On Exploiting Co-Channel Interference to Improve Secret Communications Over a Wiretap Channel

†‡Lingxiang Li, ‡Athina P. Petropulu, †Zhi Chen
†National Key Lab. on Commun., UESTC, Chengdu 611731, China
‡Dept. of ECE, Rutgers–The State University of New Jersey, New Brunswick, NJ 08854, USA
Email: lingxiang.li@rutgers.edu; athinap@rutgers.edu; chenzhi@uestc.edu.cn

Abstract—**This paper considers a network 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. Our goal is to identify the secrecy rate performance benefits that can be brought by exploiting co-channel interference. We consider two scenarios: 1) the non-confidential pair designs its precoding matrix in favor of the confidential one, referred to as the altruistic scenario; 2) the non-confidential pair is selfish and it requires to communicate with its maximum achievable D.o.F.. The maximum achievable S.D.o.F. of the wiretap channel for both scenarios is obtained in closed form. Based on these analytical expressions, we further determine the number of antennas needed at the non-confidential connection in order to achieve an S.D.o.F. for the wiretap channel equal to the degrees of freedom (D.o.F.).**

I. Introduction

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 [1]–[6] on exploiting CCI to enhance secrecy. [1]–[4] consider the scenario of a K-user interference channel in which the users wish to establish secure communication against an eavesdropper. Specifically, [1]–[3] consider the single-antenna case and examine the achievable secrecy degrees of freedom (S.D.o.F.) by applying interference alignment techniques. The work of [4] considers the multi-antenna case and proposes interference-alignment-based algorithms for the sake of maximizing the achievable secrecy sum rate. In [5], [6], 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. [5], [6] maximize the secrecy transmission rate of the confidential connection subject to a quality of service constraint for the non-confidential connection.

In this paper, we consider a two-user wiretap interference network as in [5], [6], except that, unlike [5], [6], which assume the single input single-output (SISO) case or multi-input single-output (MISO) case, we address the most general multi-input multi-output (MIMO) case, i.e., a 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. Our goal is to identify the secrecy rate performance benefits that can be brought by exploiting CCI. Since determining the exact maximum achievable secrecy rate of a helper-assisted wiretap channel, or of an interference channel is a very difficult problem [7]–[10], we consider the high signal-to-noise ratio (SNR) behavior of the achievable secrecy rate, i.e., the S.D.o.F. as an alternative. A similar alternative has also been considered in [1]–[3], [11]–[14].

In [15], we have fully described the dependence of the S.D.o.F. region on the number of antennas, and we have constructed precoding matrices achieving S.D.o.F. pairs on the S.D.o.F. region boundary. Here as a supplement to the work in [15], we examine two special points of the boundary, i.e., the maximum achievable S.D.o.F. for the following two scenarios: 1) the non-confidential pair designs its precoding matrix in favor of the confidential one, referred to as the altruistic scenario; 2) the non-confidential pair is selfish and it requires to communicate with its maximum achievable D.o.F.. Specifically, we give the maximum achievable S.D.o.F. (See eq. (7) and eq. (12), eq. (16) for each scenario, respectively). We determine the number of antennas needed at the non-confidential connection in order to achieve an S.D.o.F. equal to the maximum achievable D.o.F. (see *Proposition 1*). And we give numerical results to verify the achievable rates for both scenarios. We should note that in the first scenario the maximum achievable S.D.o.F. equals that of a MIMO Gaussian wiretap channel with a multi-antenna cooperative jammer, which has also been studied in [11]–[14]. Our result is more general because, unlike [11]–[13] it applies to any number of antennas. Our conference work [14] also applies to any number of antennas. However, the result here is more general since it provides the performance balance between two users.

Notation: $\lfloor a \rfloor$ denotes the biggest integer which is less or equal to a; $|a|$ is the absolute value of a; $\mathbf{A}^H$, $\mathrm{tr}\{\mathbf{A}\}$, $\mathrm{rank}\{\mathbf{A}\}$, and $|\mathbf{A}|$ stand for the hermitian transpose, trace, rank and determinant of the matrix $\mathbf{A}$, respectively; $\mathbf{A}(:, i:j)$ denotes the columns from i to j of $\mathbf{A}$; $\mathrm{span}(\mathbf{A})$ denotes the subspace spanned by the columns of $\mathbf{A}$; $\mathrm{span}(\mathbf{A}) \cap \mathrm{span}(\mathbf{B}) = \mathbf{0}$ 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 $\mathbf{A}$. We use lower case

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.

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

bold to denote vectors.

II. System Model and Problem Statement

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

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

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

$$\mathbf{y}_e = \mathbf{G}_1\mathbf{V}\mathbf{s}_1 + \mathbf{G}_2\mathbf{W}\mathbf{s}_2 + \mathbf{n}_e. \qquad (2)$$

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 [16].
3) All channel matrices are full rank. Global channel state information (CSI) is available, including the CSI for the eavesdropper. This is possible in situations in which the eavesdropper is an active member of the network, and thus its whereabouts and behavior can be monitored.

The achievable secrecy rate for transmitting the message $\mathbf{s}_1$ and $\mathbf{s}_2$ are respectively given as [17]

$$R_s^1 = (R_d^1 - R_e)^+, R_s^2 = R_d^2.$$

where

$$R_d^1 = \log|\mathbf{I} + (\mathbf{I} + \mathbf{H}_{12}\mathbf{Q}_w\mathbf{H}_{12}^H)^{-1}\mathbf{H}_{11}\mathbf{Q}_v\mathbf{H}_{11}^H|, \qquad (3a)$$

$$R_d^2 = \log|\mathbf{I} + (\mathbf{I} + \mathbf{H}_{21}\mathbf{Q}_v\mathbf{H}_{21}^H)^{-1}\mathbf{H}_{22}\mathbf{Q}_w\mathbf{H}_{22}^H|, \qquad (3b)$$

$$R_e = \log|\mathbf{I} + (\mathbf{I} + \mathbf{G}_2\mathbf{Q}_w\mathbf{G}_2^H)^{-1}\mathbf{G}_1\mathbf{Q}_v\mathbf{G}_1^H|, \qquad (3c)$$

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.

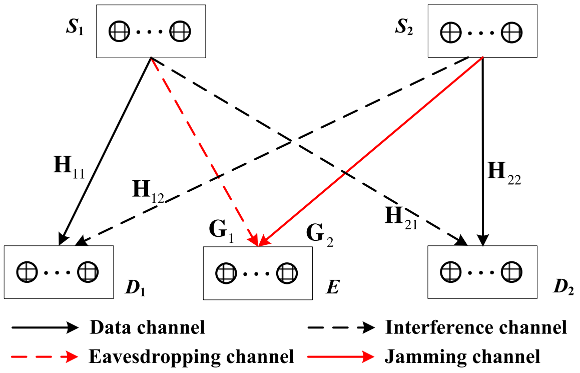

Fig. 1: A MIMO two-user wiretap interference channel

From (3a)-(3c), one can see that the rate performance of the two users are coupled with each other. In order to gain some insight into the balance of the rate performance between the two users, in [15], we have computed the boundary of the *achievable secrecy degrees of freedom region*, which is defined as follows,

$$\mathcal{D} \triangleq \bigcup_{(\mathbf{V},\mathbf{W})\in\mathcal{I}} (d_s^1, d_s^2). \qquad (4)$$

Here $\mathcal{I} \triangleq \{(\mathbf{V},\mathbf{W})|\text{tr}\{\mathbf{V}\mathbf{V}^H\} = P, \text{tr}\{\mathbf{W}\mathbf{W}^H\} = P\}$, with P denoting the transmit power budget. d_s^i denotes the high SNR behavior of the achievable secrecy rate, i.e.,

$$d_s^i \triangleq \lim_{P\to\infty} \frac{R_s^i}{\log\ P}, i \in \{1,2\}. \qquad (5)$$

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 $d_s^1 = \hat{d}_s^1$. On combining *Proposition 3* and *Corollary 1* of [15], it holds that in order to determine the outer boundary of $\mathcal{D}$, we only need to focus on the set $\hat{\mathcal{I}}$, which is defined as follows,

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

$$\bar{\mathcal{I}}_2 \triangleq \{(\mathbf{V},\mathbf{W})|\text{span}(\mathbf{H}_{11}\mathbf{V}) \cap \text{span}(\mathbf{H}_{12}\mathbf{W}) = \mathbf{0}\}. \qquad (6)$$

We divide the set satisfying $\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w}$ into six subsets, i.e., Sub_{I},..., Sub_{VI}, and determine the number of linear independent precoding vector pairs that should be considered in each subset, i.e., d_{I},...,d_{VI}, respectively. *Corollary 2* of [15] shows that for $(\mathbf{V},\mathbf{W}) \in \hat{\mathcal{I}}$ the achieved S.D.o.F. is $d_s^1 = \text{rank}\{\mathbf{H}_{11}\mathbf{V}\}$. Thus, our problem of interest reduces to selecting precoding vector pairs from these six subsets for constructing 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. Due to the lack of space, here we only summarize the results with Table I, which provides the basis for the analysis to follow. For more details, please refer to Section V. A of [15].

In the following, we will consider two scenarios: 1) the non-confidential pair designs its precoding matrix in favor of the confidential one, referred to as the altruistic scenario; 2) the non-confidential pair is selfish and it requires to communicate with its maximum achievable D.o.F.. Our goal is to analyze the maximum achievable S.D.o.F. for each scenario, which corresponds to a special point on the S.D.o.F. region boundary. Thus, to accomplish our goal, we only need to focus on constructing precoding matrices base on Table I.

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 $(\mathbf{v}, \mathbf{w})$**
Sub_{I}	$d_{\text{I}} = (N_s^1 - N_e - N_d^2)^+$
Sub_{II}	$d_{\text{II}} = \min\{N_d^2, (N_s^1 - N_e)^+\}$
Sub_{III}	$d_{\text{III}} = (\min\{(N_s^1 - N_d^2)^+, N_e\} + \min\{(N_s^2 - N_d^1)^+, N_e\} - N_e)^+$
Sub_{IV}	$d_{\text{IV}} = (\min\{N_s^1, N_e\} + \min\{(N_s^2 - N_d^1)^+, N_e\} - N_e)^+ - d_{\text{III}}$
Sub_{V}	$d_{\text{V}} = (\min\{(N_s^1 - N_d^2)^+, N_e\} + \min\{N_s^2, N_e\} - N_e)^+ - d_{\text{III}}$
Sub_{VI}	$d_{\text{VI}} = (\min\{N_s^1, N_e\} + \min\{N_s^2, N_e\} - N_e)^+ - (d_{\text{III}} + d_{\text{IV}} + d_{\text{V}})$

III. Discussions on the Maximum Achievable S.D.o.F. of the Wiretap Channel

A. The altruistic scenario: the non-confidential pair designs its precoding matrix in favor of the confidential one

Based on *Corollary 2* of [15], we see that our problem for maximizing d_s^1 is including as more precoding vector pairs as possible in $(\mathbf{V}, \mathbf{W})$. In Table I, we divide the set which satisfies $\mathbf{G}_1\mathbf{v} = \mathbf{G}_2\mathbf{w}$ into six subsets. Due to the requirement in (6), it holds that more precoding vector pairs can be included in $(\mathbf{V}, \mathbf{W})$ by choosing precoding vector pairs from the subsets with smaller a, where $a \triangleq \text{rank}\{\mathbf{H}_{11}\mathbf{v}\} + \text{rank}\{\mathbf{H}_{12}\mathbf{w}\}$. For example, $a = 1$ for Sub_{IV} while $a = 2$ for Sub_{VI}. We can select at most N_d^1 precoding vector pairs from Sub_{IV}, in which $a = 1$, while we can select only $\lfloor N_d^1/2 \rfloor$ precoding vector pairs from Sub_{VI}, in which $a = 2$. In addition, since the achieved S.D.o.F. is $d_s^1 = \text{rank}\{\mathbf{H}_{11}\mathbf{V}\}$, a greater value of d_s^1 can be achieved with precoding vector pairs from Sub_{IV}. Therefore, in the construction of $(\mathbf{V}, \mathbf{W})$, the precoding vector pairs from the first four subsets have the same priority, and the precoding vector pairs from the last two subsets have the same priority. Moreover, a precoding vector pair from the first four subsets has higher priority than that one from the last two subsets. If $N_d^1 \leq d_{\text{I}} + d_{\text{II}} + d_{\text{III}} + d_{\text{IV}}$, we just select N_d^1 precoding vector pairs from $Sub_{\text{I}} \cup Sub_{\text{II}} \cup Sub_{\text{III}} \cup Sub_{\text{IV}}$; otherwise, we first select all the precoding vector pairs in $Sub_{\text{I}} \cup Sub_{\text{II}} \cup Sub_{\text{III}} \cup Sub_{\text{IV}}$, and then we pick $\lfloor \frac{N_d^1 - (d_{\text{I}} + d_{\text{II}} + d_{\text{III}} + d_{\text{IV}})}{2} \rfloor$ precoding vector pairs from $Sub_{\text{V}} \cup Sub_{\text{VI}}$.

Summarizing, the maximum achievable value of d_s^1 is

$$\bar{d}_s^1 = \min\{d_{a=1} + d_{a=2}^{\star}, N_d^1\}, \tag{7}$$

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

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

Proposition 1: In order to achieve an S.D.o.F. for the wiretap channel *S*$_1$-*D*$_1$-*E* equal to $\{N_s^1, N_d^1\}$, i.e., the D.o.F. for the channel *S*$_1$-*D*$_1$, the number of antennas needed at *S*$_2$ should satisfy the following conditions:

1) if $|N_s^1 - N_d^1| < \min\{N_s^1, N_e\}$, it requires that $N_s^2 \geq N_e + N_d^1 - |N_s^1 - N_d^1|$;
2) if $N_d^1 - N_s^1 \geq \min\{N_s^1, N_e\}$, it requires that $N_s^2 \geq N_e$;
3) if $N_s^1 \geq N_e + N_d^1$, there are no requirements on N_s^2.

Proof: Please see Appendix A. ■

Example 1: Consider the case $N_s^1 = N_d^1 = N_e = 4$. According to *Proposition 1*, it shows that if $N_s^2 \geq 8$, an S.D.o.F. of 4, which equals the D.o.F. for the channel *S*$_1$-*D*$_1$, can be achieved. This result matches that of [11].

Example 2: Consider the case $(N_s^1, N_d^1, N_e) = (5, 4, 4)$ and $(N_s^1, N_d^1, N_e) = (4, 8, 5)$, respectively. By *Proposition 1* it shows that an S.D.o.F. of 4 can be achieved if $N_s^2 \geq 7$ and $N_s^2 \geq 5$, respectively. This indicates that the increase in N_s^1 or N_d^1 can reduce the requirement on the number of antennas at *S*$_2$. We should note this result is not revealed in [11] where only the symmetric case with $N_s^1 = N_d^1 = N_e$ is studied.

B. The selfish scenario: the non-confidential pair is selfish and it requires to communicate with its maximum achievable D.o.F.

Since in this case the non-confidential pair is selfish, it requires to communicate with its maximum achievable D.o.F., which is $\bar{d}_s^2 = \min\{N_s^2, N_d^2\}$.

Due to (6) it holds that $d_s^1 + \dim\{\text{span}(\mathbf{H}_{12}\mathbf{W})\} \leq N_d^1$. Thus,

$$\bar{d}_s^2 \leq (\max\{N_s^2, N_d^1\} - d_s^1)^+. \tag{8}$$

On the other hand, assume that z columns of $\mathbf{V}$ 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,

$$\bar{d}_s^2 \leq (N_d^2 - z)^+. \tag{9}$$

In the following, we consider two distinct cases for discussing the maximum achievable value of d_s^1, which is denoted with $\underline{d}_s^1$.

(i) For the case of $N_s^2 > N_d^2$, (8) becomes

$$d_s^1 \leq \max\{N_s^2, N_d^1\} - N_d^2. \tag{10}$$

Eq. (9) indicates that $z = 0$, and thus all of the signal steams sent by *S*$_1$ should not interfere with *D*$_2$. That is, Sub_{II}, Sub_{IV} and Sub_{VI} are not under consideration. Applying (7), we obtain

$$d_s^1 \leq \min\{d_{\text{I}} + d_{\text{III}} + \beta^{\star}, N_d^1\}, \tag{11}$$

where $\beta^{\star} = \min\{d_{\text{V}}, \lfloor (N_d^1 - d_{\text{I}} - d_{\text{III}})^+/2 \rfloor\}$. Combining (10) and (11), we arrive at

$$\underline{d}_s^1 = \min\{d_{\text{I}} + d_{\text{III}} + \beta^{\star}, \max\{N_s^2, N_d^1\} - N_d^2, N_d^1\}. \tag{12}$$

(ii) For the case of $N_s^2 \leq N_d^2$, (8) becomes

$$d_s^1 \leq \max\{N_s^2, N_d^1\} - N_s^2, \tag{13}$$

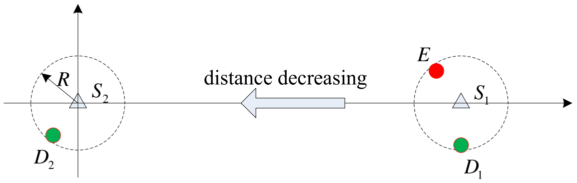

Fig. 2: Model used for numerical experiments

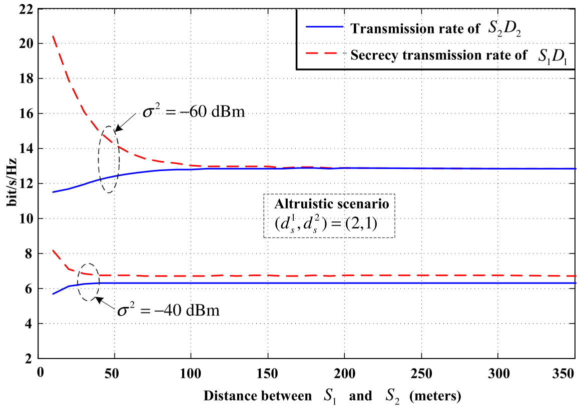

Fig. 3: Achievable rates versus S_1-S_2 distance.

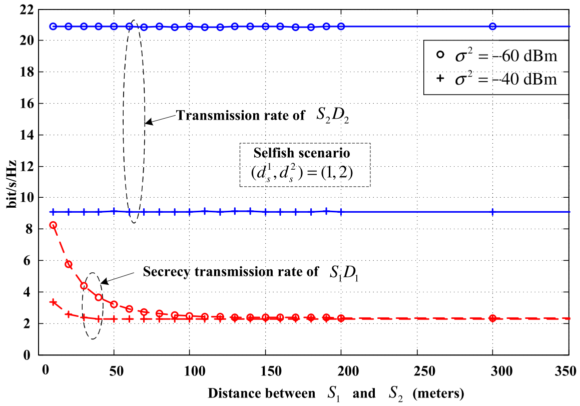

Fig. 4: Achievable rates versus S_1-S_2 distance

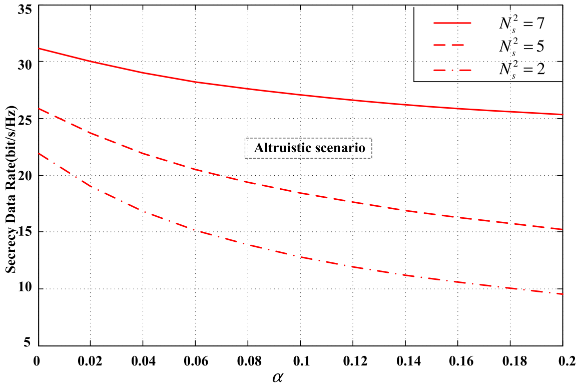

Fig. 5: Achievable secrecy rate of S_1-D_1 versus the uncertainty of the eavesdropper's channels α.

which indicates that $d_s^1 = 0$ when $N_s^2 \geq N_d^1$. So, in the following, we will only consider the case of $N_s^2 < N_d^1$, where it holds that $d_{\mathrm{III}} = d_{\mathrm{IV}} = 0$. On the other hand, eq. (9) indicates that $z \leq N_d^2 - N_s^2$. So, $\xi = \min\{d_{\mathrm{VI}}, (N_d^2 - N_s^2 - d_{\mathrm{II}})^+\} + d_{\mathrm{V}}$, where ξ denotes the maximum number of pairs that can be chosen from Sub_{V} and Sub_{VI}. Applying (7), we get

$$d_s^1 \leq \min\{d_{\mathrm{I}} + \hat{d}_{\mathrm{II}} + \xi^\star, N_d^1\}, \tag{14}$$

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

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

Combining (13) and (14), we arrive at

$$\underline{d}_s^1 = \min\{d_{\mathrm{I}} + \hat{d}_{\mathrm{II}} + \xi^\star, \max\{N_s^2, N_d^1\} - N_s^2\}. \tag{16}$$

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

Example 3: Consider the case $(N_s^1, N_d^1, N_e) = (6, 5, 5)$, $(N_s^2, N_d^2) = (6, 4)$. Based on Table I we get that $d_{\mathrm{I}} = 0$, $d_{\mathrm{II}} = 1$, $d_{\mathrm{III}} = 0$, $d_{\mathrm{IV}} = 1$, $d_{\mathrm{V}} = 2$, $d_{\mathrm{VI}} = 2$. According to (7), the maximum achievable S.D.o.F. in the altruistic scenario is 3. By contrast, in the selfish scenario, the non-confidential connection requires to communicate with a D.o.F. of 4. According to (12), an S.D.o.F. equal to 2 can be achieved.

IV. Numerical Results

In this section, we give some numerical results on the achievable rates. The precoding matrices are constructed with Table III of [15]. As illustrated in Fig. 2, S_2 is located at a fixed two-dimensional coordinates (0,0) (unit: meters), while S_1 moves from (350,0) to (10,0). Simulation parameters are the same as that of [15], if we do not specify here.

Fig. 3 and Fig. 4 illustrate the achievable transmission rates for the altruistic scenario and the selfish scenario, respectively. In particular, we set $(N_s^1, N_d^1, N_e) = (5, 4, 4)$ and $(N_s^2, N_d^2) = (2, 2)$. According to (7) and (12), $(d_s^1, d_s^2) = (2, 1)$ and $(d_s^1, d_s^2) = (1, 2)$ can be achieved for the altruistic scenario and the selfish scenario, respectively. Results show that for both scenarios, the achievable secrecy transmission rate of S_1-D_1 increases monotonically as S_1 moves close to S_2. In contrast, with the decreasing of the source-source distance, the achievable transmission rate of S_2-D_2 decreases for the altruistic scenario and remains unchanged for the selfish scenario. As compared with the decrease in the transmission rate of S_2-D_2, the increase in the secrecy transmission rate of S_1-D_1 is drastic. Therefore, the network performance benefits when the two users get closer.

In Fig. 5, we plot the achievable secrecy rate for the altruistic scenario with imperfect CSI of the eavesdropper's channels, with α denoting the variance of the channel error term. In particular, we set $(N_s^1, N_d^1, N_e) = (5, 4, 4)$, $N_d^2 = 2$, and let N_s^2 vary from 2 to 7. The noise power is set as $\sigma^2 = -60$dBm. S_1 and S_2 are located at (10,0) and (0,0), respectively. According to (7), we see that an S.D.o.F. of 2, 3 and 4 can be achieved for the case of $N_s^2 = 2$, $N_s^2 = 5$, and $N_s^2 = 7$, respectively. It can be observed that the achievable secrecy rate drops with the increase of channel uncertainties. Fortunately, when the number of antennas N_s^2 increases, this secrecy rate performance degradation is smaller. On the other hand, on comparing the secrecy transmission rate of S_1-D_1 for the case $N_s^2 = 2$ with that in Fig. 3, one can see that the secrecy rate achieved for the case where $\alpha = 0.1$ and S_1-

S_2 distance of 10 meters, is almost equal to the secrecy rate achieved for the case where $\alpha = 0$ and S_1-S_2 distance of 100 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.

V. Conclusion

We have addressed analytically the maximum achievable secrecy degrees of freedoms (S.D.o.F.) of a MIMO Gaussian wiretap interference channel, aided by the interference generated by another source-destination pair that exchanges public messages. Based on these analytical expressions, we further determine the number of antennas needed at S_2 in order to achieve an S.D.o.F. equal to the maximum achievable D.o.F. of the channel S_1-D_1. The result shows that not only the increase in N_s^1, but also the increase of N_d^1 can reduce the requirement on the number of antennas at S_2, which suggests that in wiretap interference networks, in order to achieve a certain value of S.D.o.F., one can cooperatively adjust the number of antennas at S_1, S_2 and D_1. Numerical results show that the network performance benefits when the two users get closer. This is interesting. It tells us that in wiretap interference networks, the secrecy rate degradation due to CSI estimation error can be counteracted by bringing the two users closer together.

VI. Proof of *Proposition 1*

Our proof is based on the analysis of (7). In the following, we will consider two distinct cases, i.e., $N_s^1 \geq N_d^1$ and $N_s^1 < N_d^1$. For ease of exposition, let $s(N, M, K) = (\min\{M, N\} + \min\{K, N\} - N)^+$.

(i) For the case of $N_s^1 \geq N_d^1$, it holds that the D.o.F. of the channel S_1-D_1 equals N_d^1, which, combined with (7), indicates that in order to achieve an S.D.o.F. equal to the D.o.F. of the channel S_1-D_1, we should have

$$d_{a=1} \geq N_d^1. \tag{17}$$

With Table I, it can be derived that $d_{a=1} = (N_s^1 - N_e)^+ + s(N_e, (N_s^2 - N_d^1)^+, N_s^1)$. In addition, $N_d^1 - (N_s^1 - N_e)^+ = N_d^1 - N_s^1 + \min\{N_s^1, N_e\}$. So (17) is equivalent to

$$s(N_e, (N_s^2 - N_d^1)^+, N_s^1) \geq N_d^1 - N_s^1 + \min\{N_s^1, N_e\}. \tag{18}$$

If $N_d^1 + \min\{N_s^1, N_e\} \leq N_s^1$, (18) holds true for any values of N_s^2; otherwise, we should have

$$\min\{(N_s^2 - N_d^1)^+, N_e\} - N_e \geq N_d^1 - N_s^1,$$

which holds true when

$$N_s^2 \geq N_e + 2N_d^1 - N_s^1 = N_e + N_d^1 + N_d^1 - N_s^1. \tag{19}$$

(ii) For the case of $N_s^1 < N_d^1$, it holds that the D.o.F. of the channel S_1-D_1 equals N_s^1. So in order to achieve an S.D.o.F. equal to the D.o.F. of the channel S_1-D_1, the total number of linear independent precoding vectors in Table I should be N_s^1, which requires that $N_s^2 \geq N_e$. Further, in order to meet (6), we should have

$$d_{a=1} + 2d^{\star}_{a=2} \leq N_d^1. \tag{20}$$

According to Table I, it can be derived that $d_{a=1} + 2d^{\star}_{a=2} = (N_s^1 - N_e)^+ + 2s(N_e, N_s^2, N_s^1) - s(N_e, (N_s^2 - N_d^1)^+, N_s^1)$. In addition, $s(N_e, N_s^2, N_s^1) = \min\{N_e, N_s^1\}$ due to $N_s^2 \geq N_e$. Therefore, (20) is equivalent to $s(N_e, (N_s^2 - N_d^1)^+, N_s^1) \geq (N_s^1 - N_e)^+ + 2\min\{N_e, N_s^1\} - N_d^1$, where the right hand equals $N_s^1 - N_d^1 + \min\{N_s^1, N_e\}$. Thus,

$$s(N_e, (N_s^2 - N_d^1)^+, N_s^1) \geq N_s^1 - N_d^1 + \min\{N_s^1, N_e\}. \tag{21}$$

If $N_s^1 + \min\{N_s^1, N_e\} \leq N_d^1$, (21) holds true for any $N_s^2 \geq N_e$; otherwise, we should have

$$\min\{(N_s^2 - N_d^1)^+, N_e\} - N_e \geq N_s^1 - N_d^1,$$

which holds true when

$$N_s^2 \geq N_e + N_s^1 = N_e + N_d^1 + N_s^1 - N_d^1. \tag{22}$$

Summarizing the above two cases, we arrive at that

1) if $|N_s^1 - N_d^1| < \min\{N_s^1, N_e\}$, it requires that $N_s^2 \geq N_e + N_d^1 - |N_s^1 - N_d^1|$;
2) if $N_d^1 - N_s^1 \geq \min\{N_s^1, N_e\}$, it requires that $N_s^2 \geq N_e$;
3) If $N_s^1 \geq N_e + N_d^1$, there are no requirements on N_s^2.

This completes the proof.

References

[1] 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.

[2] ——, "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.

[3] 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.

[4] 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.*

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[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] 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.

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

[13] ——, "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.

[14] L. Li, Z. Chen, J. Fang, and A. Petropulu, "Secrecy degrees of freedom of a MIMO Gaussian wiretap channel with a cooperative jammer," in *Proc. IEEE ICASSP (accepted)*, Shanghai, China, Mar. 2016.

[15] L. Li, A. Petropulu, Z. Chen, and J. Fang, "Improving wireless physical layer security via exploiting co-channel interference," *[online], Available: http://arxiv.org/abs/1602.06847.*

[16] 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.

[17] 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.