Secrecy Degrees of Freedom of a MIMO Gaussian Wiretap Channel with a Cooperative Jammer

†‡Lingxiang Li, †Zhi Chen, †Jun Fang, ‡Athina P. Petropulu
†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: ll673@scarletmail.rutgers.edu; {chenzhi, JunFang}@uestc.edu.cn; athinap@rutgers.edu

***Abstract*—This paper considers secrecy communication from a signal processing point of view, and studies the maximal achievable secrecy degrees of freedoms (S.D.o.F.) of a helper-assisted Gaussian wiretap channel, consisting of a source, a legitimate receiver, an eavesdropper and an external helper. Each terminal is equipped with multiple antennas. We first propose a cooperative secrecy transmission scheme, and show that it achieves the maximal secrecy degrees of freedom. We then propose a heuristic method, through which, we solve analytically the optimization problem associated with the proposed cooperative secrecy transmission scheme. By this way, we obtain the maximal achievable S.D.o.F. and also the precoding matrices which achieve the maximal S.D.o.F. in closed-form.**

I. Introduction

Cooperative jamming approaches have attracted intense attention in recent years. However, their advantage comes from optimally designed input covariance matrices, which are difficult to obtain due to the nonlinear nature of the problem. For the single-antenna eavesdropper case, several techniques have been proposed. For example, in [1]–[3], a suboptimal but cost efficient null-space jamming scheme that spreads the jamming signal within the null-space of the legitimate receiver's channel is proposed. In [4]–[8], algorithms are proposed to find the optimal solution using a combination of convex optimization and one-dimensional search. For the multi-antenna eavesdropper case, [9] designs the jamming signals so that they align into a pre-specified jamming subspace at the legitimate receiver, and span the entire received signal space at the eavesdropper. In [10], [11], iterative algorithms are proposed, which alternatively design the transmit covariance matrix of the legitimate transmitter and the cooperative jammer. Also, the work of [12] provides a closed-form expression for the structure of the jamming signal covariance matrix that guarantees secrecy rate larger than the secrecy capacity of the wiretap channel with no cooperative jamming signals.

To the best of the authors' knowledge, determining the exact secrecy capacity of a helper-assisted multi-input multi-output (MIMO) Gaussian wiretap channel has not been previously addressed. In order to gain more insight into how the secrecy capacity of a helper-assisted MIMO Gaussian wiretap channel behaves, one can examine the rate at which the secrecy capacity scales with $\log(P)$, i.e., the maximal achievable secrecy degrees of freedom (S.D.o.F.) [9], [13]–[17]. The work of [9] considers the scenario where a large number of helpers is available, and exploits multiuser diversity via opportunistic helper selection to enhance secrecy. The works of [15]–[17] consider special scenarios with certain constraints on antenna configurations, and determine the maximal achievable S.D.o.F via real interference alignment and signal space alignment. In this paper, we aim to determine the maximal achievable S.D.o.F for a more general MIMO helper-assisted Gaussian wiretap channel, with no constraints on antenna configurations. Although we derive the achievable S.D.o.F from a signal processing point of view, our S.D.o.F. result matches that of [16], [17], which was derived from the information theory point of view. We should note that the work of [14] also investigates the achievable S.D.o.F from the signal processing point of view. However, different from our work, the work of [14] makes the assumption the number of source antennas is greater than the sum of the number of antennas at the legitimate receiver and the eavesdropper, and also introduces additional zero-forcing constraints in order to reduce the degree of difficulty.

To examine the maximal achievable S.D.o.F., we first introduce a cooperative secrecy transmission scheme, which targets at maximizing the dimension of the subspace spanned by the message signal received at the legitimate receiver, under the constraints that the message and jamming signals lie in different subspaces at the legitimate receiver, but are aligned into the same subspace at the eavesdropper. We then give a critical proposition, proving that the proposed secrecy transmission scheme is sufficient to achieve the maximal achievable S.D.o.F.. Consequently, the original S.D.o.F. maximization reduces to the newly introduced optimization problem. Subsequently, we solve analytically the newly introduced optimization problem, thus obtaining the maximal achievable S.D.o.F. of the helper-assisted MIMO Gaussian wiretap channel in closed-form. Our analytical results uncover the connection between the maximal achievable S.D.o.F. and antenna configurations, thus shedding light on how the maximal achievable secrecy rate behaves.

Notation: $\mathbf{A}^H$, $\mathrm{tr}\{\mathbf{A}\}$, $\mathrm{rank}\{\mathbf{A}\}$, and $|\mathbf{A}|$ stand for the hermitian transpose, trace, rank and determinant of the matrix $\mathbf{A}$, respectively; $\mathbf{A}(:,j)$ indicates the j-th column of $\mathbf{A}$ while and $\mathbf{A}(:,i:j)$ denotes the columns from i to j of $\mathbf{A}$. $\mathrm{span}(\mathbf{A})$ is the subspace spanned by the columns of $\mathbf{A}$;$\mathrm{null}(\mathbf{A})$ denotes the null space of $\mathbf{A}$; Besides, $(a)^+ \triangleq \max(a,0)$.

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.

II. System Model and Problem Statement

We consider the MIMO Gaussian wiretap channel with a cooperative jammer (see Fig.1) where the source, the legitimate receiver, the eavesdropper and the external helper are equipped with N_a, N_b, N_e and N_j antennas, respectively. The source wishes to send its message, $\mathbf{x} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$, to the legitimate receiver, without being eavesdropped by the eavesdropper. Towards that objective, the source is aided by a cooperative terminal, which simultaneously transmits jamming signal, $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$, to confuse the eavesdropper. The signals received at the legitimate receiver and the eavesdropper can be respectively expressed as

$$\mathbf{y}_d = \mathbf{H}_1\mathbf{V}\mathbf{x} + \mathbf{G}_2\mathbf{W}\mathbf{z} + \mathbf{n}_d \tag{1a}$$

$$\mathbf{y}_e = \mathbf{G}_1\mathbf{V}\mathbf{x} + \mathbf{H}_2\mathbf{W}\mathbf{z} + \mathbf{n}_e, \tag{1b}$$

where $\mathbf{V}$ and $\mathbf{W}$ are the precoding matrices at the source and the helper, respectively; $\mathbf{n}_d \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ represent noise at the legitimate receiver and the eavesdropper, respectively; $\mathbf{G}_2 \in \mathbb{C}^{N_b \times N_j}$ and $\mathbf{H}_2 \in \mathbb{C}^{N_e \times N_j}$ represent the helper to legitimate receiver and the helper to eavesdropper channel matrices, respectively; $\mathbf{H}_1 \in \mathbb{C}^{N_b \times N_a}$ and $\mathbf{G}_1 \in \mathbb{C}^{N_e \times N_a}$ denote the channel matrix from the source to the legitimate receiver and the source to the eavesdropper, respectively.

All channels are assumed to be flat fading. We assume that global channel state information (CSI) is available, including the CSI for the eavesdropper. This is possible in situations in which the eavesdropper is normally an active member of the network, communicating nonconfidential information with the other parties in other time slots [12]. A minimum-Mean-Square-Error (MMSE) receiver is considered at the legitimate receiver and the eavesdropper. The rate at the legitimate receiver and the eavesdropper can be respectively expressed as

$$R_d = \log|\mathbf{I} + (\mathbf{I} + \mathbf{G}_2\mathbf{Q}_j\mathbf{G}_2^H)^{-1}\mathbf{H}_1\mathbf{Q}_a\mathbf{H}_1^H| \tag{2a}$$

$$R_e = \log|\mathbf{I} + (\mathbf{I} + \mathbf{H}_2\mathbf{Q}_j\mathbf{H}_2^H)^{-1}\mathbf{G}_1\mathbf{Q}_a\mathbf{G}_1^H|, \tag{2b}$$

where $\mathbf{Q}_a \triangleq \mathbf{V}\mathbf{V}^H$ and $\mathbf{Q}_j \triangleq \mathbf{W}\mathbf{W}^H$ are the transmit covariance matrices at the source and the helper, respectively.

According to [18], the maximal secrecy rate for transmitting the message $\mathbf{x}$ is given as [1]

$$C_s \triangleq \max_{\{\mathbf{Q}_a \succeq \mathbf{0}, \mathbf{Q}_j \succeq \mathbf{0}\}} R_d - R_e$$
$$\text{s.t. } \mathrm{tr}\{\mathbf{Q}_a\} + \mathrm{tr}\{\mathbf{Q}_j\} \leq P, \tag{3}$$

where P is a given total transmit power budget and C_s denotes the maximal achievable secrecy rate, also known as the secrecy capacity. Correspondingly, the maximal achievable S.D.o.F. is given as [13]

$$s.d.o.f \triangleq \lim_{P\to\infty} \frac{C_s}{\log P}. \tag{4}$$

[1]For a given point $\{\mathbf{Q}_a, \mathbf{Q}_j\}$, the achieved secrecy rate is $(R_d - R_e)^+$. For ease of exposition, the trivial case with zero achievable secrecy rate is omitted.

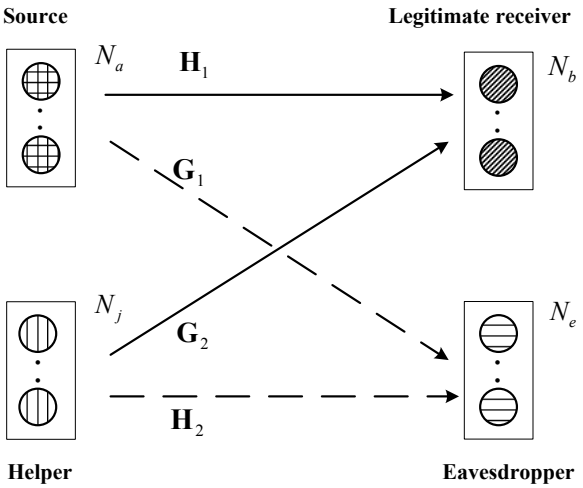

Fig. 1: MIMO wiretap channel with an external helper

Generally, the optimization problem of (3) is nonconvex. It is challenging and still an open problem to determine the exact secrecy capacity. In this paper, we analytically examine the maximal achievable S.D.o.F. and determine its connection to antenna configurations, thus offering insights into the secrecy capacity. In the sequel, we first introduce a cooperative secrecy transmission scheme, and prove its optimality in the sense of achieving the maximal S.D.o.F.. Then, by analytically solving the optimization problem associated with the proposed cooperative secrecy transmission scheme, we obtain the maximal achievable S.D.o.F. and also the precoding matrices which achieve the maximal S.D.o.F. in closed-form.

III. Cooperative Secrecy Transmission Scheme

In the proposed cooperative secrecy transmission scheme, the subspace spanned by the message signal had no intersection with the subspace spanned by the jamming signal at the legitimate receiver, and belongs to the subspace spanned by the jamming signal at the eavesdropper. In this way, the legitimate receiver can see an interference-free message signal, such that R_d scales with $\log(P)$. Simultaneously, the eavesdropper can only see a distorted version of the message signal, such that R_e converges to a constant as P approaches to infinity. Among the feasible points, we choose the one which maximizes the dimension of the subspace spanned by the message signal received at the legitimate receiver, i.e.,

$$d \triangleq \max_{\{\mathbf{V},\mathbf{W}\}} \mathrm{rank}\{\mathbf{H}_1\mathbf{V}\} \tag{5a}$$

$$\text{s.t. } \mathrm{span}(\mathbf{G}_1\mathbf{V}) \subset \mathrm{span}(\mathbf{H}_2\mathbf{W}) \tag{5b}$$

$$\mathrm{span}(\mathbf{G}_2\mathbf{W}) \cap \mathrm{span}(\mathbf{H}_1\mathbf{V}) = \{\mathbf{0}\}. \tag{5c}$$

Proposition 1: The maximal achievable secrecy degrees of freedom, defined in (4), equal to d. That is, $s.d.o.f = d$.

Proof: We first prove that for any given optimal solution to (5), $\{\bar{\mathbf{V}}, \bar{\mathbf{W}}\}$, the achieved S.D.o.F is greater than $\mathrm{rank}\{\mathbf{H}_1\bar{\mathbf{V}}\}$, thus giving the proof of $s.d.o.f. \geq d$. We then prove that for any given point of $\{\mathbf{V}, \mathbf{W}\}$, we can always find another feasible point for the problem of (5),

$\{\mathbf{V}', \mathbf{W}'\}$, such that $\mathrm{rank}\{\mathbf{H}_1\mathbf{V}'\}$ is no less than the achieved S.D.o.F.. Besides, $\mathrm{rank}\{\mathbf{H}_1\mathbf{V}'\} \leq d$ by definition. Therefore, $s.d.o.f. \leq d$. Combining these two facts, we conclude $s.d.o.f. = d$. Please refer to Appendix E of a longer version of this paper [19] for more details. ∎

Remark 1: Proposition 1 shows that in the considered helper-assisted wiretap channel, the proposed transmission scheme is sufficient to achieve the maximal S.D.o.F.. Thus, to determine the maximal achievable S.D.o.F., we only need to focus on solving the optimization problem (5).

IV. A Heuristic Method to Solve (5)

In this section, we first give a heuristic method which gives a closed-form feasible point $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ to (5), followed by the derivation of $d^\star \triangleq \mathrm{rank}\{\mathbf{H}_1\hat{\mathbf{V}}\}$ in closed-form. We then prove that $d = d^\star$. In this way, we solve (5) analytically.

The key idea of our proposed heuristic method is to use the antennas available at the source and the helper in a cooperative way more efficiently. To this end, we first divide the cooperation between the source and the helper into three categories, according to the number of signal dimension we need to spend at the legitimate receiver and helper in order to achieve one S.D.o.F. Denote a and b as the number of signal dimension we need at the legitimate receiver and the helper, respectively. Denote $\mathbf{v}$ and $\mathbf{w}$ as the beamforming vector at the source and the helper, respectively. To get one S.D.o.F, we should design $\mathbf{v}$ and $\mathbf{w}$ in a cooperative way such that $\{\mathbf{v}, \mathbf{w}\}$ is feasible to (5), i.e., $\mathrm{span}(\mathbf{G}_1\mathbf{v}) = \mathrm{span}(\mathbf{H}_2\mathbf{w})$ and $\mathrm{span}(\mathbf{H}_1\mathbf{v}) \cap \mathrm{span}(\mathbf{G}_2\mathbf{w}) = \{\mathbf{0}\}$. Then we have the following three kinds of cooperation.

C1: $(a, b) = (1, 0)$, which is feasible if $N_a > N_e$. Let $\mathbf{w} = \mathbf{0}$, and choose $\mathbf{v}$ such that $\mathbf{G}_1\mathbf{v} = 0$, then $\{\mathbf{v}, \mathbf{w}\}$ is feasible to (5). Besides, $\mathbf{w} = \mathbf{0}$, thus $a = 1$ and $b = 0$.

C2: $(a, b) = (1, 1)$, which is feasible if $N_j > N_b$ and $\mathrm{span}(\mathbf{G}_1) \cap \mathrm{span}(\mathbf{H}_2\mathbf{\Gamma}) \neq \{\mathbf{0}\}$. Here, $\mathbf{\Gamma} = \mathrm{null}(\mathbf{G}_2) \in \mathbb{C}^{N_a \times (N_j - N_b)}$. Choose $\mathbf{v}$ and $\mathbf{w}$ such that $\mathrm{span}(\mathbf{G}_1\mathbf{v}) = \mathrm{span}(\mathbf{H}_2\mathbf{w})$ and $\mathbf{G}_2\mathbf{w} = \mathbf{0}$, then $\{\mathbf{v}, \mathbf{w}\}$ is feasible to (5). Besides, $\mathbf{G}_2\mathbf{w} = \mathbf{0}$, thus $a = 1$ and $b = 1$.

C3: $(a, b) = (2, 1)$, which is feasible if $\mathrm{span}(\mathbf{G}_1) \cap \mathrm{span}(\mathbf{H}_2) \neq \{\mathbf{0}\}$. Choose $\mathbf{v}$ and $\mathbf{w}$ such that $\mathrm{span}(\mathbf{G}_1\mathbf{v}) = \mathrm{span}(\mathbf{H}_2\mathbf{w})$. Different from C1 and C2, $\mathbf{G}_1\mathbf{v} = 0$ and $\mathbf{G}_2\mathbf{w} = \mathbf{0}$ may not hold true here. Thus, in order to make $\{\mathbf{v}, \mathbf{w}\}$ feasible to (5), we should have $a = 2$ and $b = 1$.

Clearly, from C1 to C3, the cooperation efficiency between the source and the helper decreases since the need for the number of signal dimension increases. Thus, in the heuristic method, we check the feasibility of C1 first, followed by C2 and then C3. For more details of our heuristic method, please refer to Table I. Notice that in Table I, $\mathrm{null}(\mathbf{G}_1)$ returns an empty matrix when $N_a \leq N_e$, and the definition of the *GSVD Transform* function $\mathrm{gsvd}(\bullet, \bullet)$ is given in a longer version of this paper [19].

In the sequel, we prove that $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ is a feasible solution for (5), and derive the closed-form expression for $d^\star$. We distinguish our discussion into four cases, as in Table I.

In *Case I* and *Case II*, it is clear that $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ is feasible to (5) and $d^\star = \mathrm{rank}\{\mathbf{H}_1\hat{\mathbf{V}}\} = \min\{N_a, N_b\}$.

In *Case III*, for the subcase of $d_0 + d_1 \geq N_b$, $\hat{\mathbf{V}} = [\mathbf{V}_0, \mathbf{V}_1]$ and $\hat{\mathbf{W}} = \mathbf{W}_1$. According to (6), we get $\mathrm{span}(\mathbf{G}_2\mathbf{W}_1) = \{\mathbf{0}\}$ and $\mathrm{span}(\mathbf{H}_2\mathbf{W}_1) = \mathrm{span}(\mathbf{G}_1\mathbf{V}_1)$. In addition, $\mathbf{G}_1\mathbf{V}_0 = \mathbf{0}$. So, $\mathrm{span}(\mathbf{H}_2\hat{\mathbf{W}}) = \mathrm{span}(\mathbf{G}_1\hat{\mathbf{V}})$ and $\mathrm{span}(\mathbf{H}_1\hat{\mathbf{V}}) \bigcap \mathrm{span}(\mathbf{G}_2\hat{\mathbf{W}}) = \{\mathbf{0}\}$, which indicate that $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ is feasible to (5). Furthermore, $\mathbf{V}_0$ is orthogonal with $\mathbf{V}_1$ by definition, thus

$$d^\star = \mathrm{rank}\{[\mathbf{V}_0, \mathbf{V}_1]\} = \mathrm{rank}\{\mathbf{V}_0\} + \mathrm{rank}\{\mathbf{V}_1\} = N_b.$$

For the subcase of $d_0 + d_1 < N_b$, $\hat{\mathbf{V}} = [\mathbf{V}_0, \mathbf{V}_1, \mathbf{V}_2]$ and $\hat{\mathbf{W}} = [\mathbf{W}_1, \mathbf{W}_2]$. As in the subcase of $d_0 + d_1 \geq N_b$, $\mathbf{G}_1\mathbf{V}_0 = \mathbf{0}$, $\mathrm{span}(\mathbf{G}_2\mathbf{W}_1) = \{\mathbf{0}\}$ and $\mathrm{span}(\mathbf{H}_2\mathbf{W}_1) = \mathrm{span}(\mathbf{G}_1\mathbf{V}_1)$. In addition, according to (7), $\mathrm{span}(\mathbf{H}_2\mathbf{W}_2) = \mathrm{span}(\mathbf{G}_1\mathbf{V}_2)$ and $d_2 = \min\{s_4, \lfloor \frac{N_b - (d_0 + d_1)}{2} \rfloor\}$. Thus, $\mathrm{span}(\mathbf{H}_2\hat{\mathbf{W}}) = \mathrm{span}(\mathbf{G}_1\hat{\mathbf{V}})$ and $\mathrm{span}(\mathbf{H}_1\hat{\mathbf{V}}) \bigcap \mathrm{span}(\mathbf{G}_2\hat{\mathbf{W}}) = \{\mathbf{0}\}$, which indicate that $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ is feasible to (5). Furthermore, $[\mathbf{V}_0, \mathbf{V}_1]$ is orthogonal with $\mathbf{V}_2$ by definition, thus

$$\begin{aligned} d^\star =& \mathrm{rank}\{[\mathbf{V}_0, \mathbf{V}_1, \mathbf{V}_2]\} = \mathrm{rank}\{[\mathbf{V}_0, \mathbf{V}_1]\} + \mathrm{rank}\{\mathbf{V}_2\} \\ =& \mathrm{rank}\{\mathbf{V}_0\} + \mathrm{rank}\{\mathbf{V}_1\} + \mathrm{rank}\{\mathbf{V}_2\} \\ =& \min\{d_0 + d_1 + d_2, N_a\}. \end{aligned}$$

In *Case IV*, $\hat{\mathbf{V}} = [\mathbf{V}_0, \mathbf{V}_2]$ and $\hat{\mathbf{W}} = \mathbf{W}_2$. According to (8), $\mathrm{span}(\mathbf{H}_2\mathbf{W}_2) = \mathrm{span}(\mathbf{G}_1\mathbf{V}_2)$, which, together

TABLE I: A heuristic method to obtain $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ which is feasible to (5)

Case I: $N_a \geq N_e + N_b$. Let $\hat{\mathbf{V}} = \mathrm{null}(\mathbf{G}_1)$ and $\hat{\mathbf{W}} = \mathbf{0}$.

Case II: $N_j \geq N_b + N_e$. Let $\hat{\mathbf{W}} = \mathrm{null}(\mathbf{G}_2) \in \mathbb{C}^{N_a \times (N_j - N_b)}$ and $\hat{\mathbf{V}}$ be the right singular matrix of $\mathbf{H}_1$.

Case III: $N_a < N_e + N_b$ and $N_b < N_j < N_e + N_b$. For a start, let $\mathbf{V}_0 = \mathrm{null}(\mathbf{G}_1)$ and $d_0 = (N_a - N_e)^+$. Secondly, denote $\bar{\mathbf{H}}_2 = \mathbf{H}_2\mathbf{\Gamma} \in \mathbb{C}^{N_e \times (N_j - N_b)}$ where $\mathbf{\Gamma} = \mathrm{null}(\mathbf{G}_2) \in \mathbb{C}^{N_a \times (N_j - N_b)}$. Denote $\bar{\mathbf{G}}_1 = \mathbf{G}_1\mathbf{V}_0^c$ where $\mathbf{V}_0^c = \mathrm{null}(\mathbf{V}_0^H) \in \mathbb{C}^{N_a \times N_e}$. Invoking the *GSVD Transform* of $(\bar{\mathbf{H}}_2^H, \bar{\mathbf{G}}_1^H)$ yields

$$(\mathbf{\Psi}_1, \mathbf{\Psi}_2, \mathbf{D}_1, \mathbf{D}_2, \mathbf{X}, k_3, r_3, s_3) = \mathrm{gsvd}(\bar{\mathbf{H}}_2^H, \bar{\mathbf{G}}_1^H). \quad (6)$$

Subsequently, let $d_1 = s_3$, $c_3 = r_3 + N_e - k_3$, and check

1) If $d_0 + d_1 \geq N_b$, let $\mathbf{W}_1 = \mathbf{\Gamma}\mathbf{\Psi}_1(:, r_3 + 1 : r_3 + N_b - d_0)$ and $\mathbf{V}_1 = \mathbf{V}_0^c\mathbf{\Psi}_2(:, c_3 + 1 : c_3 + N_b - d_0)$. Lastly, let $\hat{\mathbf{V}} = [\mathbf{V}_0, \mathbf{V}_1]$ and $\hat{\mathbf{W}} = \mathbf{W}_1$.
2) Otherwise, let $\mathbf{W}_1 = \mathbf{\Gamma}\mathbf{\Psi}_1(:, r_3 + 1 : r_3 + s_3)$ and $\mathbf{V}_1 = \mathbf{V}_0^c\mathbf{\Psi}_2(:, c_3 + 1 : c_3 + s_3)$. Thirdly, denote $\mathbf{V}_{01}^c = \mathrm{null}([\mathbf{V}_0, \mathbf{V}_1]^H) \in \mathbb{C}^{N_a \times (N_a - d_0 - d_1)}$ and $\tilde{\mathbf{G}}_1 = \mathbf{G}_1\mathbf{V}_{01}^c$. Invoking the *GSVD Transform* of $(\mathbf{H}_2^H, \tilde{\mathbf{G}}_1^H)$ yields

$$(\tilde{\mathbf{\Psi}}_1, \tilde{\mathbf{\Psi}}_2, \tilde{\mathbf{D}}_1, \tilde{\mathbf{D}}_2, \tilde{\mathbf{X}}, k_4, r_4, s_4) = \mathrm{gsvd}(\mathbf{H}_2^H, \tilde{\mathbf{G}}_1^H). \quad (7)$$

Then let $\mathbf{W}_2 = \tilde{\mathbf{\Psi}}_1(:, r_4 + 1 : r_4 + d_2)$ and $\mathbf{V}_2 = \mathbf{V}_{01}^c\tilde{\mathbf{\Psi}}_2(:, c_4 + 1 : c_4 + d_2)$ in which $d_2 = \min\{s_4, \lfloor \frac{N_b - (d_0 + d_1)}{2} \rfloor\}$ and $c_4 = r_4 + (N_a - d_0 - d_1) - k_4$. Lastly, let $\hat{\mathbf{V}} = [\mathbf{V}_0, \mathbf{V}_1, \mathbf{V}_2]$ and $\hat{\mathbf{W}} = [\mathbf{W}_1, \mathbf{W}_2]$.

Case IV: $N_a < N_e + N_b$ and $N_j \leq N_b$. For a start, let $\mathbf{V}_0 = \mathrm{null}(\mathbf{G}_1)$ and $d_0 = (N_a - N_e)^+$. Secondly, denote $\mathbf{V}_0^c = \mathrm{null}(\mathbf{V}_0^H) \in \mathbb{C}^{N_a \times N_e}$ and $\bar{\mathbf{G}}_1 = \mathbf{G}_1\mathbf{V}_0^c$. Invoking the *GSVD Transform* of $(\mathbf{H}_2^H, \bar{\mathbf{G}}_1^H)$ yields

$$(\mathbf{\Psi}_1, \mathbf{\Psi}_2, \mathbf{D}_1, \mathbf{D}_2, \mathbf{X}, k_4, r_4, s_4) = \mathrm{gsvd}(\mathbf{H}_2^H, \bar{\mathbf{G}}_1^H). \quad (8)$$

Then let $\mathbf{W}_2 = \mathbf{\Psi}_1(:, r_4 + 1 : r_4 + d_2)$ and $\mathbf{V}_2 = \mathbf{V}_0^c\mathbf{\Psi}_2(:, c_4 + 1 : c_4 + d_4)$ in which $d_2 = \min\{s_4, \lfloor \frac{N_b - d_0}{2} \rfloor\}$ and $c_4 = r_4 + N_a - k_4$. Lastly, let $\hat{\mathbf{V}} = [\mathbf{V}_0, \mathbf{V}_2]$ and $\hat{\mathbf{W}} = \mathbf{W}_2$.

TABLE II: Summary of the closed-form results on $s.d.o.f.$

Inequalities on the number of antennas at terminals	$s.d.o.f.$
$N_a \geq N_e + N_b$	$\min\{N_a, N_b\}$
$N_j \geq N_e + N_b$	
$2N_b + N_e - N_j \leq N_a < N_e + N_b$ $N_b < N_j < N_e + N_b$	
$N_b + N_e - N_j < N_a < 2N_b + N_e - N_j$ $N_b < N_j < N_e + N_b$	$N_a + N_j - (N_b + N_e) + \min\{s, \lfloor \frac{2N_b+N_e-N_a-N_j}{2} \rfloor\}$ $s = \min\{N_b + N_e - N_j, N_e\} + \min\{N_j, N_e\} - N_e$
$N_e < N_a < N_e + N_b$, $N_j \leq N_b$	$N_a - N_e + \min\{s, \lfloor \frac{N_b+N_e-N_a}{2} \rfloor\}$, $s = \min\{N_j, N_e\}$
$N_a \leq N_b + N_e - N_j$, $N_b < N_j < N_e + N_b$	$\min\{s, \lfloor \frac{N_b}{2} \rfloor\}$
$N_a \leq N_e$, $N_j \leq N_b$	$s = \min\{N_a, N_e\} + \min\{N_j, N_e\} - \min\{N_a + N_j, N_e\}$

with $\mathbf{G}_1\mathbf{V}_0 = \mathbf{0}$, gives $\text{span}(\mathbf{H}_2\hat{\mathbf{W}}) = \text{span}(\mathbf{G}_1\hat{\mathbf{V}})$. In addition, $\text{span}(\mathbf{H}_1\hat{\mathbf{V}}) \cap \text{span}(\mathbf{G}_2\hat{\mathbf{W}}) = \{\mathbf{0}\}$ due to $d_2 = \min\{s_4, \lfloor \frac{N_b-d_0}{2} \rfloor\}$. Thus, $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ is feasible to (5). Furthermore, $\mathbf{V}_0$ is orthogonal with $\mathbf{V}_2$ by definition, thus

$$\begin{aligned} d^\star =& \text{rank}\{[\mathbf{V}_0, \mathbf{V}_2]\} = \text{rank}\{\mathbf{V}_0\} + \text{rank}\{\mathbf{V}_2\} \\ =& \min\{d_0 + d_2, N_a\}. \end{aligned}$$

Summarizing the above four cases, we can rewrite $d^\star$ into a more compact form as follows:

$$d^\star = \min\{d_0^\star + d_1^\star + d_2^\star, N_a, N_b\}, \tag{9}$$

in which

$$d_0^\star = (N_a - N_e)^+ \tag{10a}$$

$$d_1^\star = (\min\{N_a, N_e\} + (N_j - N_b)^+ - N_e)^+ \tag{10b}$$

$$d_2^\star = \min\{s, (\lfloor \frac{N_b - (d_0^\star + d_1^\star)}{2} \rfloor)^+\}. \tag{10c}$$

Here, $s \triangleq \min\{N_a - (d_0^\star + d_1^\star), N_e\} + \min\{N_j, N_e\} - \min\{N_a - (d_0^\star + d_1^\star) + N_j, N_e\}$.

Proposition 2: On d defined in (5), we have $d = d^\star$.

Proof: By definition, $d \geq d^\star$ holds true. On the other hand, for any feasible point of the problem of (5), $\{\tilde{\mathbf{V}}, \tilde{\mathbf{W}}\}$, $\text{rank}\{\mathbf{H}_1\tilde{\mathbf{V}}\} \leq d^\star$. Therefore, $d \leq d^\star$. Combining these two facts, we conclude $d = d^\star$. Due to the space limitation, please refer to Appendix F of a longer version of this paper [19] for more details. ■

Remark 2: According to Proposition 2, it is straight-forward that the feasible solution $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ given in Table I is also the optimal solution to (5).

V. Maximal Achievable S.D.o.F.

In this section, we give the maximal achievable S.D.o.F. and also the precoding matrices which achieve the maximal S.D.o.F. in closed-form.

Theorem 1: Consider a helper-assisted MIMO Gaussian wiretap channel, as depicted in Fig.1,

$$s.d.o.f. = d^\star, \tag{11}$$

where $d^\star$ is given in (9). Moreover, the precoding matrices $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ given in Table I achieve the maximal S.D.o.F..

Proof: Combining Proposition 1 and Proposition 2, it is clear that $s.d.o.f. = d^\star$. This completes the proof. ■

Remark 3: To gain more insight into $s.d.o.f.$, we give Table II which clarifies the connection of $s.d.o.f.$ to the antenna configurations.

Corollary 1: The feasible point $\{\hat{\mathbf{V}}, \hat{\mathbf{W}}\}$ for the optimization problem of (5), given in Table I, serves as a S.D.o.F.-optimal solution to the secrecy rate maximization problem in (3). It achieves the maximal S.D.o.F.. Moreover, Table II clarifies the maximal achievable S.D.o.F. of a helper-assisted MIMO Gaussian wiretap channel, and reveals its specific connection to the number of antennas at each terminal.

Proof: With Theorem 1, it is straight-forward to arrive at these conclusions. This completes the proof. ■

Corollary 2: When $N_b > 1$, the maximal achievable S.D.o.F. of a helper-assisted MIMO Gaussian wiretap channel is zero if and only if $N_e \geq N_a + N_j$. When $N_b = 1$, the maximal achievable S.D.o.F. of a helper-assisted MIMO Gaussian wiretap channel is zero if and only if $N_e \geq N_a + N_j - 1$.

Proof: According to Table II, it is easy to verify that $s.d.o.f. = 0$ can only happen when $N_a \leq N_e$ and $N_j \leq N_e + N_b - N_a$. With these two inequalities, we then distinguish our discussion into three subcases, and give the proof. For more details, please refer to Appendix G of our paper [19]. ■

VI. Conclusion

We have examined maximal achievable secrecy degrees of freedoms (S.D.o.F.) of a MIMO Gaussian wiretap channel, where a multi-antenna external helper is available. We have addressed the S.D.o.F. maximization analytically. Specifically, we have obtained an analytical S.D.o.F.-optimal solution to the secrecy rate maximization problem, based on which, we have obtained the maximal achievable S.D.o.F. in closed-form. These results uncovered the connection between the maximal achievable S.D.o.F. and antenna configurations, thus shedding light on how the secrecy capacity of a helper-assisted MIMO Gaussian wiretap channel behaves. Our analytical results prove that for the special case of single-antenna legitimate receiver, a S.D.o.F. of 1 can be achieved if and only if $N_e < N_a + N_j - 1$; for the case of multi-antenna legitimate receiver, the maximal achievable S.D.o.F. is zero if and only if $N_e \geq N_a + N_j$.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[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] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[9] 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.

[10] Q. Li, M. Hong, H.-T. Wai, and et. al, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, May 2013.

[11] Z. Chu, K. Cumanan, Z. Ding, and et. al, "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.

[12] 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.

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

[14] T. Tsiligkaridis, "Secure MIMO communications under quantized channel feedback in the presence of jamming," *IEEE Trans. Signal Process.*, vol. 62, no. 23, pp. 6265–6275, Dec. 2014.

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

[16] M. Nafea and A. Yener, "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.

[17] ——, "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.

[18] 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.

[19] L. Li, Z. Chen, J. Fang, and A. P. Petropulu, "On the secrecy capacity of MIMO Gaussian wiretap channel with a cooperative jammer," *[online], Available: http://arxiv.org/abs/1509.04624*.