This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

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 proposed expressions are functions of the number of antennas at each terminal, and apply to any number of antennas, thus constituting an advancement over prior works that have considered only fixed antenna configurations.**

***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 over beamforming vectors or power allocation, 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. Our network comprises a source destination pair exchanging confidential messages, another pair exchanging public messages, and a passive eavesdropper who is interested in the communications of the former pair. 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 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]. Since we only care about the achievable

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). The work was performed when L. Li was a visiting student at Rutgers University

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).

This work was supported in part by the National Natural Science Foundation of China under Grant 61571089, and by the High-Tech Research and Development (863) Program of China under Grand 2015AA01A707.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

S.D.o.F., we do not optimize the achievable secrecy rate over power allocation. Thus, it can be expected that, for the SISO and MISO cases, the schemes of [23], [24] would respectively outperform the proposed scheme in terms of the secrecy rate. 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 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. (36) and (37), respectively) corresponding to when only one user communicates information, the strict S.D.o.F. region boundary (see eq. (44)), and the ending points of the strict S.D.o.F. region boundary, *E*1 and *E*2 (see eq. (45) and (54), 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 II).

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 in our work 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; $\mathbf{A}^T$, $\mathbf{A}^H$, $\mathrm{tr}\{\mathbf{A}\}$, $\mathrm{rank}\{\mathbf{A}\}$, 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 $\mathbf{A}$; $\mathrm{span}(\mathbf{A})$ and $\mathrm{span}(\mathbf{A})^\perp$ are the subspace spanned by the columns of $\mathbf{A}$ and its orthogonal complement, respectively; $\mathrm{null}(\mathbf{A})$ denotes the null space of $\mathbf{A}$; $\mathrm{span}(\mathbf{A}) \setminus \mathrm{span}(\mathbf{B}) \triangleq \{\mathbf{x}|\mathbf{x} \in \mathrm{span}(\mathbf{A}), \mathbf{x} \notin \mathrm{span}(\mathbf{B})\}$; $\mathrm{span}(\mathbf{A}) \cap \mathrm{span}(\mathbf{B}) = \mathbf{0}$ means that $\mathrm{span}(\mathbf{A})$ and $\mathrm{span}(\mathbf{B})$ have no intersections; $\dim\{\mathrm{span}(\mathbf{A})\}$ represents the number of dimension of the subspace spanned by the columns of $\mathbf{A}$; $\mathbf{\Gamma}(\mathbf{A})$ denotes the orthogonal basis of $\mathrm{null}(\mathbf{A})$; $\mathbf{A}^\perp$ denotes the orthogonal basis of $\mathrm{null}(\mathbf{A}^H)$. We use lower case bold to denote vectors.

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 $(\mathbf{A}^H, \mathbf{B}^H)$ [32] returns unitary matrices $\mathbf{\Psi}_1 \in \mathbb{C}^{M\times M}$ and $\mathbf{\Psi}_2 \in \mathbb{C}^{K\times K}$, 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 $\mathbf{X} \in \mathbb{C}^{N\times k}$ with $\mathrm{rank}\{\mathbf{X}\} = k$, such that

$$\mathbf{A}^H = \mathbf{\Psi}_1 \mathbf{D}_1 \mathbf{X}^H, \tag{1a}$$

$$\mathbf{B}^H = \mathbf{\Psi}_2 \mathbf{D}_2 \mathbf{X}^H, \tag{1b}$$

with

$$\mathbf{D}_1 = \begin{matrix} M-s-r \\ s \\ r \end{matrix} \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Lambda}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_r \end{bmatrix}, \tag{2a}$$

$$\mathbf{D}_2 = \begin{matrix} p \\ s \\ K-s-p \end{matrix} \begin{bmatrix} \mathbf{I}_p & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Lambda}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}. \tag{2b}$$

Here 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

$$k \triangleq \mathrm{rank}\{[(\mathbf{A}^H)^T, (\mathbf{B}^H)^T]^T\} = \min\{M+K, N\}, \tag{3a}$$

$$p \triangleq \dim\{\mathrm{span}(\mathbf{A})^\perp \cap \mathrm{span}(\mathbf{B})\} = k - \min\{M, N\}, \tag{3b}$$

$$r \triangleq \dim\{\mathrm{span}(\mathbf{A}) \cap \mathrm{span}(\mathbf{B})^\perp\} = k - \min\{K, N\}, \tag{3c}$$

$$\begin{aligned} s &\triangleq \dim\{\mathrm{span}(\mathbf{A}) \cap \mathrm{span}(\mathbf{B})\} = k - p - r \\ &= (\min\{M,N\} + \min\{K,N\} - N)^+. \end{aligned} \tag{3d}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

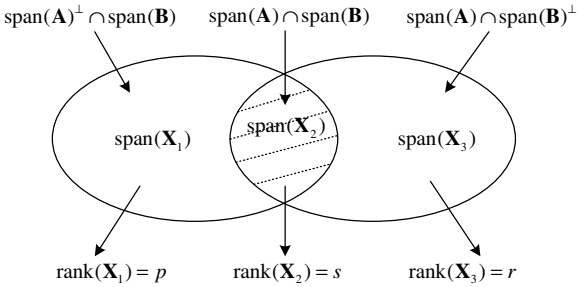

Fig. 1: The geometric relationship between the subspaces $\mathrm{span}(\mathbf{A})$ and $\mathrm{span}(\mathbf{B})$.

We can rewrite (1a) and (1b) as,

$$\mathbf{A}[\mathbf{\Psi}_{11}\ \mathbf{\Psi}_{12}\ \mathbf{\Psi}_{13}] = [\mathbf{X}_1\ \mathbf{X}_2\ \mathbf{X}_3]\mathbf{D}_1^H, \tag{4a}$$

$$\mathbf{B}[\mathbf{\Psi}_{21}\ \mathbf{\Psi}_{22}\ \mathbf{\Psi}_{23}] = [\mathbf{X}_1\ \mathbf{X}_2\ \mathbf{X}_3]\mathbf{D}_2^H. \tag{4b}$$

with $\mathbf{\Psi}_{11}$, $\mathbf{\Psi}_{12}$ and $\mathbf{\Psi}_{13}$ being the first $M-s-r$, the following s, and the remaining r columns of of $\mathbf{\Psi}_1$, respectively; $\mathbf{\Psi}_{21}$, $\mathbf{\Psi}_{22}$ and $\mathbf{\Psi}_{23}$ being the first p, the following s, and the remaining $K-s-p$ columns of $\mathbf{\Psi}_1$, respectively. In addition, $\mathbf{X}_1$, $\mathbf{X}_2$ and $\mathbf{X}_3$ denote the first p, the following s, and the remaining r columns of $\mathbf{X}$, respectively.

With the GSVD decomposition, one can decompose the union of $\mathrm{span}(\mathbf{A})$ and $\mathrm{span}(\mathbf{B})$ into three subspaces, as shown in Fig. 1.

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 GSVD of $(\mathbf{A}^H, \mathbf{B}^H)$.

(i) $\mathbf{Av} = \mathbf{Bw} \neq \mathbf{0}$ holds true if and only if

$$\mathbf{v} = \begin{bmatrix} \mathbf{\Psi}_{12}\mathbf{\Lambda}_1^{-1} & \mathbf{\Gamma}(\mathbf{A}) \end{bmatrix} \begin{bmatrix} \mathbf{y}_s \\ \mathbf{y}_1 \end{bmatrix}, \tag{5a}$$

$$\mathbf{w} = \begin{bmatrix} \mathbf{\Psi}_{22}\mathbf{\Lambda}_2^{-1} & \mathbf{\Gamma}(\mathbf{B}) \end{bmatrix} \begin{bmatrix} \mathbf{y}_s \\ \mathbf{y}_2 \end{bmatrix}, \tag{5b}$$

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

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

Proof: See Appendix A. ■

III. System Model and Problem Statement

We consider a MIMO interference network (see Fig. 2), which consists of a wiretap channel S_1-D_1-E and a point-to-point channel S_2-D_2. 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. The eavesdropper is an unauthorized user as far as the information of S_1-D_1 is concerned. We assume that the eavesdropper is a passive node whose whereabouts can be monitored. The S_2-D_2 is a pair that exchanges public messages, and we assume that it is a trusted pair, which is willing to cooperate with S_1-D_1. While communicating with D_2, S_2 generates interference for the 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 by S_1 and S_2, respectively. Each message is precoded before transmission.

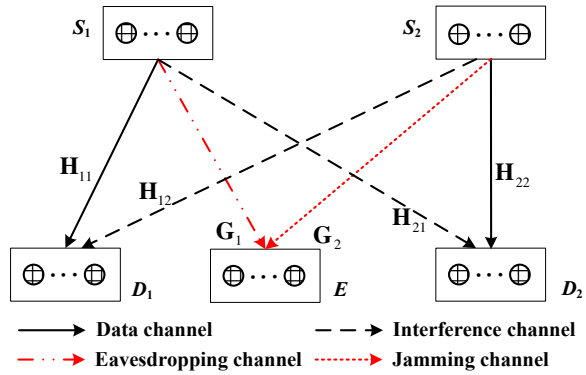

Fig. 2: A MIMO two-user wiretap interference channel.

The signals received at the legitimate receiver D_i can be expressed as

$$\mathbf{y}_d^i = \mathbf{H}_{i1}\mathbf{V}\mathbf{s}_1 + \mathbf{H}_{i2}\mathbf{W}\mathbf{s}_2 + \mathbf{n}_d^i, i = 1, 2, \tag{6}$$

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

$$\mathbf{y}_e = \mathbf{G}_1\mathbf{V}\mathbf{s}_1 + \mathbf{G}_2\mathbf{W}\mathbf{s}_2 + \mathbf{n}_e. \tag{7}$$

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 a passive network user and 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]

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

$$R_s^2 = R_d^2, \tag{9}$$

where

$$R_d^1 = \log|\mathbf{I} + (\mathbf{I} + \mathbf{H}_{12}\mathbf{Q}_w\mathbf{H}_{12}^H)^{-1}\mathbf{H}_{11}\mathbf{Q}_v\mathbf{H}_{11}^H|, \tag{10a}$$

$$R_d^2 = \log|\mathbf{I} + (\mathbf{I} + \mathbf{H}_{21}\mathbf{Q}_v\mathbf{H}_{21}^H)^{-1}\mathbf{H}_{22}\mathbf{Q}_w\mathbf{H}_{22}^H|, \tag{10b}$$

$$R_e = \log|\mathbf{I} + (\mathbf{I} + \mathbf{G}_2\mathbf{Q}_w\mathbf{G}_2^H)^{-1}\mathbf{G}_1\mathbf{Q}_v\mathbf{G}_1^H|, \tag{10c}$$

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., $\mathcal{R} \triangleq \bigcup_{(\mathbf{V},\mathbf{W})\in\mathcal{I}} (R_s^1, R_s^2)$, 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

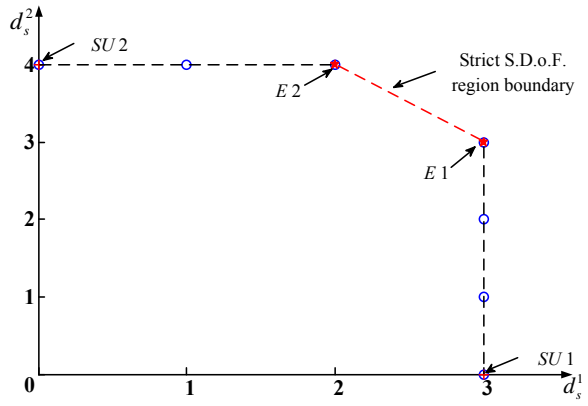

Fig. 3: Achievable S.D.o.F. region boundary.

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

$$\mathcal{D} \triangleq \bigcup_{(\mathbf{V},\mathbf{W})\in\mathcal{I}} (d_s^1, d_s^2), \tag{11}$$

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

$$d_s^i \triangleq \lim_{P\to\infty} \frac{R_s^i}{\log P}, i \in \{1,2\}. \tag{12}$$

As shown in Fig. 3, 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 $\mathcal{D}$ as a function of the number of antennas. Towards 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 construct the precoding matrices which achieve that boundary.

IV. Cooperative Secrecy Transmission Scheme

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

$$d_s^1(\mathbf{V},\mathbf{W}) = n(\mathbf{V},\mathbf{W}) - m(\mathbf{V},\mathbf{W}), \tag{13a}$$
$$d_s^2(\mathbf{V},\mathbf{W}) = \dim\{\mathrm{span}(\mathbf{H}_{22}\mathbf{W}) \setminus \mathrm{span}(\mathbf{H}_{21}\mathbf{V})\}, \tag{13b}$$

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

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 sent by S_1 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 infinity. In other words, the precoding matrix pair 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

$$\bar{\mathcal{I}}_1 \triangleq \{(\mathbf{V},\mathbf{W}) | \mathrm{span}(\mathbf{G}_1\mathbf{V}) \subset \mathrm{span}(\mathbf{G}_2\mathbf{W})\}, \tag{14a}$$
$$\bar{\mathcal{I}}_2 \triangleq \{(\mathbf{V},\mathbf{W}) | \mathrm{span}(\mathbf{H}_{11}\mathbf{V}) \cap \mathrm{span}(\mathbf{H}_{12}\mathbf{W}) = \mathbf{0}\}. \tag{14b}$$

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

Proposition 3: Let

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

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

$$\hat{\mathcal{D}} \triangleq \bigcup_{(\mathbf{V},\mathbf{W})\in\hat{\mathcal{I}}} (d_s^1, d_s^2), \tag{16}$$

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

$$\hat{\mathcal{I}} \triangleq \{(\mathbf{V},\mathbf{W}) | \mathbf{G}_1\mathbf{V} = \mathbf{G}_2\mathbf{W}(:, 1:K_v), (\mathbf{V},\mathbf{W}) \in \bar{\mathcal{I}}\}. \tag{17}$$

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 $d_s^1 = \mathrm{rank}(\mathbf{H}_{11}\mathbf{V})$.

Proof: See Appendix E. ∎

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. (17)). Further, *Corollary 2* shows that for $(\mathbf{V},\mathbf{W}) \in \hat{\mathcal{I}}$ the achieved S.D.o.F. is $d_s^1 = \mathrm{rank}\{\mathbf{H}_{11}\mathbf{V}\}$. In this section we construct the 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.

Let $(\mathbf{v},\mathbf{w})$ denote the precoding vector pairs comprising $(\mathbf{V},\mathbf{W})$. Obviously we are interested in linearly independent

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

vectors. 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 $\mathbf{w} \neq \mathbf{0}$, this interference signal from S_2 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, d_s^1 increases as we include more linear independent precoding vector pairs in $(\mathbf{V}, \mathbf{W})$. Third, the maximum number of linear precoding vector pairs is determined by (14b), which requires that

$$\dim\{\text{span}(\mathbf{H}_{11}\mathbf{V})\} + \dim\{\text{span}(\mathbf{H}_{12}\mathbf{W})\} \leq N_d^1. \quad (18)$$

Fourth, the maximum dimension of the interference-free subspace at D_2 depends on whether D_2 experiences interference from S_1. Motivated by these observations, we will divide the set of $(\mathbf{v}, \mathbf{w})$ which satisfies $\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w}$ into six subsets, namely, Sub_{I},..., Sub_{VI}.

Sub_{I}: The message signal sent by S_1 spreads within the null space of the eavesdropping channel, and does not interfere with D_2. Sub_{II}: The message signal sent by S_1 spreads within the null space of the eavesdropping channel, but does interfere with D_2. Sub_{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. Sub_{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 signal sent by S_1 interferes with D_2. Sub_{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. Sub_{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.

We say a subset has higher priority when its precoding vector pairs have the potential to achieve a greater (d_s^1, d_s^2). Among the above six subsets, some subsets have higher priority than others. In the construction of $(\mathbf{V}, \mathbf{W})$, we will select as many precoding vector pairs $(\mathbf{v}, \mathbf{w})$ from the subset with higher priority as possible. As it will become clear in the following, the formula for $\mathbf{v}$ in the different subsets may have some common basis vectors. In that case, and since we are interested in linearly independent $\mathbf{v}$'s, the common basis vectors will only be attributed to the subset with the highest priority. Based on these two observations, in the following, we will determine the number of linear independent precoding vector pairs that should be considered in Sub_{I},..., Sub_{VI}, i.e., d_{I},...,d_{VI}, respectively. In addition, we will give the formulas of $\mathbf{v}$ and $\mathbf{w}$ of each subset, respectively.

I) Sub_{I}: The precoding vector pairs in Sub_{I} satisfy

$$\mathbf{G}_1\mathbf{v} = \mathbf{0}, \quad (19a)$$

$$\mathbf{H}_{21}\mathbf{v} = \mathbf{0}. \quad (19b)$$

Further, it holds that $\mathbf{G}_2\mathbf{w} = \mathbf{G}_1\mathbf{v} = \mathbf{0}$. The case in which $\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} = 0$ and $\mathbf{w} \neq 0$ is not considered here, because even if $\mathbf{w} \neq 0$, this interference signal from S_2 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 (19b), 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. Thus, the formula of $\mathbf{v}$ in Sub_{I} is

$$\mathbf{v} = \mathbf{\Gamma}(\mathbf{G}_1)\mathbf{\Gamma}(\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1))\mathbf{z}, \quad (20)$$

with $\mathbf{z}$ being a nonzero vector with appropriate length. Since all the channel matrices are assumed to be full rank, the number of linearly independent vectors described by (20), i.e., d_{I}, is

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

Sub_{I} has the highest priority since its precoding vector pairs have the potential to achieve the greatest (d_s^1, d_s^2). Thus, a number of $(N_s^1 - N_e - N_d^2)^+$ precoding vector pairs in Sub_{I} should be considered.

II) Sub_{II}: The vectors in Sub_{II} satisfy

$$\mathbf{G}_1\mathbf{v} = \mathbf{0}, \quad (22a)$$

$$\mathbf{H}_{21}\mathbf{v} \neq \mathbf{0}. \quad (22b)$$

The vectors $\mathbf{v}$ satisfying (22a) are of the form $\mathbf{\Gamma}(\mathbf{G}_1)\mathbf{x}$. Since $\mathbf{H}_{21}$ is independent of $\mathbf{G}_1$, for precoding vectors satisfying (22a), $\mathbf{H}_{21}\mathbf{v} \neq 0$ holds true with probability one. So, the vectors $\mathbf{v}$ in Sub_{II} are of the form $\mathbf{\Gamma}(\mathbf{G}_1)\mathbf{x}$. Since we want linearly 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, in Sub_{II} we will only consider the following vectors:

$$\mathbf{v} = \mathbf{\Gamma}(\mathbf{G}_1)\mathbf{\Gamma}^{\perp}(\mathbf{H}_{21}\mathbf{\Gamma}(\mathbf{G}_1))\mathbf{z}. \quad (23)$$

The number of linearly independent precoding vectors given by (23) is

$$d_{\text{II}} \leq (N_s^1 - N_e)^+ - d_{\text{I}} = \min\{N_d^2, (N_s^1 - N_e)^+\}. \quad (24)$$

Although we will see that Sub_{II} shares some common basis vectors with some other subsets, because Sub_{II} has higher priority than those, a number of $\min\{N_d^2, (N_s^1 - N_e)^+\}$ precoding vector pairs in Sub_{II} should be considered.

III) Sub_{III}: The precoding vector pairs in Sub_{III} satisfy

$$\mathbf{H}_{12}\mathbf{w} = \mathbf{0}, \quad (25a)$$

$$\mathbf{H}_{21}\mathbf{v} = \mathbf{0}, \quad (25b)$$

$$\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}. \quad (25c)$$

Substituting $\mathbf{v} = \mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{x}$ and $\mathbf{w} = \mathbf{\Gamma}(\mathbf{H}_{12})\mathbf{y}$ into (25c) yields,

$$\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{x} = \mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12})\mathbf{y} \neq \mathbf{0}. \quad (26)$$

Letting $\mathbf{A} = \mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21})$, $\mathbf{B} = \mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12})$, and applying *Proposition 1*(i), we obtain $\mathbf{x}$ which satisfies (26), i.e.,

$$\mathbf{x} = \hat{\mathbf{\Psi}}_{12}\hat{\mathbf{\Lambda}}_1^{-1}\mathbf{z} + \mathbf{\Gamma}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))\mathbf{z}_1,$$

with $\mathbf{z}_1$ being any vector with appropriate length. Here, $\hat{\mathbf{\Psi}}_{12}$, $\hat{\mathbf{\Lambda}}_1$ and $\hat{s}$ (to be used below) correspond to the $\mathbf{\Psi}_{12}$, $\mathbf{\Lambda}_1$ and s

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

TABLE I: The number of linear independent precoding vector pairs that should be considered in each subset.

subsets	the number of linear independent precoding vector pairs $(\mathbf{v},\mathbf{w})$ that should be considered
$Sub_{\rm I}$	$d_{\rm I}=(N_s^1-N_e-N_d^2)^+$
$Sub_{\rm II}$	$d_{\rm II}=(N_s^1-N_e)^+-d_{\rm I}=\min\{N_d^2,(N_s^1-N_e)^+\}$
$Sub_{\rm III}$	$d_{\rm III}=\hat{s}=(\min\{(N_s^1-N_d^2)^+,N_e\}+\min\{(N_s^2-N_d^1)^+,N_e\}-N_e)^+$
$Sub_{\rm IV}$	$d_{\rm IV}=\bar{s}-d_{\rm III}=(\min\{N_s^1,N_e\}+\min\{(N_s^2-N_d^1)^+,N_e\}-N_e)^+-d_{\rm III}$
$Sub_{\rm V}$	$d_{\rm V}=\breve{s}-d_{\rm III}=(\min\{(N_s^1-N_d^2)^+,N_e\}+\min\{N_s^2,N_e\}-N_e)^+-d_{\rm III}$
$Sub_{\rm VI}$	$d_{\rm VI}=d_s-(d_{\rm III}+d_{\rm IV}+d_{\rm V})=(\min\{N_s^1,N_e\}+\min\{N_s^2,N_e\}-N_e)^+-(d_{\rm III}+d_{\rm IV}+d_{\rm V})$

of *Proposition 1*, and arise due to the GSVD of $(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))^H$ and $(\mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12}))^H$. Thus, the formula for $\mathbf{v}$ in this subspace is of the form $\mathbf{\Gamma}(\mathbf{H}_{21})\hat{\mathbf{\Psi}}_{12}\hat{\mathbf{\Lambda}}_1^{-1}\mathbf{z}+\mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{\Gamma}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))\mathbf{z}_1$. Noting that some of those basis vectors, i.e., the columns of $\mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{\Gamma}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))$, also span the solution space of a subset with higher priority, i.e., $Sub_{\rm I}$, we will only consider the following vectors:

$$\mathbf{v}=\mathbf{\Gamma}(\mathbf{H}_{21})\hat{\mathbf{\Psi}}_{12}\hat{\mathbf{\Lambda}}_1^{-1}\mathbf{z},\mathbf{w}=\mathbf{\Gamma}(\mathbf{H}_{12})\hat{\mathbf{\Psi}}_{22}\hat{\mathbf{\Lambda}}_2^{-1}\mathbf{z}. \tag{27}$$

The number of linearly independent $\mathbf{v}$'s described by (27), i.e., $d_{\rm III}$, is $d_{\rm III}\le\hat{s}$. Since $Sub_{\rm III}$ has higher priority than the remaining subsets, i.e., $Sub_{\rm IV}$, $Sub_{\rm V}$ and $Sub_{\rm VI}$, a number of $\hat{s}$ precoding vector pairs in $Sub_{\rm III}$ should be considered.

IV) $Sub_{\rm IV}$: The precoding vector pairs in $Sub_{\rm IV}$ satisfy

$$\mathbf{H}_{12}\mathbf{w}=\mathbf{0}, \tag{28a}$$
$$\mathbf{H}_{21}\mathbf{v}\neq\mathbf{0}, \tag{28b}$$
$$\mathbf{G}_1\mathbf{v}=\mathbf{G}_2\mathbf{w}\neq\mathbf{0}. \tag{28c}$$

Substituting $\mathbf{w}=\mathbf{\Gamma}(\mathbf{H}_{12})\mathbf{y}$ into (28c), we get

$$\mathbf{G}_1\mathbf{v}=\mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12})\mathbf{y}\neq\mathbf{0}. \tag{29}$$

Letting $\mathbf{A}=\mathbf{G}_1$, $\mathbf{B}=\mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12})$, and applying *Proposition 1*(i), we get that $\mathbf{v}$ is of the form

$$\mathbf{v}=\bar{\mathbf{\Psi}}_{12}\bar{\mathbf{\Lambda}}_1^{-1}\mathbf{z}+\mathbf{\Gamma}(\mathbf{G}_1)\mathbf{z}_1.$$

Here, $\bar{\mathbf{\Psi}}_{12}$, $\bar{\mathbf{\Lambda}}_1$ and $\bar{s}$ (to be used below) correspond to the $\mathbf{\Psi}_{12}$, $\mathbf{\Lambda}_1$ and s of *Proposition 1*, and arise due to the GSVD of $\mathbf{G}_1^H$ and $(\mathbf{G}_2\mathbf{\Gamma}(\mathbf{H}_{12}))^H$. Noting that the columns of $\mathbf{\Gamma}(\mathbf{G}_1)$, also span the solution space of $\mathbf{v}$ in $Sub_{\rm I}\cup Sub_{\rm II}$, here we only consider the following precoding vectors:

$$\mathbf{v}=\bar{\mathbf{\Psi}}_{12}\bar{\mathbf{\Lambda}}_1^{-1}\mathbf{z},\mathbf{w}=\mathbf{\Gamma}(\mathbf{H}_{12})\bar{\mathbf{\Psi}}_{22}\bar{\mathbf{\Lambda}}_2^{-1}\mathbf{z}. \tag{30}$$

In the above we used the fact that since $\mathbf{H}_{21}$ is independent of $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{H}_{12}$, for precoding vector pairs in (30), $\mathbf{H}_{21}\mathbf{v}\neq 0$ holds true with probability one.

On combining (25a)-(25c) with (28a)-(28c), it holds that

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

By *Proposition 1*(ii), the number of linearly independent vectors given by (30), i.e., $d_{\rm IV}$, satisfies $d_{\rm III}+d_{\rm IV}\le\bar{s}$. Thus, $d_{\rm IV}\le\bar{s}-d_{\rm III}=\bar{s}-\hat{s}$. Although we will see that $Sub_{\rm IV}$ shares some common basis vectors with another subsequent subset, since $Sub_{\rm IV}$ has higher priority, a number of $\bar{s}-\hat{s}$ precoding vector pairs in $Sub_{\rm IV}$ should be considered.

V) $Sub_{\rm V}$: The precoding vector pairs in $Sub_{\rm V}$ satisfy

$$\mathbf{H}_{12}\mathbf{w}\neq\mathbf{0}, \tag{31a}$$
$$\mathbf{H}_{21}\mathbf{v}=\mathbf{0}, \tag{31b}$$
$$\mathbf{G}_1\mathbf{v}=\mathbf{G}_2\mathbf{w}\neq\mathbf{0}. \tag{31c}$$

Substituting $\mathbf{v}=\mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{x}$ into (31c), we obtain

$$\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{x}=\mathbf{G}_2\mathbf{w}\neq\mathbf{0}. \tag{32}$$

Letting $\mathbf{A}=\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21})$, $\mathbf{B}=\mathbf{G}_2$, and applying *Proposition 1*(i), we obtain $\mathbf{x}$ which satisfies (32), i.e.,

$$\mathbf{x}=\breve{\mathbf{\Psi}}_{12}\breve{\mathbf{\Lambda}}_1^{-1}\mathbf{z}+\mathbf{\Gamma}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))\mathbf{z}_1.$$

Here, $\breve{\mathbf{\Psi}}_{12}$, $\breve{\mathbf{\Lambda}}_1$ and $\breve{s}$ (to be used below) correspond to the $\mathbf{\Psi}_{12}$, $\mathbf{\Lambda}_1$ and s of *Proposition 1*, and arise due to the GSVD of $(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))^H$ and $\mathbf{G}_2^H$. Thus, the linearly independent vectors in this subspace are of the form $\mathbf{\Gamma}(\mathbf{H}_{21})\breve{\mathbf{\Psi}}_{12}\breve{\mathbf{\Lambda}}_1^{-1}\mathbf{z}+\mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{\Gamma}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))\mathbf{z}_1$. Noting that the columns of $\mathbf{\Gamma}(\mathbf{H}_{21})\mathbf{\Gamma}(\mathbf{G}_1\mathbf{\Gamma}(\mathbf{H}_{21}))$ also span the solution space of $\mathbf{v}$ in $Sub_{\rm I}$, here we only consider the following precoding vectors:

$$\mathbf{v}=\mathbf{\Gamma}(\mathbf{H}_{21})\breve{\mathbf{\Psi}}_{12}\breve{\mathbf{\Lambda}}_1^{-1}\mathbf{z},\mathbf{w}=\breve{\mathbf{\Psi}}_{22}\breve{\mathbf{\Lambda}}_2^{-1}\mathbf{z}. \tag{33}$$

On combining (25a)-(25c) with (31a)-(31c), it holds that

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

By *Proposition 1*(ii), it holds that $d_{\rm III}+d_{\rm V}\le\breve{s}$. Thus, $d_{\rm V}\le\breve{s}-d_{\rm III}=\breve{s}-\hat{s}$. Among the last two subsets, $Sub_{\rm V}$ has higher priority than $Sub_{\rm VI}$. Thus, a number of $\breve{s}-\hat{s}$ precoding vector pairs in $Sub_{\rm V}$ should be considered.

VI) $Sub_{\rm VI}$: The precoding vector pairs in $Sub_{\rm VI}$ satisfy

$$\mathbf{H}_{12}\mathbf{w}\neq\mathbf{0}, \tag{34a}$$
$$\mathbf{H}_{21}\mathbf{v}\neq\mathbf{0}, \tag{34b}$$
$$\mathbf{G}_1\mathbf{v}=\mathbf{G}_2\mathbf{w}\neq\mathbf{0}. \tag{34c}$$

Letting $\mathbf{A}=\mathbf{G}_1$, $\mathbf{B}=\mathbf{G}_2$, and applying *Proposition 1*(i), we obtain $\mathbf{v}$ which satisfies (34c), i.e.,

$$\mathbf{v}=\tilde{\mathbf{\Psi}}_{12}\tilde{\mathbf{\Lambda}}_1^{-1}\mathbf{z}+\mathbf{\Gamma}(\mathbf{G}_1)\mathbf{z}_1.$$

Here, $\tilde{\mathbf{\Psi}}_{12}$, $\tilde{\mathbf{\Lambda}}_1$ and $\tilde{s}$ (to be used below) correspond to the $\mathbf{\Psi}_{12}$, $\mathbf{\Lambda}_1$ and s of *Proposition 1*, and arise due to the GSVD of $\mathbf{G}_1^H$ and $\mathbf{G}_2^H$. Noting that some of the basis vectors of $\mathbf{v}$, i.e., $\mathbf{\Gamma}(\mathbf{G}_1)$, also span the solution space of $\mathbf{v}$ in $Sub_{\rm I}\cup Sub_{\rm II}$, in $Sub_{\rm VI}$ we only consider the following precoding vectors,

$$\mathbf{v}=\tilde{\mathbf{\Psi}}_{12}\tilde{\mathbf{\Lambda}}_1^{-1}\mathbf{z},\mathbf{w}=\tilde{\mathbf{\Psi}}_{22}\tilde{\mathbf{\Lambda}}_2^{-1}\mathbf{z}. \tag{35}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

On combining (34a)-(34c) with (25a)-(25c), (28a)-(28c) and (31a)-(31c), it holds that $Sub_{\rm III} \cup Sub_{\rm IV} \cup Sub_{\rm V} \cup Sub_{\rm VI} = \{(\mathbf{v},\mathbf{w})|\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w} \neq \mathbf{0}\}$. By *Proposition 1*(ii), we have $d_{\rm III}+d_{\rm IV}+d_{\rm V}+d_{\rm VI} \leq \tilde{s}$, and so $d_{\rm VI} = \tilde{s}-(d_{\rm III}+d_{\rm IV}+d_{\rm V})$.

Based on the above discussion, and using (3d), Table I provides the number of linear independent vectors that should be considered in each subset, as function of the number of antennas.

A. 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 $(\mathbf{V},\mathbf{W})$. Since the pair S_2-D_2 does not communicate, we do not need to care about whether the message signal sent by S_1 interferes with D_2 or not. 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 the one from the last two subsets. If $N_d^1 \leq d_{\rm I}+d_{\rm II}+d_{\rm III}+d_{\rm IV}$, we just select N_d^1 precoding vector pairs from $Sub_{\rm I} \cup Sub_{\rm II} \cup Sub_{\rm III} \cup Sub_{\rm IV}$; otherwise, we first select all the precoding vector pairs in $Sub_{\rm I} \cup Sub_{\rm II} \cup Sub_{\rm III} \cup Sub_{\rm IV}$, and then we pick $\lfloor \frac{N_d^1-(d_{\rm I}+d_{\rm II}+d_{\rm III}+d_{\rm IV})}{2} \rfloor$ precoding vector pairs from $Sub_{\rm V} \cup Sub_{\rm VI}$. Summarizing, the maximum achievable value of d_s^1 is,

$$\bar{d}_s^1 = \min\{d_{a=1}+d_{a=2}^{\star}, N_d^1\}, \tag{36}$$

where $a \triangleq \mathrm{rank}\{\mathbf{H}_{11}\mathbf{v}\}+\mathrm{rank}\{\mathbf{H}_{12}\mathbf{w}\}$, $d_{a=1} = d_{\rm I}+d_{\rm II}+d_{\rm III}+d_{\rm IV}$, and

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

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 $d_{\rm I}=0$, $d_{\rm II}=0$, $d_{\rm III}=0$, $d_{\rm IV}=3$, $d_{\rm V}=0$, $d_{\rm VI}=3$. Since $N_d^1 = d_{\rm I}+d_{\rm II}+d_{\rm III}+d_{\rm IV}$, we first select three precoding vector pairs in $Sub_{\rm IV}$. We cannot pick any more precoding vector pairs without violating (18) since in that case the the remaining signal dimension at D_1 is $N_d^1 - d_{\rm IV} = 0$. 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 $d_{\rm I}=0$, $d_{\rm II}=1$, $d_{\rm III}=0$, $d_{\rm IV}=1$, $d_{\rm V}=2$, $d_{\rm VI}=2$. Since $N_d^1 > d_{\rm I}+d_{\rm II}+d_{\rm III}+d_{\rm IV}$, we first select all the precoding vector pairs in $Sub_{\rm II}$ and $Sub_{\rm IV}$, 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 $Sub_{\rm V}$ and $Sub_{\rm VI}$, we can at most pick one pair, i.e., $(\mathbf{v}_3,\mathbf{w}_3)$. For either $Sub_{\rm V}$ or $Sub_{\rm VI}$, 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, (18) would be violated. Concluding, we can select a total of 3 precoding vector pairs, and based on *Corollary 2*, $\bar{d}_s^1 = 3$.

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,

$$\bar{d}_s^2 = \min\{N_s^2, N_d^2\}. \tag{37}$$

B. 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,

$$\hat{d}_s^2(z) \leq (N_d^2-z)^+. \tag{38}$$

In addition, it holds that $\hat{d}_s^1 + \dim\{\mathrm{span}(\mathbf{H}_{12}\mathbf{W})\} \leq N_d^1$ due to (18). So,

$$\mathrm{rank}\{\mathbf{W}\} \leq (\max\{N_s^2, N_d^1\} - \hat{d}_s^1)^+. \tag{39}$$

Combining (37), (38) and (39), we get the maximum achievable value of d_s^2, i.e.,

$$\hat{d}_s^2(z) = \min\{N_s^2, (\max\{N_s^2, N_d^1\}-\hat{d}_s^1)^+, (N_d^2-z)^+\}. \tag{40}$$

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 $(\hat{d}_s^1 - (d_{\rm V}+d_{\rm I}+d_{\rm III}))^+$. Due to the constraint $d_s^1 = \hat{d}_s^1$ and the fact that $a=2$ for the precoding vector pairs from $Sub_{\rm V}$, we have limitations on the number of pairs that can be selected from $Sub_{\rm V}$. For example, consider the case $d_{\rm I}+d_{\rm III}=2$, $d_{\rm V}=2$, $N_d^1=3$ 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 to choose at least one pair from $Sub_{\rm V}$. Noting that (18) should be satisfied for $(\mathbf{V},\mathbf{W}) \in \hat{\mathcal{I}}$ and $a=2$ for the pairs from $Sub_{\rm V}$, if we have picked one pair from $Sub_{\rm V}$, 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 $a=2$ for the precoding vector pairs from $Sub_{\rm V}$, we cannot select any pairs from $Sub_{\rm V}$, and so the minimum value of z equals 1.

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

$$\begin{aligned} y_{\max} \triangleq \max_{x,y}\ & y \\ \text{s.t.}\ & x+y = \hat{d}_s^1, && \text{(41a)} \\ & x+2y \leq N_d^1, && \text{(41b)} \\ & 0 \leq x \leq d_{\rm I}+d_{\rm II}+d_{\rm III}+d_{\rm IV}, && \text{(41c)} \\ & 0 \leq y \leq d_{\rm V}+d_{\rm VI}. && \text{(41d)} \end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

Substituting $x = \hat{d}_s^1 - y$ into (41b), we arrive at $y \leq N_d^1 - \hat{d}_s^1$, which combined with (41c) and (41d) gives

$$y_{\max} = \min\{N_d^1 - \hat{d}_s^1, d_{\rm V} + d_{\rm VI}, \hat{d}_s^1\}. \tag{42}$$

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

$$z_{\min}(\hat{d}_s^1) = (\hat{d}_s^1 - (\min\{y_{\max}, d_{\rm V}\} + d_{\rm I} + d_{\rm III}))^+. \tag{43}$$

Substituting (43) into (40), we obtain the maximum value of d_s^2, i.e.,

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

Remark 2: For any given values of d_s^1, we can derive a maximum achievable value of d_s^2 based on (44). 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 (44);
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 (44), 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 (44), 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 $(\hat{d}_s^1, \hat{d}_s^2) = (2, 4)$.

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

As shown in Fig. 3, *E*1 and *E*2 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 E*1($\bar{d}_s^1$, $\underline{d}_s^2$). According to (36), 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 (42)-(44), we arrive at

$$\underline{d}_s^2 = \min\{N_s^2, (\max\{N_s^2, N_d^1\} - \bar{d}_s^1)^+, (N_d^2 - z_{\min}(\bar{d}_s^1))^+\}. \tag{45}$$

*2) The ending point E*2($\underline{d}_s^1$, $\bar{d}_s^2$). According to the previous analysis on the single-user point of *SU*2(0, $\bar{d}_s^2$), we obtain $\bar{d}_s^2 = \min\{N_s^2, N_d^2\}$, which, combined with (40), gives

$$\min\{N_s^2, N_d^2\} \leq \max\{N_s^2, N_d^1\} - \underline{d}_s^1, \tag{46a}$$
$$\min\{N_s^2, N_d^2\} \leq N_d^2 - z. \tag{46b}$$

In the following, we consider two distinct cases.

(i) For the case of $N_s^2 > N_d^2$, (46a) becomes

$$\underline{d}_s^1 \leq \max\{N_s^2, N_d^1\} - N_d^2. \tag{47}$$

Besides, (46b) indicates that $z = 0$, and thus all of the signal steams sent by S_1 should not interfere with D_2. That is, $Sub_{\rm II}$, $Sub_{\rm IV}$ and $Sub_{\rm VI}$ are not under consideration. Applying (36), we obtain

$$\underline{d}_s^1 \leq \min\{d_{\rm I} + d_{\rm III} + \beta^\star, N_d^1\}, \tag{48}$$

where $\beta^\star = \min\{d_{\rm V}, \lfloor (N_d^1 - d_{\rm I} - d_{\rm III})^+/2 \rfloor\}$. Combining (47) and (48), we arrive at

$$\underline{d}_s^1 = \min\{d_{\rm I} + d_{\rm III} + \beta^\star, \max\{N_s^2, N_d^1\} - N_d^2, N_d^1\}. \tag{49}$$

(ii) For the case of $N_s^2 \leq N_d^2$, (46a) becomes

$$\underline{d}_s^1 \leq \max\{N_s^2, N_d^1\} - N_s^2, \tag{50}$$

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 $d_{\rm III} = d_{\rm IV} = 0$. In addition, (46b) indicates that $z \leq N_d^2 - N_s^2$. Therefore, $\xi = \min\{d_{\rm VI}, (N_d^2 - N_s^2 - d_{\rm II})^+\} + d_{\rm V}$, where ξ denotes the maximum number of precoding vector pairs that can be chosen from $Sub_{\rm V}$ and $Sub_{\rm VI}$. Applying (36), we get

$$\underline{d}_s^1 \leq \min\{d_{\rm I} + \hat{d}_{\rm II} + \xi^\star, N_d^1\}, \tag{51}$$

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

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

Combining (50) and (51), we arrive at

$$\underline{d}_s^1 = \min\{d_{\rm I} + \hat{d}_{\rm II} + \xi^\star, \max\{N_s^2, N_d^1\} - N_s^2\}. \tag{53}$$

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

$$\underline{d}_s^1 = \begin{cases} \min\{d_{\rm I} + d_{\rm III} + \beta^\star, \eta - N_d^2, N_d^1\}, \text{if } N_s^2 > N_d^2 \\ \min\{d_{\rm I} + \hat{d}_{\rm II} + \xi^\star, \eta - N_s^2\}, \text{if } N_s^2 \leq N_d^2 \end{cases} \tag{54}$$

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

TABLE II: 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 $u = \min\{\hat{d}_s^1, \min\{y_{\max}, d_{\rm V}\} + d_{\rm I} + d_{\rm III}\}$, $t = \hat{d}_s^1 - u$;
2. $(\mathbf{V}_{\rm o}, \mathbf{W}_{\rm o}) \leftarrow$ select u precoding vector pairs from $Sub_{\rm o}$;
3. $(\mathbf{V}_{\rm e}, \mathbf{W}_{\rm e}) \leftarrow$ select t precoding vector pairs from $Sub_{\rm e}$;
4. $\mathbf{V} \leftarrow [\mathbf{V}_{\rm o}\ \mathbf{V}_{\rm e}]$;
5. $\mathbf{W}_1 \leftarrow [\mathbf{W}_{\rm o}\ \mathbf{W}_{\rm e}]$;
6. Let $\check{d}_s^2 = \hat{d}_s^2 - \text{rank}(\mathbf{W}_1)$;
7. **if** $\check{d}_s^2 > 0$
8. Let $\tilde{d}_s^2 = \min\{\check{d}_s^2, (N_s^2 - N_d^1)^+\}$;
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. $\mathbf{W} \leftarrow [\mathbf{W}_1\ \mathbf{W}_2\ \mathbf{R}(:, 1 : \check{d}_s^2 - \tilde{d}_s^2)]$;
12. **else**
13. $\mathbf{W} \leftarrow \mathbf{W}_1$;
14. **end**
15. **Output:** $(\mathbf{V}, \mathbf{W})$.

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

achieve the S.D.o.F. pairs on the S.D.o.F. region boundary. In particular, by selecting $u = \min\{\hat{d}_s^1, \min\{y_{\max}, d_{\rm V}\} + d_{\rm I} + d_{\rm III}\}$ pairs from $Sub_{\rm o} \triangleq Sub_{\rm I} \cup Sub_{\rm III} \cup Sub_{\rm V}$ and $t = \hat{d}_s^1 - u$ pairs from $Sub_{\rm e} \triangleq Sub_{\rm II} \cup Sub_{\rm IV} \cup Sub_{\rm VI}$, subject to the number of pairs selected from $Sub_{\rm V} \cup Sub_{\rm VI}$ 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. (44)), interference-free subspace for D_2. Further, if $\hat{d}_s^2 \le \text{rank}(\mathbf{W}(:, 1:K_v))$, 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 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) $\mathbf{H}_{22} = \mathbf{USR}^H$. 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 $u = 2$, $d_{\rm I} = d_{\rm III} = 0$ and $d_{\rm V} = 2$, we first select two precoding vector pairs in $Sub_{\rm V}$, 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 $\mathbf{H}_{11}\mathbf{v}_1 \neq 0$, $\mathbf{H}_{11}\mathbf{v}_2 \neq 0$, $\mathbf{H}_{12}\mathbf{w}_4 \neq 0$ and $\mathbf{H}_{22}\mathbf{w}_i \neq 0, i = 1, \cdots, 4$, 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 II. 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 (20), (23), (27), (30), (33) and (35), respectively.

Remark 3: In light of (13a) and (13b) 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 $(\mathbf{VA}, \mathbf{WB})$ 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.

VII. Numerical Results

In this section, we conduct simulations to validate our theoretical findings. The results are obtained over $100,000$

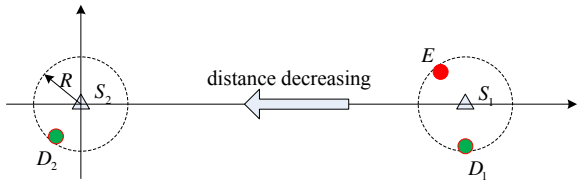

Fig. 4: Model used for numerical experiments.

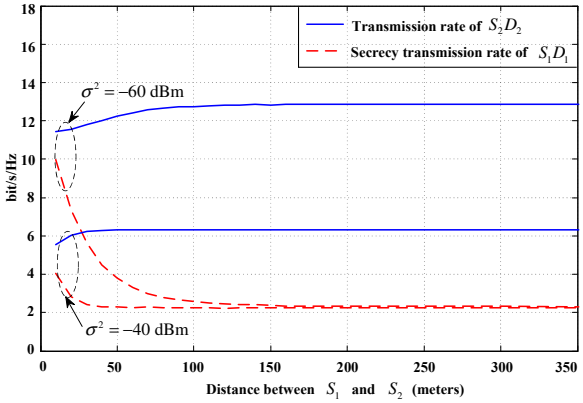

Fig. 5: Average achievable rates versus S_1-S_2 distance.

Monte Carlo runs as follows. We consider a system model as illustrated in Fig. 4. For simplicity, we consider antenna numbers $N_s^1 = N_d^1 \triangleq N_1$, and $N_s^2 = N_d^2 \triangleq N_2$. In each run, we place D_i and E uniformly at random on a ring of radius $1 \le R \le 10$ (unit: meters) and center located at S_i. The channels are modeled as multipath flat fading. The effect of the channel between any transmit-receive pair on the transmitted signal is modeled by a multiplicative scalar of the form $d^{-c/2}e^{j\theta}$ [36], where d is the distance between the two terminals, c is the path loss exponent and θ is a random phase, which is taken to be uniformly distributed within $[0, 2\pi)$. The value of c is typically in the range of 2 to 4. In our simulations we set $c = 3.5$. We assume that the distances of different combinations of transmit-receive antennas corresponding to the same link are the same, and as such the corresponding path loss is the same. S_2 is located at a point (0,0) (unit: meters), while S_1 moves from (350,0) to (10,0). The transmit power is $P = 0$dBm.

Fig. 5 illustrates the average achievable secrecy transmission rate of the user S_1-D_1, and also the average achievable transmission rate of the user S_2-D_2 as function of the S_1-S_2 distance. Here, we set $N_1 = 4$, $N_2 = 2$ and $N_e = 5$. Two different noise power levels are considered, i.e., $\sigma^2 = -60$dBm and $\sigma^2 = -40$dBm. According to (44), 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 II, and compute the achievable transmission rate of each user according to (8) and (9), respectively. Exact knowledge of the channels is assumed in the computation. It can be seen in Fig. 5 that the average achievable secrecy transmission rate of S_1-D_1 increases monotonically as S_1 moves close to S_2. In contrast, the average achievable transmission rate of S_2-D_2 decreases with a decrease in the S_1-S_2 distance. As compared with the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

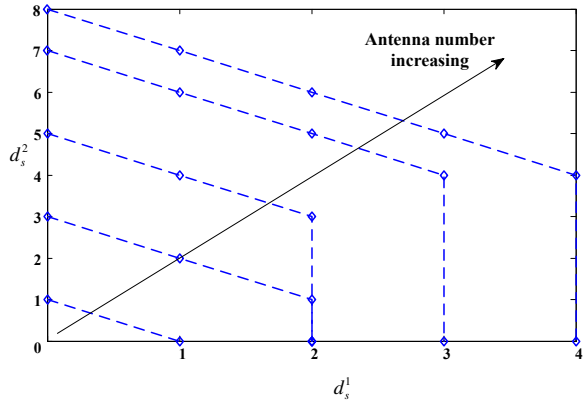

Fig. 6: Achievable secrecy degrees of freedom region with an increasing number of antennas at S_2-D_2. $N_1 = 4$, $N_e = 4$.

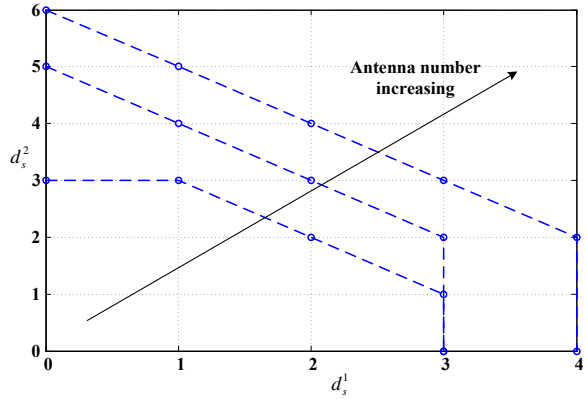

Fig. 7: Achievable secrecy degrees of freedom region with an increasing number of antennas at S_2-D_2. $N_1 = 4$, $N_e = 2$.

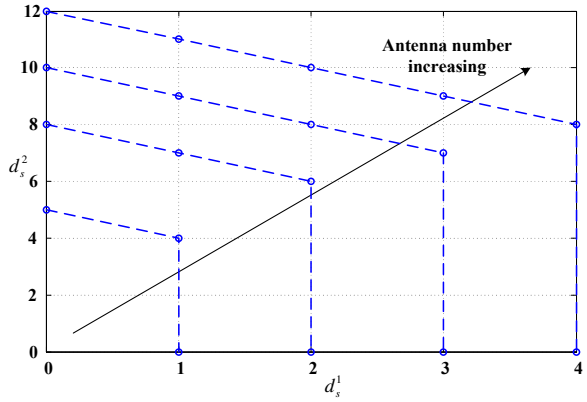

Fig. 8: Achievable secrecy degrees of freedom region with an increasing number of antennas at S_2-D_2. $N_1 = 4$, $N_e = 8$.

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. This should be expected, since the receive SNR at both E and D_1 reduces as S_1 moves close to S_2. In addition, we have designed the precoding matrices at S_1 and S_2, such that at E the signals received from S_1 and S_2 are aligned into a common subspace, while at D_1, the signals received from S_1 and S_2 are aligned into different subspaces. Therefore, the degradation of SNR at E would be more severe than the degradation at D_1.

Fig. 6, 7 and 8 illustrate the achievable secrecy degrees of freedom region with an increasing value of N_2, for different ratios of N_1/N_e. We compute the achievable secrecy degrees of freedom region according to (44). As expected, the secrecy degrees of freedom region expands with an increasing N_2. Note that previous work [37] 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, one can see that, for each case, by exploiting CCI an S.D.o.F. of N_1 can be achieved as long as N_2 is large enough. One can see that there is no non-strict S.D.o.F. region boundary for the second user in Fig. 6 and 8. This can be explained as follows. For the case of $N_s^1 = N_d^1 \leq N_e$ and $N_s^2 = N_d^2 = N_2$, (46b) becomes $z \leq 0$. Thus, the message sent by S_1 should fall in the null space of $\mathbf{H}_{21}$, which is impossible for the case of $N_1 \leq N_2$. In addition, for the case of $N_1 > N_2$, by Sec. V we see that the subsets with $\mathbf{v}$ satisfying $\mathbf{H}_{21}\mathbf{v} = \mathbf{0}$, i.e., Sub_{III} and Sub_{V}, are empty since it holds that $(N_s^1 - N_d^2)^+ + N_s^2 \leq N_e$. Concluding, for both cases it holds that $\underline{d}_s^1 = 0$, and no non-strict S.D.o.F. region boundary point exists for the second user.

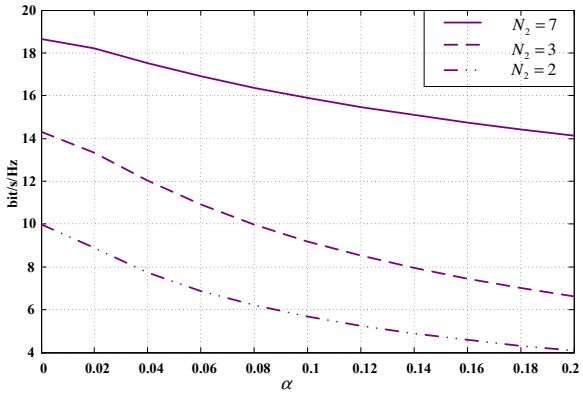

Fig. 9: Average achievable secrecy rate of S_1-D_1 versus the uncertainty of the eavesdropper's channels α. $N_1 = 4$, $N_e = 5$.

A. The achievable secrecy rate of S_1-D_1 with Imperfect CSI

In practice, perfect channel estimates, and in particular channel phase estimates are difficult to obtain. Since the proposed precoding matrix design highly depends on the eavesdropper channels, we next examine the secrecy rate performance in the presence of imperfect eavesdropper channel estimates. We model imperfect CSI through a Gauss-Markov uncertainty of the form [38]

$$\mathbf{G}_i = d_{ei}^{-c/2}\left(\sqrt{1-\alpha^2}\bar{\mathbf{G}}_i + \alpha\Delta\bar{\mathbf{G}}_i\right), \qquad (55)$$

where $0 \leq \alpha \leq 1$ denotes the channel uncertainty. $\alpha = 0$ and $\alpha = 1$ correspond to perfect channel knowledge and no CSI knowledge, respectively. 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. S_1 and S_2 are located at (10,0) and (0,0), respectively. The noise power $\sigma^2 = -60$dBm. According to (44), we see that the S.D.o.F. pairs (1,1), (2,2) and (3,4) can be achieved for the case of $N_2 = 2$, $N_2 = 3$ and $N_2 = 7$, respectively. For these S.D.o.F. pairs, we construct the precoding matrices $\mathbf{V}$ and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

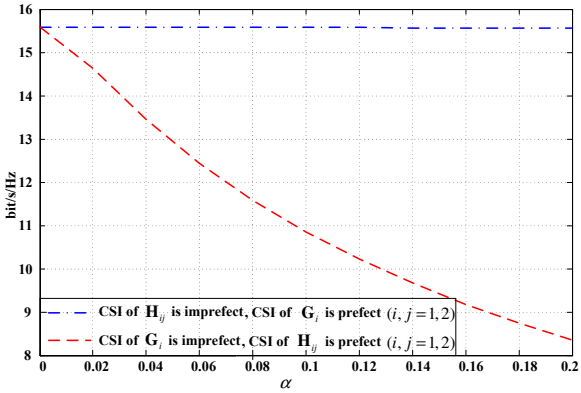

Fig. 10: Average achievable secrecy rate of S_1-D_1 versus the channel uncertainty α. $N_1 = N_e = 4$, $N_2 = 2$.

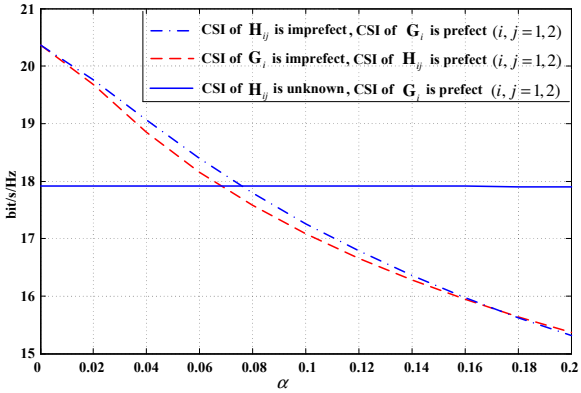

Fig. 11: Average achievable secrecy rate of S_1-D_1 versus the channel uncertainty α. $N_1 = N_e = 4$, $N_2 = 6$.

$\mathbf{W}$ according to Table II with the estimated channels, subject to power being equally allocated between different signal streams. The achievable secrecy transmission rate is computed according to (8). It can be observed that the average achievable secrecy rate drops with the increase of channel uncertainty. Fortunately, when the number of antennas N_2 increases, this secrecy rate performance degradation is smaller. On the other hand, on comparing the average secrecy transmission rate of S_1-D_1 for the case $N_2 = 2$ with that in Fig. 5, one can see that the average secrecy rate achieved for the case where $\alpha = 0.1$ and S_1-S_2 distance of 10 meters, is almost equal to the average secrecy rate achieved for the case where $\alpha = 0$ and S_1-S_2 distance of 50 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.

In Fig. 10 and 11, we compare the average achievable secrecy rate of S_1-D_1 for the case in which $\mathbf{G}_j$, $j = 1, 2$, are imperfect and that for the case in which $\mathbf{H}_{ij}$, $i = 1, 2$, $j = 1, 2$, are imperfect. The same model as in (55) was used. According to (44), the S.D.o.F. pairs (2,0) and (3,3) can be achieved for the case of $N_2 = 2$ and $N_2 = 6$, respectively. The precoding matrix pairs and the corresponding achievable secrecy rate are computed in the same way as in Fig. 9. One can see that when $N_s^2 \leq N_d^1$, the achievable secrecy rate degrades sharply with the increase of the eavesdropper's channel uncertainty, while it remains unchanged with the increase of the legitimate channels' uncertainty. On the other hand, when $N_s^2 > N_d^1$, the achievable secrecy rate degrades sharply with α for both the eavesdropper and legitimate channel uncertainties. From Table II, one can see that in addition to $\mathbf{G}_1$ and $\mathbf{G}_2$, the other factors that would affect the resulted precoding matrices are $\mathbf{\Gamma}(\mathbf{H}_{12})$, $\mathbf{\Gamma}(\mathbf{H}_{21})$ and $\mathbf{H}_{22}$. The channels $\mathbf{H}_{21}$ and $\mathbf{H}_{22}$ will only affect the achievable transmission rate of S_2-D_2, since in the proposed scheme we only care about the number of linear independent signal streams received at D_1. For the case of $N_s^2 \leq N_d^1$, $\mathbf{H}_{12}$ does not enter in the construction of the precoding matrices, and so the proposed scheme is robust to the legitimate channel estimate error.

We should note that when $\mathbf{H}_{ij}$, $i = 1, 2$, $j = 1, 2$ are unknown, by some slight changes the proposed scheme still works. When $\mathbf{H}_{12}$ and $\mathbf{H}_{21}$ are unknown, we are not able to obtain a precoding vector with which the message signal does not interfere with the unintended user, and so in Table I, $d_{\mathrm{I}} = d_{\mathrm{III}} = d_{\mathrm{IV}} = d_{\mathrm{V}} = 0$, $d_{\mathrm{II}} = (N_s^1 - N_e)^+$ and $d_{\mathrm{VI}} = d_s$. In addition, (40) becomes

$$\hat{d}_s^2 = \min\{N_s^2, (N_d^1 - \hat{d}_s^1)^+, (N_d^2 - \hat{d}_s^1)^+\}, \qquad (56)$$

based on which we can obtain the boundary point of the achievable S.D.o.F. region. Substituting these results into Table II, we are able to construct a precoding matrix pair achieving S.D.o.F. pairs on the S.D.o.F. region boundary. According to (56), one can see that for the case $N_1 = N_e = 4$ and $N_2 = 6$ the S.D.o.F. pair (2,2) can be achieved. For this S.D.o.F. pair, we compute the precoding matrix pair and plot the average achievable secrecy rate of S_1-D_1 in Fig. 11. As expected, the average achievable secrecy rate remains unchanged with an increasing α.

Concluding, one can see that the eavesdropper's channel uncertainty is more dangerous. This should be expected, as in the proposed scheme, the achievable secrecy rate of S_1-D_1 depends directly on $\mathbf{G}_1$ and $\mathbf{G}_2$, but only on the null space of $\mathbf{H}_{12}$.

B. Comparison of a special case of the proposed scheme with existing schemes in terms of the average achievable secrecy rate of $\mathrm{S_1}$-$\mathrm{D_1}$

When 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, our system model reduces to a wiretap channel with a cooperative jammer. This kind of wiretap channel is considered in [3] and [8], where several iterative algorithms are proposed for maximizing the achievable secrecy rate. In Fig. 12, we plot the average achievable secrecy rate of S_1-D_1 versus the S_1-S_2 distance. The noise power $\sigma^2 = -60$dBm is considered. To reduce computation time (the method of [3] is time-assuming since it involves numerical search), in this simulation we assume that D_1 and E are respectively located right above and right below S_1, with a distance of 10 meters from S_1. D_2 is located right below S_2, with a distance of 10 meters from S_2. In the proposed scheme, we assume that each transmitter has an average transmit power constraint of P. In contrast, the work of [3] considers a sum transmit power constraint at the source and the helper. For

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

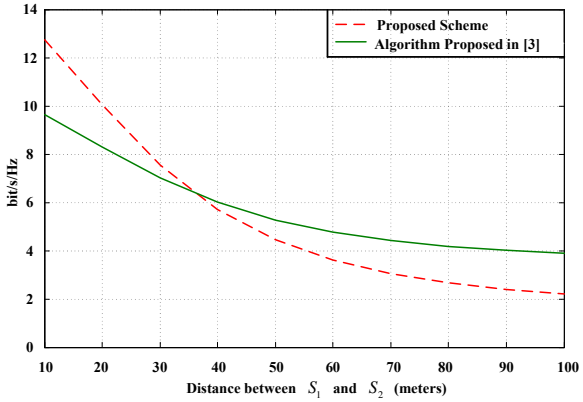

Fig. 12: Average achievable secrecy rate of S_1-D_1 versus S_1-S_2 distance. $N_1 = 4$, $N_e = 5$ and $N_2 = 6$.

the sake of fairness, we set the sum transmit power constraint as $2P$. The secrecy rate maximization method proposed by [3] is derived under a power covariance constraint, and so we maximize the achievable secrecy rate over 100 randomly selected power covariance matrices $\mathbf{S}$. According to (36), a single-user S.D.o.F. $\bar{d}_s^1 = 2$ can be achieved. For this S.D.o.F., we construct the precoding matrices $\mathbf{V}$ and $\mathbf{W}$ according to Table II.

One can see that the average achievable secrecy transmission rate by both schemes increases monotonically as S_1 moves close to S_2. Moreover, when the distance between S_1 and S_2 is short our proposed scheme outperforms that of [3], while for longer distances the method of [3] achieves higher average secrecy rate. This should be expected, as the proposed scheme is optimal in terms of S.D.o.F., which indicates that it is near-optimal in terms of secrecy rate performance in the high SNR regime, and a longer distance of S_1-S_2 indicates a severer path loss, which corresponds to a smaller receive SNR. The method of [3] involves numerical search for maximizing the achievable secrecy rate over the power allocation between transmitters, and also the covariance matrix $\mathbf{S}$, subject to an average power constraint $\mathrm{tr}\{\mathbf{S}\} \leq 2P$. In contrast, the proposed scheme provides closed-form precoding matrices, and the method for constructing precoding matrix pairs, given in Table II, at most involves four GSVDs, four SVDs and three matrix multiplications, with the dimension of matrices no greater than $\max\{N_s^1, N_s^2, N_d^1, N_d^2, N_e\} \times \max\{N_s^1, N_s^2, N_d^1, N_d^2, N_e\}$. Thus, the proposed scheme has a computational advantage of the scheme of [3]. We should note that since the algorithm proposed by [8] also involves numerical search and no global optimal solution can be guaranteed, the comparison of our work with [8] would be similar as that with [3].

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. As expected, the secrecy rate degradation due to CSI estimate error can be counteracted by bringing the two users closer together.

In this work, we have assumed that the noise at the receivers is Gaussian, in which case the optimal signaling at the source is Gaussian. However, due to some real-world constraints, such as the use of discrete constellations, the inputs are non-Gaussian (see [39] and references therein). Thus, further work is needed to take non-Gaussian inputs into account. Also, we have considered equal power allocation between different signal streams, and the precoding matrix pair derived is asymptotically optimal in the high SNR regimes. One could consider the optimal power allocation strategies, which could improve the secrecy rate performance in the low SNR regimes.

Appendix A
Proof of *Proposition 1*

By 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, $\mathbf{A}\mathbf{v} = \mathbf{B}\mathbf{w}$ holds true if $\mathbf{v}$ and $\mathbf{w}$ are given by (5a) and (5b), respectively. Next, we prove by contradiction that $\mathbf{A}\mathbf{v} = \mathbf{B}\mathbf{w}$ holds true only if $\mathbf{v} \in \mathrm{span}(\mathbf{\Phi}_1)$, where $\mathbf{\Phi}_1 \triangleq \left[\begin{array}{cc} \mathbf{\Psi}_{12}\mathbf{\Lambda}_1^{-1} & \mathbf{\Gamma}(\mathbf{A}) \end{array}\right]$; the argument for $\mathbf{w}$ is similar. Assume that there exists a nonzero vector $\bar{\mathbf{v}} \notin \mathrm{span}(\mathbf{\Phi}_1)$ satisfying $\mathbf{A}\bar{\mathbf{v}} = \mathbf{B}\mathbf{w}$. 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 $\mathbf{A}\bar{\mathbf{v}} = \mathbf{B}\mathbf{w}$. In addition, by the GSVD decomposition $\mathrm{span}(\mathbf{X}_2) = \mathrm{span}(\mathbf{A}\mathbf{\Phi}_1)$. Thus, $\mathbf{A}\bar{\mathbf{v}} \in \mathrm{span}(\mathbf{A}\mathbf{\Phi}_1)$, which contradicts with $\mathbf{A}\bar{\mathbf{v}} \notin \mathrm{span}(\mathbf{A}\mathbf{\Phi}_1)$. This completes the proof of the first conclusion.

According to the GSVD, $\mathbf{A}\mathbf{\Psi}_{11} = \mathbf{0}$. Thus, $\mathrm{span}(\mathbf{\Psi}_{11}) \subset \mathrm{span}(\mathbf{\Gamma}(\mathbf{A}))$. In addition, $\mathrm{rank}(\mathbf{\Psi}_{11}) = M - r - s = M - \min\{M, N\} = (M - N)^+$, which indicates that the linear independent vectors in $\mathrm{span}(\mathbf{\Psi}_{11})$ is the same as that in $\mathrm{span}(\mathbf{\Gamma}(\mathbf{A}))$. So, $\mathrm{span}(\mathbf{\Psi}_{11}) = \mathrm{span}(\mathbf{\Gamma}(\mathbf{A}))$. Since $\mathbf{\Psi}_1$ is an unitary matrix, it holds that $\mathrm{span}(\mathbf{\Psi}_{12}) \cap \mathrm{span}(\mathbf{\Psi}_{11}) = \mathbf{0}$. Therefore, $\mathrm{span}(\mathbf{\Psi}_{12}) \cap \mathrm{span}(\mathbf{\Gamma}(\mathbf{A})) = \mathbf{0}$, which, combined with (5a), indicates that the number of linearly independent vectors $\mathbf{v}$ satisfying $\mathbf{A}\mathbf{v} = \mathbf{B}\mathbf{w} \neq \mathbf{0}$ is $s + \dim\{\mathrm{null}(\mathbf{A})\}$. 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 $\mathrm{tr}\{\bar{\mathbf{Q}}_v\} = \mathrm{tr}\{\bar{\mathbf{Q}}_w\} = 1$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

Correspondingly, (10a) can be rewritten as

$$R_d^1 = \log|\mathbf{I} + (\mathbf{I} + P\mathbf{H}_{12}\bar{\mathbf{Q}}_w\mathbf{H}_{12}^H)^{-1}\mathbf{H}_{11}\bar{\mathbf{Q}}_v\mathbf{H}_{11}^H P|. \quad (57)$$

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 (57), we obtain

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

Therefore,

$$\begin{aligned}&\lim_{P\to\infty} R_d^1/\log(P)\\ =&\lim_{P\to\infty}\frac{\log|\mathbf{I} + \mathbf{U}_1(\mathbf{\Sigma}_1)^{-1}\mathbf{U}_1^H\mathbf{\Theta}_2 + \mathbf{U}_0\mathbf{U}_0^H\mathbf{\Theta}_2 P|}{\log(P)}\\ =&\lim_{P\to\infty}\frac{\log|\mathbf{I} + (\frac{1}{P}\mathbf{U}_1(\mathbf{\Sigma}_1)^{-1}\mathbf{U}_1^H + \mathbf{U}_0\mathbf{U}_0^H)\mathbf{\Theta}_2 P|}{\log(P)}\\ =&\lim_{P\to\infty}\frac{\log|\mathbf{I} + \mathbf{U}_0\mathbf{U}_0^H\mathbf{H}_{11}\mathbf{V}\mathbf{V}^H\mathbf{H}_{11}^H|}{\log(P)}\\ =&\mathrm{rank}\{\mathbf{U}_0\mathbf{U}_0^H\mathbf{H}_{11}\mathbf{V}\mathbf{V}^H\mathbf{H}_{11}^H\} \quad (58)\\ =&\dim\{\mathrm{span}(\mathbf{H}_{11}\mathbf{V})\setminus\mathrm{span}(\mathbf{H}_{12}\mathbf{W})\} \quad (59)\end{aligned}$$

where (58) 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 $\mathbf{A}$. (59) comes from the fact that $\mathbf{U}_0\mathbf{U}_0^H$ is the projection matrix of the subspace $\mathrm{span}(\mathbf{H}_{12}\mathbf{W})^\perp$.

Applying similar derivations from (57) to (59) yields

$$\lim_{P\to\infty}\frac{R_d^2}{\log(P)} = \dim\{\mathrm{span}(\mathbf{H}_{22}\mathbf{W})\setminus\mathrm{span}(\mathbf{H}_{21}\mathbf{V})\}, \quad (60)$$

$$\lim_{P\to\infty}\frac{R_e}{\log(P)} = \dim\{\mathrm{span}(\mathbf{G}_1\mathbf{V})\setminus\mathrm{span}(\mathbf{G}_2\mathbf{W})\}. \quad (61)$$

Substituting (59)-(61) into (12), we arrive at (13a) and (13b). 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 will show that for any given precoding matrices $(\mathbf{V},\mathbf{W}) \in \mathcal{I}$, we can always find another precoding matrix pair $(\mathbf{V}',\mathbf{W}) \in \bar{\mathcal{I}}$, which satisfy $d_s^1(\mathbf{V},\mathbf{W}) \le d_s^1(\mathbf{V}',\mathbf{W})$ and $d_s^2(\mathbf{V},\mathbf{W}) \le d_s^2(\mathbf{V}',\mathbf{W})$. 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 $\bar{\mathcal{D}}$.

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

Firstly, by letting $\mathbf{A} = \mathbf{H}_{12}\mathbf{W}$, $\mathbf{B} = \mathbf{H}_{11}\mathbf{V}$, and applying the GSVD decomposition in Sec. II, we arrive at

$$\begin{aligned}d_s^1(\mathbf{V},\mathbf{W}) &= n(\mathbf{V},\mathbf{W}) - m(\mathbf{V},\mathbf{W})\\ &= \mathrm{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\mathbf{\Psi}}_{21}\} - m(\mathbf{V},\mathbf{W}) \quad (62a)\\ &\le \mathrm{rank}\{\mathbf{H}_{11}\mathbf{V}\hat{\mathbf{\Psi}}_{21}\} - m(\mathbf{V}\hat{\mathbf{\Psi}}_{21},\mathbf{W}), \quad (62b)\end{aligned}$$

where (62b) holds true due to $m(\mathbf{V},\mathbf{W}) \ge m(\mathbf{V}\hat{\mathbf{\Psi}}_{21},\mathbf{W})$. Here, $\hat{\mathbf{\Psi}}_{21}$ corresponds to $\mathbf{\Psi}_{21}$, and arises due to the GSVD of $(\mathbf{H}_{12}\mathbf{W})^H$ and $(\mathbf{H}_{11}\mathbf{V})^H$. Let $\hat{\mathbf{V}} = \mathbf{V}\hat{\mathbf{\Psi}}_{21}$, and then $\mathrm{span}(\mathbf{H}_{11}\hat{\mathbf{V}}) \cap \mathrm{span}(\mathbf{H}_{12}\mathbf{W}) = \mathbf{0}$.

Secondly, by letting $\mathbf{A} = \mathbf{G}_2\mathbf{W}$, $\mathbf{B} = \mathbf{G}_1\hat{\mathbf{V}}$, and applying the GSVD decomposition in Sec. II, we arrive at

$$\begin{aligned}&\mathrm{rank}\{\mathbf{H}_{11}\hat{\mathbf{V}}\} - m(\hat{\mathbf{V}},\mathbf{W})\\ &= \mathrm{rank}\{\mathbf{H}_{11}\hat{\mathbf{V}}\} - \mathrm{rank}\{\breve{\mathbf{\Psi}}_{21}\} \quad (63a)\\ &\le \mathrm{rank}\{\mathbf{H}_{11}\hat{\mathbf{V}}\breve{\mathbf{\Psi}}_2^1\}. \quad (63b)\end{aligned}$$

where $\breve{\mathbf{\Psi}}_2^1 \triangleq [\breve{\mathbf{\Psi}}_{22}\ \breve{\mathbf{\Psi}}_{23}]$. Here, $\breve{\mathbf{\Psi}}_{21}$, $\breve{\mathbf{\Psi}}_{22}$ and $\breve{\mathbf{\Psi}}_{23}$ correspond to $\mathbf{\Psi}_{21}$, $\mathbf{\Psi}_{22}$ and $\mathbf{\Psi}_{23}$, and arise due to the GSVD of $(\mathbf{G}_2\mathbf{W})^H$ and $(\mathbf{G}_1\hat{\mathbf{V}})^H$. (63b) holds true, because $\mathrm{rank}\{\mathbf{H}_{11}\hat{\mathbf{V}}\} \le \mathrm{rank}\{\mathbf{H}_{11}\hat{\mathbf{V}}\breve{\mathbf{\Psi}}_2^1\} + \mathrm{rank}\{\mathbf{H}_{11}\hat{\mathbf{V}}\breve{\mathbf{\Psi}}_{21}\}$ and $\mathrm{rank}\{\mathbf{H}_{11}\hat{\mathbf{V}}\breve{\mathbf{\Psi}}_{21}\} \le \mathrm{rank}\{\breve{\mathbf{\Psi}}_{21}\}$.

Let $\mathbf{V}' = \hat{\mathbf{V}}\breve{\mathbf{\Psi}}_2^1$. Then, $\mathrm{span}(\mathbf{G}_1\mathbf{V}') \subset \mathrm{span}(\mathbf{G}_2\mathbf{W})$ and $\mathrm{span}(\mathbf{H}_{11}\mathbf{V}') \cap \mathrm{span}(\mathbf{H}_{12}\mathbf{W}) = \mathbf{0}$. Thus, $(\mathbf{V}',\mathbf{W}) \in \bar{\mathcal{I}}$, which combined with *Corollary 2*, indicates that

$$d_s^1(\mathbf{V}',\mathbf{W}) = \mathrm{rank}\{\mathbf{H}_{11}\mathbf{V}'\}.$$

In addition, combining (62a)-(62b) with (63a)-(63b), we have

$$d_s^1(\mathbf{V},\mathbf{W}) \le \mathrm{rank}\{\mathbf{H}_{11}\mathbf{V}'\}.$$

So, $d_s^1(\mathbf{V},\mathbf{W}) \le d_s^1(\mathbf{V}',\mathbf{W})$. Besides, since $\mathrm{span}(\mathbf{H}_{21}\mathbf{V}') \subset \mathrm{span}(\mathbf{H}_{21}\mathbf{V})$, it holds that $d_s^2(\mathbf{V},\mathbf{W}) \le d_s^2(\mathbf{V}',\mathbf{W})$. 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 $\mathrm{rank}\{\mathbf{G}_2\mathbf{W}\} = \min\{K_w, N_e\}$.

In the following, we consider two distinct cases.

(i) For the case of $K_w \ge N_e$, it holds that $\mathrm{rank}\{\mathbf{G}_2\mathbf{W}\} = N_e$. Denote $\mathbf{G}_2\mathbf{W} = [\mathbf{U}_1\ \mathbf{U}_0]\begin{bmatrix}\mathbf{\Sigma}_1 & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}\begin{bmatrix}\mathbf{T}_1^H\\ \mathbf{T}_0^H\end{bmatrix}$ 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,

$$\mathbf{G}_1\mathbf{V} = \mathbf{G}_2\mathbf{W}\mathbf{T}_1(\mathbf{G}_2\mathbf{W}\mathbf{T}_1)^{-1}\mathbf{G}_1\mathbf{V} = \mathbf{G}_2\mathbf{W}\mathbf{B}. \quad (64)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTSP.2016.2600516, IEEE Journal of Selected Topics in Signal Processing

(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.,

$$\mathbf{P} = \mathbf{G}_2\mathbf{W}((\mathbf{G}_2\mathbf{W})^H\mathbf{G}_2\mathbf{W})^{-1}(\mathbf{G}_2\mathbf{W})^H. \quad (65)$$

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

$$\mathbf{G}_1\mathbf{V} = \mathbf{P}\mathbf{G}_1\mathbf{V}. \quad (66)$$

Substituting (65) into (66) 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

$$\mathbf{G}_1\mathbf{V} = \mathbf{G}_2\mathbf{W}\mathbf{B}. \quad (67)$$

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.

APPENDIX E
PROOF OF *Corollary 2*

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

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

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 mes-

sages," *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] H. Inaltekin, M. Chiang, H. V. Poor, and S. B. Wicker, "On unbounded path-loss models: Effects of singularity on wireless network performance," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1078–1092, Sep. 2009.

[37] 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.

[38] B. Nosrat-Makouei, J. G. Andrews, and R. W. Heath, "MIMO interference alignment over correlated channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2783–2794, Jun. 2011.

[39] F. Pérez-Cruz and Miguel R. D. Rodrigues and S. Verdú, "MIMO Gaussian Channels With Arbitrary Inputs: Optimal Precoding and Power Allocation," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1070–1084, Mar. 2010.

Lingxiang Li received the B.S. degree from Central South University, Changsha, China, in 2010, and the M.S. degree from University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2013, all in Electrical Engineering. Since September 2013, she has been working towards the Ph.D. degree at the National Key Lab of Science and Technology on Communications (NCL), UESTC. She is currently a vising Ph.D. student of the Electrical and Computer Engineering (ECE) Department at Rutgers, under the supervision of Professor Athina P. Petropulu. Her current research interests lie in the areas of signal processing for wireless communications, including multiple-input multiple-output systems, cooperative communication, and physical-layer security.

Athina P. Petropulu (F'08) received her undergraduate degree from the National Technical University of Athens, Greece, and the M.Sc. and Ph.D. degrees from Northeastern University, Boston MA, all in Electrical and Computer Engineering. Since 2010, she is Professor of the Electrical and Computer Engineering (ECE) Department at Rutgers, having served as chair of the department during 2010-2016. Before that she was faculty at Drexel University. Dr. Petropulu's research interests span the area of statistical signal processing, wireless communications, signal processing in networking, physical layer security, and radar signal processing. Her research has been funded by various government industry sponsors including the National Science Foundation, the Office of Naval research, the US Army, the National Institute of Health, the Whitaker Foundation, Lockheed Martin.

Dr. Petropulu is Fellow of IEEE and recipient of the 1995 Presidential Faculty Fellow Award given by NSF and the White House. She has served as Editor-in-Chief of the IEEE Transactions on Signal Processing (2009-2011), IEEE Signal Processing Society Vice President-Conferences (2006-2008), and member-at-large of the IEEE Signal Processing Board of Governors. She was the General Chair of the 2005 International Conference on Acoustics Speech and Signal Processing (ICASSP-05), Philadelphia PA. In 2005 she received the IEEE Signal Processing Magazine Best Paper Award, and in 2012 the IEEE Signal Processing Society Meritorious Service Award for "exemplary service in technical leadership capacities". More info on her work can be found at www.ece.rutgers.edu/~cspl.

Zhi Chen received the B. Eng, M. Eng., and Ph.D. degrees in Electrical Engineering from University of Electronic Science and Technology of China (UESTC), in 1997, 2000, 2006, respectively. In April 2006, he joined the National Key Lab of Science and Technology on Communications (NCL), UESTC, and worked as professor in this lab from August 2013. He was a visiting scholar at University of California, Riverside during 2010-2011. His current research interests include 5G mobile communications, tactile internet, and Terahertz communication. Dr. Chen has served as a reviewer for various international journals and conferences, including IEEE Transactions on Vehicular Technology, IEEE Transactions on Signal Processing, etc.

Jun Fang (M'08) received the B.S. and M.S. degrees from the Xidian University, Xi'an, China in 1998 and 2001, respectively, and the Ph.D. degree from the National University of Singapore, Singapore, in 2006, all in electrical engineering. During 2006, he was a postdoctoral research associate in the Department of Electrical and Computer Engineering, Duke University. From January 2007 to December 2010, he was a research associate with the Department of Electrical and Computer Engineering, Stevens Institute of Technology. Since January 2011, he has been with the University of Electronic of Science and Technology of China. His current research interests include sparse theory and compressed sensing, and Bayesian inference. Dr. Fang received the IEEE Jack Neubauer Memorial Award in 2013 for the best systems paper published in the IEEE Transactions on Vehicular Technology. He is an Associate Technical Editor for IEEE Communications Magazine, and an Associate Editor for IEEE Signal Processing Letters.