymbol{\Psi}}_1') \cap \text{span}(\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1) = \mathbf{0}. \quad (74)$$

Combining (73) and (74), we arrive at

$$(\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1, \mathbf{W}\hat{\boldsymbol{\Psi}}_1'\breve{\boldsymbol{\Psi}}_1') \in \bar{\mathcal{I}}. \quad (75)$$

Let $\mathbf{V}' = \mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1$ and $\mathbf{W}' = \mathbf{W}\hat{\boldsymbol{\Psi}}_1'\breve{\boldsymbol{\Psi}}_1'$. According to *Corollary 2*, $d_s^1(\mathbf{V}', \mathbf{W}') = \text{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\boldsymbol{\Psi}}_2^0\breve{\boldsymbol{\Psi}}_2^1\}$, which together with (72), gives $d_s^1(\mathbf{V}, \mathbf{W}) \leq d_s^1(\mathbf{V}', \mathbf{W}')$. Besides, $\text{span}(\mathbf{H}_{21}\mathbf{V}') \subset \text{span}(\mathbf{H}_{21}\mathbf{V})$ and $\text{span}(\mathbf{H}_{22}\mathbf{W}') = \text{span}(\mathbf{H}_{22}\mathbf{W})$. So $d_s^2(\mathbf{V}, \mathbf{W}) \leq d_s^2(\mathbf{V}', \mathbf{W}')$. This completes the proof.

APPENDIX D
PROOF OF *Corollary 1*

Since by definition $\hat{\mathcal{I}} \subset \bar{\mathcal{I}}$, it holds that $\hat{\mathcal{D}} \subset \bar{\mathcal{D}}$. In the sequel, we will show that for any given $(\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}$, we can always construct another feasible point $(\mathbf{V}^\star, \mathbf{W}^\star) \in \hat{\mathcal{I}}$, which satisfy $d_s^1(\mathbf{V}^\star, \mathbf{W}^\star) = d_s^1(\mathbf{V}, \mathbf{W})$ and $d_s^2(\mathbf{V}^\star, \mathbf{W}^\star) = d_s^2(\mathbf{V}, \mathbf{W})$, thus giving the proof of $\hat{\mathcal{D}} \supset \bar{\mathcal{D}}$. Concluding, it holds that $\bar{\mathcal{D}} = \hat{\mathcal{D}}$.

For any given $(\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}$, $\mathbf{V} \in \mathbb{C}^{N_s^1 \times K_v}$, $\mathbf{W} \in \mathbb{C}^{N_s^2 \times K_w}$, we should have $(\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}_1$ and $(\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}_2$. Since all channel matrices are assumed to be full rank, it holds that $\text{rank}\{\mathbf{G}_2\mathbf{W}\} = \min\{K_w, N_e\}$.

In the following, we consider two distinct cases.

(i) For the case of $K_w \geq N_e$, it holds that $\text{rank}\{\mathbf{G}_2\mathbf{W}\} = N_e$. Denote $\mathbf{G}_2\mathbf{W} = [\mathbf{U}_1 \ \mathbf{U}_0]\begin{bmatrix} \boldsymbol{\Sigma}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}\begin{bmatrix} \mathbf{T}_1^H \\ \mathbf{T}_0^H \end{bmatrix}$ as the SVD of $\mathbf{G}_2\mathbf{W}$. Then, the matrix $\mathbf{G}_2\mathbf{W}\mathbf{T}_1$ is invertible. Let $\mathbf{B} = \mathbf{T}_1(\mathbf{G}_2\mathbf{W}\mathbf{T}_1)^{-1}\mathbf{G}_1\mathbf{V}$. Then,

$$\mathbf{G}_1\mathbf{V} = \mathbf{G}_2\mathbf{W}\mathbf{T}_1(\mathbf{G}_2\mathbf{W}\mathbf{T}_1)^{-1}\mathbf{G}_1\mathbf{V} = \mathbf{G}_2\mathbf{W}\mathbf{B}. \quad (76)$$

(ii) For the case of $K_w < N_e$, $\mathbf{G}_2\mathbf{W}$ is full column rank. Let $\mathbf{P}$ be the projection matrix of $\mathbf{G}_2\mathbf{W}$, i.e.,

$$\mathbf{P} = \mathbf{G}_2\mathbf{W}((\mathbf{G}_2\mathbf{W})^H\mathbf{G}_2\mathbf{W})^{-1}(\mathbf{G}_2\mathbf{W})^H. \qquad (77)$$

Due to $(\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}_1$, it holds that

$$\mathbf{G}_1\mathbf{V} = \mathbf{P}\mathbf{G}_1\mathbf{V}. \qquad (78)$$

Substituting (77) into (78) and letting $\mathbf{B} = ((\mathbf{G}_2\mathbf{W})^H\mathbf{G}_2\mathbf{W})^{-1}(\mathbf{G}_2\mathbf{W})^H\mathbf{G}_1\mathbf{V}$, we arrive at

$$\mathbf{G}_1\mathbf{V} = \mathbf{G}_2\mathbf{W}\mathbf{B}. \qquad (79)$$

Let $\mathbf{V}^\star = \mathbf{V}$ and $\mathbf{W}^\star = \mathbf{W}[\mathbf{B}\ \mathbf{B}^\perp]$. Summarizing the above two cases, for both cases it holds that

$$\mathbf{G}_1\mathbf{V}^\star = \mathbf{G}_2\mathbf{W}^\star(:, 1 : K_v),$$

which, combined with $(\mathbf{V}, \mathbf{W}) \in \bar{\mathcal{I}}_2$, implies that $(\mathbf{V}^\star, \mathbf{W}^\star) \in \hat{\mathcal{I}}$. On the other hand, since the matrix $[\mathbf{B}\ \mathbf{B}^\perp]$ is invertible, it holds that $d_s^1(\mathbf{V}^\star, \mathbf{W}^\star) = d_s^1(\mathbf{V}, \mathbf{W})$ and $d_s^2(\mathbf{V}^\star, \mathbf{W}^\star) = d_s^2(\mathbf{V}, \mathbf{W})$. This completes the proof.

REFERENCES

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

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

[3] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[4] L. Li, Z. Chen, and J. Fang, "On secrecy capacity of Gaussian wiretap channel aided by a cooperative jammer," *IEEE Signal Process. Lett.*, vol. 21, no. 11, pp. 1356–1360, Nov. 2014.

[5] H.-T. Chiang and J. S. Lehnert, "Optimal cooperative jamming for security," in *Proc. IEEE MILCOM*, Baltimore, MD, Nov. 2011, pp. 125–130.

[6] S. A. A. Fakoorian and A. L. Swindlehurst, "Secrecy capacity of MISO Gaussian wiretap channel with a cooperative jammer," in *Proc. IEEE SPAWC*, San Francisco, CA, Jun. 2011, pp. 416–420.

[7] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[8] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[9] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[10] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[11] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[12] S. Luo, J. Li, and A. P. Petropulu, "Uncoordinated cooperative jamming for secret communications," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 7, pp. 1081–1090, Jul. 2013.

[13] D. S. Kalogerias, N. Chatzipanagiotis, M. M. Zavlanos, and A. P. Petropulu, "Mobile jammers for secrecy rate maximization in cooperative networks," in *Proc. IEEE ICASSP*, Vancouver, Canada, May 2013, pp. 2901–2905.

[14] J. Wang and A. Swindlehurst, "Cooperative jamming in MIMO ad hoc networks," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, Nov. 2009, pp. 1719–1723.

[15] J. H. Lee and W. Choi, "Multiuser diversity for secrecy communications using opportunistic jammer selection: secure DoF and jammer scaling law," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 828–839, Feb. 2014.

[16] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," vol. 14, no. 10, pp. 885–887, Oct. 2010.

[17] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 640–649, Sep. 2011.

[18] O. O. Koyluoglu and H. E. Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.

[19] 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.

[20] ——, "Secure degrees of freedom region of the Gaussian interference channel with secrecy constraints," in *Proc. IEEE ITW*, Hobart, Tasmania, Australia, Nov. 2014, pp. 361–365.

[21] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[22] T. T. Vu, H. H. Kha, T. Q. Duong, and N.-S. Vo, "On the interference alignment designs for secure multiuser MIMO systems," *[online], Available: http://arxiv.org/abs/1508.00349*.

[23] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3810–3823, Jul. 2015.

[24] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[25] M. Nafea and A. Yener, "How many antennas does a cooperative jammer need for achieving the degrees of freedom of multiple antenna Gaussian channels in the presence of an eavesdropper?" in *Proc. Allerton Conf.*, Allerton House, UIUC, Illinois, USA, Oct. 2013, pp. 774–780.

[26] ——, "Secure degrees of freedom for the MIMO wiretap channel with a multiantenna cooperative jammer," in *Proc. IEEE ITW*, Hobart, Australia, Nov. 2014, pp. 626–630.

[27] ——, "Secure degrees of freedom of N-N-M wiretap channel with a K-antenna cooperative jammer," in *Proc. IEEE ICC*, London, United Kingdom, Jun. 2015, pp. 4169–4174.

[28] A. Agustin and J. Vidal, "Improved interference alignment precoding for the MIMO X channel," in *Proc. IEEE ICC*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[29] T. Gou and S. A. Jafar, "Degrees of freedom of the K-user $M \times N$ MIMO interference channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6040–6057, Dec. 2010.

[30] C. M. Yetis, T. Gou, S. A. Jafar, and A. H. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4771–4782, Sep. 2010.

[31] J. Chen, Q. T. Zhang, and G. Chen, "Joint space decomposition-and-synthesis approach and achievable DoF regions for K-user MIMO interference channels," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2304–2316, May 2014.

[32] C. Paige and M. A. Saunders, "Towards a generalized singular value decomposition," *SIAM J. Numer. Anal.*, vol. 18, no. 3, pp. 398–405, Jun. 1981.

[33] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[34] 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.

[35] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4971, Aug. 2011.

[36] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-II: the MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.