Cooperative Secrecy Beamforming in Wiretap Interference Channels

Lingxiang Li, Chuan Huang, *Member, IEEE*, and Zhi Chen, *Member, IEEE*

***Abstract*—This paper exploits co-channel interference (CCI) to secure the multi-antenna wiretap IFC consisting of two source-destination-eavesdropper triples, where each source-destination link is wiretapped by an external eavesdropper. To this end, we first propose a cooperative secrecy beamforming scheme, which is proved to be sufficient and necessary to achieve the secure degrees of freedom (S.D.o.F.) pair (1,1). By investigating the feasibility of the proposed beamforming scheme, we obtain the sufficient and necessary condition and also the beamforming vectors in closed-form to achieve the S.D.o.F pair (1,1). To the best of our knowledge, this is the first time that the benefit brought by CCI has been quantified.**

***Index Terms*—Cooperative beamforming, interference channel, physical layer security, secure degrees of freedom.**

I. Introduction

In THE context of physical (PHY) layer security, techniques such as multi-input multi-output (MIMO), cooperative jamming, and relaying, etc, have been extensively studied to improve the secrecy transmission rate of a source-destination pair [1]–[9]. However, [1]–[9] only considered one source-destination pair with secrecy constraints, which fail to meet the requirement of accommodating more users within the future wireless networks [10]. Recently, there are growing research interests in secrecy communication over the K-user interference channel (IFC), where multiple source-destination pairs work on the same frequency band and the same time interval such that the network-level secrecy throughput can be further boosted [11]–[16]. Specifically, the authors in [11]–[13] considered the scenario of K-user IFC with only one external eavesdropper, in which K source-destination pairs wish to have secure communication against the eavesdropper. The authors in [14]–[16] studied the scenario of K-user IFC with confidential messages, where there are no external eavesdroppers and each source-destination pair wishes to secure its communication against the remaining $K-1$ destinations.

This paper considers a different wiretap IFC scenario consisting of two source-destination-eavesdropper triples, where each source-destination link is wiretapped by an unique external eavesdropper. Such scenario exists in multi-cell networks, where each base station (BS) serves multiple users including the legitimate receiver and the eavesdropper. And the eavesdropper is normally an active member of the network, communicating information with BS in other time slots. Unlike the K-user IFC scenario studied in [11]–[16], here each eavesdropper is external and has no interest in the signal from the other source. Hence, to each eavesdropper, the signal from the other source is co-channel interference (CCI). From the viewpoint of physical layer security, CCI at the eavesdropper acts as the harmful jamming signal and so it is beneficial for improving the secrecy rate. Motivated by these observations, we try to exploit CCI to secure the wiretap interference channel. By this way, we identify the conditions that the antenna numbers should satisfy in order to ensure the secure degrees of freedom (S.D.o.F.) pair (1,1) being achievable, thus offering insights into the maximal achievable secrecy rate region.

As compared with the secrecy rate maximization problem considered in [1]–[9], the secrecy rate region maximization problem considered here is more complicated since it involves balancing the secrecy transmission rate of two confidential messages. To deal with this issue, we first introduce a cooperative secrecy beamforming scheme, where the CCI from the other source is zero-forced at the destination and is aligned within the space spanned by the signal from the source at the eavesdropper. We then give a rigorous proposition, proving that the S.D.o.F. pair (1,1) can be achieved if and only if the proposed scheme is feasible. Consequently, the original achievability problem reduces to check the feasibility of the proposed scheme. As compared with the former, the latter is easier since it only involves solving some linear equations. Resorting to subspace decomposition techniques, we obtain the conditions and also the beamforming vectors in closed-form to achieve the S.D.o.F pair (1,1).

II. System Model

We consider a wiretap interference channel where source $\mathbf{S}_i$, $i = 1, 2$, intends to send independent and confidential message x_i to destination $\mathbf{D}_i$, without being wiretapped by eavesdropper $\mathbf{E}_i$ (please see Fig. 1). Both $\mathbf{D}_i$ and $\mathbf{E}_i$ are only interested in x_i, hence the message from $\mathbf{S}_j$, $j \neq i$, is treated as the CCI signal. For $i = 1, 2$, $\mathbf{S}_i$ and $\mathbf{E}_i$ are equipped with $M_i \geq 2$ and $N_i \geq 2$ antennas, respectively, and $\mathbf{D}_i$ is with only one antenna. We assume that the global channel state information (CSI) is available, including the CSI for the eavesdroppers. Our goal is

Manuscript received July 27, 2015; revised September 24, 2015; accepted October 10, 2015. Date of publication October 13, 2015; date of current version October 26, 2015. This work was supported in part by the National Natural Science Foundation of China under Grants 61571089 and 61501093, and by the High-Tech Research and Development (863) Program of China under Grant 2015AA011309. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Francesco Verde.

L. Li, C. Huang and Z. Chen are with the National Key Laboratory on Communications, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China (e-mail: LiLX@std.uestc.edu.cn; walk22talk@gmail.com; lingxiang_li_uestc@hotmail.com; huangch@uestc.edu.cn; chenzhi@uestc.edu.cn).

(*Corresponding author: C. Huang*.)

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

Digital Object Identifier 10.1109/LSP.2015.2490602

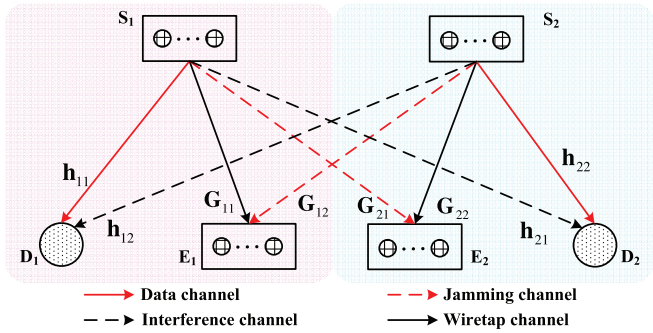

Fig. 1. Wiretap interference channel.

to deliberately introduce CCI via cooperative beamforming at $\mathbf{S}_1$ and $\mathbf{S}_2$ to degrade the eavesdropper's channel quality, and thus to improve the secrecy rate performance.

Denote by $\mathbf{v}_i$ and $P_i^\star$ the beamforming vector and the transmit power at $\mathbf{S}_i$, respectively, with $|\mathbf{v}_i|^2 = 1$. Denote by $n_i \sim \mathcal{CN}(0,1)$ and $\mathbf{n}_e^i \sim \mathcal{CN}(0,\mathbf{I})$ the noise at the i-th destination and the i-th eavesdropper, respectively. The signals received at D_i and E_i can thus be expressed as, respectively,

$$y_i = P_i^\star \mathbf{h}_{ii}\mathbf{v}_i x_i + P_j^\star \mathbf{h}_{ij}\mathbf{v}_j x_j + n_i, i \in \{1,2\}, \quad (1)$$

$$\mathbf{z}_i = P_i^\star \mathbf{G}_{ii}\mathbf{v}_i x_i + P_j^\star \mathbf{G}_{ij}\mathbf{v}_j x_j + \mathbf{n}_e^i, i \in \{1,2\}, \quad (2)$$

where $\mathbf{h}_{ik}$ and $\mathbf{G}_{ik}$ represent the end-to-end channel coefficient matrices, with entries independent of each other and distributed as $\mathcal{CN}(0,1)$. The message $x_i \sim \mathcal{CN}(0,1)$. According to [2], the achievable secrecy rate for transmitting the message x_i is given as

$$R_s^i = \left[\log(1+\gamma_D^i) - \log(1+\gamma_E^i)\right]^+, i \in \{1,2\}, \quad (3)$$

in which the received signal-to-noise ratio (SNR) at $\mathbf{D}_i$ and $\mathbf{E}_i$ are, respectively,

$$\gamma_D^i = P_i^\star |\mathbf{h}_{ii}\mathbf{v}_i|^2/(1+|P_j^\star \mathbf{h}_{ij}\mathbf{v}_j|^2), \quad (4)$$

$$\gamma_E^i = P_i^\star \mathbf{v}_i^H \mathbf{G}_{ii}^H (\mathbf{I} + P_j^\star \mathbf{G}_{ij}\mathbf{v}_j\mathbf{v}_j^H\mathbf{G}_{ij}^H)^{-1}\mathbf{G}_{ii}\mathbf{v}_i. \quad (5)$$

Correspondingly, the achieved S.D.o.F., i.e., the rate at which R_s^i scales with $\log(P_i^\star)$, is defined as [17]

$$d_s^i \triangleq \lim_{P_i^\star \to \infty} (R_s^i/\log P_i^\star), i \in \{1,2\}. \quad (6)$$

Combining (3)–(6), it is obvious to see that the upper bound (component-wise) of the S.D.o.F. pair is $(d_s^1, d_s^2) = (1,1)$. In this paper, we aim to identify the conditions that the antenna numbers should satisfy to ensure the S.D.o.F. pair (1,1) being achievable, and determine the beamforming vectors to achieve it. Such achievability problem is generally difficult to solve since it requires to face several coupled generalized eigenvector problems. In the sequel, we first introduce a cooperative secrecy beamforming scheme, and prove its optimality in the sense of achieving the maximum S.D.o.F. pair (1,1). Then, by studying the feasibility of the proposed beamforming scheme, we obtain the conditions and also the beamforming vectors in closed-form to achieve the S.D.o.F. pair (1,1).

III. Cooperative Secrecy Beamforming Scheme

In order to secure the wiretap interference channel via exploiting CCI, in this section, we propose a cooperative secrecy beamforming scheme. In this proposed beamforming scheme, the CCI from the other source is zero-forced at the destination and is aligned within the space spanned by the signal from the source at the eavesdropper. In this way, $\mathbf{D}_i$ can see an interference-free signal of x_i, such that γ_D^i scales with the transmit power $P_i^\star$. Simultaneously, $\mathbf{E}_i$ can only see an interference signal of x_i, such that γ_E^i converges to a constant as $P_1^\star$ and $P_2^\star$ approach to infinity. Denote by $\mathrm{span}(\mathbf{A})$ the subspace spanned by the columns of $\mathbf{A}$, the proposed cooperative beamforming scheme can then be formulated as follows,

$$\begin{aligned} \text{find} \quad & \{\mathbf{v}_1, \mathbf{v}_2\} \\ \text{s.t.} \quad & \mathrm{span}(\mathbf{G}_{11}\mathbf{v}_1) = \mathrm{span}(\mathbf{G}_{12}\mathbf{v}_2), && (7a) \\ & \mathrm{span}(\mathbf{G}_{21}\mathbf{v}_1) = \mathrm{span}(\mathbf{G}_{22}\mathbf{v}_2), && (7b) \\ & |\mathbf{h}_{12}\mathbf{v}_2| = 0, |\mathbf{h}_{11}\mathbf{v}_1| > 0, && (7c) \\ & |\mathbf{h}_{21}\mathbf{v}_1| = 0, |\mathbf{h}_{22}\mathbf{v}_2| > 0. && (7d) \end{aligned}$$

Proposition 1: For the considered wiretap interference channel, the S.D.o.F. pair $(d_s^1, d_s^2) = (1,1)$ can be achieved if and only if the optimization (7) returns a nonempty set.

Proof: See Appendix A. ■

Remark 1: Proposition 1 shows that in the considered wiretap interference channel, the proposed beamforming scheme is sufficient and necessary to achieve the maximum S.D.o.F. pair (1,1). Thus, to investigate the conditions under which the maximum S.D.o.F. pair (1,1) can be achieved, we only need to focus on analyzing the conditions under which the optimization (7) returns a nonempty set.

IV. Conditions to Achieve $(d_s^1, d_s^2) = (1,1)$

In this section, we study the feasibility of the proposed beamforming scheme, thus giving the sufficient and necessary condition to achieve the maximum S.D.o.F pair (1,1).

Theorem 1: For the considered wiretap interference channel, the S.D.o.F. pair $(d_s^1, d_s^2) = (1,1)$ can be achieved if and only if $N_{\min} \leq [\min\{M_1 - 1, N_{\max}\} + \min\{M_2 - 1, N_{\max}\} - N_{\max}]^+$, where $N_{\min} = \min\{N_1, N_2\}$ and $N_{\max} = \max\{N_1, N_2\}$.

Proof: We start with the constraints (7c) and (7d). Without loss of generality, let $\mathbf{v}_1 = \mathbf{\Gamma}_1\bar{\mathbf{v}}_1$ and $\mathbf{v}_2 = \mathbf{\Gamma}_2\bar{\mathbf{v}}_2$, where $\bar{\mathbf{v}}_1$ and $\bar{\mathbf{v}}_2$ are nonzero vectors. Moreover, $\mathbf{\Gamma}_1 \triangleq \mathrm{null}(\mathbf{h}_{21}) \in \mathbb{C}^{M_1 \times (M_1-1)}$ and $\mathbf{\Gamma}_2 \triangleq \mathrm{null}(\mathbf{h}_{12}) \in \mathbb{C}^{M_2 \times (M_2-1)}$. Substituting $\mathbf{v}_1 = \mathbf{\Gamma}_1\bar{\mathbf{v}}_1$ and $\mathbf{v}_2 = \mathbf{\Gamma}_2\bar{\mathbf{v}}_2$ into (7), we transform the optimization (7) into an equivalent form as follows,

$$\begin{aligned} \underset{\{\bar{\mathbf{v}}_1 \neq \mathbf{0}, \bar{\mathbf{v}}_1 \neq \mathbf{0}\}}{\text{find}} \quad & \{\bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2\} \\ \text{s.t.} \quad & \mathrm{span}(\bar{\mathbf{G}}_{11}\bar{\mathbf{v}}_1) = \mathrm{span}(\bar{\mathbf{G}}_{12}\bar{\mathbf{v}}_2), && (8a) \\ & \mathrm{span}(\bar{\mathbf{G}}_{21}\bar{\mathbf{v}}_1) = \mathrm{span}(\bar{\mathbf{G}}_{22}\bar{\mathbf{v}}_2), && (8b) \end{aligned}$$

where $\bar{\mathbf{G}}_{11} \triangleq \mathbf{G}_{11}\mathbf{\Gamma}_1$, $\bar{\mathbf{G}}_{12} \triangleq \mathbf{G}_{12}\mathbf{\Gamma}_2$, $\bar{\mathbf{G}}_{21} \triangleq \mathbf{G}_{21}\mathbf{\Gamma}_1$ and $\bar{\mathbf{G}}_{22} \triangleq \mathbf{G}_{22}\mathbf{\Gamma}_2$.

Before proceeding to investigate the feasibility of the optimization (8), we first give Proposition 2 which provides the basis for the following derivations. With Proposition 2, the dimension of the variable is reduced. Hence in this paper, we also refer to it as the *Dimension Reduction Proposition*. Please refer to Appendix B for the proof of Proposition 2.

Proposition 2 (Dimension Reduction): Given two matrices $\mathbf{H} \in \mathbb{C}^{N \times M}$ and $\mathbf{G} \in \mathbb{C}^{N \times K}$. Let $s = [\min\{M,N\} + \min\{K,N\} - N]^+$. When $s > 0$, there exist full column-rank matrices $\mathbf{X}_s \in \mathbb{C}^{N \times s}$, $\mathbf{\Psi}_{1s} \in \mathbb{C}^{M \times s}$ and $\mathbf{\Psi}_{2s} \in \mathbb{C}^{K \times s}$, such that $\mathbf{H}\mathbf{\Psi}_{1s} = \mathbf{X}_s$ and $\mathbf{G}\mathbf{\Psi}_{2s} = \mathbf{X}_s$. Moreover, $\mathrm{span}(\mathbf{H}\mathbf{v}_1) =$

$\text{span}(\mathbf{G}\mathbf{v}_2)$ holds true for some nonzero vectors $\{\mathbf{v}_1, \mathbf{v}_2\}$ if and only if we could find another nonzero vector $\mathbf{x} \in \mathbb{C}^{s\times 1}$ such that $\mathbf{v}_1 = \mathbf{\Psi}_{1s}\mathbf{x}$ and $\mathbf{v}_2 = \mathbf{\Psi}_{2s}\mathbf{x}$.

Invoking the generalized singular value decomposition (GSVD) of $(\bar{\mathbf{G}}_{11}^H, \bar{\mathbf{G}}_{12}^H)$ and applying Proposition 2, we find that when $s = [\min\{M_1-1, N_1\} + \min\{M_2-1, N_1\} - N_1]^+ > 0$, there exist full column-rank matrices $\mathbf{X}_s \in \mathbb{C}^{N_1\times s}$, $\mathbf{\Psi}_{1s} \in \mathbb{C}^{(M_1-1)\times s}$ and $\mathbf{\Psi}_{2s} \in \mathbb{C}^{(M_2-1)\times s}$, such that $\bar{\mathbf{G}}_{11}\mathbf{\Psi}_{1s} = \mathbf{X}_s$ and $\bar{\mathbf{G}}_{12}\mathbf{\Psi}_{2s} = \mathbf{X}_s$. Moreover, (8a) holds true for some nonzero vectors $\{\bar{\mathbf{v}}_1, \bar{\mathbf{v}}_2\}$ if and only if we could find another nonzero vector $\mathbf{x} \in \mathbb{C}^{s\times 1}$ such that $\bar{\mathbf{v}}_1 = \mathbf{\Psi}_{1s}\mathbf{x}$ and $\bar{\mathbf{v}}_2 = \mathbf{\Psi}_{2s}\mathbf{x}$. Thus, the optimization (8) can be recast as

$$\underset{\{\mathbf{x}\neq\mathbf{0}, \lambda\neq 0\}}{\text{find}} \ \bar{\mathbf{G}}_{21}\mathbf{\Psi}_{1s}\mathbf{x} = \lambda\bar{\mathbf{G}}_{22}\mathbf{\Psi}_{2s}\mathbf{x}. \tag{9}$$

In Appendix C, we prove that the optimization (9) returns a nonempty set if and only if $N_2 \le s$. Therefore, the optimization (8) returns a nonempty set if and only if

$$N_2 \le [\min\{M_1-1, N_1\} + \min\{M_2-1, N_1\} - N_1]^+ \tag{10}$$

Similarly, invoking the GSVD of $(\bar{\mathbf{G}}_{21}^H, \bar{\mathbf{G}}_{22}^H)$ and applying the same derivations from (8) to (10), we find that the optimization (8) returns a nonempty set if and only if

$$N_1 \le [\min\{M_1-1, N_2\} + \min\{M_2-1, N_2\} - N_2]^+ \tag{11}$$

Let $N_{\min} = \min\{N_1, N_2\}$ and $N_{\max} = \max\{N_1, N_2\}$. Combining (10) and (11), we arrive at that the optimization (8), and thus the optimization (7), returns a nonempty set if and only if $N_{\min} \le [\min\{M_1-1, N_{\max}\} + \min\{M_2-1, N_{\max}\} - N_{\max}]^+$, which together with Proposition 1, indicates Theorem 1. This completes the proof. ■

Remark 2: Theorem 1 shows that, with our proposed scheme, the condition to achieve the S.D.o.F. pair (1,1) is relaxed. For instance, assume $M = M_1 = M_2$ and $N = N_1 = N_2$. With the zero-forcing (ZF) scheme, the S.D.o.F. pair (1,1) can be achieved if and only if $M \ge N+2$. While according to Theorem 1, with our proposed scheme, the S.D.o.F. pair (1,1) can be achieved if and only if $M \ge N+1$. Moreover, with our proposed scheme, the spectral efficiency in the wiretap interference channel doubles as compared with that in the wiretap channel consisting of one source-destination-eavesdropper triple. Specifically, the former achieves the sum S.D.o.F. of 2 while the latter only achieves the S.D.o.F. of 1, both with $M \ge N+1$ and the same bandwith.

V. Solutions to Achieve $(d_s^1, d_s^2) = (1, 1)$

In this section, we derive the beamforming vectors which achieve the S.D.o.F. pair $(d_s^1, d_s^2) = (1,1)$ in closed-form. Without loss of generality, assume $N_{\max} = N_1$ and $N_{\min} = N_2$. According to Theorem 1, we only consider the case that the S.D.o.F. pair (1,1) can be achieved, i.e., $N_2 \le s = [\min\{M_1-1, N_1\} + \min\{M_2-1, N_1\} - N_1]^+$.

Proposition 3: For the considered wiretap interference channel, the following beamforming vectors can achieve the S.D.o.F. pair $(d_s^1, d_s^2) = (1,1)$,

$$\mathbf{v}_1^\star = \mathbf{\Gamma}_1\mathbf{\Psi}_{1s}\mathbf{x}/|\mathbf{\Gamma}_1\mathbf{\Psi}_{1s}\mathbf{x}|, \tag{12a}$$

$$\mathbf{v}_2^\star = \mathbf{\Gamma}_2\mathbf{\Psi}_{2s}\mathbf{x}/|\mathbf{\Gamma}_2\mathbf{\Psi}_{2s}\mathbf{x}|, \tag{12b}$$

where $\mathbf{\Psi}_{1s}$ and $\mathbf{\Psi}_{2s}$ are obtained according to (16), and $\mathbf{x}$ is determined as follows,

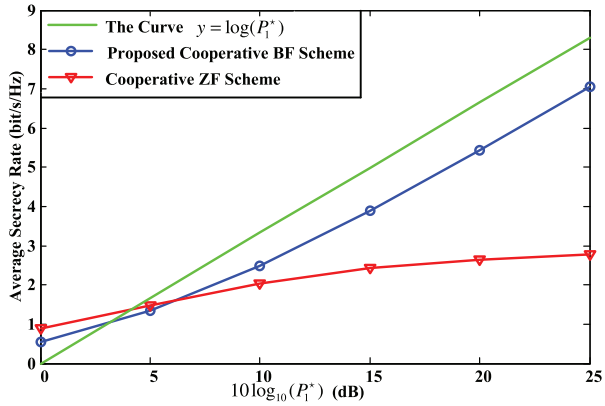

Fig. 2. Average secrecy rate versus $P_1^\star$. $M_1 = M_2 = 4$, $N_1 = N_2 = 3$.

1) for the case of $N_2 < s$, $\mathbf{x} = \mathbf{\Gamma}_0\mathbf{x}_0$ where $\mathbf{x}_0 \in \mathbb{C}^{s\times(s-N_2)}$ is an arbitrary nonzero vector, and $\mathbf{\Gamma}_0 \triangleq \text{null}(\mathbf{G}_{21}\mathbf{\Gamma}_1\mathbf{\Psi}_{1s} - \lambda\mathbf{G}_{22}\mathbf{\Gamma}_2\mathbf{\Psi}_{2s})$ with λ being an arbitrary nonzero constant.
2) for the case of $N_2 = s$, $\mathbf{x}$ is the eigenvector corresponding to the nonzero eigenvalue of the matrix $(\mathbf{G}_{22}\mathbf{\Gamma}_2\mathbf{\Psi}_{2s})^{-1}\mathbf{G}_{21}\mathbf{\Gamma}_1\mathbf{\Psi}_{1s}$.

Proof: Substituting (12a) and (12b) into (7), it is easy to verify that (7a)–(7d) are satisfied. Thus, the S.D.o.F. pair (1,1) is achieved. This completes the proof. ■

VI. Numerical Results

Fig. 2 illustrates the achievable secrecy rate of different schemes for transmitting the message x_1[1]. Results are averaged over 1000 independent channel trials. The line labeled as "Proposed Cooperative BF Scheme" illustrates the secrecy rate achieved by the proposed scheme. The line labeled as "Cooperative ZF Scheme" gives the secrecy rate achieved by the scheme which completely nulls out the CCI at the destination but does not care about the CCI at the eavesdropper. Specifically, in the Cooperative ZF Scheme, the beamforming vectors $\mathbf{v}_i' = \mathbf{\Gamma}_i\bar{\mathbf{v}}_i/|\mathbf{\Gamma}_i\bar{\mathbf{v}}_i|$, $i = 1, 2$, where $\bar{\mathbf{v}}_i$ is proportional to the eigenvector corresponding to the largest eigenvalue of the matrix $(\mathbf{I} + P_1^\star\bar{\mathbf{G}}_{ii}\bar{\mathbf{G}}_{ii}^H)^{-1}(\mathbf{I} + P_1^\star\bar{\mathbf{h}}_{ii}\bar{\mathbf{h}}_{ii}^H)$ with $\bar{\mathbf{h}}_{ii} = \mathbf{h}_{ii}\mathbf{\Gamma}_i$. It shows that in the high SNR regime, the secrecy rate achieved by the proposed scheme increases linearly with $\log(P_1^\star)$. In contrast, there exists a performance ceiling on the secrecy rate achieved by the Cooperative ZF Scheme. Moreover, the line labeled as Proposed Cooperative BF Scheme is parallel to the curve $y = \log(P_1^\star)$ in high SNR regime indicating that the S.D.o.F. equal to 1 is achieved by our proposed scheme.

VII. Conclusion

In order to secure the multi-antenna wiretap interference channel, we first proposed a cooperative secrecy beamforming scheme which is proved to be sufficient and necessary to achieve the S.D.o.F pair (1,1). By studying the feasibility of the proposed beamforming scheme, we obtained the conditions and also the beamforming vectors in closed-form to achieve the S.D.o.F pair (1,1). We found that via exploiting the CCI in the wiretap interference channel, the condition to achieve the S.D.o.F pair (1,1) is relaxed. Moreover, the spectral efficiency in the considered wiretap interference channel doubles as

[1]Numerical results of the achievable secrecy rate for transmitting the message x_2 are similar and are omitted due to the lack of space.

compared with that in the wiretap channel consisting of one source-destination-eavesdropper triple.

Appendix A
Proof of Proposition 1

Clearly, if the optimization problem of (7) returns a nonempty set, then the S.D.o.F. pair $(d_s^1, d_s^2) = (1, 1)$ can be achieved. Thus, **the sufficiency** holds true. We now prove **the necessity** by contradiction. Let $R_e^1 = \log(1 + \gamma_E^1)$, $R_d^1 = \log(1 + \gamma_D^1)$. Assume that the optimization (7) returns an empty set, and then at least one of the constraints in (7) does not hold true. We test (7a)–(7d) one by one:

1) If (7a) does not hold true, there exists a direction along which the eavesdropper $\mathbf{E}_1$ can extract the desired signal without interference. Thus, the rate at which R_e^1 scales with $\log(P_1)$ is 1. In addition, the rate at which R_d^1 scales with $\log(P_1)$ is at most 1 for the multi-input single-output (MISO) source-receiver channel. Thus, by definition, we have $d_s^1 = 0$.
2) If (7b) does not hold true, $d_s^2 = 0$. The proof is the same as that of 1).
3) If (7c) does not hold true, $|\mathbf{h}_{12}\mathbf{v}_2| = 0$ or $|\mathbf{h}_{11}\mathbf{v}_1| > 0$. From (4), it is clear that R_d^1 converges to a constant when P_1 approaches to infinity, which indicates that $d_s^1 = 0$.
4) If (5d) does not hold true, $|\mathbf{h}_{21}\mathbf{v}_1| = 0$ or $|\mathbf{h}_{22}\mathbf{v}_1| > 0$. Thus, $d_s^2 = 0$, where the proof is the same as that of 3).

To summarize, if the optimization (7) returns an empty set, it follows that the S.D.o.F. pair $(d_s^1, d_s^2) \neq (1, 1)$. Therefore, if the S.D.o.F. pair $(d_s^1, d_s^2) = (1, 1)$, the optimization (7) returns a nonempty set. This completes the proof.

Appendix B
Proof of Proposition 2

Let $k = \min\{M + K, N\}$, $p = k - \min\{M, N\}$, $r = k - \min\{K, N\}$, and $s = [\min\{M, N\} + \min\{K, N\} - N]^+$. According to [18], the generalized singular value decomposition (GSVD) of $(\mathbf{H}^H, \mathbf{G}^H)$ 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 $\text{rank}\{\mathbf{X}\} = k$, such that

$$\mathbf{H}\Psi_1 = \mathbf{X}\mathbf{D}_1^H, \mathbf{G}\Psi_2 = \mathbf{X}\mathbf{D}_2^H, \tag{13}$$

in which $\mathbf{D}_1 = \begin{bmatrix} \mathbf{I}_r & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{S}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}$, $\mathbf{D}_2 = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{S}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_p \end{bmatrix}$. Here the diagonal entries of $\mathbf{S}_1 \in \mathbb{R}^{s\times s}$ and $\mathbf{S}_2 \in \mathbb{R}^{s\times s}$ are greater than 0, and $\mathbf{D}_1^H\mathbf{D}_1 + \mathbf{D}_2^H\mathbf{D}_2 = \mathbf{I}$.

Letting $\bar{\mathbf{\Psi}}_1 = \mathbf{\Psi}_1(:, r+1 : r+s)$, $\bar{\mathbf{\Psi}}_2 = \mathbf{\Psi}_2(:, K-s-p+1 : K-p)$, $\mathbf{X}_1 = \mathbf{X}(:, 1 : r)$, $\mathbf{X}_s = \mathbf{X}(:, r+1 : r+s)$ and $\mathbf{X}_3 = \mathbf{X}(:, r+s+1 : k)$, and substituting them into (13), we arrive at

$$\mathbf{H}\bar{\mathbf{\Psi}}_1 = \mathbf{X}_s\mathbf{S}_1, \mathbf{G}\bar{\mathbf{\Psi}}_2 = \mathbf{X}_s\mathbf{S}_2. \tag{14}$$

In addition, both $\mathbf{S}_1$ and $\mathbf{S}_2$ are invertible. Thus

$$\mathbf{H}\mathbf{\Psi}_{1s} = \mathbf{X}_s, \mathbf{G}\mathbf{\Psi}_{2s} = \mathbf{X}_s, \tag{15}$$

where

$$\mathbf{\Psi}_{1s} = \bar{\mathbf{\Psi}}_1\mathbf{S}_1^{-1}, \mathbf{\Psi}_{2s} = \bar{\mathbf{\Psi}}_2\mathbf{S}_2^{-1}, \tag{16}$$

with $\text{rank}\{\mathbf{\Psi}_{1s}\} = \text{rank}\{\mathbf{\Psi}_{2s}\} = \text{rank}\{\mathbf{X}_s\} = s$.

On the other hand, according to the specific structure of $\mathbf{D}_1$ and $\mathbf{D}_2$, it is clear to see that $\text{span}(\mathbf{H}\mathbf{v}_1) = \text{span}(\mathbf{G}\mathbf{v}_2)$ holds true for some nonzero vectors $\{\mathbf{v}_1, \mathbf{v}_2\}$ if and only if we could find another nonzero vector $\mathbf{x} \in \mathbb{C}^{s\times 1}$ such that $\mathbf{v}_1 = \mathbf{\Psi}_{1s}\mathbf{x}, \mathbf{v}_2 = \mathbf{\Psi}_{2s}\mathbf{x}$. This completes the proof.

Appendix C
Proof of The Fact That The Optimization (9) Returns A Nonempty Set If and Only If $N_2 \leq s$

Denote by $\mathbf{A} = \bar{\mathbf{G}}_{21}\mathbf{\Psi}_{1s} \in \mathbb{C}^{N_2\times s}$ and $\mathbf{B} = \bar{\mathbf{G}}_{22}\mathbf{\Psi}_{2s} \in \mathbb{C}^{N_2\times s}$. Generally speaking, $\text{rank}\{\mathbf{A}\} = \text{rank}\{\mathbf{B}\} = s$. In the sequel, we distinguish the discussion into four cases.

1) $N_2 < s$. Then $\text{rank}\{\mathbf{A} - \lambda\mathbf{B}\} \leq N_2 < s$. Let $\mathbf{x} = \mathbf{\Gamma}_0\mathbf{x}_0$ where $\mathbf{\Gamma}_0 = \text{null}(\mathbf{A} - \lambda\mathbf{B})$ and $\mathbf{x}_0$ is an arbitrary nonzero vector. Then the constraint in (9) is satisfied.
2) $N_2 = s$. Then $\mathbf{B}$ is invertible. Let λ be the nonzero eigenvalue and $\mathbf{x}$ be the corresponding eigenvector of the matrix $\mathbf{B}^{-1}\mathbf{A}$, and then the constraint in (9) is satisfied.
3) $s < N_2 < 2s$. We give the proof by contradiction. Assume that there exist nonzero λ_0 and $\mathbf{x}_0$ such that

$$\mathbf{A}\mathbf{x}_0 = \lambda_0\mathbf{B}\mathbf{x}_0 = \mathbf{b}. \tag{17}$$

Invoking the GSVD of $(\mathbf{A}^H, \lambda_0^H\mathbf{B}^H)$ and applying Proposition 2, we find that (17) holds true for some nonzero vector $\mathbf{x}_0$ if and only if we could find another nonzero vector $\mathbf{x}_1 \in \mathbb{C}^{s_1\times 1}$ such that

$$\mathbf{\Phi}_{11}\mathbf{x}_1 = \mathbf{\Phi}_{12}\mathbf{x}_1 = \mathbf{x}_0, \tag{18}$$

where $s_1 = 2s - N_2 < s$, and $\mathbf{\Phi}_{11} \in \mathbb{C}^{s\times s_1}$ and $\mathbf{\Phi}_{12} \in \mathbb{C}^{s\times s_1}$ are full column-rank matrices. Since $\mathbf{A}$ and $\mathbf{B}$ are independent of each other, $\mathbf{\Phi}_{11}$ and $\mathbf{\Phi}_{12}$ are also independent of each other. Therefore, if $s_1 \leq 1$, (18) cannot be true; otherwise, invoking the GSVD of $(\mathbf{\Phi}_{11}^H, \mathbf{\Phi}_{12}^H)$ and applying Proposition 2, we arrive at that (18) holds true if and only if we could find another nonzero vector $\mathbf{x}_2 \in \mathbb{C}^{s_2\times 1}$ such that

$$\mathbf{\Phi}_{21}\mathbf{x}_2 = \mathbf{\Phi}_{22}\mathbf{x}_2 = \mathbf{x}_1, \tag{19}$$

where $s_2 = 2s_1 - s = 3s - 2N_2 < s_1$, $\mathbf{\Phi}_{21} \in \mathbb{C}^{s_1\times s_2}$ and $\mathbf{\Phi}_{22} \in \mathbb{C}^{s_1\times s_2}$ are full rank matrices. Noting that (19) has the same form as (17), inductively, we conclude that we cannot find nonzero λ_0 and $\mathbf{x}_0$ such that (17) holds true. Thus, the optimization (9) returns an empty set.
4) $N_2 \geq 2s$. Let $\mathbf{C} = [\mathbf{A} : -\lambda\mathbf{B}]$ and $\mathbf{D} = [\mathbf{A}^T : -\lambda\mathbf{B}^T]^T$. Then $\text{rank}\{\mathbf{C}\} = 2s$ and $\text{rank}\{\mathbf{D}\} = s$. According to [18], we have $\text{rank}\{\mathbf{A} - \lambda\mathbf{B}\} \leq \min\{\text{rank}\{\mathbf{C}\}, \text{rank}\{\mathbf{D}\}\} = s$ and $\text{rank}\{\mathbf{A} - \lambda\mathbf{B}\} \geq \text{rank}\{\mathbf{C}\} + \text{rank}\{\mathbf{D}\} - \text{rank}\{\mathbf{A}\} - \text{rank}\{\mathbf{B}\} = s$. Therefore, $\text{rank}\{\mathbf{A} - \lambda\mathbf{B}\} = s$, which indicates that the optimization (9) returns an empty set.

Combining the above four cases, we conclude that the optimization (9) returns a nonempty set if and only if $N_2 \leq s$. This completes the proof.

This paper previously published in IEEE Signal Processing Letters

REFERENCES

[1] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[2] 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.

[3] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC-2005-Fall*, Texas, USA, 2005, pp. 1906–1910.

[4] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The gaussian wiretap channel with a helping interferer," in *Proc. IEEE ISIT*, Ontario, Canada, Jul. 2008, pp. 389–393.

[5] 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.

[6] L. Li, Z. Chen, and J. Fang, "On secrecy capacity of helper-assisted wiretap channel with an out-of-band link," *IEEE Signal Process. Lett.*, vol. 22, no. 9, pp. 1288–1292, Nov. 2015.

[7] 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.

[8] 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.

[9] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[10] Cisco, "Cisco visual networking index: Global mobile data traffic forecast 2014-2019," 2015 [Online]. Available: http://www.cisco.com

[11] S. Agrawal and S. Vishwanath, "On the secrecy rate of interference networks using structured codes," in *Proc. IEEE ISIT*, Seoul, Korea, Jun. 2009, pp. 2091–2095.

[12] 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.

[13] 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.

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

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

[16] J. Ni, K.-K. Wong, and Z. Fei *et al.*, "Secrecy-rate balancing for two-user MISO interference channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 1, pp. 6–9, Feb. 2014.

[17] Y. Liang, G. Kramer, H. V. Poor, and S. S. Shitz, "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 5, pp. 1–13, Mar. 2009.

[18] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1985.

This paper previously published in IEEE Signal Processing Letters