Secure Degrees of Freedom of $N \times N \times M$ Wiretap Channel with a K-Antenna Cooperative Jammer

Mohamed Nafea and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802.
msn139@psu.edu *yener@engr.psu.edu*

***Abstract*—The secure degrees of freedom (s.d.o.f.) of a multiantenna Gaussian wiretap channel with N antennas at the transmitter and receiver and an arbitrary number of antennas, M, at the wiretapper is characterized when a multiantenna cooperative jammer (CJ) is available as a helper. This generalizes our previous result that assumed the same number of antennas at the eavesdropper as the legitimate parties. In particular, for arbitrary values of N and M, the s.d.o.f. is derived for all possible values of the number of antenna at the CJ, K. The achievability is based on a variety of signalling, beamforming, and alignment techniques which vary according to the value of K, whether M is larger than, smaller than, or equal to N, and whether the s.d.o.f. is integer valued or not an integer. The converse is based on combining an upper bound for the s.d.o.f. which allows for cooperation between the transmitter and CJ and holds for some values of K, with another upper bound which exploits the secrecy and reliability constraints and holds for other values of K.**

I. Introduction

Wireless communication systems are vulnerable to eavesdropping attacks due to the open nature of the medium. Physical layer security in wireless systems has its roots in reference [1]. The idea of this approach is to exploit the presence of noise in the communication channels between the legitimate parties, and to an eavesdropper which overhears the legitimate communication, in order to prevent the eavesdropper from retrieving any information. This approach has been extended to a variety of network models, see for example [2]–[10].

The introduction of *cooperative jamming* to the wiretap channel (WTC) model allowed to create an advantage for the legitimate channel over the eavesdropper channel [3]. The idea is to transmit a jamming signal which reduces the reception capability of the eavesdropper, while causing the least possible harm at the intended receiver. The jamming signal can be sent either by a legitimate transmitter in the network [3], [4], or by an external cooperative jammer (CJ) augmented to the network [5], [6]. Reference [5] showed that employing a single antenna CJ in a single antenna Gaussian WTC increases its s.d.o.f. from zero to $\frac{1}{2}$. The s.d.o.f. of various single antenna Gaussian WTC models has been derived in [4], [5] with the aid of cooperative jamming and structured signaling techniques.

Following the footsteps in the literature of the single antenna case, the secrecy capacity of a multiantenna Gaussian WTC, with the number of antennas at the eavesdropper greater than or equal to the number of antennas at the transmitter, does not scale with the signal to noise ratio (SNR), leading to zero s.d.o.f. [7]. In this case, a multiantenna CJ is useful to provide a secrecy rate that scales with transmit power, i.e., non-zero s.d.o.f. Towards this end, reference [8] considered a multiantenna Gaussian WTC with a K-antenna CJ, and N antennas at each of the other three terminals, and characterized the s.d.o.f. of the channel for some N and for all possible values of K. In this work, we extend the result in [8] to the case where the eavesdropper has a number of antennas, M, which is not necessarily equal to N. Note that the channel has positive s.d.o.f. when $M < N$ even without the help of the CJ; we include this case in the s.d.o.f. characterization for the sake of completeness. The s.d.o.f. result derived in this paper matches the achievable s.d.o.f. derived in [9], [10] which are special cases for $\{M = N, K = 2N\}, \{M = N, K = 2N-1\}, \{N = 1, K = M\}$, and real channel gains.

Similar to [8], we show that when the channel has integer valued s.d.o.f., Gaussian signaling at the transmitter and CJ is sufficient, and when the s.d.o.f. is non-integer, structured signaling along with a combination of signal space and signal scale alignment are needed. However, in order to exploit (overcome) the decrease (increase) in the number of eavesdropper's antennas, M, with respect to N, careful beamforming techniques have to be applied at the transmitter and CJ. The converse is developed by deriving two upper bounds for the s.d.o.f. for two different ranges of K, and combining them for each of the cases $M \leq N$ and $M > N$. The first bound is derived by allowing for full cooperation between the transmitter and CJ, and holds for a certain range of K, and the second bound is derived by utilizing the secrecy and reliability constraints, and holds for other values of K.

Comprehensively, this study provides a high SNR characterization for the secrecy rates of a multiantenna WTC with a wiretapper that possibly has *more spatial resources* than the legitimate parties, and when a multiantenna helper is available for communication. In the remainder of the paper, the channel model and the main result are described in Sections II and III. The converse and achievability proofs are provided in Sections IV and V. Section VI concludes the paper.

Notation: The set of integers $\{-Q, \cdots, Q\}$ is denoted by $(-Q, Q)_{\mathbb{Z}}$. $\mathbf{0}_{m\times n}$ denotes an $m \times n$ matrix of zeros. $\mathcal{N}(\mathbf{A})$ and $||\mathbf{A}||$ denote the null space and the induced norm of matrix $\mathbf{A}$.

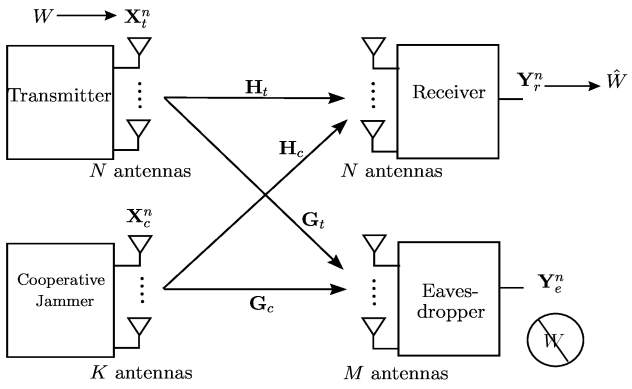

Fig. 1. $(N \times N \times M)$ multiple antenna Gaussian Wiretap Channel with a K-antenna Cooperative Jammer.

† denotes pseudo inverse operation. $\mathbf{V}_i^j$ denotes the ith to jth component in a vector $\mathbf{V}$, $||\mathbf{V}||$ denotes its Euclidean norm.

II. Channel Model and Definitions

We consider a multiple antenna Gaussian wiretap channel (WTC) with an N-antenna transmitter, N-antenna receiver, M-antenna eavesdropper, and a K-antenna cooperative jammer (CJ), as shown in Fig. 1. The received signals at the legitimate receiver and the 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, $\mathbf{H}_t \in \mathbb{C}^{N\times N}$, $\mathbf{H}_c \in \mathbb{C}^{N\times K}$, $\mathbf{G}_t \in \mathbb{C}^{M\times N}$, $\mathbf{G}_c \in \mathbb{C}^{M\times K}$ are the channel gain matrices. The channel gains are static and randomly drawn from a *complex valued* distribution. $\mathbf{Z}_r(n) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$ and $\mathbf{Z}_e(n) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M)$ are the circularly symmetric complex Gaussian noise at the receiver and eavesdropper at the nth channel use. $\mathbf{Z}_r(n)$ and $\mathbf{Z}_e(n)$ are independent and both are independent and identically distributed (i.i.d.) across the time index. We omit the index n whenever possible. We consider average power constraints on the transmitted signals, i.e., $\mathrm{E}\{\mathbf{X}_t^H\mathbf{X}_t\}, \mathrm{E}\{\mathbf{X}_c^H\mathbf{X}_c\} \leq P$. Throughout the paper, we use $\mathbf{V}^n$ to denote the n-letter extension of the random vector $\mathbf{V}$, i.e., $\mathbf{V}^n = [\mathbf{V}(1)\ \cdots \mathbf{V}(n)]$.

In this model, the transmitter wants to send a confidential message W to the legitimate receiver in the presence of the eavesdropper. The transmitter uses a stochastic encoder which maps its message W to the transmitted signal $\mathbf{X}_t^n$. Let $\hat{W}$ denote the estimate of W obtained at the receiver using its observation $\mathbf{Y}_r^n$. For reliable decoding at the receiver, and for W to be kept secret from the eavesdropper, it is required that

$$P_e = \Pr\left\{\hat{W} \neq W\right\} \leq \epsilon, \quad (3)$$

$$\frac{1}{n}H(W|\mathbf{Y}_e^n) \geq \frac{1}{n}H(W) - \epsilon. \quad (4)$$

Secrecy rate R_s is achievable if for every $\epsilon > 0$, there exists a channel code $(n, 2^{nR_s})$ such that the conditions in (3) and (4) hold. The secrecy capacity of a channel, C_s, is the supremum of all achievable secrecy rates. Achievable secure degrees of freedom (s.d.o.f.), for a given secrecy rate R_s, is defined as

$$D_s = \lim_{P\to\infty} \frac{R_s}{\log P}. \quad (5)$$

The CJ transmits a jamming signal, $\mathbf{X}_c^n$. The jamming signal does not carry any information, and has no underlying codebook. The secret message W is not known by the CJ.

III. Main Result

Theorem 1 *The s.d.o.f. of the $N \times N \times M$ Gaussian WTC with a K-antenna CJ is given by*

$$D_s = \begin{cases} [K+N-M]^+, & \text{for } 0 \leq K \leq M - N_{\min} \\ N - N_{\min}, & \text{for } M - N_{\min} < K \leq N_{\max} \\ \frac{K+N-M}{2}, & \text{for } N_{\max} < K \leq N+M, \end{cases} \quad (6)$$

where $N_{\min} = \frac{\min\{N,M\}}{2}$ and $N_{\max} = \max\{N, M\}$.

The s.d.o.f. at $K = N+M$ is equal to N, which is the degrees of freedom of the N-antenna Gaussian channel with no secrecy constraint. Thus, increasing K over $N+M$ can not increase the s.d.o.f. of the channel over N. Equation (6) shows the behavior of the s.d.o.f. associated with increasing K form 0 to $N+M$. Perhaps surprisingly, the s.d.o.f. of the channel is not increased by increasing K from $M - \lfloor\frac{\min\{N.M\}}{2}\rfloor$ to $\max\{N, M\}$. This behavior can be attributed to the high SNR analysis considered in this paper, i.e., the increase in the secrecy capacity of the channel associated with increasing K in the aforementioned range diminishes at high SNR.

IV. Converse

A. $0 \leq K \leq M$

We consider a multiantenna Gaussian WTC with an $N+K$-antenna transmitter, N-antenna receiver and M-antenna eavesdropper. The s.d.o.f. of this channel gives an upper bound for the s.d.o.f. of the channel in (1), (2). At high SNR, the secrecy capacity of this channel, C_s, takes the asymptotic form [7]

$$C_s(P) = \log\det\left(\mathbf{I}_N + \frac{P}{p}\bar{\mathbf{H}}\bar{\mathbf{G}}^\sharp\bar{\mathbf{H}}^H\right) + o(\log P), \quad (7)$$

where $\bar{\mathbf{H}}$, $\bar{\mathbf{G}}$ are the channel gain matrices to the receiver and eavesdropper, and $\bar{\mathbf{G}}^\sharp$ is the projection matrix onto $\mathcal{N}(\bar{\mathbf{G}})$. $p = \dim(\mathcal{N}(\bar{\mathbf{H}})^\perp \cap \mathcal{N}(\bar{\mathbf{G}}))$, where $\mathcal{N}(\bar{\mathbf{H}})^\perp$ is the space orthogonal to $\mathcal{N}(\bar{\mathbf{H}})$. If a vector $\mathbf{x}$ belongs to $\mathcal{N}(\bar{\mathbf{G}})$, it almost surely (a.s.) belongs to $\mathcal{N}(\bar{\mathbf{H}})^\perp$, for all $0 \leq K \leq M$, due to the independently and randomly generated channel gains. Thus, $p = \dim(\mathcal{N}(\bar{\mathbf{G}})) = [K+N-M]^+$. We also have [7]

$$\bar{\mathbf{H}}\bar{\mathbf{G}}^\sharp\bar{\mathbf{H}}^H = \mathbf{\Psi}\begin{bmatrix}\mathbf{0}_{(N-p)\times(N-p)} & \mathbf{0}_{(N-p)\times p} \\ \mathbf{0}_{p\times(N-p)} & \mathbf{\Omega}\end{bmatrix}\mathbf{\Psi}^H, \quad (8)$$

where $\mathbf{\Psi}$ is a unitary matrix and $\mathbf{\Omega}$ is a non-singular matrix.

Thus, it can be shown that $C_s(P) = p\log P + o(\log P)$ [8], and hence, the s.d.o.f. of the channel in (1), (2) is bounded as

$$D_s \leq \lim_{P\to\infty} \frac{p\log P + o(\log P)}{\log P} = [K+N-M]^+. \quad (9)$$

B. $\max\{N, M\} \leq K \leq N + M$

We derive another upper bound for the s.d.o.f. which holds for $\max\{N, M\} \leq K \leq N+M$. Let ϕ_i, $i = 1, 2, 3, 4$, denote constants which do not depend on the power P. Similar to [8], the secrecy rate R_s can be upper bounded as

$$nR_s \leq h(\tilde{\mathbf{X}}_t^n) + h(\tilde{\mathbf{X}}_c^n) - h(\mathbf{Y}_e^n) + n\phi_1, \tag{10}$$

where $\tilde{\mathbf{X}}_t = \mathbf{X}_t + \tilde{\mathbf{Z}}_t$, $\tilde{\mathbf{X}}_c = \mathbf{X}_c + \tilde{\mathbf{Z}}_c$ are noisy versions of the transmitted signals. $\tilde{\mathbf{Z}}_t \sim \mathcal{CN}(\mathbf{0}, \mathbf{K}_t)$, $\tilde{\mathbf{Z}}_c \sim \mathcal{CN}(\mathbf{0}, \mathbf{K}_c)$ are independent, each is independent from $\{\mathbf{X}_t, \mathbf{X}_c, \mathbf{Z}_r, \mathbf{Z}_e\}$, and i.i.d. across n. $\mathbf{K}_t$, $\mathbf{K}_c$ are chosen as $\mathbf{K}_t = \rho^2 \mathbf{I}_N$, $\mathbf{K}_c = \rho^2 \mathbf{I}_K$, where $0 < \rho \leq 1/\max\{||\mathbf{H}_c^H||, \sqrt{||\mathbf{G}_t^H||^2 + ||\mathbf{G}_c^H||^2}\}$ [8]. We now consider the following two cases.

Case 1: $M \leq N$

A stochastically equivalent form of $\mathbf{Z}_e$ is $\mathbf{Z}_e' = \mathbf{G}_t \tilde{\mathbf{Z}}_t + \tilde{\mathbf{Z}}_e$, where $\tilde{\mathbf{Z}}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M - \mathbf{G}_t \mathbf{K}_t \mathbf{G}_t^H)$ is independent from $\{\tilde{\mathbf{Z}}_t, \tilde{\mathbf{Z}}_c, \mathbf{X}_t, \mathbf{X}_c, \mathbf{Z}_r\}$, and i.i.d. over n. Thus, a stochastically equivalent form of $\mathbf{Y}_e^n$ is $\mathbf{Y}_e'^n = \mathbf{G}_t \tilde{\mathbf{X}}_t^n + \mathbf{G}_c \mathbf{X}_c^n + \tilde{\mathbf{Z}}_e^n$. Let $\tilde{X}_{t_k}$ be the kth element of $\tilde{\mathbf{X}}_t = [\tilde{\mathbf{X}}_{t_1}^T \ \tilde{\mathbf{X}}_{t_2}^T]^T$, where $\tilde{\mathbf{X}}_{t_1} = [\tilde{X}_{t_1} \cdots \tilde{X}_{t_M}]^T$, $\tilde{\mathbf{X}}_{t_2} = [\tilde{X}_{t_{M+1}} \cdots \tilde{X}_{t_N}]^T$, and let $\mathbf{G}_t = [\mathbf{G}_{t_1} \ \mathbf{G}_{t_2}]$, $\mathbf{G}_{t_1} \in \mathbb{C}^{M \times M}$, $\mathbf{G}_{t_2} \in \mathbb{C}^{M \times (N-M)}$. Thus,

$$h(\mathbf{Y}_e^n) = h(\mathbf{Y}_e'^n) = h(\mathbf{G}_t \tilde{\mathbf{X}}_t^n + \mathbf{G}_c \mathbf{X}_c^n + \tilde{\mathbf{Z}}_e^n) \tag{11}$$

$$\geq h(\mathbf{G}_t \tilde{\mathbf{X}}_t^n) = h(\mathbf{G}_{t_1} \tilde{\mathbf{X}}_{t_1}^n + \mathbf{G}_{t_2} \tilde{\mathbf{X}}_{t_2}^n) \tag{12}$$

$$\geq h(\mathbf{G}_{t_1} \tilde{\mathbf{X}}_{t_1}^n | \tilde{\mathbf{X}}_{t_2}^n) = h(\tilde{\mathbf{X}}_{t_1}^n | \tilde{\mathbf{X}}_{t_2}^n) + n \log |\det(\mathbf{G}_{t_1})|. \tag{13}$$

Substituting (13) in (10) gives

$$nR_s \leq h(\tilde{\mathbf{X}}_{t_2}^n) + h(\tilde{\mathbf{X}}_c^n) + n\phi_2. \tag{14}$$

Let $\tilde{X}_{c_k}$ be the kth element of $\tilde{\mathbf{X}}_c = [\tilde{\mathbf{X}}_{c_1}^T \ \tilde{\mathbf{X}}_{c_2}^T]^T$, $\tilde{\mathbf{X}}_{c_1} = [\tilde{X}_{c_1} \cdots \tilde{X}_{c_N}]^T$, $\tilde{\mathbf{X}}_{c_2} = [\tilde{X}_{c_{N+1}} \cdots \tilde{X}_{c_K}]^T$. Let $\mathbf{H}_c = [\mathbf{H}_{c_1} \ \mathbf{H}_{c_2}]$, $\mathbf{H}_{c_1} \in \mathbb{C}^{N \times N}, \mathbf{H}_{c_2} \in \mathbb{C}^{N \times (K-N)}$. Using the reliability constraint in (3), another upper bound on R_s is [8]

$$nR_s \leq h(\mathbf{Y}_r^n) - h(\tilde{\mathbf{X}}_{c_1}^n | \tilde{\mathbf{X}}_{c_2}^n) - n \log |\det(\mathbf{H}_{c_1})|. \tag{15}$$

Let $\mathbf{Y}_r = [Y_{r_1} \cdots Y_{r_N}]^T$. Summing (14) and (15) yields

$$nR_s \leq \frac{1}{2} \left\{ h(\mathbf{Y}_r^n) + h(\tilde{\mathbf{X}}_{t_2}^n) + h(\tilde{\mathbf{X}}_{c_2}^n) \right\} + n\phi_3 \tag{16}$$

$$\leq \frac{1}{2} \sum_{i=1}^{n} \Bigg\{ \sum_{k=1}^{N} h(Y_{r_k}(i)) + \sum_{k=M+1}^{N} h(\tilde{X}_{t_k}(i)) + \sum_{k=N+1}^{K} h(\tilde{X}_{c_k}(i)) \Bigg\} + n\phi_3. \tag{17}$$

For all $i = 1, \cdots, n$, $k = 1, \cdots, N$, $j = 1, \cdots, K$, we have

$$h(Y_{r_k}(i)) \leq \log 2\pi e + \log(1 + h^2 P) \tag{18}$$

$$h(\tilde{X}_{t_k}(i)), h(\tilde{X}_{c_j}(i)) \leq \log 2\pi e + \log(\rho^2 + P), \tag{19}$$

where $h^2 = \max_k \left(||\mathbf{h}_{t_k}^{r^T}||^2 + ||\mathbf{h}_{c_k}^{r^T}||^2 \right)$; $\mathbf{h}_{t_k}^r, \mathbf{h}_{c_k}^r$ are the kth row vectors of $\mathbf{H}_t, \mathbf{H}_c$ [8]. Substituting (18), (19) in (17) gives

$$R_s \leq \frac{N}{2} \log(1 + h^2 P) + \frac{K - M}{2} \log(\rho^2 + P) + \phi_4. \tag{20}$$

Thus, the s.d.o.f. is upper bounded as $D_s \leq \frac{K+N-M}{2}$.

Case 2: $M > N$

Let us write $\mathbf{X}_c$,$\mathbf{H}_c$ as $\mathbf{X}_c = [\mathbf{X}_{c_1}'^T \ \mathbf{X}_{c_2}'^T]^T$, $\mathbf{H}_c = [\mathbf{H}_{c_1}' \ \mathbf{H}_{c_2}']$, where $\mathbf{X}_{c_1}' = [X_{c_1} \cdots X_{c_{M-N}}]^T$, $\mathbf{X}_{c_2}' = [\mathbf{X}_{c_{21}}'^T \ \mathbf{X}_{c_{22}}'^T]^T$, $\mathbf{X}_{c_{21}}' = [X_{c_{M-N+1}} \cdots X_{c_M}]^T$, $\mathbf{X}_{c_{22}}' = [X_{c_{M+1}} \cdots X_{c_K}]^T$, and $\mathbf{H}_{c_1}' \in \mathbb{C}^{N \times (M-N)}$, $\mathbf{H}_{c_2}' = [\mathbf{H}_{c_{21}}' \ \mathbf{H}_{c_{22}}']$, $\mathbf{H}_{c_{21}}' \in \mathbb{C}^{N \times N}$, $\mathbf{H}_{c_{22}}' \in \mathbb{C}^{N \times (K-M)}$. Consider a modified channel where the CJ uses only the last $K + N - M$ of its K antennas. Thus, the transmitted signals in the modified channel are $\mathbf{X}_t^n$ and $\mathbf{X}_{c_2}'^n$, and hence, the legitimate receiver receives $\bar{\mathbf{Y}}_r^n = \mathbf{H}_t \mathbf{X}_t^n + \mathbf{H}_{c_2}' \mathbf{X}_{c_2}'^n + \mathbf{Z}_r^n$. The jamming signal behaves as noise. Thus, the reliable rate, i.e., the rate which satisfies the reliability constraint, of the modified channel, $\bar{R}$, is an upper bound for that of the original channel, R. Since R_s satisfies the reliability and secrecy constraints in (3) and (4), we have

$$nR_s \leq nR \leq n\bar{R} \leq I(\mathbf{X}_t^n; \bar{\mathbf{Y}}_r^n) \tag{21}$$

$$\leq h(\bar{\mathbf{Y}}_r^n) - h(\mathbf{H}_{c_2}' \tilde{\mathbf{X}}_{c_2}'^n) \tag{22}$$

$$\leq h(\bar{\mathbf{Y}}_r^n) - h(\tilde{\mathbf{X}}_{c_{21}}'^n | \tilde{\mathbf{X}}_{c_{22}}'^n) - n \log |\det(\mathbf{H}_{c_{21}}')|. \tag{23}$$

Another stochastically equivalent form of $\mathbf{Z}_e$ is $\mathbf{Z}_e'' = \mathbf{G}_t \tilde{\mathbf{Z}}_t + \mathbf{G}_c \tilde{\mathbf{Z}}_c + \tilde{\mathbf{Z}}_e'$, where $\tilde{\mathbf{Z}}_e' \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M - \mathbf{G}_t \mathbf{K}_t \mathbf{G}_t^H - \mathbf{G}_c \mathbf{K}_c \mathbf{G}_c^H)$ is independent from $\{\tilde{\mathbf{Z}}_t, \tilde{\mathbf{Z}}_c, \mathbf{X}_t, \mathbf{X}_c, \mathbf{Z}_r\}$, and i.i.d. over n. Thus, $h(\mathbf{Y}_e^n) = h(\mathbf{G}_t \tilde{\mathbf{X}}_t^n + \mathbf{G}_c \tilde{\mathbf{X}}_c^n + \tilde{\mathbf{Z}}_e'^n)$. Let $\mathbf{G}_c = [\mathbf{G}_{c_1} \ \mathbf{G}_{c_2}]$, where $\mathbf{G}_{c_1} \in \mathbb{C}^{M \times (M-N)}$, $\mathbf{G}_{c_2} \in \mathbb{C}^{M \times (K+N-M)}$. Similar to going from (11) to (13), we have

$$h(\mathbf{Y}_e^n) \geq h(\tilde{\mathbf{X}}_t^n) + h(\tilde{\mathbf{X}}_{c_1}'^n | \tilde{\mathbf{X}}_{c_2}'^n) + n \log |\det[\mathbf{G}_t \ \mathbf{G}_{c_1}]|. \tag{24}$$

Using (10), (23), and (24), we have

$$nR_s \leq \frac{1}{2} \{ h(\bar{\mathbf{Y}}_r^n) + h(\tilde{\mathbf{X}}_{c_{22}}'^n) \} + n\phi_2. \tag{25}$$

Let $\bar{h}$ be a constant which does not depend on the power P. Using similar analysis as in the previous case, we obtain

$$R_s \leq \frac{N}{2} \log(1 + \bar{h}^2 P) + \frac{K - M}{2} \log(\rho^2 + P) + n\phi_3. \tag{26}$$

Thus, the s.d.o.f. is upper bounded as $D_s \leq \frac{K+N-M}{2}$.

C. Obtaining the Upper Bound

For $M \leq N$, the upper bound derived in Section IV-A is equal to $K + N - M$ for all $0 \leq K \leq M$, while the upper bound derived in Section IV-B, at $K = N$, is equal to $N - \frac{M}{2}$. Since $N - \frac{M}{2} < K + N - M$ for all $\frac{M}{2} < K \leq N$, the s.d.o.f. can be upper bounded by $N - \frac{M}{2}$ for all $\frac{M}{2} < K \leq N$. Combining these statements, we have, for $M \leq N$,

$$D_s \leq \begin{cases} K + N - M, & \text{for } 0 \leq K \leq \frac{M}{2} \\ N - \frac{M}{2}, & \text{for } \frac{M}{2} < K \leq N \\ \frac{K+N-M}{2}, & \text{for } N < K \leq N + M. \end{cases} \tag{27}$$

Using similar argument when $M > N$, we have

$$D_s \leq \begin{cases} 0, & \text{for } 0 \leq K \leq M - N \\ K + N - M, & \text{for } M - N < K \leq M - \frac{N}{2} \\ \frac{N}{2}, & \text{for } M - \frac{N}{2} < K \leq M \\ \frac{K+N-M}{2}, & \text{for } M < K \leq N + M. \end{cases} \tag{28}$$

By combining (27) and (28), we obtain the upper bound in (6). In the next Section, we shall see the achievability of (6).

V. Achievable Schemes

We provide the achievability proof for Theorem 1 by showing the achievability of (27) when $M \leq N$, and of (28) when $M > N$. We consider i.i.d. transmitted signals over the channel uses. $\mathbf{X}_c^n$ is independent from $\mathbf{X}_t^n$, and hence the following secrecy rate is achievable by *stochastic encoding* [2]

$$R_s = [I(\mathbf{X}_t; \mathbf{Y}_r) - I(\mathbf{X}_t; \mathbf{Y}_e)]^+. \tag{29}$$

The transmitted signals at the transmitter and the CJ are

$$\mathbf{X}_t = \mathbf{P}_t \mathbf{U}_t, \qquad \mathbf{X}_c = \mathbf{P}_c \mathbf{V}_c, \tag{30}$$

where $\mathbf{U}_t = [U_1 \cdots U_d]^T$, $\mathbf{V}_c = [V_1 \cdots V_l]^T$ are the information and jamming streams, respectively. $\mathbf{P}_t = [\mathbf{p}_{t_1} \cdots \mathbf{p}_{t_d}]$, $\mathbf{P}_c = [\mathbf{p}_{c_1} \cdots \mathbf{p}_{c_l}]$ are the precoding matrices at the transmitter and the CJ. Let us now state the following lemma.

Lemma 1 *Consider two matrices $\mathbf{E}_1 \in \mathbb{C}^{N \times K}$ and $\mathbf{E}_2 \in \mathbb{C}^{K \times M}$, where $N, M < K$. If $\mathbf{E}_2$ is full column rank, and $\mathbf{E}_1$ has all of its entries independently and randomly drawn according to some continuous distribution, then* $\mathrm{rank}\{\mathbf{E}_1\mathbf{E}_2\} = \min\{N, M\}$ *almost surely.*

Proof: The proof of Lemma 1 follows from a straightforward generalization of the Appendix in [9]. ■

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

The transmitter exploits the advantage of having more antennas than the eavesdropper by sending $N - M$ out of its $d = K + N - M$ Gaussian independent streams over $\mathcal{N}(\mathbf{G}_t)$. The CJ sends $l = K$ independent Gaussian jamming streams to cover the K information streams visible to the eavesdropper. Since the total number of received streams at the receiver, $2K + N - M$, is less than or equal to N, the receiver can decode all the information and jamming streams at high SNR.

The transmitted signals are given by (30) with $d = K+N-M$, $l = K$, $\mathbf{U}_t \sim \mathcal{CN}(\mathbf{0}, \bar{P}\mathbf{I}_d)$, $\mathbf{V}_c \sim \mathcal{CN}(\mathbf{0}, \bar{P}\mathbf{I}_l)$, $\mathbf{P}_c = \mathbf{I}_l$, $\mathbf{P}_t = [\mathbf{P}_{t,a}\ \mathbf{P}_{t,n}]$, $\mathbf{P}_{t,a} = \mathbf{G}_t^\dagger \mathbf{G}_c$, $\mathbf{P}_{t,n}$ is chosen such that its $N-M$ columns span $\mathcal{N}(\mathbf{G}_t)$. $\bar{P} = \frac{1}{\alpha}P$, where α is a constant chosen to satisfy the power constraints [8]. Thus, we have

$$\mathbf{Y}_r = \begin{bmatrix}\mathbf{H}_t\mathbf{P}_t & \mathbf{H}_c\end{bmatrix} \begin{bmatrix}\mathbf{U}_t \\ \mathbf{V}_c\end{bmatrix} + \mathbf{Z}_r \tag{31}$$

$$\mathbf{Y}_e = \mathbf{G}_c(\mathbf{U}_{t1}^{\,l} + \mathbf{V}_c) + \mathbf{Z}_e. \tag{32}$$

In order to compute $I(\mathbf{X}_t; \mathbf{Y}_r)$, we show that $[\mathbf{H}_t\mathbf{P}_t\ \mathbf{H}_c]$ is a.s. full column-rank. The columns of $\mathbf{P}_{t,a} = \mathbf{G}_t^\dagger \mathbf{G}_c$ are a.s. linearly independent (l.i.) due to the randomly generated channel gains, and the columns of $\mathbf{P}_{t,n}$ are l.i. since they span $\mathcal{N}(\mathbf{G}_t)$. In addition, each of the columns of $\mathbf{P}_{t,a}$ is l.i. from the columns of $\mathbf{P}_{t,n}$ since $\mathbf{G}_t\mathbf{P}_{t,a} = \mathbf{G}_c$, and hence $\mathbf{G}_t\mathbf{p}_{t_i} \neq \mathbf{0}$ for all $i = 1, 2, \cdots, K$. Thus $\mathbf{P}_t = [\mathbf{P}_{t,a}\ \mathbf{P}_{t,n}]$ is full column rank. Using Lemma 1, where $[\mathbf{H}_t\mathbf{P}_t\ \mathbf{H}_c]$ can be written as

$$\begin{bmatrix}\mathbf{H}_t\mathbf{P}_t & \mathbf{H}_c\end{bmatrix} = \begin{bmatrix}\mathbf{H}_t & \mathbf{H}_c\end{bmatrix} \begin{bmatrix}\mathbf{P}_t & \mathbf{0}_{N\times K} \\ \mathbf{0}_{K\times d} & \mathbf{I}_K\end{bmatrix}, \tag{33}$$

shows that $[\mathbf{H}_t\mathbf{P}_t\ \mathbf{H}_c]$ is a.s. full column rank. Thus,

$$I(\mathbf{X}_t; \mathbf{Y}_r) \geq d \log P + o(\log P). \tag{34}$$

Next, using (32), $I(\mathbf{X}_t; \mathbf{Y}_e)$ is upper bounded as

$$I(\mathbf{X}_t; \mathbf{Y}_e) = \log \frac{\det(\mathbf{I}_K + 2\bar{P}\mathbf{G}_c^H\mathbf{G}_c)}{\det(\mathbf{I}_K + \bar{P}\mathbf{G}_c^H\mathbf{G}_c)} \leq K. \tag{35}$$

Substituting (34) and (35) in (29), we have

$$R_s \geq d \log P + o(\log P) - K \tag{36}$$

$$= (K + N - M) \log P + o(\log P), \tag{37}$$

and using (5), the achievable s.d.o.f. is $D_s \geq K + N - M$.

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

For M is even, $K = \frac{M}{2}$, where $M \leq N$, the achievable s.d.o.f., using the scheme in the previous case, is equal to $N - \frac{M}{2}$. However, from (27), the s.d.o.f. of the channel is upper bounded by $N - \frac{M}{2}$ for all $\frac{M}{2} < K \leq N$. Thus, when $M \leq N$ and M is even, the achievable scheme for $K = \frac{M}{2}$ in the previous case can be used to achieve the s.d.o.f. for all $\frac{M}{2} < K \leq N$. Since $K > \frac{M}{2}$, the CJ chooses the precoder $\mathbf{P}_c = [\mathbf{I}_l\ \ \mathbf{0}_{l\times K-l}]^T$ so that it utilizes only $l = \frac{M}{2}$ out of its K antennas and sends l Gaussian streams. The transmitter uses $\mathbf{P}_t = [\mathbf{P}_{t,a}\ \mathbf{P}_{t,n}]$, where $\mathbf{P}_{t,a} = \mathbf{G}_t^\dagger \mathbf{G}_c \mathbf{P}_c$, $\mathbf{P}_{t,n}$ is defined as in the previous case, to send $d = N - \frac{M}{2}$ Gaussian information streams. Using the same analysis as in the previous case, it can be shown that the s.d.o.f. is bounded as $D_s \geq N - \frac{M}{2}$.

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

For this case, using a similar scheme as in Section V-B can only achieve $N - \frac{M+1}{2}$ s.d.o.f., since Gaussian signaling can not achieve fractional s.d.o.f. for the channel. In order to achieve the s.d.o.f. of the channel for this case, we utilize structured signaling both for transmission and jamming, and propose utilizing joint signal space alignment and the complex field equivalent of real interference alignment [8], [11], [12]. The transmitter and the CJ send $d = N - \frac{M-1}{2}$ and $l = \frac{M+1}{2}$ independent structured streams, respectively. The linear precoding at the transmitter and CJ is similar to the previous case. The transmitted signals are given by (30), with $d = N - \frac{M-1}{2}$, $l = \frac{M+1}{2}$, $\mathbf{P}_c$ and $\mathbf{P}_t$ are defined as in the previous case, $U_i = U_{i_{\mathrm{Re}}} + jU_{i_{\mathrm{Im}}}$, $V_k = V_{k_{\mathrm{Re}}} + jV_{k_{\mathrm{Im}}}$, for all $i = 2, 3, \cdots, d$ and $k = 2, 3, \cdots, l$, and the random variables U_1, V_1, $\{U_{i_{\mathrm{Re}}}\}_{i=2}^d$, $\{U_{i_{\mathrm{Im}}}\}_{i=2}^d$, $\{V_{i_{\mathrm{Re}}}\}_{i=2}^l$, and $\{V_{i_{\mathrm{Im}}}\}_{i=2}^l$ are i.i.d. uniform over the set $\{a(-Q, Q)_{\mathbb{Z}}\}$. The values for a and the integer Q are chosen, to satisfy the power constraints, as [8]

$$Q = P^{\frac{1-\epsilon}{2+\epsilon}} - \nu, \qquad a = \gamma P^{\frac{3\epsilon}{2(2+\epsilon)}}, \tag{38}$$

where $\epsilon > 0$ is chosen arbitrarily small, and ν, γ are constants.

The eavesdropper's received signal is given by (32) with $\tilde{\mathbf{G}}_c = \mathbf{G}_c\mathbf{P}_c$ instead of $\mathbf{G}_c$. Thus, similar to [8], we have

$$I(\mathbf{X}_t; \mathbf{Y}_e) \leq M \log \frac{4Q+1}{2Q+1} \leq M. \tag{39}$$

Let $\mathbf{A} = \mathbf{H}_t\mathbf{P}_t = [\mathbf{a}_1 \cdots \mathbf{a}_d]$, $\mathbf{H}'_c = \mathbf{H}_c\mathbf{P}_c = [\mathbf{h}_{c_1} \cdots \mathbf{h}_{c_l}]$. The legitimate receiver (i) receives

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

(ii) chooses $\mathbf{b}$ such that $\mathbf{b} \perp \text{span}\{\mathbf{a}_2, \cdots, \mathbf{a}_d, \mathbf{h}_{c_2}, \cdots, \mathbf{h}_{c_l}\}$, (iii) multiplies its received signal in (40) by

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

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

$$\widetilde{Y}_{r_1} = \mathbf{b}^H\mathbf{a}_1 U_1 + \mathbf{b}^H\mathbf{h}_{c_1} V_1 + \mathbf{b}^H\mathbf{Z}_r \tag{42}$$

$$\widetilde{\mathbf{Y}}_{r_2}^N = \widetilde{\mathbf{A}}\mathbf{U}_t + \widetilde{\mathbf{H}}_c\mathbf{V}_c + \mathbf{Z}_{r2}^{\ N}, \tag{43}$$

$\widetilde{\mathbf{A}} = [\tilde{\mathbf{a}}_1 \cdots \tilde{\mathbf{a}}_d]$, $\tilde{\mathbf{a}}_i = \mathbf{a}_i{}_2^N$ for all $i = 1, 2, \cdots, d$, and $\widetilde{\mathbf{H}}_c$ is defined similarly, (iv) uses $\widetilde{Y}_{r_1}$ to decode U_1 and V_1 using the complex field extension of real interference alignment as described in [8], [11] where $\mathbf{b}^H\mathbf{a}_1$ and $\mathbf{b}^H\mathbf{h}_{c_1}$ are rationally independent, (v) subtracts the effect of the decoded U_1 and V_1 from its received signal to obtain $\mathbf{Y}'_r = \mathbf{B}[(\mathbf{U}_{t2}^{\ d})^T \ (\mathbf{V}_{c2}^{\ l})^T]^T + \mathbf{Z}_{r2}^{\ N}$, where $\mathbf{B} = [\tilde{\mathbf{a}}_2 \cdots \tilde{\mathbf{a}}_d \ \tilde{\mathbf{h}}_{c_2} \cdots \tilde{\mathbf{h}}_{c_l}]$ is shown to be a.s. full rank using Lemma 1 as in Section V-A, and finally (vi) zero forces $\mathbf{Y}'_r$ in order to decode $U_2, \cdots, U_d$.

Using similar analysis as in [8], $I(\mathbf{X}_t; \mathbf{Y}_r)$ is bounded as

$$I(\mathbf{X}_t; \mathbf{Y}_r) \geq \frac{1-\epsilon}{2+\epsilon}(2N - M)\log P + o(\log P). \tag{44}$$

Substituting (39), (44) in (29), the s.d.o.f. is lower bounded as

$$D_s \geq \frac{(1-\epsilon)(2N-M)}{2+\epsilon}. \tag{45}$$

Since $\epsilon > 0$ is arbitrarily small, s.d.o.f. of $N - \frac{M}{2}$ is achievable.

D. Case 4: $M \leq N$, $N < K \leq N + M$, and $K + N - M$ is even

The transmitter sends $d = \frac{K+N-M}{2}$ independent Gaussian streams using similar linear precoding as in the previous cases. The CJ takes advantage of having more antennas than the receiver by sending $K-N$ out of its $l = \frac{K+M-N}{2}$ independent Gaussian streams over the null space of $\widetilde{\mathbf{H}}_c$, leaving only $g = \frac{M+N-K}{2}$ jamming streams visible to the receiver. Linear processing at the receiver is sufficient for decoding the d information and the g jamming streams at high SNR.

The transmitted signals are given by (30) with $d = \frac{K+N-M}{2}$, $l = \frac{K+M-N}{2}$, $\mathbf{P}_c = [\mathbf{P}_{c,\text{I}} \ \mathbf{P}_{c,n}]$, where

$$\mathbf{P}_{c,\text{I}} = \begin{bmatrix} \mathbf{I}_g \\ \mathbf{0}_{K-g\times g} \end{bmatrix}, \tag{46}$$

and $\mathbf{P}_{c,n}$ is chosen so that its $K - N$ columns span $\mathcal{N}(\mathbf{H}_c)$, $\mathbf{P}_t = [\mathbf{P}_{t,a} \ \mathbf{P}_{t,n}]$, where $\mathbf{P}_{t,a} = \mathbf{G}_t^{\dagger}\mathbf{G}_c\mathbf{P}_c$. $\mathbf{U}_t$, $\mathbf{V}_c$, $\mathbf{P}_{t,n}$ are defined as in Section V-A. The eavesdropper's received signal is given by (32) with $\tilde{\mathbf{G}}_c = \mathbf{G}_c\mathbf{P}_c$ instead of $\mathbf{G}_c$. As in Section V-A, $I(\mathbf{X}_t; \mathbf{Y}_e)$ is upper bounded as $I(\mathbf{X}_t; \mathbf{Y}_e) \leq l$. The received signal at the receiver is given by

$$\mathbf{Y}_r = \begin{bmatrix} \mathbf{H}_t\mathbf{P}_t & \mathbf{H}_c\mathbf{P}_{c,\text{I}} \end{bmatrix} \begin{bmatrix} \mathbf{U}_t \\ \mathbf{V}_{c1}^{\ g} \end{bmatrix} + \mathbf{Z}_r, \tag{47}$$

where it can be shown, using Lemma 1, that $[\mathbf{H}_t\mathbf{P}_t \ \ \mathbf{H}_c\mathbf{P}_{c,\text{I}}]$ is a.s. full rank. Thus, we have

$$I(\mathbf{X}_t; \mathbf{Y}_r) \geq d\log P + o(\log P), \tag{48}$$

and hence the s.d.o.f. is lower bounded as $D_s \geq \frac{K+N-M}{2}$.

E. Case 5: $M \leq N$, $N < K \leq N + M$, and $K + N - M$ is odd

The achievable scheme for this case combines the techniques used in Sections V-C and V-D: (i) the transmitter sends $d = \frac{K+N-M+1}{2}$ structured information streams, $N-M$ out of which are sent over $\mathcal{N}(\mathbf{G}_t)$, (ii) the CJ sends $l = \frac{K+M-N+1}{2}$ structured jamming streams, $K-N$ out of which are sent over $\mathcal{N}(\mathbf{H}_c)$, (iii) the information and jamming streams are aligned at the eavesdropper, (iv) the receiver uses the projection and cancellation techniques described in Section V-C to decode $U_1, \cdots, U_d$. Using similar analysis as in Sections V-C and V-D, it can be shown that the s.d.o.f. of $\frac{K+N-M}{2}$ is achievable for this case, which completes the achievability proof for (27). Next, we show the achievability of (28), when $M > N$.

F. Case 6: $M > N$ and $M - N < K \leq M - \frac{N}{2}$

The achievable scheme for this case involves transmitting d independent Gaussian information streams and d independent Gaussian jamming streams, where $d = K + N - M$. Having $M > N$ precludes the sufficiency of $\mathbf{P}_t$ for achieving the alignment of the information and jamming streams at the eavesdropper. Thus, both the transmitter and CJ choose their linear precoding in order to achieve the alignment condition.

The transmitted signals are given by (30), with $d = l = K + N - M$, $\mathbf{U}_t, \mathbf{V}_c \sim \mathcal{CN}(\mathbf{0}, \bar{P}\mathbf{I}_d)$, and $\bar{P}$ is defined as in Section V-A. $\mathbf{P}_t$, $\mathbf{P}_c$ are chosen as follows: Let $\mathbf{G} = [\mathbf{G}_t \ -\mathbf{G}_c] \in \mathbb{C}^{M\times(N+K)}$, and let $\mathbf{Q} \in \mathbb{C}^{(N+K)\times d}$ be randomly chosen such that its columns span $\mathcal{N}(\mathbf{G})$. Let $\mathbf{Q} = [\mathbf{Q}_1^T \ \ \mathbf{Q}_2^T]^T$, where $\mathbf{Q}_1 \in \mathbb{C}^{N\times d}$ and $\mathbf{Q}_2 \in \mathbb{C}^{K\times d}$. Set $\mathbf{P}_t = \mathbf{Q}_1$ and $\mathbf{P}_c = \mathbf{Q}_2$. This choice results in $\mathbf{G}_t\mathbf{P}_t = \mathbf{G}_c\mathbf{P}_c$. Thus, the eavesdropper receives a signal as in (32) with $\mathbf{U}_t$ and $\tilde{\mathbf{G}}_c = \mathbf{G}_c\mathbf{P}_c$ instead of $\mathbf{U}_t{}_1^{\ l}$ and $\mathbf{G}_c$, and $I(\mathbf{X}_t; \mathbf{Y}_e)$ is upper bounded as $I(\mathbf{X}_t; \mathbf{Y}_e) \leq K + N - M$. On the other hand, the receiver receives

$$\mathbf{Y}_r = \begin{bmatrix} \mathbf{H}_t\mathbf{P}_t & \mathbf{H}_c\mathbf{P}_c \end{bmatrix} \begin{bmatrix} \mathbf{U}_t \\ \mathbf{V}_c \end{bmatrix} + \mathbf{Z}_r. \tag{49}$$

Without conditioning on $\mathbf{G}_t$ and $\mathbf{G}_c$, the matrix $\mathbf{Q}$ has all of its entries independently and randomly drawn according to some continuous distribution, and hence, each of $\mathbf{P}_t$ and $\mathbf{P}_c$ is a.s. full column rank. Using Lemma 1, we can show that $[\mathbf{H}_t\mathbf{P}_t \ \ \mathbf{H}_c\mathbf{P}_c]$ is a.s. full column rank, and hence $I(\mathbf{X}_t; \mathbf{Y}_r) \geq (K + N - M)\log P + o(\log P)$. Thus, using (29) and (5), we have $D_s \geq K + N - M$ for this case.

G. Case 7: $M > N$, $M - \frac{N}{2} < K \leq M$, and N is even

Using a similar argument as in Section V-B, the scheme in the previous case, with $K = M - \frac{N}{2}$, can be used to achieve the s.d.o.f. of the channel for all $M - \frac{N}{2} < K \leq M$, when $M > N$ and N is even. However, since $\dim(\mathcal{N}(\mathbf{G})) = N + K - M > \frac{N}{2}$, the $\frac{N}{2}$ columns of $\mathbf{Q}$ are chosen as l.i. vectors from $\mathcal{N}(\mathbf{G})$.

Following the same analysis as in the previous case, the s.d.o.f. for this case is lower bounded as $D_s \geq \frac{N}{2}$.

H. Case 8: $M > N$, $M - \frac{N}{2} < K \leq M$, and N is odd

Each of the transmitter and the CJ sends $d = \frac{N+1}{2}$ independent structured streams. Both the transmitter and the CJ choose their precoding matrices as in Section V-F. The receiver employs the decoding scheme in Sections V-C, V-E. Using similar analysis as in Sections V-C, V-F, the s.d.o.f. of $\frac{N}{2}$ is shown to be achievable for this case.

I. Case 9: $M > N$, $M < K \leq N + M$, and $K + N - M$ is even

For this case, d independent Gaussian information and d independent Gaussian jamming streams are transmitted, where $d = \frac{K+N-M}{2}$. In addition to choosing its precoding matrix jointly with the transmitter to satisfy the alignment of the information and jamming streams at the eavesdropper, the CJ chooses its precoding matrix, $\mathbf{P}_c$, so that $K - M$ out of its d jamming streams are sent over $\mathcal{N}(\mathbf{H}_c)$, leaving only $g = \frac{M+N-K}{2}$ streams visible to the receiver.

The transmitted signals are given by (30) with $d = l = \frac{K+N-M}{2}$, and $\mathbf{U}_t, \mathbf{V}_c$ are defined as in Section V-F. Let $\mathbf{P}_t = [\mathbf{P}_{t,1} \ \mathbf{P}_{t,2}]$, and $\mathbf{P}_c = [\mathbf{P}_{c,1} \ \mathbf{P}_{c,2}]$, where $\mathbf{P}_{t,1} \in \mathbb{C}^{N\times g}$, $\mathbf{P}_{t,2} \in \mathbb{C}^{N\times(K-M)}$, $\mathbf{P}_{c,1} \in \mathbb{C}^{K\times g}$, and $\mathbf{P}_{c,2} \in \mathbb{C}^{K\times(K-M)}$. $\mathbf{P}_t$ and $\mathbf{P}_c$ are chosen as follows: Let $\mathbf{G} = [\mathbf{G}_t \ -\mathbf{G}_c] \in \mathbb{C}^{M\times(N+K)}$, and let $\mathbf{G}' \in \mathbb{C}^{(M+N)\times(N+K)}$ be expressed as

$$\mathbf{G}' = \begin{bmatrix} \mathbf{G}_t & -\mathbf{G}_c \\ \mathbf{0}_{N\times N} & \mathbf{H}_c \end{bmatrix}. \tag{50}$$

Let $\mathbf{Q}' \in \mathbb{C}^{(N+K)\times(K-M)}$ be randomly chosen such that its columns span $\mathcal{N}(\mathbf{G}')$, and let the columns of $\mathbf{Q} \in \mathbb{C}^{(N+K)\times g}$ be randomly chosen as l.i. vectors in $\mathcal{N}(\mathbf{G})$, and not in $\mathcal{N}(\mathbf{G}')$. Let $\mathbf{Q} = [\mathbf{Q}_1^T \ \mathbf{Q}_2^T]^T$, $\mathbf{Q}' = [\mathbf{Q}_1'^T \ \mathbf{Q}_2'^T]^T$, and set $\mathbf{P}_{t,1} = \mathbf{Q}_1$, $\mathbf{P}_{t,2} = \mathbf{Q}_1'$, $\mathbf{P}_{c,1} = \mathbf{Q}_2$, and $\mathbf{P}_{c,2} = \mathbf{Q}_2'$. This choice results in $\mathbf{G}_t\mathbf{P}_t = \mathbf{G}_c\mathbf{P}_c$ and $\mathbf{H}_c\mathbf{P}_{c,2} = \mathbf{0}_{N\times(K-M)}$. Thus, the eavesdropper's received signal is as in (32) with $\mathbf{U}_t$ and $\tilde{\mathbf{G}}_c = \mathbf{G}_c\mathbf{P}_c$ instead of $\mathbf{U}_{t1}^{l}$ and $\mathbf{G}_c$, and hence $I(\mathbf{X}_t; \mathbf{Y}_e) \leq \frac{K+N-M}{2}$. The receiver's received signal is

$$\mathbf{Y}_r = \begin{bmatrix} \mathbf{H}_t\mathbf{P}_t & \mathbf{H}_c\mathbf{P}_{c,1} \end{bmatrix} \begin{bmatrix} \mathbf{U}_t \\ \mathbf{V}_{c1}^{g} \end{bmatrix} + \mathbf{Z}_r. \tag{51}$$

Due to the random generation of the channel gains, each of $\mathbf{P}_t$ and $\mathbf{P}_{c,1}$ is a.s. full column rank. Using Lemma 1, $[\mathbf{H}_t\mathbf{P}_t \quad \mathbf{H}_c\mathbf{P}_{c,1}]$ is a.s. full column rank, and hence, $I(\mathbf{X}_t; \mathbf{Y}_r) \geq \frac{K+N-M}{2}\log P + o(\log P)$, and the s.d.o.f. for this case is lower bounded as $D_s \geq \frac{K+N-M}{2}$.

J. Case 10: $M > N$, $M < K \leq N + M$, and $K + N - M$ is odd

Let $\mathbf{U}_t$ and $\mathbf{V}_c$ be defined as in Section V-C with $d = l = \frac{K+N-M+1}{2}$, and let $\mathbf{P}_t$ and $\mathbf{P}_c$ be chosen as in Section V-I with $g = \frac{M+N-K+1}{2}$. Using a similar decoding scheme at the receiver as in Sections V-C, V-E, and V-H, we can show that the s.d.o.f. is lower bounded as $D_s \geq \frac{K+N-M}{2}$ for this case, which completes the proof of achievability of (28). Thus, we have completed the proof for Theorem 1.

VI. Conclusion

We have studied the $(N \times N \times M)$ multiple antenna Gaussian wiretap channel (WTC) with a K-antenna cooperative jammer (CJ). We have characterized the secure degrees of freedom for this channel for all possible values of K. Similar to [8], we have shown that the integer valued secure degrees of freedom is achieved by a scheme which involves linear precoding, linear receiver processing, and Gaussian signalling, while the non-integer secure degrees of freedom requires transmitting structured signals, along with a decoding scheme at the receiver which combines both the signal space and signal scale alignment, to be achieved. We have also seen that, extending the case where the eavesdropper is assumed to have the same number of antennas as the legitimate terminals, i.e., $M = N$, to the case where M is arbitrary entails the use of more intricate precoding at the transmitter and CJ to exploit the advantage of having fewer antennas at the eavesdropper than the legitimate terminals, or to overcome the disadvantage of M being larger than N.

In this paper, we have studied the model where the number of transmit antennas at the legitimate transmitter, N_t, is equal to the number of receiving antennas at the legitimate receiver, N_r, i.e., a symmetric model. The asymmetric case with $N_t \neq N_r$ is the focus of ongoing work where similar techniques yield the secure degrees of freedom and care must be exercised handling a large number of subcases for different ranges of the number of antennas.

References

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

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339–3487, 1978.

[3] E. Tekin and A. Yener, "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] J. Xie and S. Ulukus, "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.

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

[6] 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.

[7] 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.

[8] M. Nafea and A. Yener, "Secure degrees of freedom for the MIMO wiretap channel with a multiantenna cooperative jammer," *in IEEE Information Theory Workshop*, Nov. 2014.

[9] ——, "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.

[10] ——, "Degrees of freedom of the single antenna Gaussian wiretap channel with a helper irrespective of the number of antennas at the eavesdropper," *in IEEE GlobalSIP Symposium on Cyber-Security and Privacy*, Dec. 2013.

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

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