Secure Degrees of Freedom for the MIMO Wiretap Channel with a Multiantenna Cooperative Jammer

Mohamed Nafea and Aylin Yener

Department of Electrical Engineering, The Pennsylvania State University, University Park, PA 16802

***Abstract*—A multiple antenna Gaussian wiretap channel with a multiantenna cooperative jammer (CJ) is considered and the secure degrees of freedom (s.d.o.f.), with N antennas at the sender, receiver, and eavesdropper, is derived for all possible values of the number of antennas at the cooperative jammer, K. In particular, the upper and lower bounds for the s.d.o.f. are provided for different ranges of K and shown to coincide. Gaussian signaling both for transmission and jamming is shown to be sufficient to achieve the s.d.o.f. of the channel, when the s.d.o.f. is integer-valued. By contrast, when the channel has a non-integer s.d.o.f., structured signaling and joint signal space and signal scale alignment are employed to achieve the s.d.o.f.**

I. Introduction

Information theoretic secrecy [1] guarantees secure communication in the presence of an eavesdropper. Information theoretic secrecy of multiterminal and multiantenna channels has been studied extensively, e.g., [2]–[9]. In particular, the Gaussian wiretap channel (WTC) with a *cooperative jammer* (CJ) was studied in [2]–[8]. A CJ can improve the secrecy rate and even the prelog factor of the secrecy rate, i.e., the secure degrees of freedom (s.d.o.f.) [5]. Relying on cooperative jamming and structured signaling, [6], [7] identified the s.d.o.f. for several single-antenna WTC models. In this paper, we extend [6] to a multiantenna secure communication scenario.

We focus on a multiantenna Gaussian WTC with a K-antenna CJ and N antennas at each of the transmitter, receiver, and wiretapper. For $0 \leq K \leq 2N$, we characterize the s.d.o.f. arriving at the s.d.o.f. of N at $K = 2N$, concluding that increasing K over $2N$ cannot improve the s.d.o.f. We derive an upper bound on the s.d.o.f. which allows for cooperation between the transmitter and CJ, and show that this bound is tight for $0 \leq K \leq \frac{N}{2}$. Next, for $N \leq K \leq 2N$, we derive another upper bound which incorporates both the secrecy and reliability constraints. We use this upper bound for $K = N$ to upper bound the s.d.o.f. for all $\frac{N}{2} < K < N$. We show that increasing K from $\lceil \frac{N}{2} \rceil$ to N does not increase the s.d.o.f.

Next, we divide $0 \leq K \leq 2N$ into five different ranges and propose an achievable scheme which meets with the derived upper bound for each range. Whenever the s.d.o.f. is integer-valued, we show that Gaussian signaling at the transmitter and the CJ is sufficient to achieve the s.d.o.f. of the channel. By contrast, when the s.d.o.f. is not an integer, structured signaling along with joint signal space and signal scale alignment are needed. When K is larger than N, a linear precoder is utilized at the CJ so that some jamming signals are transmitted over directions invisible to the legitimate receiver.

This work was supported by NSF Grants CCF 09-64362, 13-19338 and CNS 13-14719.

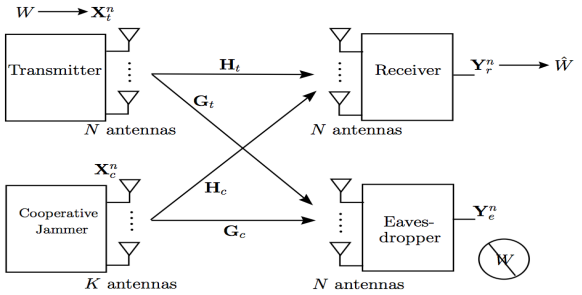

Fig. 1. MIMO Gaussian WTC with a multiantenna CJ.

Overall, this study settles the secrecy capacity of the $N \times N \times N$ MIMO wiretap channel in the high SNR, when a multiantenna CJ is available as a helper. As compared to the single antenna counterpart that uses real interference alignment with one dimensional lattices, here we need to use a variety of spatial and signal scale alignment techniques in concert to coordinate multiple antenna transmissions.

Notation: For matrix $\mathbf{A}$, $||\mathbf{A}||$ denotes its *induced* norm. For vector $\mathbf{V}$, $\mathbf{V}_i^j = [V_i \cdots V_j]^T$, where $1 \leq i < j \leq n$, and $||\mathbf{V}||$ denotes Euclidean norm. $\mathbf{0}_{m\times n}$ denotes an $m \times n$ matrix of zeros. The set of integers $\{-Q, \cdots, Q\}$ is denoted by $(-Q, Q)_{\mathbb{Z}}$. $\mathbb{Z}[j]$ denotes the set of complex integers.

II. Channel Model and Definitions

We consider a multiantenna Gaussian WTC composed of a transmitter, a receiver, an eavesdropper each with N antennas, and a K-antenna CJ, see Fig.1. The received signals at the receiver and eavesdropper at the nth channel use are given by

$$\mathbf{Y}_r(n) = \mathbf{H}_t\mathbf{X}_t(n) + \mathbf{H}_c\mathbf{X}_c(n) + \mathbf{Z}_r(n) \quad (1)$$

$$\mathbf{Y}_e(n) = \mathbf{G}_t\mathbf{X}_t(n) + \mathbf{G}_c\mathbf{X}_c(n) + \mathbf{Z}_e(n), \quad (2)$$

where $\mathbf{X}_t(n)$, $\mathbf{X}_c(n)$ are the transmitted signals from the transmitter and CJ, respectively. $\mathbf{H}_t, \mathbf{G}_t \in \mathbb{C}^{N\times N}$ are the transmitter's channel matrices to the legitimate receiver and to the eavesdropper, and $\mathbf{H}_c, \mathbf{G}_c \in \mathbb{C}^{N\times K}$ are the channel matrices from the CJ to the legitimate receiver and eavesdropper. The channel gains are static, and *complex-valued*. $\mathbf{Z}_r(n)$ and $\mathbf{Z}_e(n)$ denote the complex Gaussian noise at the nth channel use, i.e., $\mathbf{Z}_r(n), \mathbf{Z}_e(n) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$, are independent from one another and both are independent and identically

978-1-4799-5999-0/14/$31.00 ©2014 IEEE

distributed (i.i.d.) across[1] n. The power constraints at the transmitter and CJ are $\mathrm{E}\left\{\mathbf{X}_t^H\mathbf{X}_t\right\}$, $\mathrm{E}\left\{\mathbf{X}_c^H\mathbf{X}_c\right\} \le P$.

Let $\mathbf{X}_t^n = [\mathbf{X}_t(1)\cdots\mathbf{X}_t(n)]$. $\mathbf{X}_c^n, \mathbf{Y}_r^n, \mathbf{Y}_e^n, \mathbf{Z}_r^n, \mathbf{Z}_e^n$ are defined similarly. The transmitter intends to send a secret message $W \in \mathcal{W}$ to the legitimate receiver in the presence of the eavesdropper. W is mapped into the transmitted signal $\mathbf{X}_t^n \in \mathcal{X}_t^n$ by using a stochastic encoder $f : \mathcal{W} \mapsto \mathcal{X}_t^n$ at the transmitter. The receiver forms an estimate of W, denoted by $\hat{W}$. Secrecy rate R_s is achievable if for any $\epsilon > 0$, there exists a channel code, $\left(2^{nR_s}, n\right)$, such that

$$\Pr\left\{\hat{W} \neq W\right\} \le \epsilon; \quad \frac{1}{n}H(W|\mathbf{Y}_e^n) \ge \frac{1}{n}H(W) - \epsilon. \tag{3}$$

The achievable s.d.o.f. for a given secrecy rate, R_s, is

$$D_s = \lim_{P\to\infty} \frac{R_s}{\log P}. \tag{4}$$

The CJ transmits $\mathbf{X}_c^n \in \mathcal{X}_c^n$. The jamming signal $\mathbf{X}_c^n$ is not meant to convey a message. There is no common randomness between the transmitter and the CJ.

III. Main Result

Theorem 1 *The s.d.o.f. of the multiantenna Gaussian WTC with a K-antenna CJ and N antennas at each of its nodes is*

$$D_s = \begin{cases} K, & \text{for } 0 \le K \le \frac{N}{2} \\ \frac{N}{2}, & \text{for } \frac{N}{2} < K \le N \\ \frac{K}{2}, & \text{for } N < K \le 2N. \end{cases} \tag{5}$$

Theorem 1 provides a complete characterization for the s.d.o.f. of the channel. The s.d.o.f. for $K = 2N$ is equal to N, that is equal to the d.o.f. of the N-antenna Gaussian channel with no secrecy constraint. Thus, the s.d.o.f. can not be increased by increasing K over $2N$. Interestingly, Theorem 1 shows that the s.d.o.f. of the channel is not increased by increasing K from $\left\lceil \frac{N}{2} \right\rceil$ to N. In Sections IV and V, we provide the converse and achievability proofs for Theorem 1.

IV. Converse

A. $0 \le K \le N$

We allow for cooperation between the transmitter and CJ, obtain, in effect a multiantenna Gaussian WTC with $N+K$-antenna transmitter, N-antenna receiver, and N-antenna eavesdropper. The secrecy rate of this channel is bounded as [9]

$$\bar{R}_s \le \log\det\left(\mathbf{I}_N + \frac{P}{K}\bar{\mathbf{H}}\bar{\mathbf{G}}^{\sharp}\bar{\mathbf{H}}^H\right) + o(\log P), \tag{6}$$

where $\bar{\mathbf{H}}, \bar{\mathbf{G}} \in \mathbb{C}^{N\times N+K}$ are the channel matrices from the combined transmitter to the receiver and eavesdropper, and $\bar{\mathbf{G}}^{\sharp}$ is the projection matrix onto $\mathcal{N}(\bar{\mathbf{G}})$. We also have [9]

$$\bar{\mathbf{H}}\bar{\mathbf{G}}^{\sharp}\bar{\mathbf{H}}^H = \mathbf{\Psi}\begin{bmatrix} \mathbf{0}_{N-K\times N-K} & \mathbf{0}_{N-K\times K} \\ \mathbf{0}_{K\times N-K} & \mathbf{\Omega} \end{bmatrix}\mathbf{\Psi}^H, \tag{7}$$

where $\mathbf{\Psi}$ is a unitary matrix and $\mathbf{\Omega}$ is a non-singular matrix. By substituting (7) in (6), it can be easily shown that

$$\bar{R}_s \le K\log P + o(\log P). \tag{8}$$

[1]Throughout the paper, we omit index n whenever possible.

The secrecy rate for the original channel, R_s, is upper bounded by $\bar{R}_s$. Using (4), the s.d.o.f., D_s, is *upper bounded by* K.

B. $N \le K \le 2N$

Here, we extend the converse proof in [6] to the multi-antenna channel. Let ϕ_i, $i = 1, \cdots, 6$, denote constants that do not depend on the power P. R_s can be upper bounded as

$$\begin{aligned} nR_s = H(W) &\le H(W|\mathbf{Y}_e^n) + n\epsilon - H(W|\mathbf{Y}_r^n) + n\delta && (9)\\ &\le I(W;\mathbf{Y}_r^n|\mathbf{Y}_e^n) + n\phi_1 && (10)\\ &\le h(\mathbf{Y}_r^n|\mathbf{Y}_e^n) - h(\mathbf{Y}_r^n|W\mathbf{Y}_e^n\mathbf{X}_t^n\mathbf{X}_c^n) + n\phi_1 && (11)\\ &= h(\mathbf{Y}_r^n\mathbf{Y}_e^n) - h(\mathbf{Y}_e^n) - h(\mathbf{Z}_r^n) + n\phi_1. && (12)\end{aligned}$$

(9) follows from (3) and Fano's inequality; $\phi_1 = \epsilon + \delta$.

Define $\tilde{\mathbf{X}}_t = \mathbf{X}_t + \tilde{\mathbf{Z}}_t$, $\tilde{\mathbf{X}}_c = \mathbf{X}_c + \tilde{\mathbf{Z}}_c$, where $\tilde{\mathbf{Z}}_t \sim \mathcal{CN}(\mathbf{0}, \mathbf{K}_t)$ and $\tilde{\mathbf{Z}}_c \sim \mathcal{CN}(\mathbf{0}, \mathbf{K}_c)$. $\mathbf{K}_t, \mathbf{K}_c$ are chosen as $\mathbf{K}_t = \rho^2\mathbf{I}_N$, $\mathbf{K}_c = \beta^2\mathbf{I}_K$, where $0 < \rho \le \frac{1}{||\mathbf{G}_t^H||}$ and $0 < \beta \le \frac{1}{||\mathbf{H}_c^H||}$. $\tilde{\mathbf{Z}}_t$ is independent from $\tilde{\mathbf{Z}}_c$ and both are independent from $\{\mathbf{X}_t, \mathbf{X}_c, \mathbf{Z}_r, \mathbf{Z}_e\}$. $\tilde{\mathbf{Z}}_t^n, \tilde{\mathbf{Z}}_c^n$ are i.i.d. sequences of $\tilde{\mathbf{Z}}_t, \tilde{\mathbf{Z}}_c$, respectively. Let $\tilde{\mathbf{Z}}_1 = -\mathbf{H}_t\tilde{\mathbf{Z}}_t - \mathbf{H}_c\tilde{\mathbf{Z}}_c + \mathbf{Z}_r$ and $\tilde{\mathbf{Z}}_2 = -\mathbf{G}_t\tilde{\mathbf{Z}}_t - \mathbf{G}_c\tilde{\mathbf{Z}}_c + \mathbf{Z}_e$, where $\tilde{\mathbf{Z}}_1 \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma}_{\tilde{\mathbf{Z}}_1})$, $\tilde{\mathbf{Z}}_2 \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma}_{\tilde{\mathbf{Z}}_2})$, $\mathbf{\Sigma}_{\tilde{\mathbf{Z}}_1} = \mathbf{H}_t\mathbf{K}_t\mathbf{H}_t^H + \mathbf{H}_c\mathbf{K}_c\mathbf{H}_c^H + \mathbf{I}_N$, and $\mathbf{\Sigma}_{\tilde{\mathbf{Z}}_2} = \mathbf{G}_t\mathbf{K}_t\mathbf{G}_t^H + \mathbf{G}_c\mathbf{K}_c\mathbf{G}_c^H + \mathbf{I}_N$. $\tilde{\mathbf{Z}}_1^n, \tilde{\mathbf{Z}}_2^n$ are i.i.d. sequences of $\tilde{\mathbf{Z}}_1, \tilde{\mathbf{Z}}_2$. Thus, using (12), we have

$$\begin{aligned} nR_s &\le h(\mathbf{Y}_r^n\mathbf{Y}_e^n\tilde{\mathbf{X}}_t^n\tilde{\mathbf{X}}_c^n) - h(\tilde{\mathbf{X}}_t^n\tilde{\mathbf{X}}_c^n|\mathbf{Y}_r^n\mathbf{Y}_e^n) \\ &\qquad - h(\mathbf{Y}_e^n) + n\phi_2 && (13)\\ &\le h(\tilde{\mathbf{X}}_t^n\tilde{\mathbf{X}}_c^n) + h(\mathbf{Y}_r^n|\tilde{\mathbf{X}}_t^n\tilde{\mathbf{X}}_c^n) + h(\mathbf{Y}_e^n|\tilde{\mathbf{X}}_t^n\tilde{\mathbf{X}}_c^n) \\ &\qquad - h(\tilde{\mathbf{X}}_t^n\tilde{\mathbf{X}}_c^n|\mathbf{Y}_r^n\mathbf{Y}_e^n\mathbf{X}_t^n\mathbf{X}_c^n) - h(\mathbf{Y}_e^n) + n\phi_2 && (14)\\ &\le h(\tilde{\mathbf{X}}_t^n) + h(\tilde{\mathbf{X}}_c^n) + h(\tilde{\mathbf{Z}}_1^n|\tilde{\mathbf{X}}_t^n\tilde{\mathbf{X}}_c^n) + h(\tilde{\mathbf{Z}}_2^n|\tilde{\mathbf{X}}_t^n\tilde{\mathbf{X}}_c^n) \\ &\qquad - h(\tilde{\mathbf{Z}}_t^n\tilde{\mathbf{Z}}_c^n) - h(\mathbf{Y}_e^n) + n\phi_2 && (15)\\ &\le h(\tilde{\mathbf{X}}_t^n) + h(\tilde{\mathbf{X}}_c^n) - h(\mathbf{Y}_e^n) + n\phi_3. && (16)\end{aligned}$$

Using infinite divisibility of Gaussian distribution, a stochastically equivalent form of $\mathbf{Z}_e$ is $\mathbf{Z}_e' = \mathbf{G}_t\tilde{\mathbf{Z}}_t + \tilde{\mathbf{Z}}_e$. $\tilde{\mathbf{Z}}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N - \mathbf{G}_t\mathbf{K}_t\mathbf{G}_t^H)$ is independent from $\{\tilde{\mathbf{Z}}_t, \tilde{\mathbf{Z}}_c, \mathbf{X}_t, \mathbf{X}_c, \mathbf{Z}_r\}$. Thus, a stochastically equivalent form of $\mathbf{Y}_e^n$ is $\mathbf{Y}_e'^n = \mathbf{G}_t\tilde{\mathbf{X}}_t^n + \mathbf{G}_c\mathbf{X}_c^n + \tilde{\mathbf{Z}}_e^n$. Since $\mathbf{G}_t\tilde{\mathbf{X}}_t^n, \mathbf{G}_c\mathbf{X}_c^n + \tilde{\mathbf{Z}}_e^n$ are independent, we have

$$\begin{aligned} h(\mathbf{Y}_e^n) = h(\mathbf{Y}_e'^n) &\ge h(\mathbf{G}_t\tilde{\mathbf{X}}_t^n) && (17)\\ &= h(\tilde{\mathbf{X}}_t^n) + n\log\det(\mathbf{G}_t). && (18)\end{aligned}$$

Substituting (18) in (16) gives us

$$nR_s \le h(\tilde{\mathbf{X}}_{c_2}^n) + h(\tilde{\mathbf{X}}_{c_1}^n|\tilde{\mathbf{X}}_{c_2}^n) + n\phi_4, \tag{19}$$

where $\tilde{\mathbf{X}}_{c_1} = [\tilde{X}_{c_1}\cdots\tilde{X}_{c_N}]^T, \tilde{\mathbf{X}}_{c_2} = [\tilde{X}_{c_{N+1}}\cdots\tilde{X}_{c_K}]^T$, and $\tilde{X}_{c_i} = X_{c_i} + \tilde{Z}_{c_i}$. Let $\mathbf{h}_{c_k}$ be the kth column vector of $\mathbf{H}_c = [\mathbf{H}_{c_1}\ \mathbf{H}_{c_2}]$, $\mathbf{H}_{c_1} = [\mathbf{h}_{c_1}\cdots\mathbf{h}_{c_N}]$ and $\mathbf{H}_{c_2} = [\mathbf{h}_{c_{N+1}}\cdots\mathbf{h}_{c_K}]$. In order to reliably transmit the message W, we must have

$$\begin{aligned} nR_s \le I(\mathbf{X}_t^n;\mathbf{Y}_r^n) &= h(\mathbf{Y}_r^n) - h(\mathbf{H}_c\mathbf{X}_c^n + \mathbf{Z}_r^n) && (20)\\ &\le h(\mathbf{Y}_r^n) - h(\mathbf{H}_{c_1}\tilde{\mathbf{X}}_{c_1}^n + \mathbf{H}_{c_2}\tilde{\mathbf{X}}_{c_2}^n) && (21)\\ &\le h(\mathbf{Y}_r^n) - h(\mathbf{H}_{c_1}\tilde{\mathbf{X}}_{c_1}^n|\mathbf{H}_{c_2}\tilde{\mathbf{X}}_{c_2}^n) && (22)\end{aligned}$$

$$\leq h(\mathbf{Y}_r^n) - h(\mathbf{H}_{c_1}\tilde{\mathbf{X}}_{c_1}^n|\tilde{\mathbf{X}}_{c_2}^n) \quad (23)$$

$$= h(\mathbf{Y}_r^n) - h(\tilde{\mathbf{X}}_{c_1}^n|\tilde{\mathbf{X}}_{c_2}^n) - n\log\det(\mathbf{H}_{c_1}), \quad (24)$$

where (21) follows similar to (17), and (22) follows since for correlated $\mathbf{X}$ and $\mathbf{Y}$, $h(\mathbf{X}+\mathbf{Y}) \geq h(\mathbf{X}+\mathbf{Y}|\mathbf{Y}) = h(\mathbf{X}|\mathbf{Y})$.

Combining (19) and (24), we get

$$nR_s \leq \frac{1}{2}\sum_{i=1}^{n}\left(\sum_{k=1}^{N} h(Y_{r_k}(i)) + \sum_{k=N+1}^{K} h(\tilde{X}_{c_k}(i))\right) + n\phi_5. \quad (25)$$

Using Cauchy-Schwarz inequality and the power constraints, we can show that the variance of $Y_{r_k}(i)$ is bounded as $\mathrm{Var}\{Y_{r_k}(i)\} \leq 1 + h^2P$, where $h^2 = \max_k \left(||\mathbf{h}_{t_k}^{r^T}||^2 + ||\mathbf{h}_{c_k}^{r^T}||^2\right)$, and $\mathbf{h}_{t_k}^r, \mathbf{h}_{c_k}^r$ are the kth row vectors of $\mathbf{H}_t$ and $\mathbf{H}_c$. Thus, $h(Y_{r_k}(i)) \leq \log 2\pi e(1+h^2P)$. Similarly, we can show that $h(\tilde{X}_{c_k}(i)) \leq \log 2\pi e(\beta^2+P)$. Thus,

$$R_s \leq \frac{N}{2}\log(1+h^2P) + \frac{K-N}{2}\log(\beta^2+P) + \phi_6, \quad (26)$$

and the s.d.o.f. is upper bounded as $D_s \leq \frac{K}{2}$.

C. Obtaining the upper bound for all K

We use the upper bound obtained in Section IV-A for $0 \leq K \leq \frac{N}{2}$, and the upper bound obtained in Section IV-B for $N \leq K \leq 2N$. By comparing the two, it is evident that the upper bound from Section IV-A is greater than $\frac{N}{2}$ for $\frac{N}{2} < K \leq N$. Since we know, from Section IV-B, that at $K = N$, the upper bound is $\frac{N}{2}$, we can use $\frac{N}{2}$ as the upper bound for $\frac{N}{2} < K \leq N$. Combining these statements, we get (5). Next, we shall see the achievability of (5).

V. Achievable Schemes

We divide the range $0 \leq K \leq 2N$ into five cases and propose an achievable scheme for each case. For all the achievable schemes, we have the n-letter signals, $\mathbf{X}_t^n$ and $\mathbf{X}_c^n$, as i.i.d. sequences. Since $\mathbf{X}_c^n$ is independent from $\mathbf{X}_t^n$, we have in effect a memoryless WTC, and the following secrecy rate is achievable by stochastic encoding [1]:

$$R_s = [I(\mathbf{X}_t;\mathbf{Y}_r) - I(\mathbf{X}_t;\mathbf{Y}_e)]^+. \quad (27)$$

A. Case 1: $0 \leq K \leq \frac{N}{2}$

The transmitter sends K independent Gaussian information streams and the CJ sends K independent Gaussian jamming streams. Since $2K \leq N$, the legitimate receiver can decode all the information and jamming streams at high SNR. The transmitter chooses a precoder, $\mathbf{P}_t$, which aligns its information streams over the jamming streams at the eavesdropper. The signals transmitted by the transmitter and the CJ are

$$\mathbf{X}_t = \mathbf{P}_t\mathbf{U}_t, \qquad \mathbf{X}_c = \mathbf{J}_c\mathbf{V}_c, \quad (28)$$

where $\mathbf{U}_t, \mathbf{V}_c \sim \mathcal{CN}(\mathbf{0}, \bar{P}\mathbf{I}_K)$. $\mathbf{U}_t$ and $\mathbf{V}_c$ are the information and jamming streams, respectively. $\mathbf{P}_t = \mathbf{G}_t^{-1}\mathbf{G}_c = [\mathbf{p}_{t_1}\cdots\mathbf{p}_{t_K}]$, and $\mathbf{J}_c = \mathbf{I}_K$. $\bar{P} = \frac{1}{\alpha}P$, where $\alpha = \max\{K, \sum_{i=1}^{K}||\mathbf{p}_{t_i}||^2\}$ to satisfy the power constraints. The received signals are expressed as

$$\mathbf{Y}_r = \begin{bmatrix}\mathbf{H}_t\mathbf{G}_t^{-1}\mathbf{G}_c & \mathbf{H}_c\end{bmatrix}\begin{bmatrix}\mathbf{U}_t^T & \mathbf{V}_c^T\end{bmatrix}^T + \mathbf{Z}_r \quad (29)$$

$$\mathbf{Y}_e = \mathbf{G}_c(\mathbf{U}_t + \mathbf{V}_c) + \mathbf{Z}_e. \quad (30)$$

We lower bound (27) as follows. First, $\begin{bmatrix}\mathbf{H}_t\mathbf{G}_t^{-1}\mathbf{G}_c & \mathbf{H}_c\end{bmatrix}$ is almost surely (a.s.) full column-rank. Thus,

$$I(\mathbf{X}_t;\mathbf{Y}_r) \geq K\log P + o(\log P). \quad (31)$$

Next, we upper bound the term $I(\mathbf{X}_t;\mathbf{Y}_e)$ as follows:

$$I(\mathbf{X}_t;\mathbf{Y}_e) = \log\frac{\det(\mathbf{I}_K + 2\bar{P}\mathbf{G}_c^H\mathbf{G}_c)}{\det(\mathbf{I}_K + \bar{P}\mathbf{G}_c^H\mathbf{G}_c)} \leq K. \quad (32)$$

By substituting (31) and (32) in (27), we have

$$R_s \geq K\log P + o(\log P) - K. \quad (33)$$

Hence, the achievable s.d.o.f. is lower bounded as $D_s \geq K$.

B. Case 2: $\frac{N}{2} < K \leq N$ and N is even

The s.d.o.f. is upper bounded by $\frac{N}{2}$ for all $\frac{N}{2} < K \leq N$. When N is even, the achievable scheme for $K = \frac{N}{2}$ can be used to achieve the s.d.o.f. of the channel for all $\frac{N}{2} < K \leq N$. The transmitted signals are given by (28), with $\mathbf{J}_c = [\mathbf{I}_{\frac{N}{2}} \ \mathbf{0}_{\frac{N}{2}\times K-\frac{N}{2}}]^T$, $\mathbf{P}_t = \mathbf{G}_t^{-1}\mathbf{G}_c\mathbf{J}_c$, $\mathbf{U}_t, \mathbf{V}_c \sim \mathcal{CN}(\mathbf{0}, \bar{P}\mathbf{I}_{\frac{N}{2}})$. Using the same analysis as in the previous case, the achievable s.d.o.f. is $\frac{N}{2}$ for any $\frac{N}{2} < K \leq N$, where N is even.

C. Case 3: $\frac{N}{2} < K \leq N$ and N is odd

For this case, we utilize structured signaling both at the transmitter and the CJ. In particular, we propose to use joint signal space alignment and the complex field equivalent of real interference alignment [10], [11]. The transmitter and CJ send $\frac{N+1}{2}$ streams each. The transmitter aligns its information streams over the jamming at the eavesdropper. The legitimate receiver projects its received signal over a direction orthogonal to all but one information and one jamming streams, decodes these two streams from the projection, and subtracts their effect from its received signal, leaving $N-1$ spatial dimensions for the other streams. For notational simplicity, let $d = \frac{N+1}{2}$.

The transmitted signals are given by (28) with $\mathbf{J}_c = [\mathbf{I}_d \ \mathbf{0}_{d\times K-d}]^T$, $\mathbf{P}_t = \mathbf{G}_t^{-1}\mathbf{G}_c\mathbf{J}_c$, $\mathbf{U}_t = [U_1\cdots U_d]^T$, $\mathbf{V}_c = [V_1\cdots V_d]^T$, $U_i = U_{i_{\mathrm{Re}}} + jU_{i_{\mathrm{Im}}}$, $V_i = V_{i_{\mathrm{Re}}} + jV_{i_{\mathrm{Im}}}$, for $i = 2,\cdots,d$, and U_1, V_1, $\{U_{i_{\mathrm{Re}}}\}_{i=2}^d$, $\{U_{i_{\mathrm{Im}}}\}_{i=2}^d$, $\{V_{i_{\mathrm{Re}}}\}_{i=2}^d$, $\{V_{i_{\mathrm{Im}}}\}_{i=2}^d$ are i.i.d. uniform over the set $\{a(-Q,Q)_{\mathbb{Z}}\}$. The values for a and the integer Q are chosen as

$$Q = P^{\frac{1-\epsilon}{2+\epsilon}} - \nu, \quad a = \gamma P^{\frac{3\epsilon}{2(2+\epsilon)}}, \quad (34)$$

where $\epsilon > 0$ can be arbitrarily small, and ν, γ are constants.

Let $\tilde{\mathbf{G}}_c = \mathbf{G}_c\mathbf{J}_c$. The received signal at the eavesdropper is

$$\mathbf{Y}_e = \tilde{\mathbf{G}}_c(\mathbf{U}_t + \mathbf{V}_c) + \mathbf{Z}_e. \quad (35)$$

We upper bound $I(\mathbf{X}_t;\mathbf{Y}_e)$ as follows:

$$I(\mathbf{X}_t;\mathbf{Y}_e) \leq I(\mathbf{X}_t;\mathbf{Y}_e,\mathbf{Z}_e) = I(\mathbf{X}_t;\mathbf{Y}_e|\mathbf{Z}_e) \quad (36)$$

$$= H\left(\tilde{\mathbf{G}}_c(\mathbf{U}_t + \mathbf{V}_c)\right) - H\left(\tilde{\mathbf{G}}_c\mathbf{V}_c\right) \quad (37)$$

$$= H(\mathbf{U}_t + \mathbf{V}_c) - H(\mathbf{V}_c) \tag{38}$$

$$\leq (2d-1)\log\left(\frac{4Q+1}{2Q+1}\right) \leq N, \tag{39}$$

where (38) follows since the mappings $\mathbf{U}_t + \mathbf{V}_c \mapsto \tilde{\mathbf{G}}_c(\mathbf{U}_t + \mathbf{V}_c)$, $\mathbf{V}_c \mapsto \tilde{\mathbf{G}}_c\mathbf{V}_c$ are invertible, since the entries of $\tilde{\mathbf{G}}_c$ are *rationally independent*[2]. Next, we derive a lower bound for $I(\mathbf{X}_t; \mathbf{Y}_r)$. The received signal at the legitimate receiver is

$$\mathbf{Y}_r = \mathbf{A}\mathbf{U}_t + \bar{\mathbf{H}}_c\mathbf{V}_c + \mathbf{Z}_r, \tag{40}$$

where $\mathbf{A} = \mathbf{H}_t\mathbf{G}_t^{-1}\mathbf{G}_c\mathbf{J}_c$ and $\bar{\mathbf{H}}_c = \mathbf{H}_c\mathbf{J}_c$. Let $\mathbf{a}_i$ and $\mathbf{h}_{c_i}$ be the ith column vectors of $\mathbf{A}$ and $\bar{\mathbf{H}}_c$, respectively. The legitimate receiver chooses $\mathbf{b} \in \mathbb{C}^N$ such that $\mathbf{b} \perp \text{span}\{\mathbf{a}_2, \cdots, \mathbf{a}_d, \mathbf{h}_{c_2}, \cdots, \mathbf{h}_{c_d}\}$ and multiplies its received signal by the decoding matrix,

$$\mathbf{D} = \begin{bmatrix} \mathbf{b}^H \\ \mathbf{0}_{N-1\times 1} \quad \mathbf{I}_{N-1} \end{bmatrix}, \tag{41}$$

to obtain $\widetilde{\mathbf{Y}}_r = \mathbf{D}\mathbf{Y}_r = [\widetilde{Y}_{r_1} \;\; (\widetilde{\mathbf{Y}}_{r_2}^N)^T]^T$, where

$$\widetilde{Y}_{r_1} = f_1U_1 + f_2V_1 + Z' \tag{42}$$

$$\widetilde{\mathbf{Y}}_{r_2}^N = \widetilde{\mathbf{A}}\mathbf{U}_t + \widetilde{\mathbf{H}}_c\mathbf{V}_c + \mathbf{Z}_{r_2}^N, \tag{43}$$

$f_1 = \mathbf{b}^H\mathbf{a}_1$, $f_2 = \mathbf{b}^H\mathbf{h}_{c_1}$, $Z' = \mathbf{b}^H\mathbf{Z}_r$, $\widetilde{\mathbf{A}} = [\tilde{\mathbf{a}}_1 \cdots \tilde{\mathbf{a}}_d]$, $\widetilde{\mathbf{H}}_c = [\tilde{\mathbf{h}}_{c_1} \cdots \tilde{\mathbf{h}}_{c_d}]$, $\tilde{\mathbf{a}}_i = \mathbf{a}_{i_2}^N$, and $\tilde{\mathbf{h}}_{c_i} = \mathbf{h}_{c_{i_2}}^N$.

The legitimate receiver uses $\widetilde{Y}_{r_1}$ to decode U_1 and V_1. Since f_1, f_2 are a.s. rationally independent, the mapping $(U_1, V_1) \mapsto f_1U_1 + f_2V_1$ is bijective (i.e., invertible) [10]. The legitimate receiver employs a hard decision decoder which maps $\widetilde{Y}_{r_1} \in \tilde{\mathcal{Y}}_{r_1}$ to the nearest point in the constellation $\mathcal{R}_1 = f_1\mathcal{U}_1 + f_2\mathcal{V}_1$, where $\mathcal{U}_1, \mathcal{V}_1 = \{a(-Q, Q)_{\mathbb{Z}}\}$. Then, the legitimate receiver passes the output of the hard decision decoder through the bijective map $f_1U_1 + f_2V_1 \mapsto (U_1, V_1)$ to decode both U_1, V_1, and subtracts their effect from $\widetilde{\mathbf{Y}}_{r_2}^N$ to obtain

$$\bar{\mathbf{Y}}_r = \mathbf{B}\begin{bmatrix} \mathbf{U}_{t_2}^{d^T} & \mathbf{V}_{c_2}^{d^T} \end{bmatrix}^T + \mathbf{Z}_{r_2}^N. \tag{44}$$

$\mathbf{B} = \begin{bmatrix} \tilde{\mathbf{a}}_2 \cdots \tilde{\mathbf{a}}_d & \tilde{\mathbf{h}}_{c_2} \cdots \tilde{\mathbf{h}}_{c_d} \end{bmatrix} \in \mathbb{C}^{N-1\times N-1}$ is a.s. full rank due to the random generation assumption on the channel gains. Finally, by zero forcing, the receiver obtains $\mathbf{U}_{t_2}^d$ from $\bar{\mathbf{Y}}_r$.

The term $I(\mathbf{X}_t; \mathbf{Y}_r)$ is lower bounded as follows:

$$I(\mathbf{X}_t; \mathbf{Y}_r) \geq I(\mathbf{U}_t; \widetilde{\mathbf{Y}}_r) \tag{45}$$

$$\geq I(U_1; \widetilde{Y}_{r_1}) + I(\mathbf{U}_{t_2}^d; \widetilde{\mathbf{Y}}_{r_2}^N | U_1\widetilde{Y}_{r_1}), \tag{46}$$

where (45) follows since $\mathbf{U}_t \to \mathbf{X}_t \to \mathbf{Y}_r \to \widetilde{\mathbf{Y}}_r$ forms a Markov chain. The term $I(U_1; \widetilde{Y}_{r_1})$ can be bounded as

$$I(U_1; \widetilde{Y}_{r_1}) = H(U_1) - H(U_1|\widetilde{Y}_{r_1}) \tag{47}$$

$$\geq H(U_1) - 1 - P_{e_1}\log|\mathcal{U}_1| \tag{48}$$

$$= (1 - P_{e_1})\log(2Q+1) - 1, \tag{49}$$

where $P_{e_1} = \Pr\{\hat{U}_1 \neq U_1\}$, and (48) follows from Fano's inequality. Since the mapping $(U_1, V_1) \mapsto f_1U_1 + f_2V_1$ is invertible, the only source for error is the Gaussian noise Z'.

$$P_{e_1} \leq \Pr\left\{(\hat{U}_1, \hat{V}_1) \neq (U_1, V_1)\right\} \tag{50}$$

$$\leq \Pr\left\{|Z'| \geq \frac{d_{\min}}{2}\right\} = \exp\left(\frac{-d_{\min}^2}{4||\mathbf{b}||^2}\right), \tag{51}$$

where $|Z'| \sim \text{Rayleigh}(\frac{||\mathbf{b}||}{\sqrt{2}})$ and $d_{\min}$ is the minimum distance between points in the constellation $\mathcal{R}_1$, which can be lower bounded using the following lemma [10], [11].

Lemma 1 *For almost all* $\mathbf{z} \in \mathbb{C}^n$ *and for all* $\epsilon > 0$,

$$|p + \mathbf{z}.\mathbf{q}| > \left(\max_i q_i\right)^{-\left(\frac{n-1+\epsilon}{2}\right)}, \tag{52}$$

holds for all $\mathbf{q} \in \mathbb{Z}^n$, $p \in \mathbb{Z}$ *except for finitely many of them.*

Thus, for almost all channel gains, $d_{\min}$ is

$$d_{\min} = \inf_{U_1, V_1 \in \{a(-2Q, 2Q)_{\mathbb{Z}}\}} |f_1U_1 + f_2V_1| \tag{53}$$

$$\geq \frac{a|f_1|}{(2Q)^{\frac{\epsilon}{2}}} \geq \gamma|f_1|2^{-\frac{\epsilon}{2}}P^{\frac{\epsilon}{2}}. \tag{54}$$

Substituting (54) in (51) gives $P_{e_1} \leq \exp(-\mu P^{\epsilon})$, where $\mu = \frac{\gamma^2|f_1|^2 2^{-\epsilon}}{4||\mathbf{b}||^2}$. Using (34) and (49), we have

$$I(U_1; \widetilde{Y}_{r_1}) \geq \frac{1-\epsilon}{2+\epsilon}\log P + o(\log P). \tag{55}$$

Next, we lower bound the term $I(\mathbf{U}_{t_2}^d; \widetilde{\mathbf{Y}}_{r_2}^N | U_1\widetilde{Y}_{r_1})$. Define $\widetilde{\mathbf{B}} = [\mathbf{0}_{N-1\times 1} \;\; \mathbf{I}_{N-1}] - \frac{1}{f_2}\tilde{\mathbf{h}}_{c_1}\mathbf{b}^H$; $\bar{\mathbf{Y}}_r' = \mathbf{B}\begin{bmatrix} \mathbf{U}_{t_2}^{d^T} & \mathbf{V}_{c_2}^{d^T} \end{bmatrix}^T + \widetilde{\mathbf{B}}\mathbf{Z}_r$; $\widehat{\mathbf{Y}}_r' = \mathbf{B}^{-1}\bar{\mathbf{Y}}_r' = \begin{bmatrix} \mathbf{U}_{t_2}^{d^T} & \mathbf{V}_{c_2}^{d^T} \end{bmatrix}^T + \mathbf{B}^{-1}\widetilde{\mathbf{B}}\mathbf{Z}_r$, and $P_{e_2}^d = \Pr\{\hat{\mathbf{U}}_{t_2}^d \neq \mathbf{U}_{t_2}^d\}$. Thus, we have

$$I(\mathbf{U}_{t_2}^d; \widetilde{\mathbf{Y}}_{r_2}^N | U_1\widetilde{Y}_{r_1}) = I\left(\mathbf{U}_{t_2}^d; \widetilde{\mathbf{Y}}_{r_2}^N | U_1, f_2V_1 + Z'\right) \tag{56}$$

$$= I(\mathbf{U}_{t_2}^d; \bar{\mathbf{Y}}_r' | f_2V_1 + Z) \tag{57}$$

$$\geq I(\mathbf{U}_{t_2}^d; \bar{\mathbf{Y}}_r') \geq I(\mathbf{U}_{t_2}^d; \widehat{\mathbf{Y}}_r') \tag{58}$$

$$\geq \left(1 - P_{e_2}^d\right)\log(2Q+1)^{N-1} - 1. \tag{59}$$

Let $\widehat{\mathbf{Z}}_r = \boldsymbol{\Xi}\mathbf{Z}_r = [\hat{Z}_{r_2} \cdots \hat{Z}_{r_N}]^T$, where $\boldsymbol{\Xi} = \mathbf{B}^{-1}\widetilde{\mathbf{B}}$. Thus, $\widehat{\mathbf{Z}}_r \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Xi}\boldsymbol{\Xi}^H)$ and $|\hat{Z}_{r_i}| \sim \text{Rayleigh}(\sigma_i)$, where $\sigma_i^2 = \boldsymbol{\Xi}\boldsymbol{\Xi}^H(i,i)$. Using the union bound, we have

$$P_{e_2}^d \leq \sum_{i=2}^{d}\Pr\left\{\hat{U}_i \neq U_i\right\} \leq \sum_{i=2}^{d}\Pr\left\{|\hat{Z}_{r_i}| \geq \frac{a}{2}\right\} \tag{60}$$

$$\leq \frac{N-1}{2}\exp(-\mu' P^{\epsilon'}), \tag{61}$$

where $\mu' = \frac{\gamma^2}{8\sigma_{\max}^2}$, $\sigma_{\max} = \max_i \sigma_i$, and $\epsilon' = \frac{3\epsilon}{2+\epsilon}$. Thus,

$$I(\mathbf{U}_{t_2}^d; \widetilde{\mathbf{Y}}_{r_2}^N | U_1\widetilde{Y}_{r_1}) \geq \frac{1-\epsilon}{2+\epsilon}(N-1)\log P + o(\log P). \tag{62}$$

Thus, substituting (55) and (62) in (46) gives us

$$I(\mathbf{X}_t; \mathbf{Y}_r) \geq \frac{1-\epsilon}{2+\epsilon}N\log P + o(\log P), \tag{63}$$

[2]A set of complex numbers $\{c_1, \cdots, c_L\}$ are rationally independent if there is no set of rational numbers $\{r_1, \cdots, r_L\}$, rather than the all zeros set, such that $\sum_{i=1}^{L} r_ic_i = 0$ [10].

and using (4), (27), (39), and (63) results in $D_s \geq \frac{1-\epsilon}{2+\epsilon}N$. Since $\epsilon > 0$ is arbitrarily small, we can achieve s.d.o.f. of $\frac{N}{2}$.

D. Case 4: $N < K \leq 2N$ and K is even

The achievable scheme for this case involves transmitting $\frac{K}{2}$ Gaussian information and $\frac{K}{2}$ Gaussian jamming streams. The CJ sends $K-N$ out of its $\frac{K}{2}$ streams over the null space of $\mathbf{H}_c$, $\mathcal{N}(\mathbf{H}_c)$, leaving only $N-\frac{K}{2}$ streams visible to the legitimate receiver. At high SNR, the legitimate receiver can decode the $\frac{K}{2}$ information and the $N-\frac{K}{2}$ jamming streams. For notational simplicity, let $g = N-\frac{K}{2}$. The transmitted signals are given by (28), with $\mathbf{P}_t = \mathbf{G}_t^{-1}\mathbf{G}_c\mathbf{J}_c$, $\mathbf{J}_c = [\mathbf{J}_{\mathrm{I}}\ \mathbf{J}_n]$, $\mathbf{J}_{\mathrm{I}} = [\mathbf{I}_g\ \mathbf{0}_{g\times K-g}]^T$, $\mathbf{J}_n = [\mathbf{n}_1 \cdots \mathbf{n}_{K-N}]$, where $\{\mathbf{n}_1, \cdots, \mathbf{n}_{K-N}\}$ span $\mathcal{N}(\mathbf{H}_c)$, $\mathbf{U}_t, \mathbf{V}_c \sim \mathcal{CN}(\mathbf{0}, \bar{P}\mathbf{I}_{\frac{K}{2}})$, $\bar{P} = \frac{1}{\alpha'}P$, and α' is chosen to satisfy the power constraints.

Let $\mathbf{A} = \mathbf{H}_t\mathbf{G}_t^{-1}\mathbf{G}_c$. The received signals are given by

$$\mathbf{Y}_r = \bar{\mathbf{B}}\begin{bmatrix}\mathbf{U}_t^T & \mathbf{V}_{c_1}^{g^T}\end{bmatrix}^T + \mathbf{Z}_r \tag{64}$$

$$\mathbf{Y}_e = \mathbf{G}_c\mathbf{J}_c(\mathbf{U}_t + \mathbf{V}_c) + \mathbf{Z}_e, \tag{65}$$

where $\bar{\mathbf{B}} = \begin{bmatrix}\mathbf{A}\mathbf{J}_{\mathrm{I}} & \mathbf{A}\mathbf{J}_n & \mathbf{H}_c\mathbf{J}_{\mathrm{I}}\end{bmatrix} \in \mathbb{C}^{N\times N}$ can be written as

$$\bar{\mathbf{B}} = \begin{bmatrix}\mathbf{A} & \mathbf{H}_c\end{bmatrix}\begin{bmatrix}\mathbf{J}_{\mathrm{I}} & \mathbf{J}_n & \mathbf{0}_{K\times g}\\ \mathbf{0}_{K\times g} & \mathbf{0}_{K\times K-N} & \mathbf{J}_{\mathrm{I}}\end{bmatrix}. \tag{66}$$

By extending the proof in the Appendix in [8], we can show that $\bar{\mathbf{B}}$ is a.s. full rank. Thus, we have $I(\mathbf{X}_t;\mathbf{Y}_r) = \frac{K}{2}\log P + o(\log P)$. Similar to (32), we have $I(\mathbf{X}_t;\mathbf{Y}_e) \leq \frac{K}{2}$. Thus, the s.d.o.f. is lower bounded as $D_s \geq \frac{K}{2}$.

E. Case 5: $N < K \leq 2N$ and K is odd

The transmitter sends $\frac{K+1}{2}$ structured information and the CJ sends $\frac{K+1}{2}$ structured jamming streams. The CJ sends $K-N$ out of its streams over $\mathcal{N}(\mathbf{H}_c)$. The legitimate receiver projects its received signal over a direction orthogonal to all but one information and one jamming streams, decodes these two streams from the projection, and subtracts their effect from its received signal to decode the other information streams. Let $m = \frac{K+1}{2}$ and $l = N - \frac{K-1}{2}$. The transmitted signals are given by (28), with $\mathbf{P}_t = \mathbf{G}_t^{-1}\mathbf{G}_c\mathbf{J}_c$, $\mathbf{J}_c = [\mathbf{J}_{\mathrm{I}}\ \mathbf{J}_n]$, $\mathbf{J}_{\mathrm{I}} = [\mathbf{I}_l\ \mathbf{0}_{l\times K-l}]^T$, $\mathbf{J}_n$ is defined as in the previous subsection, and $\mathbf{U}_t, \mathbf{V}_c \in \mathbb{Z}^m[j]$, a, Q are defined as in Section V-C. Similar to going from (36) to (39), we have $I(\mathbf{X}_t;\mathbf{Y}_e) \leq K$.

The received signal at the legitimate receiver is given by

$$\mathbf{Y}_r = \begin{bmatrix}\mathbf{A} & \bar{\mathbf{H}}_c\end{bmatrix}\begin{bmatrix}\mathbf{U}_t^T & \mathbf{V}_{c_1}^{l^T}\end{bmatrix}^T + \mathbf{Z}_r, \tag{67}$$

where $\mathbf{A} = \mathbf{H}_t\mathbf{G}_t^{-1}\mathbf{G}_c\mathbf{J}_c$, $\bar{\mathbf{H}}_c = \mathbf{H}_c\mathbf{J}_{\mathrm{I}}$. The receiver chooses $\mathbf{b} \perp \mathrm{span}\{\mathbf{a}_2, \cdots, \mathbf{a}_m, \mathbf{h}_{c_2}, \cdots, \mathbf{h}_{c_l}\}$ and multiplies its received signal by $\mathbf{D}$ in (41) to obtain $\widetilde{\mathbf{Y}}_r = [\widetilde{Y}_{r_1}\ (\widetilde{\mathbf{Y}}_{r_2}^N)^T]^T$. Using similar analysis as in Section V-C, we have

$$I(\mathbf{X}_t;\mathbf{Y}_r) \geq I(U_1;\widetilde{Y}_{r_1}) + I(\mathbf{U}_{t_2}^m;\widetilde{\mathbf{Y}}_{r_2}^N|U_1\widetilde{Y}_{r_1}) \tag{68}$$

$$I(U_1;\widetilde{Y}_{r_1}) \geq \frac{1-\epsilon}{2+\epsilon}\log P + o(\log P) \tag{69}$$

$$I(\mathbf{U}_{t_2}^m;\widetilde{\mathbf{Y}}_{r_2}^N|U_1\widetilde{Y}_{r_1}) \geq I(\mathbf{U}_{t_2}^m;\bar{\mathbf{Y}}_r''), \tag{70}$$

where $\epsilon > 0$ is arbitrarily small. $\bar{\mathbf{Y}}_r''$, in (70), is given by

$$\bar{\mathbf{Y}}_r'' = \widehat{\mathbf{B}}\begin{bmatrix}\mathbf{U}_{t_2}^{m^T} & \mathbf{V}_{c_2}^{l^T}\end{bmatrix}^T + \widetilde{\mathbf{B}}\mathbf{Z}_r, \tag{71}$$

where $\widehat{\mathbf{B}} = [\tilde{\mathbf{a}}_2 \cdots \tilde{\mathbf{a}}_m\ \tilde{\mathbf{h}}_{c_2} \cdots \tilde{\mathbf{h}}_{c_l}]$. Using the argument in Section V-D, $\widehat{\mathbf{B}}$ is a.s. full rank. Define $\widehat{\mathbf{Y}}_r'' = \widehat{\mathbf{B}}^{-1}\bar{\mathbf{Y}}_r''$. Thus,

$$I(\mathbf{U}_{t_2}^m;\widetilde{\mathbf{Y}}_{r_2}^N|U_1\widetilde{Y}_{r_1}) \geq I(\mathbf{U}_{t_2}^m;\widehat{\mathbf{Y}}_r'') \tag{72}$$

$$\geq \frac{1-\epsilon}{2+\epsilon}(K-1)\log P + o(\log P), \tag{73}$$

Thus, $D_s \geq \frac{1-\epsilon}{2+\epsilon}K$. Since ϵ is arbitrarily small, the s.d.o.f. of $\frac{K}{2}$ is achievable, which completes the proof for Theorem 1.

VI. Conclusion

We have characterized the s.d.o.f. for the multiantenna Gaussian wiretap channel with a K-antenna cooperative jammer (CJ) and N antennas at each of its nodes for all possible values of K. We have shown that when the s.d.o.f. of the channel is integer-valued, the s.d.o.f. can be achieved by a scheme which involves linear precoding, Gaussian signaling both for transmission and jamming, and linear receiver processing. In contrast, we have proved that, when the s.d.o.f. is non-integer, a scheme which employs structured signaling along with joint signal space and signal scale alignment achieves the s.d.o.f. of the channel. The converse was proved by allowing for cooperation between the transmitter and CJ for a certain range of K, and by incorporating both the secrecy and reliability constraints, for the other values of K. Although we identified its prelog factor, the secrecy capacity of this model remains open and deserves further attention.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *44th Annual Allerton Conf. On Communication, Control, and Computing*, Sep. 2006.

[3] ——, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[4] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Info. Theory*, vol. 57, no. 5, pp. 3153–3167, 2011.

[5] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Info. Theory*, vol. 60, no. 4, pp. 2121–2138, 2014.

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

[7] ——, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *Submitted to IEEE Trans. Info. Theory*, 2013, arXiv preprint arXiv:1305.7214.

[8] 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 51st Annual Allerton Conference on Communication, Control, and Computing*, Oct. 2013.

[9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-Part II: The MIMOME wiretap channel," *IEEE Trans. Info. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[10] M. A. Maddah-Ali, "On the degrees of freedom of the compound MIMO broadcast channels with finite states," 2009, arXiv preprint arXiv:0909.5006.

[11] D. Kleinbock, "Baker-sprindzhuk conjectures for complex analytic manifolds," 2002, arXiv preprint math/0210369.