Cooperative Jamming for MIMO Wiretap Channels

Shuiyin Liu, Yi Hong, and Emanuele Viterbo
ECSE Department, Monash University
Melbourne, VIC 3800, Australia
Email: shuiyin.liu, yi.hong, emanuele.viterbo@monash.edu

***Abstract*—This paper addresses secure communications over MIMO wiretap channels with the help of multiple cooperative jammers. The worst-case scenario for Alice, Bob and jammers is considered: Eve has the knowledge of all channel matrices, while neither her channel matrix nor her location is known to the remaining terminals. We propose an artificial noise aided cooperative jamming (AN-CJ) scheme, allowing the total jamming signals to be nulled at Bob. The new scheme is valid for the case where the eavesdropper has more antennas than the transmitter. To evaluate the performance of the AN-CJ scheme, we first derive a closed-form expression for the achievable ergodic secrecy rate with Gaussian input alphabets. Then, we show how Gaussian input alphabets achieve the ergodic secrecy capacity.**

I. Introduction

The broadcast nature of wireless channels allows unauthorized users in the coverage area to overhear the transmitted signals. Physical layer security, pioneered by Wyner [1], is concerned with the channel coding technologies such that, the information leakage between a transmitter (Alice) and an eavesdropper (Eve) vanishes as the codeword length tends to infinity [2]. The notion of *secrecy capacity* was thereby introduced to characterize the maximum transmission rate from Alice to the intended user (Bob), below which Eve receives zero bits of information [3]. The secrecy capacity of ergodic fading channels was determined in [4]. The quasi-static fading channel was initially examined in [5], where the secrecy capacity outage probability is characterized. The secrecy capacity of MIMO wiretap channel was derived in [6]. The achievable ergodic secrecy rate has been widely adopted as a metric of security [7–11]

Recently, there have been considerable efforts devoted to increasing the secrecy rate by adding controlled interference at Eve, so called *artificial noise* (AN) [7] for the MIMO case. In the AN scheme, Alice aligns an additive white Gaussian noise (AWGN) signal, named "artificial noise", within the null space between Alice and Bob, thus only Eve is jammed. The most significant weakness of this approach is its assumption: Alice must have more antennas than Eve [7].

In this paper, we consider the use of the AN scheme to a MIMO cooperative jammer case (AN-CJ): the helping interference (the AN in the null space between the jammer and BoB) is generated from third-party jammers. This interference is only harmful to Eve, but not Bob. In our scheme, *(i)* no upper bound on Eve's antenna number is assumed; *(ii)* none of Alice, Bob and jammers need to know Eve's channel information; *(iii)* Eve has perfect knowledge of all terminals' channel information. A similar approach under different assumptions was proposed in [12] (see Sec. II for details).

This work is supported by ARC under Grant Discovery Project No. DP130100336.

Note that our scheme is quite different from the conventional cooperative jamming schemes in [8–11]. Specifically, the authors in [8,9] considered a multiuser case over AWGN channels, where the multiple users act as jammers and emit interferences to both Eve and Bob, assuming the jammers can cause more harm to Eve than to Bob. All these existing schemes in [8–11] required the perfect Eve's channel information at Alice or jammers.

The main contribution of the paper is to study the secrecy rate achieved by the proposed AN-CJ scheme.

- Derivation of the ergodic secrecy rate with Gaussian input alphabets, as a function of Eve's SNR, Bob's SNR, jamming power allocation schemes, and the number of antennas of Alice, Bob, Eve, and the jammers.
- Derivation of a sufficient condition for the achievability of ergodic secrecy capacity using Gaussian input alphabets.

The paper is organized as follows: Section II presents the system model, followed by the analysis of secrecy rate in Section III. Section IV analyzes the achievability of the ergodic secrecy capacity. Conclusions are drawn in Section V. Proofs of the theorems are given in Appendix.

Notation: Matrices and column vectors are denoted by upper and lowercase boldface letters, and the Hermitian transpose, inverse, pseudoinverse of a matrix $\mathbf{B}$ by $\mathbf{B}^H$, $\mathbf{B}^{-1}$, and $\mathbf{B}^\dagger$, respectively. $|\mathbf{B}|$ denotes the determinant of $\mathbf{B}$. $\mathbf{I}_n$ denotes the identity matrix of size n. An $m \times n$ null matrix is denoted by $\mathbf{0}_{m\times n}$. We write $\triangleq$ for equality in definition. A circularly symmetric complex Gaussian random variable X with variance σ^2 is defined as $X \backsim \mathcal{N}_{\mathbb{C}}(0,\sigma^2)$. The real, complex, integer and complex integer numbers are denoted by $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$ and $\mathbb{Z}[i]$, respectively. $I(X;Y)$ represents the mutual information of two random variables X and Y. We use the standard asymptotic notation $f(x) = O(g(x))$ when $\limsup_{x\to\infty} |f(x)/g(x)| < \infty$. $\lceil x \rfloor$ rounds to the closest integer. A central complex Wishart matrix $\mathbf{A} \in \mathbb{C}^{m\times m}$ with n degrees of freedom and covariance matrix $\mathbf{\Sigma}$, is defined as $\mathbf{A} \backsim W_m(n,\mathbf{\Sigma})$.

II. System Model

We consider a MIMO wiretap system model consisting of a transmitter (Alice), an intended receiver (Bob), and a

passive eavesdropper (Eve), with $N_{\rm A}$, $N_{\rm B}$, and $N_{\rm E}$ antennas, respectively. Let $\mathbf{H} \in \mathbb{C}^{N_{\rm B}\times N_{\rm A}}$ and $\mathbf{G} \in \mathbb{C}^{N_{\rm E}\times N_{\rm A}}$ be the channel matrices between Alice to Bob and Alice to Eve, respectively. Additionally, a set of N friendly jammers $\{\mathrm{J}_i\}_1^N$ are used to jam Eve, where each one has $N_{\mathrm{J},i}$ antennas, respectively (see Fig. 1). We assume that $N_{\rm B} \geq N_{\rm A}$ and $N_{\mathrm{J},i} > N_{\rm B}$. Let $N_{\rm J} = \sum_{i=1}^N N_{\mathrm{J},i}$ be the total number of antennas among all the jammers.

For the purpose of evaluating the achievable secrecy rate, we assume that the codewords used at Alice are Gaussian input alphabets, that is, Alice sends a complex vector $\mathbf{u} \in \mathbb{C}^{N_{\rm A}\times 1}$ with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\rm u}^2)$.

Let the matrices $\{\mathbf{H}_{\mathrm{JB},i}\}_1^N$ represent the channels from J_i to Bob, for $1 \leq i \leq N$. Suppose that J_i knows $\mathbf{H}_{\mathrm{JB},i}$, using the AN scheme [7], the $i^{\rm th}$ jammer transmits

$$\mathbf{x}_{\mathrm{J},i} = \mathbf{Z}_i \mathbf{v}_i, \tag{1}$$

where $\mathbf{v}_i \in \mathbb{C}^{(N_{\mathrm{J},i}-N_{\rm B})\times 1}$ is the "artificial noise" with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\rm v}^2)$, and $\mathbf{Z}_i = \mathrm{null}(\mathbf{H}_{\mathrm{JB},i})$ represents the null space of $\mathbf{H}_{\mathrm{JB},i}$, i.e., $\mathbf{H}_{\mathrm{JB},i}\mathbf{Z}_i = \mathbf{0}_{N_{\rm B}\times(N_{\mathrm{J},i}-N_{\rm B})}$. The vectors $\mathbf{u}$ and $\{\mathbf{v}_i\}_1^N$ are assumed to be mutually independent.

The signals received by Bob and Eve are given by

$$\mathbf{z} = \mathbf{H}\mathbf{u} + \sum_{i=1}^N \mathbf{H}_{\mathrm{JB},i}\mathbf{Z}_i\mathbf{v}_i + \mathbf{n}_{\rm B} = \mathbf{H}\mathbf{u} + \mathbf{n}_{\rm B}, \tag{2}$$

$$\mathbf{y} = \mathbf{G}\mathbf{u} + \sum_{i=1}^N \mathbf{H}_{\mathrm{JE},i}\mathbf{Z}_i\mathbf{v}_i + \mathbf{n}_{\rm E}, \tag{3}$$

where $\mathbf{n}_{\rm B}$ and $\mathbf{n}_{\rm E}$ are AWGN at Bob and Eve, respectively, with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\rm B}^2)$ and $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\rm E}^2)$. $\mathbf{H}_{\mathrm{JE},i} \in \mathbb{C}^{N_{\rm E}\times N_{\mathrm{J},i}}$ is the channel matrix between jammer J_i and Eve. All channel matrices, including $\mathbf{H}$, $\mathbf{G}$, $\{\mathbf{H}_{\mathrm{JB},i}\}_1^N$ and $\{\mathbf{H}_{\mathrm{JE},i}\}_1^N$, are assumed to be mutually independent (i.e., all terminals are not co-located) and have i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, 1)$.

We set the average transmit power constraints $P_{\rm u}$ and $P_{\rm J}$, as

$$\begin{aligned} P_{\rm u} &= \mathrm{E}(||\mathbf{u}||^2) = N_{\rm A}\sigma_{\rm u}^2, \\ P_{\rm J} &= \mathrm{E}\left(\sum_{i=1}^N ||\mathbf{x}_{\mathrm{J},i}||^2\right) = (N_{\rm J} - N\cdot N_{\rm B})\sigma_{\rm v}^2. \end{aligned} \tag{4}$$

We define Bob's and Eve's SNRs as

$$\begin{aligned} \mathrm{SNR}_{\rm B} &\triangleq \sigma_{\rm u}^2/\sigma_{\rm B}^2, \\ \mathrm{SNR}_{\rm E} &\triangleq \sigma_{\rm u}^2/\sigma_{\rm E}^2. \end{aligned} \tag{5}$$

We consider the worst-case scenario for Alice and Bob:

- Alice does not know any channel matrix.
- Bob only knows $\mathbf{H}$.
- The $i^{\rm th}$ jammer J_i only knows $\mathbf{H}_{\mathrm{JB},i}$, for all i.
- Eve has perfect knowledge of all channel matrices.
- No upper bound on $N_{\rm E}$ or $\mathrm{SNR}_{\rm E}$.

Instead, the scheme in [12] requires that

- Alice knows $\mathbf{H}$.
- Eve does not know $\{\mathbf{H}_{\mathrm{JB},i}\}_1^N$.

We show that the AN-CJ scheme is valid even if the above two restrictive assumptions are not satisfied.

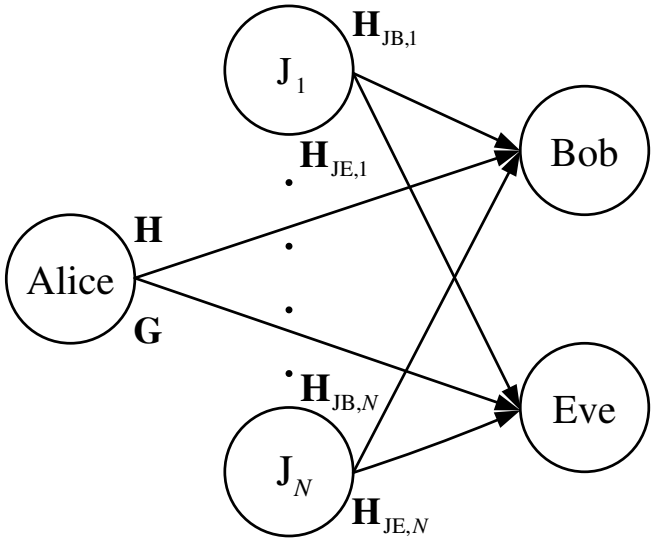

Fig. 1. Cooperative Jamming for MIMO wiretap channel.

To simplify our analysis, we define three system parameters:

- $\alpha \triangleq \sigma_{\rm u}^2/\sigma_{\rm E}^2$ ($\mathrm{SNR}_{\rm E}$)
- $\beta \triangleq \sigma_{\rm v}^2/\sigma_{\rm u}^2$ (Jamming power allocation)
- $\gamma \triangleq \sigma_{\rm E}^2/\sigma_{\rm B}^2$ (Eve-to-Bob noise-power ratio)

If $\gamma > 1$, we say Eve has a *degraded channel*. We note that

$$\mathrm{SNR}_{\rm B} = \alpha\gamma. \tag{6}$$

III. Ergodic Secrecy Rate with Gaussian Input Alphabets

In this section, we provide a detailed analysis on the ergodic secrecy rate on the AN-CJ system. To present our result, we first define some useful functions.

A. Definitions

We define ergodic secrecy capacity, as in [13]

$$\bar{C}_{\rm S} \triangleq \max_{p(\mathbf{u})} \left\{ I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N,\{\mathbf{H}_{\mathrm{JB},i}\}_1^N) \right\}. \tag{7}$$

where $I\left(X;Y|Z\right) \triangleq \mathrm{E}_Z\left[I\left(X;Y\right)|Z\right]$, following the notation in [14]. The maximum is taken over all possible input distributions $p\left(\mathbf{u}\right)$.

Since a closed form expression for $\bar{C}_{\rm S}$ is not always available, we resort to a lower bound given by

$$\bar{C}_{\rm S} \geq I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N,\{\mathbf{H}_{\mathrm{JB},i}\}_1^N) \triangleq \bar{R}_{\rm S}, \tag{8}$$

assuming Gaussian input alphabets, i.e., $\mathbf{u}$ and $\{\mathbf{v}_i\}_1^N$ are mutually independent vector with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\rm u}^2)$ and $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\rm v}^2)$, respectively.

We then define the following function, as in [15]

$$\Theta(m,n,x) \triangleq e^{-1/x} \sum_{k=0}^{m-1}\sum_{l=0}^{k}\sum_{i=0}^{2l} \left\{ \frac{(-1)^i(2l)!(n-m+i)!}{2^{2k-i}l!i!(n-m+l)!} \cdot \binom{2(k-l)}{k-l} \cdot \binom{2(l+n-m)}{2l-i} \cdot \sum_{j=0}^{n-m+i} x^{-j}\Gamma(-j,1/x) \right\}, \tag{9}$$

where $\binom{a}{b} = a!/((a-b)!b!)$ is the binomial coefficient, $n \geq m$ are positive integers, and $\Gamma(\cdot,\cdot)$ is the incomplete Gamma function.

We further define

$$N_{\min} \triangleq \min\{N_{\mathrm{E}},\, N_{\mathrm{J}} - N \cdot N_{\mathrm{B}}\}, \tag{10}$$
$$N_{\max} \triangleq \max\{N_{\mathrm{E}},\, N_{\mathrm{J}} - N \cdot N_{\mathrm{B}}\}, \tag{11}$$

$$\hat{N}_{\min} \triangleq \min\{N_{\mathrm{E}},\, D\}, \tag{12}$$
$$\hat{N}_{\max} \triangleq \max\{N_{\mathrm{E}},\, D\}, \tag{13}$$

where

$$D = N_{\mathrm{A}} + N_{\mathrm{J}} - N \cdot N_{\mathrm{B}}. \tag{14}$$

Finally, we define a set of D power ratios $\{\theta_i\}_1^D$, where

$$\theta_i \triangleq \begin{cases} \alpha & 1 \leq i \leq N_{\mathrm{A}} \\ \alpha\beta & N_{\mathrm{A}} < i \leq D \end{cases} \tag{15}$$

B. Closed-form Expression for $\bar{R}_{\mathrm{S}}$

$\bar{R}_{\mathrm{S}}$ can be evaluated using the results from [14, Th. 2], [15, Th. 1] and [16, Th. 1], leading to the following theorem.

Theorem 1:

$$\bar{R}_{\mathrm{S}} = \Theta(N_{\mathrm{A}}, N_{\mathrm{B}}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) - \Psi \tag{16}$$

where

$$\Psi = \begin{cases} K \sum_{k=1}^{\hat{N}_{\min}} \det\left(\mathbf{R}^{(k)}\right), & \beta \neq 1 \\ \Theta(\hat{N}_{\min}, \hat{N}_{\max}, \alpha), & \beta = 1 \end{cases} \tag{17}$$

$$K = \frac{(-1)^{N_{\mathrm{E}}(D-\hat{N}_{\min})}}{\Gamma_{\hat{N}_{\min}}(N_{\mathrm{E}})} \frac{\prod_{i=1}^{2} \mu_i^{m_i N_{\mathrm{E}}}}{\prod_{i=1}^{2} \Gamma_{m_i}(m_i) \prod_{i<j} (\mu_i - \mu_j)^{m_i m_j}}, \tag{18}$$

$$\Gamma_k(n) = \prod_{i=1}^{k} (n-i)!,$$

and $\mu_1 > \mu_2$ are the two distinct eigenvalues of the diagonal matrix $\mathrm{diag}\left(\left\{\theta_i^{-1}\right\}_1^D\right)$, with corresponding multiplicities m_1 and m_2 such that $m_1 + m_2 = D$. The matrix $\mathbf{R}^{(k)}$ has elements

$$r_{i,j}^{(k)} = \begin{cases} (\mu_{e_i})^{D-j-d_i} \dfrac{(D-j)!}{(D-j-d_i)!}, & \hat{N}_{\min}+1 \leq j \leq D \\ (-1)^{d_i} \dfrac{\varphi(i,j)!}{(\mu_{e_i})^{\varphi(i,j)+1}}, & 1 \leq j \leq \hat{N}_{\min},\ j \neq k \\ (-1)^{d_i} \varphi(i,j)! e^{\mu_{e_i}} \sum_{l=0}^{\varphi(i,j)} \dfrac{\Gamma(l-\varphi(i,j), \mu_{e_i})}{(\mu_{e_i})^{l+1}}, & \text{otherwise} \end{cases} \tag{19}$$

where

$$e_i = \begin{cases} 1 & 1 \leq i \leq m_1 \\ 2 & m_1 + 1 \leq i \leq D \end{cases}$$

$$d_i = \sum_{k=1}^{e_i} m_k - i,$$

$$\varphi(i,j) = N_{\mathrm{E}} - \hat{N}_{\min} + j - 1 + d_i.$$

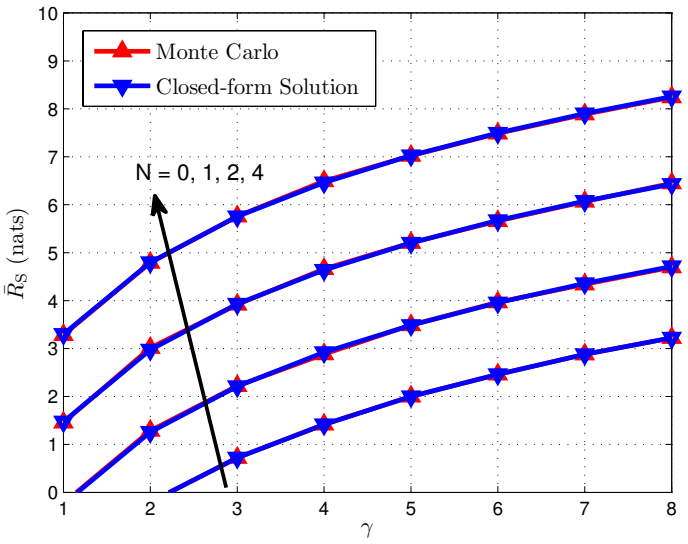

Fig. 2. $\bar{R}_{\mathrm{S}}$ vs. γ and N with $\alpha = \beta = 2$, $N_{\mathrm{A}} = N_{\mathrm{B}} = 3$, $N_{\mathrm{E}} = 5$ and $N_{\mathrm{J},i} = 5$.

Proof: See Appendix A. ■

Theorem 1 gives the exact ergodic secrecy rate for the AN-CJ scheme, with arbitrary $\mathrm{SNR}_{\mathrm{B}}$ ($\alpha\gamma$), $\mathrm{SNR}_{\mathrm{E}}$ (α), power allocation scheme (β) and N_{E}. Note that (16) can be expressed in terms of a finite number of incomplete Gamma functions, thus provides a closed-form expression for $\bar{R}_{\mathrm{S}}$.

If there is no jammer, i.e., $N = 0$, it is easy to show

$$\bar{R}_{\mathrm{S}} = \Theta(N_{\mathrm{A}}, N_{\mathrm{B}}, \alpha\gamma) - \Theta(N_{\mathrm{A}}, N_{\mathrm{E}}, \alpha). \tag{20}$$

Let us apply Theorem 1 to the analysis of an AN-CJ scheme with $\alpha = \beta = 2$ (3 dB), $N_{\mathrm{A}} = N_{\mathrm{B}} = 3$ and $N_{\mathrm{E}} = 5$. Each friendly jammer is equipped with $N_{\mathrm{J},i} = 5$ antennas. Fig. 2 shows the value of $\bar{R}_{\mathrm{S}}$ as a function of the channel degradation γ and the number of jammers N. As expected, the closed-form solution matches Monte Carlo simulation perfectly. In particular, the use of the jammers ($N > 0$) provides significantly better secrecy performance than without using the jammer ($N = 0$).

Recalling that

$$\bar{C}_{\mathrm{S}} \geq \bar{R}_{\mathrm{S}}. \tag{21}$$

The above results show that by increasing the number of jammers, positive secrecy capacity is available, even when

- Eve has a better channel than Bob.
- Eve has more antennas than Alice and Bob.

IV. Achieving Ergodic Secrecy Capacity with Gaussian Input Alphabets

In this section, we show the achievability of the ergodic secrecy capacity using Gaussian input alphabets.

Theorem 2: If $N_{\mathrm{E}} \leq N_{\mathrm{J}} - N \cdot N_{\mathrm{B}}$, as $\alpha\beta \to \infty$, then

$$\bar{C}_{\mathrm{S}} = \bar{R}_{\mathrm{S}} = \bar{C}_{\mathrm{Bob}}, \tag{22}$$

where $\bar{C}_{\mathrm{Bob}}$ represents Bob's ergodic channel capacity.

Proof: See Appendix B. ■

According to (7), a universal upper bound on the ergodic MIMO secrecy capacity is given by

$$\bar{C}_{\mathrm{S}} \leq \max_{p(\mathbf{u})} \{I(\mathbf{u};\mathbf{z}|\mathbf{H})\} = \bar{C}_{\mathrm{Bob}}. \tag{23}$$

Remark 1: Combining (22) and (23), we *de facto* show that with AN-CJ transmission scheme and Gaussian input alphabets, if $N_{\mathrm{E}} \leq N_{\mathrm{J}} - N \cdot N_{\mathrm{B}}$, the *maximum* ergodic MIMO secrecy capacity can be achieved by increasing the jamming signal power (i.e., $\alpha\beta$).

V. Conclusions

In this paper, we have considered the use of cooperative jamming to enhance the security of MIMO wiretap channel. The proposed AN-CJ scheme is designed under realistic scenarios where Eve has more antennas than Alice and Eve's channel information is not available to Alice, Bob and the friendly jammers. To characterize the performance of the AN-CJ scheme, we derived a closed-form expression for the achievable ergodic secrecy rate with Gaussian input alphabets, as a function of $\mathrm{SNR}_{\mathrm{B}}$, $\mathrm{SNR}_{\mathrm{E}}$, N_{A}, N_{B}, N_{E} and N_{J}. Furthermore, we have shown that the AN-CJ scheme with Gaussian input alphabets achieves the maximum ergodic secrecy capacity, when $N_{\mathrm{E}} \leq N_{\mathrm{J}} - N \cdot N_{\mathrm{B}}$.

Appendix

A. Proof of Theorem 1

Recalling that

$$\bar{R}_{\mathrm{S}} = I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N,\{\mathbf{H}_{\mathrm{JB},i}\}_1^N). \tag{24}$$

1) $I(\mathbf{u};\mathbf{z}|\mathbf{H})$

According to [14, Th. 2] and [15, Th. 1], we have

$$I(\mathbf{u};\mathbf{z}|\mathbf{H}) = \Theta(N_{\mathrm{A}}, N_{\mathrm{B}}, \alpha\gamma), \tag{25}$$

where $\Theta(x,y,z)$ is given in (9).

2) $I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N,\{\mathbf{H}_{\mathrm{JB},i}\}_1^N)$

Since all entries in $\mathbf{G}$, $\{\mathbf{H}_{\mathrm{JE},i}\}_1^N$ and $\{\mathbf{H}_{\mathrm{JB},i}\}_1^N$ are mutually independent, $I(\mathbf{u};\mathbf{y})$ can be expressed as a function of these independent random entries. This allows us to take two steps to compute the expected value of $I(\mathbf{u};\mathbf{y})$: we first compute $I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N)$ given $\{\mathbf{H}_{\mathrm{JB},i}\}_1^N$, then compute $\mathrm{E}_{\{\mathbf{H}_{\mathrm{JB},i}\}_1^N}\left(I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N)|\{\mathbf{H}_{\mathrm{JB},i}\}_1^N\right)$. The advantage is that for given $\{\mathbf{H}_{\mathrm{JB},i}\}_1^N$, $\{\mathbf{Z}_i\}_1^N$ are fixed and the columns of each of them form a set of orthonormal vectors. Then, using [17, Th. 1], $\{\mathbf{H}_{\mathrm{JE},i}\mathbf{Z}_i\}_1^N$ are mutually independent complex Gaussian random matrices with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\,1)$.

Based on the above analysis, we rewrite $\mathbf{y}$ in (3) as

$$\mathbf{y} = \mathbf{G}\mathbf{u} + \mathbf{Q}\mathbf{v} + \mathbf{n}_{\mathrm{E}}, \tag{26}$$

where

$$\mathbf{Q} = [\mathbf{H}_{\mathrm{JE},1}\mathbf{Z}_1,\ ...,\ \mathbf{H}_{\mathrm{JE},N}\mathbf{Z}_N] \text{ and } \mathbf{v} = \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_N \end{bmatrix}.$$

For given $\{\mathbf{H}_{\mathrm{JB},i}\}_1^N$, $\mathbf{Q} \in \mathbb{C}^{N_{\mathrm{E}} \times (N_{\mathrm{J}} - N\cdot N_{\mathrm{B}})}$ is thus a complex Gaussian random matrix with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\,1)$. Let $\mathbf{W}_1 = \mathbf{G}\mathbf{G}^H$ and $\mathbf{W}_2 = \mathbf{Q}\mathbf{Q}^H$. According to [14], we have

$$\begin{aligned} &I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N) \\ &= \mathrm{E}_{\mathbf{G},\mathbf{Q}}\left(\log \frac{\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{\sigma_{\mathrm{u}}^2}{\sigma_{\mathrm{E}}^2}\mathbf{W}_1 + \frac{\sigma_{\mathrm{v}}^2}{\sigma_{\mathrm{E}}^2}\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{\sigma_{\mathrm{v}}^2}{\sigma_{\mathrm{E}}^2}\mathbf{W}_2\right|}\right) \\ &= \mathrm{E}_{\mathbf{G},\mathbf{Q}}\left(\log|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2|\right) - \mathrm{E}_{\mathbf{Q}}\left(\log|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\beta\mathbf{W}_2|\right). \end{aligned} \tag{27}$$

According to [14, Th. 2] and [15, Th. 1], the second term of (27) equals to

$$\mathrm{E}_{\mathbf{Q}}\left(\log|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\beta\mathbf{W}_2|\right) = \Theta(N_{\min}, N_{\max}, \alpha\beta), \tag{28}$$

where $N_{\min}$ and $N_{\max}$ are given in (10) and (11), respectively.

To compute the first term of (27), we rewrite $\alpha\mathbf{W}_1 + \alpha\beta\mathbf{W}_2$ as $\hat{\mathbf{G}}\boldsymbol{\Delta}\hat{\mathbf{G}}^H$, where

$$\hat{\mathbf{G}} = [\mathbf{G}, \mathbf{Q}] \text{ and } \boldsymbol{\Delta} = \mathrm{diag}\left\{\{\theta_i\}_1^D\right\}, \tag{29}$$

where $\hat{\mathbf{G}} \in \mathbb{C}^{N_{\mathrm{E}} \times D}$ is a complex Gaussian random matrix with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\,1)$, and θ_i is defined in (15).

Case 1: If $\beta = 1$, the first term of (27) reduces to

$$\mathrm{E}_{\hat{\mathbf{G}}}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}} + \hat{\mathbf{G}}\boldsymbol{\Delta}\hat{\mathbf{G}}^H\right|\right) = \mathrm{E}_{\hat{\mathbf{G}}}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\hat{\mathbf{G}}\hat{\mathbf{G}}^H\right|\right), \tag{30}$$

where $\hat{\mathbf{G}}$ is given in (29).

According to [14, Th. 2] and [15, Th. 1], we have

$$\mathrm{E}_{\hat{\mathbf{G}}}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}} + \alpha\hat{\mathbf{G}}\hat{\mathbf{G}}^H\right|\right) = \Theta(\hat{N}_{\min}, \hat{N}_{\max}, \alpha), \tag{31}$$

where $\hat{N}_{\min}$ and $\hat{N}_{\max}$ are given in (12) and (13), respectively.

Case 2: If $\beta \neq 1$, $\boldsymbol{\Delta}^{-1}$ contains two groups of coinciding eigenvalues. According to [16, Th. 1], we have

$$\mathrm{E}_{\hat{\mathbf{G}}}\left(\log\left|\mathbf{I}_{N_{\mathrm{E}}} + \hat{\mathbf{G}}\boldsymbol{\Delta}\hat{\mathbf{G}}^H\right|\right) = K\sum_{k=1}^{\hat{N}_{\min}} \det\left(\mathbf{R}^{(k)}\right), \tag{32}$$

where $\hat{N}_{\min}$, K and $\mathbf{R}^{(k)}$ are given in (12), (18) and (19).

Based on (27), (28), (31) and (32), we have

$$\begin{aligned} & I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N,\{\mathbf{H}_{\mathrm{JB},i}\}_1^N) \\ = \ & \mathrm{E}_{\{\mathbf{H}_{\mathrm{JB},i}\}_1^N}\left(I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N)|\{\mathbf{H}_{\mathrm{JB},i}\}_1^N\right) \\ = \ & \Psi - \Theta(N_{\min}, N_{\max}, \alpha\beta), \end{aligned} \tag{33}$$

where Ψ is given in (17) and unify the cases $\beta = 1$ and $\beta \neq 1$.

By substituting (25) and (33) into (24), we have

$$\bar{R}_{\mathrm{S}} = \Theta(N_{\mathrm{A}}, N_{\mathrm{B}}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) - \Psi.$$

■

B. Proof of Theorem 2

We follow the definitions in the proof of Theorem 1. Based on (27), for given $\{\mathbf{H}_{\mathrm{JB},i}\}_1^N$, we have

$$\begin{aligned}
&I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N)) \\
&= \mathrm{E}_{\mathbf{G},\mathbf{Q}}\left(\log\frac{\left|\mathbf{I}_{N_\mathrm{E}}\sigma_\mathrm{E}^2+\sigma_\mathrm{u}^2\mathbf{W}_1+\sigma_\mathrm{v}^2\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_\mathrm{E}}\sigma_\mathrm{E}^2+\sigma_\mathrm{v}^2\mathbf{W}_2\right|}\right) \\
&\overset{a}{\leq} \mathrm{E}_{\mathbf{Q}}\left(\log\frac{\left|\mathbf{I}_{N_\mathrm{E}}\sigma_\mathrm{E}^2+\sigma_\mathrm{u}^2\mathrm{E}_{\mathbf{G}}\left(\mathbf{W}_1\right)+\sigma_\mathrm{v}^2\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_\mathrm{E}}\sigma_\mathrm{E}^2+\sigma_\mathrm{v}^2\mathbf{W}_2\right|}\right) \\
&= \mathrm{E}_{\mathbf{Q}}\left(\log\frac{\left|\mathbf{I}_{N_\mathrm{E}}+\dfrac{\sigma_\mathrm{v}^2}{\sigma_\mathrm{E}^2+N_\mathrm{A}\sigma_\mathrm{u}^2}\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_\mathrm{E}}+\dfrac{\sigma_\mathrm{v}^2}{\sigma_\mathrm{E}^2}\mathbf{W}_2\right|}\right)+N_\mathrm{E}\log\frac{\sigma_\mathrm{E}^2+N_\mathrm{A}\sigma_\mathrm{u}^2}{\sigma_\mathrm{E}^2},
\end{aligned} \tag{34}$$

where (a) holds due to the concavity of log-determinant function and Jensen's inequality.

Let

$$\mathbf{W}=\begin{cases}\mathbf{Q}\mathbf{Q}^H & \text{if } N_\mathrm{E}\leq N_\mathrm{J}-N\cdot N_\mathrm{B}\\ \mathbf{Q}^H\mathbf{Q} & \text{if } N_\mathrm{E}>N_\mathrm{J}-N\cdot N_\mathrm{B}\end{cases},$$

i.e., $\mathbf{W}\sim W_{N_{\min}}(N_{\max},\mathbf{I}_{N_{\min}})$.

Recalling the definitions of α and β in Sec. II, and based on Sylvester's determinant theorem and [15, Th. 1], the first term of (34) can be rewritten as

$$\begin{aligned}
&\mathrm{E}_{\mathbf{Q}}\left(\log\frac{\left|\mathbf{I}_{N_{\min}}+\dfrac{\alpha\beta}{1+\alpha N_\mathrm{A}}\mathbf{W}\right|}{\left|\mathbf{I}_{N_{\min}}+\alpha\beta\mathbf{W}\right|}\right) \\
&=\Theta(N_{\min},N_{\max},\alpha\beta/(1+\alpha N_\mathrm{A}))-\Theta(N_{\min},N_{\max},\alpha\beta)
\end{aligned} \tag{35}$$

where $\Theta(x,y,z)$ is given in (9).

From (34) and (35), we have

$$\begin{aligned}
&I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N,\{\mathbf{H}_{\mathrm{JB},i}\}_1^N) \\
&=\mathrm{E}_{\{\mathbf{H}_{\mathrm{JB},i}\}_1^N}\left(I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N)|\{\mathbf{H}_{\mathrm{JB},i}\}_1^N\right) \\
&\leq N_\mathrm{E}\log(1+\alpha N_\mathrm{A})-\Theta(N_{\min},N_{\max},\alpha\beta) \\
&+\Theta(N_{\min},N_{\max},\alpha\beta/(1+\alpha N_\mathrm{A})) \\
&\overset{(a)}{=}(N_\mathrm{E}-N_{\min})\log(1+\alpha N_\mathrm{A})+O\left(\frac{1}{\alpha\beta}\right),
\end{aligned} \tag{36}$$

where (a) follows from [18, Examples 2.14&2.15].

If $N_{\min}=N_\mathrm{E}$, i.e., $N_\mathrm{E}\leq N_\mathrm{J}-N\cdot N_\mathrm{B}$, as $\alpha\beta\to\infty$,

$$I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N,\{\mathbf{H}_{\mathrm{JB},i}\}_1^N)\leq 0. \tag{37}$$

Since mutual information is always non-negative, we have

$$I(\mathbf{u};\mathbf{y}|\mathbf{G},\{\mathbf{H}_{\mathrm{JE},i}\}_1^N,\{\mathbf{H}_{\mathrm{JB},i}\}_1^N)=0. \tag{38}$$

Under the same conditions, by substituting (38) into (8), we have

$$\bar{R}_\mathrm{S}=I(\mathbf{u};\mathbf{z}|\mathbf{H})=\bar{C}_\mathrm{Bob}, \tag{39}$$

where $\bar{C}_\mathrm{Bob}$ represents Bob's ergodic channel capacity. The last equation holds since the input $\mathbf{u}$ is a circularly symmetric complex Gaussian random vector with zero mean and covariance $\sigma_\mathrm{u}^2\mathbf{I}_{N_\mathrm{B}}$ [14, Th. 1].

On the other hand, from (7), we have

$$\bar{C}_\mathrm{S}\leq\max_{p(\mathbf{u})}\{I(\mathbf{u};\mathbf{z}|\mathbf{H})\}=\bar{C}_\mathrm{Bob}. \tag{40}$$

Based on (39) and (40), as $\alpha\beta\to\infty$, if $N_\mathrm{E}\leq N_\mathrm{J}-N\cdot N_\mathrm{B}$,

$$\bar{C}_\mathrm{S}=\bar{R}_\mathrm{S}=\bar{C}_\mathrm{Bob}. \tag{41}$$

■

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, pp. 40–47, 1996.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[5] M. Bloch, J. Barros, M. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[8] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[9] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, 2011.

[10] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, 2013.

[11] 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.

[12] J. Wang and A. L. Swindlehurst, "Cooperative jamming in MIMO ad-hoc networks," in *Proc. 43rd Asilomar Conf. Signals, Syst. Comput.*, Nov. 2009, pp. 1719–1723.

[13] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[14] E. Telatar, "Capacity of multi-antenna Gaussian channels," *European Transactions on Telecommunications*, vol. 10, no. 6, pp. 585–595, 1999.

[15] H. Shin and J. H. Lee, "Closed-form formulas for ergodic capacity of MIMO Rayleigh fading channels," in *Proc. IEEE Int. Conf. Commun. (ICC'03)*, Anchorage, US, May 2003, pp. 2996–3000.

[16] M. Chiani, M. Z. Win, and H. Shin, "MIMO networks: The effects of interference," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 336–349, 2010.

[17] E. Lukacs and E. P. King, "A property of the normal distribution," *Ann. Math. Statist.*, vol. 25, no. 2, pp. 389–394, 1954.

[18] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications*. North America: Now Publishers Inc., 2004.