Artificial Noise Revisited: When Eve Has more Antennas than Alice

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*—We consider secure communications over MIMO wiretap channels, in the presence of a passive eavesdropper with an unlimited number of antennas. In this scenario, we characterize the performance of the *artificial noise* scheme proposed by Goel *et al.*, and show that non-zero secrecy capacity is available even when the eavesdropper has more antennas than the transmitter. Our results are derived based on the fraction of the transmission power used for artificial noise and the ratio of the channel noise variances of the eavesdropper and the intended receiver. Finally, we investigate the attack option for the eavesdropper to drive the secrecy rate to zero by increasing the number of antennas.**

I. Introduction

The issues of establishing a private and secure link at the physical layer have known a growing interest in the past few years. Physical layer security lays its foundation on the wiretap channel [1], where the pre-exchanged secret key in Shannon's model [2] is replaced by the channel noise to provide randomness. For this model, the notion of secrecy capacity is further developed to characterize the maximum transmission rate at which the eavesdropper (Eve) is unable to obtain any information [3]. For quasi-static fading channel, the average secrecy rate is derived in [4]. For the ergodic fading channel, [5] provides a detailed analysis of secrecy capacity. In the literature, the achievable average secrecy rate has been adopted as a metric of security [4–6].

The *artificial noise* (AN) recently emerged as a promising method to increase secrecy rate [6], where the transmitter (Alice) aligns a jamming signal named artificial noise within the null space between itself and the legitimate receiver (Bob), thus AN only degrades Eve's channel. In [6], assuming that both signal and AN follow a multivariate Gaussian distribution, non-zero average secrecy rate is observed in simulation, when the number of Eve's antennas N_{E} is strictly smaller than the number of Alice's antennas N_{A}, i.e., $N_{\mathrm{E}} < N_{\mathrm{A}}$. Several channel models have been considered to generalize the idea of AN. When the number of Bob's antennas $N_{\mathrm{B}} = 1$, [7] provides an asymptotic analysis of the secrecy capacity. When all channel matrices (including Eve) are fixed and known to all the terminals, [8] provides a detailed characterization in terms of the secrecy capacity. More recently, the notion of *practical secrecy* is proposed for the AN-based systems that make use of a finite alphabet (e.g., *M*-QAM) [9]. Instead of increasing secrecy rate, Eve's error probability is maximized by the randomly distributed AN (e.g., not necessarily Gaussian).

In this work, we investigate the comprehensive relationship between secrecy capacity, multiple antennas and signal-to-noise ratio (SNR) within the framework of the original Gaussian distributed AN scheme [6]. The contributions of the paper are as follows.

- We show that the *average* secrecy capacity is achieved with Gaussian input alphabets when $N_{\mathrm{E}} \leq N_{\mathrm{A}} - N_{\mathrm{B}}$.
- We provide upper and lower bounds on both average and *instantaneous* secrecy rates with Gaussian input alphabets that accounts for arbitrary Eve's SNR and N_{E}.
- From Bob's perspective, given N_{E}, we derive the values of N_{A} and N_{B} to ensure positive average secrecy rate.
- From Eve's perspective, given N_{A} and N_{B}, we derive the value of N_{E} to null the instantaneous secrecy rate.

The paper is organized as follows: Section II presents the system model, followed by the analysis of secrecy capacity in Section III. Section IV discusses the attack to drive the secrecy rate to zero. 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 $\mathbf{B}$. Let $\{X_n, X\}$ be defined on the same probability space. We write $X_n \overset{a.s.}{\to} X$ if X_n converges to X almost surely or with probability one. The identity matrix of size n is denoted by $\mathbf{I}_n$. 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.

II. System Model

We consider a MIMO wiretap system, including a transmitter (Alice), an intended receiver (Bob), and a passive eavesdropper (Eve), with N_{A}, N_{B}, and N_{E} antennas, respectively.

This work is supported by ARC under Grant Discovery Project No. DP130100336. This research is also supported by the 2013 Monash Faculty of Engineering Seed Funding Scheme.

978-1-4799-4665-5/14/$31.00 ©2014 IEEE

We assume that the matrices $\mathbf{H} \in \mathbb{C}^{N_{\mathrm{B}} \times N_{\mathrm{A}}}$ and $\mathbf{G} \in \mathbb{C}^{N_{\mathrm{E}} \times N_{\mathrm{A}}}$ represent the channels from Alice to Bob and Alice to Eve. $\mathbf{H}$ and $\mathbf{G}$ are assumed to be independent (i.e., all terminals are not co-located) and have i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, 1)$.

Assuming $N_{\mathrm{B}} < N_{\mathrm{A}}$, $\mathbf{H}$ then has a non-trivial null space $\mathbf{Z} = \mathrm{null}(\mathbf{H})$, i.e., $\mathbf{HZ} = \mathbf{0}_{N_{\mathrm{B}} \times (N_{\mathrm{A}} - N_{\mathrm{B}})}$. Let $\mathbf{H} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^H$ be the singular value decomposition (SVD) of $\mathbf{H}$. The relationship between matrices $\mathbf{Z}$ and $\mathbf{V}$ is given by

$$\mathbf{V} = [\mathbf{V}_1, \mathbf{Z}], \tag{1}$$

where $\mathbf{V}_1$ represents the matrix with the first N_{B} columns of $\mathbf{V}$. Using the AN scheme [6], Alice transmits

$$\mathbf{x} = \mathbf{V}_1\mathbf{u} + \mathbf{Zv} = \mathbf{V}\left[\begin{array}{c} \mathbf{u} \\ \mathbf{v} \end{array}\right], \tag{2}$$

where $\mathbf{u}$ is the secret data vector and $\mathbf{v}$ is the artificial noise. Gaussian input alphabets are assumed, i.e., both $\mathbf{u} \in \mathbb{C}^{N_{\mathrm{B}} \times 1}$ and $\mathbf{v} \in \mathbb{C}^{(N_{\mathrm{A}} - N_{\mathrm{B}}) \times 1}$ are mutually independent Gaussian vector with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{u}}^2)$ and $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{v}}^2)$, respectively.

The signals received by Bob and Eve are given by

$$\mathbf{z} = \mathbf{HV}_1\mathbf{u} + \mathbf{HZv} + \mathbf{n}_{\mathrm{B}} = \mathbf{HV}_1\mathbf{u} + \mathbf{n}_{\mathrm{B}}, \tag{3}$$

$$\mathbf{y} = \mathbf{GV}_1\mathbf{u} + \mathbf{GZv} + \mathbf{n}_{\mathrm{E}}. \tag{4}$$

where $\mathbf{n}_{\mathrm{B}}$ and $\mathbf{n}_{\mathrm{E}}$ are additive white Gaussian noise vectors at Bob and Eve, respectively, with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{B}}^2)$ and $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{E}}^2)$.

From Equations (3) and (4), we see that $\mathbf{v}$ only increases eavesdropper's uncertainty about the secret message $\mathbf{u}$, but does not affect Bob.

Since $\mathbf{V}$ is unitary, the total transmission power $||\mathbf{x}||^2$ is

$$||\mathbf{x}||^2 = \left[\begin{array}{c} \mathbf{u} \\ \mathbf{v} \end{array}\right]^H \mathbf{V}^H\mathbf{V}\left[\begin{array}{c} \mathbf{u} \\ \mathbf{v} \end{array}\right] = ||\mathbf{u}||^2 + ||\mathbf{v}||^2. \tag{5}$$

We set the average transmit power constraints P_{u} and P_{v}:

$$\begin{aligned} P_{\mathrm{u}} &= \mathrm{E}\left(||\mathbf{u}||^2\right) = \sigma_{\mathrm{u}}^2 N_{\mathrm{B}}, \\ P_{\mathrm{v}} &= \mathrm{E}\left(||\mathbf{v}||^2\right) = \sigma_{\mathrm{v}}^2 (N_{\mathrm{A}} - N_{\mathrm{B}}). \end{aligned} \tag{6}$$

We define Bob's and Eve's SNRs as

$$\begin{aligned} \mathrm{SNR}_{\mathrm{B}} &\triangleq \sigma_{\mathrm{u}}^2/\sigma_{\mathrm{B}}^2, \\ \mathrm{SNR}_{\mathrm{E}} &\triangleq \sigma_{\mathrm{u}}^2/\sigma_{\mathrm{E}}^2. \end{aligned} \tag{7}$$

Throughout the paper, we assume the worst-case scenario for Alice and Bob described in [6]:

- Alice only knows $\mathbf{H}$.
- Eve knows $\mathbf{H}$, $\mathbf{G}$, $\mathbf{Z}$ and $\mathbf{V}_1$.

Different from [6], we assume no upper bound on N_{E}.

To simplify our analysis, we define three system parameters:

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

If $\gamma > 1$, we say Eve has a *degraded channel*. Note that $\mathrm{SNR}_{\mathrm{B}} = \alpha\gamma$. For convenience, we fix $\sigma_{\mathrm{B}}^2 = 1$, thus $P_{\mathrm{u}} = \alpha\gamma N_{\mathrm{B}}$.

To evaluate the asymptotic secrecy rate, we assume

- $N_{\mathrm{A}}/N_{\mathrm{E}} \to \beta_1$
- $N_{\mathrm{A}}/N_{\mathrm{B}} \to \beta_2$
- $N_{\mathrm{B}}/N_{\mathrm{E}} \to \beta_3$

III. Non-zero Secrecy Capacity

In this section, we revisit the problem of guaranteeing non-zero instantaneous and average secrecy capacities using artificial noise. To present our result, we first define some useful functions.

A. Definitions

We recall the definition of instantaneous secrecy capacity:

$$C_{\mathrm{S}} \triangleq \max_{p(\hat{\mathbf{u}})} \left\{ I(\hat{\mathbf{u}};\mathbf{z}) - I(\hat{\mathbf{u}};\mathbf{y}) \right\}, \tag{8}$$

which is a special case of the definition in [10]. The maximum is taken over all possible input distributions $p\left(\hat{\mathbf{u}}\right)$. Note that C_{S} is a random variable depending on Gaussian random matrices $\mathbf{H}$ and $\mathbf{G}$, which are embedded in $\mathbf{z}$ and $\mathbf{y}$.

We further define average secrecy capacity, as in [6]

$$\bar{C}_{\mathrm{S}} \triangleq \max_{p(\hat{\mathbf{u}})} \left\{ I(\hat{\mathbf{u}};\mathbf{z}|\mathbf{H}) - I(\hat{\mathbf{u}};\mathbf{y}|\mathbf{H},\mathbf{G}) \right\}. \tag{9}$$

where $I\left(X;Y|Z\right) \triangleq \mathrm{E}_Z\left[I\left(X;Y\right)|Z\right]$ [11].

Since closed form expressions for C_{S} and $\bar{C}_{\mathrm{S}}$ are not always available (except for Theorem 1), we often resort to lower bounds given by

$$C_{\mathrm{S}} \geq I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\mathbf{y}) \triangleq R_{\mathrm{S}}, \tag{10}$$

$$\bar{C}_{\mathrm{S}} \geq I(\mathbf{u};\mathbf{z}|\mathbf{H}) - I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G}) \triangleq \bar{R}_{\mathrm{S}}, \tag{11}$$

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

We then define the following function, as in [12]

$$\begin{aligned} \Theta(m,n,x) \triangleq e^{-1/x} \sum_{k=0}^{m-1} \sum_{l=0}^{k} \sum_{i=0}^{2l} \Bigg\{ \frac{(-1)^i (2l)!(n-m+i)!}{2^{2k-i} l! i! (n-m+l)!} \\ \cdot \left(\begin{array}{c} 2(k-l) \\ k-l \end{array}\right) \left(\begin{array}{c} 2(l+n-m) \\ 2l-i \end{array}\right) \sum_{j=0}^{n-m+i} x^{-j}\Gamma(-j, 1/x) \Bigg\}, \end{aligned} \tag{12}$$

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

Finally, we define

$$\begin{aligned} N_{\max} &= \max\left\{N_{\mathrm{E}},\, N_{\mathrm{A}} - N_{\mathrm{B}}\right\}, \\ N_{\min} &= \min\left\{N_{\mathrm{E}},\, N_{\mathrm{A}} - N_{\mathrm{B}}\right\}. \end{aligned} \tag{13}$$

B. Non-zero Average Secrecy Capacity

We provide some analytical insights relating $\bar{R}_{\mathrm{S}}$ and $\bar{C}_{\mathrm{S}}$ to N_{A}, N_{B}, N_{E}, α, β, and γ. We first derive an upper bound on $I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G})$.

Lemma 1:

$$\begin{aligned} I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G}) &\leq N_{\mathrm{E}}\log(1+\alpha N_{\mathrm{B}}) - \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ &\quad + \Theta(N_{\min}, N_{\max}, \alpha\beta/(1+\alpha N_{\mathrm{B}})) \\ &= (N_{\mathrm{E}} - N_{\min})\log\alpha N_{\mathrm{B}} + O\left(\frac{1}{\alpha}\right) + O\left(\frac{1}{\beta}\right). \end{aligned}$$

Proof: See Appendix A. ■

Lemma 1 reveals the following relation between $\bar{C}_{\text{S}}$ and $\bar{R}_{\text{S}}$.

Theorem 1: If $N_{\text{E}} \leq N_{\text{A}} - N_{\text{B}}$, as $\alpha,\ \beta \to \infty$, then

$$\bar{C}_{\text{S}} = \bar{R}_{\text{S}}. \tag{14}$$

Proof: See Appendix B. ■

In Theorem 1, we demonstrated the achievability of the average secrecy capacity of the AN scheme using Gaussian input alphabets under the above condition. This result was not given in [6], where only $\bar{R}_{\text{S}} > 0$ was observed by simulation.

The assumption that N_{E} is bounded can be un-natural in practice. In the following theorem, we derive a lower bound on the achievable rate $\bar{R}_{\text{S}}$, without any limitation on N_{E}.

Theorem 2:

$$\begin{aligned}\bar{R}_{\text{S}} &\geq \Theta(N_{\text{B}}, N_{\text{A}}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ &- N_{\text{E}} \log(1 + \alpha N_{\text{B}}) - \Theta(N_{\min}, N_{\max}, \alpha\beta/(1 + \alpha N_{\text{B}})) \triangleq \bar{R}_{\text{LB}},\end{aligned} \tag{15}$$

Proof: See Appendix C. ■

To gain further intuition, we provide the following corollary, giving a sufficient condition for positive average secrecy rate as $N_{\text{B}} \to \infty$.

Corollary 1: If $\beta_2 \to 1$, $\lim\limits_{N_{\text{B}}\to\infty} \bar{R}_{\text{S}}/N_{\text{B}} > 0$ when

$$N_{\text{E}} < N_{\text{A}} + \frac{N_{\text{B}}\left(\log\gamma - 1 + \Upsilon(P_{\text{u}})\right)}{\log P_{\text{u}} - \log\gamma}, \tag{16}$$

where

$$\Upsilon(P_{\text{u}}) = \frac{\sqrt{1+4P_{\text{u}}} - 1}{2P_{\text{u}}} + 2\tanh^{-1}\frac{1}{\sqrt{1+4P_{\text{u}}}}. \tag{17}$$

Proof: See Appendix D. ■

Corollary 1 gives an example of application of Theorem 2, and shows that positive secrecy capacity is in fact achievable for any N_{E}, thus removes the restriction $N_{\text{E}} < N_{\text{A}}$ in [6], since the second term in (16) can be increased by γ.

Example 1: Fig. 1 compares the values of $\bar{R}_{\text{S}}$ and $\bar{R}_{\text{LB}}$ in (15) as functions of N_{E} with $\alpha = \beta = 3$ dB, $\gamma = 6$ dB, $N_{\text{B}} = 3$ and $N_{\text{A}} = 4$. In this case, (16) reduces to $N_{\text{E}} < 6$. We observe that $\bar{R}_{\text{LB}} > 0$ when $N_{\text{E}} < 6$. This example shows the usability of Corollary 1 for finite numbers of antennas. Although the gap between $\bar{R}_{\text{S}}$ and $\bar{R}_{\text{LB}}$ increases with increasing N_{E}, the curve of $\bar{R}_{\text{LB}}$ can still confirm the fact that positive average secrecy rate is available even when $N_{\text{E}} \geq N_{\text{A}}$.

C. Non-zero Instantaneous Secrecy Capacity

We now analyze the instantaneous secrecy rate R_{S} as a random variable depending on the random matrices $\mathbf{G}$ and $\mathbf{H}$. An interesting case that leads to a closed form bound can be found when $\beta = 1$ (or 0 dB).

Theorem 3: If $\beta = 1$, as N_{B}, $N_{\text{A}} - N_{\text{B}}$ and $N_{\text{E}} \to \infty$ with fixed β_1, β_2 and β_3,

$$\frac{R_{\text{S}}}{N_{\text{B}}} \overset{a.s.}{\to} \Phi(P_{\text{u}},\ \beta_2) - \frac{\Phi(P_{\text{u}}/(\gamma\beta_3),\ \beta_1)}{\beta_3} + \frac{\Phi(P_{\text{u}}/(\gamma\beta_3),\ \beta_1 - \beta_3)}{\beta_3},$$

where

$$\begin{aligned}\Phi(x,\ y) \quad &\triangleq \quad y\log\left(1 + x - \frac{1}{4}\mathcal{F}(x,y)\right) - \frac{\mathcal{F}(x,y)}{4x} \\ &+ \log\left(1 + xy - \frac{1}{4}\mathcal{F}(x,y)\right),\end{aligned} \tag{18}$$

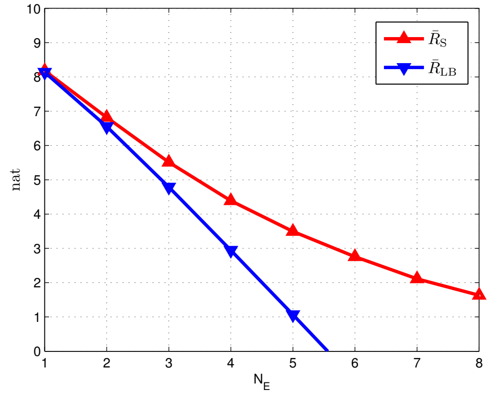

Fig. 1. $\bar{R}_{\text{S}}$ and $\bar{R}_{\text{LB}}$ vs. N_{E} with $\alpha = \beta = 3$ dB, $\gamma = 6$ dB, $N_{\text{B}} = 3$ and $N_{\text{A}} = 4$.

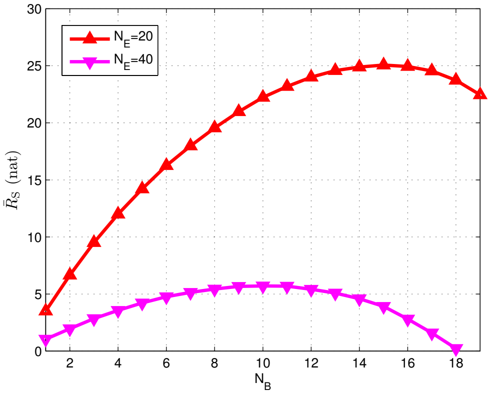

Fig. 2. $\bar{R}_{\text{S}}$ vs. N_{B} and N_{E} with $N_{\text{A}} = 20$, $\alpha = 10$ dB, $\beta = 0$ dB, and $\gamma = 3$.

$$\mathcal{F}(x,y) \triangleq \left(\sqrt{x\left(1+\sqrt{y}\right)^2 + 1} - \sqrt{x\left(1-\sqrt{y}\right)^2 + 1}\right)^2. \tag{19}$$

Proof: Using [13, Eq. 1.14], the proof is straightforward. ■

Corollary 2: Under the same assumptions of Theorem 3, if $N_{\text{E}} \geq N_{\text{A}}$ (i.e., $\beta_1 \leq 1$), as $P_{\text{u}} \to \infty$, the maximum $\bar{R}_{\text{S}}$ is achieved when

$$N_{\text{B}} = \min\left\{\max\left\{\left\lceil N_{\text{A}} - \frac{N_{\text{E}}}{1+\gamma}\right\rfloor, 1\right\}, N_{\text{A}} - 1\right\}. \tag{20}$$

Proof: Available in the journal version. ■

Corollary 2 reveals the relationship between the maximum $\bar{R}_{\text{S}}$, N_{B} and γ for given N_{A} and N_{E}: the larger the channel degradation γ is, the smaller the null space size $N_{\text{A}} - N_{\text{B}}$ is required.

Example 2: Fig. 2 shows the variation of $\bar{R}_{\text{S}}$ by simulation, as a function of N_{B} and N_{E}, with $N_{\text{A}} = 20$, $\alpha = 10$ dB, $\beta = 0$ dB, and $\gamma = 3$. We observe that for $N_{\text{E}} = 20$ and 40, $\bar{R}_{\text{S}}$ is maximized when $N_{\text{B}} = \left\lceil N_{\text{A}} - \frac{N_{\text{E}}}{1+\gamma}\right\rfloor = 15$ and 10. Once N_{B} exceeds the optimum value, $\bar{R}_{\text{S}}$ starts to decrease. Thus, Corollary 2 is very accurate even for a finite system model.

The results for general β and β_1 will be reported in the journal version.

IV. Attack on AN

In the previous section, we took the side of Alice and Bob, and we established the conditions that ensure non-zero secrecy rate for given α and N_{E}. This provided a design strategy of defence against eavesdropping. In this section, we play the part of Eve. We want to estimate how many antennas Eve needs to drive the instantaneous secrecy rate R_{S} to zero, assuming the worst case scenario that N_{A}, N_{B}, α, β, and γ are known to Eve. We define Eve's activity as the attack on the AN scheme.

In summary, attack and defence are related to upper and lower bounds on the secrecy rate, respectively.

Let $\hat{\mathbf{y}}$ be a processed form of $\mathbf{y}$. Thanks to the *data processing inequality*, we have

$$I(\mathbf{u};\mathbf{y}) \geq I(\mathbf{u};\hat{\mathbf{y}}). \tag{21}$$

Let $\hat{R}_{\mathrm{S}} \triangleq I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\hat{\mathbf{y}})$. From (10) and (21), we obtain

$$R_{\mathrm{S}} \leq \hat{R}_{\mathrm{S}}. \tag{22}$$

In other words, data processing cannot decrease R_{S}, but may be used to obtain an easily computable upper bound. We use zero-forcing (ZF) processing, since it can remove the artificial noise and hence the dependency on parameter β.

In particular, if $N_{\mathrm{E}} \geq N_{\mathrm{A}}$, $\mathbf{G}$ has a left inverse, denoted by $\mathbf{G}^{\dagger}$, then the interference term $\mathbf{GZv}$ can be removed by multiplying $\mathbf{y}$ by $\mathbf{W} = \mathbf{HG}^{\dagger}$, i.e.,

$$\mathbf{Wy} = \mathbf{HV}_1\mathbf{u} + \mathbf{Wn}_{\mathrm{E}} \triangleq \hat{\mathbf{y}}_{\mathrm{ZF}}. \tag{23}$$

Note that if $N_{\mathrm{E}} < N_{\mathrm{A}}$, ZF processing is not applicable.

Theorem 4: Let $\hat{R}_{\mathrm{S,\ ZF}} \triangleq I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\hat{\mathbf{y}}_{\mathrm{ZF}})$. As N_{A}, N_{B} and $N_{\mathrm{E}} \to \infty$ with fixed β_1, β_2 and β_3,

$$\frac{\hat{R}_{\mathrm{S,\ ZF}}}{N_{\mathrm{B}}} < \Phi\left(P_{\mathrm{u}},\ \beta_2\right) - \log\frac{P_{\mathrm{u}}(1-\sqrt{\beta_1})^2}{\gamma\beta_3}, \tag{24}$$

almost surely, where $\Phi\left(x,\ y\right)$ is given in Theorem 3.

Proof: See Appendix E. ■

From (22), for large scale system models, we have $R_{\mathrm{S}}/N_{\mathrm{B}} < \hat{R}_{\mathrm{S,\ ZF}}/N_{\mathrm{B}}$. By setting $\hat{R}_{\mathrm{S,\ ZF}}/N_{\mathrm{B}}$ equal to zero, $R_{\mathrm{S}}/N_{\mathrm{B}}$ is forced to be zero as stated in the following corollary.

Corollary 3: Under the same assumptions of Theorem 4, $R_{\mathrm{S}}/N_{\mathrm{B}} \overset{a.s.}{\to} 0$, if

$$N_{\mathrm{E}} = \left\lceil \left(\sqrt{\frac{\exp\left\{\Phi\left(P_{\mathrm{u}},\ \beta_2\right)\right\}}{\alpha}} + \sqrt{N_{\mathrm{A}}}\right)^2 \right\rceil. \tag{25}$$

Proof: The proof is straightforward. ■

Corollary 3 provides Eve an analytical expression for choosing N_{E} to attack the AN scheme.

V. Conclusions

This paper characterizes the trade-off between the multiple antennas and the secrecy rate achieved by the artificial noise scheme. By taking all the system parameters into account, we developed explicit lower and upper bounds on the secrecy rate with Gaussian input alphabets. We have shown that, the lower bound tells Alice how many antennas she needs to ensure non-zero secrecy rate, while the upper bound provides the minimum number of antennas for Eve to drive the secrecy rate to zero. Based on our analysis, we describe the antenna number race between Alice and Eve as a defence versus attack battle over physical layer security.

Appendix

A. Proof of Lemma 1

Since all entries in $\mathbf{H}$ and $\mathbf{G}$ 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 $I(\mathbf{u};\mathbf{y}|\mathbf{G})$ given $\mathbf{H}$, then compute $\mathrm{E}_{\mathbf{H}}\left[I(\mathbf{u};\mathbf{y}|\mathbf{G})|\mathbf{H}\right]$. The advantage is that for given $\mathbf{H}$, $\mathbf{V} = [\mathbf{V}_1,\ \mathbf{Z}]$ is a fixed unitary matrix. Then, using [14, Th. 1], $\mathbf{GV}_1$ and $\mathbf{GZ}$ are mutually independent complex Gaussian random matrices with i.i.d. entries $\sim \mathcal{N}_{\mathbb{C}}(0,\ 1)$.

Let $\mathbf{G}_1 = \mathbf{GV}_1$, $\mathbf{G}_2 = \mathbf{GZ}$, $\mathbf{W}_1 = \mathbf{G}_1\mathbf{G}_1^H$ and $\mathbf{W}_2 = \mathbf{G}_2\mathbf{G}_2^H$. According to [11], we have

$$\begin{aligned}
&I(\mathbf{u};\mathbf{y}|\mathbf{G}) \\
&= \mathrm{E}_{\mathbf{G}_1,\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\mathrm{E}}}\sigma_{\mathrm{E}}^2 + \sigma_{\mathrm{u}}^2\mathbf{W}_1 + \sigma_{\mathrm{v}}^2\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}\sigma_{\mathrm{E}}^2 + \sigma_{\mathrm{v}}^2\mathbf{W}_2\right|}\right) \\
&\overset{a}{\leq} \mathrm{E}_{\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\mathrm{E}}}\sigma_{\mathrm{E}}^2 + \sigma_{\mathrm{u}}^2\mathrm{E}_{\mathbf{G}_1}\left(\mathbf{W}_1\right) + \sigma_{\mathrm{v}}^2\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}\sigma_{\mathrm{E}}^2 + \sigma_{\mathrm{v}}^2\mathbf{W}_2\right|}\right) \\
&= \mathrm{E}_{\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{\sigma_{\mathrm{v}}^2}{\sigma_{\mathrm{E}}^2 + N_{\mathrm{B}}\sigma_{\mathrm{u}}^2}\mathbf{W}_2\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{\sigma_{\mathrm{v}}^2}{\sigma_{\mathrm{E}}^2}\mathbf{W}_2\right|}\right) + N_{\mathrm{E}}\log\frac{\sigma_{\mathrm{E}}^2 + N_{\mathrm{B}}\sigma_{\mathrm{u}}^2}{\sigma_{\mathrm{E}}^2},
\end{aligned} \tag{26}$$

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

Note that $\left|\mathbf{I} + \mathbf{G}_2\mathbf{G}_2^H\right| = \left|\mathbf{I} + \mathbf{G}_2^H\mathbf{G}_2\right|$ and define

$$\mathbf{W} = \begin{cases} \mathbf{G}_2\mathbf{G}_2^H & \text{if } N_{\mathrm{E}} \leq N_{\mathrm{A}} - N_{\mathrm{B}} \\ \mathbf{G}_2^H\mathbf{G}_2 & \text{if } N_{\mathrm{E}} > N_{\mathrm{A}} - N_{\mathrm{B}} \end{cases}$$

Then $\mathbf{W}$ is a Wishart matrix $\sim W_{N_{\min}}(N_{\max}, \mathbf{I}_{N_{\min}})$, where $N_{\min}$ and $N_{\max}$ are given in (13).

Recalling the definitions of α and β in Sec.II. Based on above analysis and [12, Th. 1], the first term of (26) can be written as

$$\begin{aligned}
&\mathrm{E}_{\mathbf{G}_2}\left(\log\frac{\left|\mathbf{I}_{N_{\min}} + \frac{\alpha\beta}{1+\alpha N_{\mathrm{B}}}\mathbf{W}\right|}{\left|\mathbf{I}_{N_{\min}} + \alpha\beta\mathbf{W}\right|}\right) \\
&= \Theta(N_{\min}, N_{\max}, \alpha\beta/(1+\alpha N_{\mathrm{B}})) - \Theta(N_{\min}, N_{\max}, \alpha\beta)
\end{aligned} \tag{27}$$

where $\Theta(x,y,z)$ is given in (12).

From (26) and (27), we have

$$\begin{aligned}
I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G}) &= \mathrm{E}_{\mathbf{H}}\left[I(\mathbf{u};\mathbf{y}|\mathbf{G})|\mathbf{H}\right] \\
&\leq N_{\mathrm{E}}\log(1+\alpha N_{\mathrm{B}}) - \Theta(N_{\min}, N_{\max}, \alpha\beta) \\
&\quad +\Theta(N_{\min}, N_{\max}, \alpha\beta/(1+\alpha N_{\mathrm{B}})) \\
&= (N_{\mathrm{E}} - N_{\min})\log\alpha N_{\mathrm{B}} + O\left(\frac{1}{\alpha}\right) + O\left(\frac{1}{\beta}\right).
\end{aligned}$$

■

B. Proof of Theorem 1

If $N_{\mathrm{E}} \leq N_{\mathrm{A}} - N_{\mathrm{B}}$, from Lemma 1 and (10), as α and $\beta \to \infty$,

$$\bar{R}_{\mathrm{S}} = I(\mathbf{u};\mathbf{z}|\mathbf{H}). \tag{28}$$

Moreover, we have

$$\bar{C}_{\rm S} \leq \max_{p(\hat{\mathbf{u}})} \{I(\hat{\mathbf{u}};\mathbf{z}|\mathbf{H})\} = I(\mathbf{u};\mathbf{z}|\mathbf{H}). \tag{29}$$

The last equation holds since the input $\mathbf{u}$ is a circularly symmetric complex Gaussian random vector [11, Th. 1].

Based on (28) and (29), as α and $\beta \to \infty$, we have

$$\bar{R}_{\rm S} = \bar{C}_{\rm S}.$$

■

C. Proof of Theorem 2

Since $(\mathbf{H}\mathbf{V}_1)(\mathbf{H}\mathbf{V}_1)^H = \mathbf{H}\mathbf{H}^H$, using [11, Th. 2] and [12, Th. 1], we have

$$I(\mathbf{u};\mathbf{z}|\mathbf{H}) = \mathrm{E}_{\mathbf{H}}\left(\log\left|\mathbf{I}_{N_{\rm B}} + \alpha\gamma\mathbf{H}\mathbf{H}^H\right|\right) = \Theta(N_{\rm B}, N_{\rm A}, \alpha\gamma). \tag{30}$$

where $\Theta(x, y, z)$ is given in (12).

From Lemma 1 and (30), we obtain

$$\begin{aligned} \bar{R}_{\rm S} &\geq \Theta(N_{\rm B}, N_{\rm A}, \alpha\gamma) + \Theta(N_{\min}, N_{\max}, \alpha\beta) \\ &- N_{\rm E}\log(1+\alpha N_{\rm B}) - \Theta(N_{\min}, N_{\max}, \alpha\beta/(1+\alpha N_{\rm B})), \end{aligned} \tag{31}$$

where $N_{\min}$ and $N_{\max}$ are given in (13). ■

D. Proof of Corollary 1

If $\beta_2 \to 1$, according to [11], we have

$$\lim_{N_{\rm B}\to\infty} \frac{I(\mathbf{u};\mathbf{z}|\mathbf{H})}{N_{\rm B}} = \log P_{\rm u} - 1 + \Upsilon(P_{\rm u}), \tag{32}$$

where $\Upsilon(P_{\rm u})$ is given in (17).

From Lemma 1, we have

$$\lim_{N_{\rm B}\to\infty} \frac{I(\mathbf{u};\mathbf{y}|\mathbf{H},\mathbf{G})}{N_{\rm B}} \leq \lim_{N_{\rm B}\to\infty} \frac{N_{\rm E}-N_{\min}}{N_{\rm B}} \log\frac{P_{\rm u}}{\gamma}. \tag{33}$$

Moreover, if $\beta_2 \to 1$, we have

$$N_{\min} = N_{\rm A} - N_{\rm B}. \tag{34}$$

Based on (32), (33) and (34), $\lim\limits_{N_{\rm B}\to\infty} \bar{R}_{\rm S}/N_{\rm B} > 0$ if

$$N_{\rm E} < N_{\rm A} + \frac{N_{\rm B}\left(\log\gamma - 1 + \Upsilon(P_{\rm u})\right)}{\log P_{\rm u} - \log\gamma}. \tag{35}$$

■

E. Proof of Theorem 4

We recall that

$$\hat{R}_{\text{S, ZF}} = I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\hat{\mathbf{y}}_{\rm ZF}), \tag{36}$$

According to [13, Eq. 1.14], we have

$$\lim_{N_{\rm B}\to\infty} \frac{I(\mathbf{u};\mathbf{z})}{N_{\rm B}} \overset{a.s.}{\to} \Phi\left(P_{\rm u},\, \beta_2\right), \tag{37}$$

where $\Phi(x, y)$ is given in (18).

Moreover, since $\mathbf{W} = \mathbf{H}\mathbf{G}^{\dagger}$, we have

$$\begin{aligned} &I(\mathbf{u};\hat{\mathbf{y}}_{\rm ZF}) \\ &= \log\frac{\left|\sigma_{\rm u}^2(\mathbf{H}\mathbf{V}_1)(\mathbf{H}\mathbf{V}_1)^H + \sigma_{\rm E}^2\mathbf{W}\mathbf{W}^H\right|}{\left|\sigma_{\rm E}^2\mathbf{W}\mathbf{W}^H\right|} \\ &= \log\frac{\left|\mathbf{I}_{N_{\rm B}}\sigma_{\rm u}^2 + \sigma_{\rm E}^2\mathbf{V}_1^H\left(\mathbf{G}^H\mathbf{G}\right)^{-1}\mathbf{V}_1\right|}{\left|\sigma_{\rm E}^2\mathbf{V}_1^H\left(\mathbf{G}^H\mathbf{G}\right)^{-1}\mathbf{V}_1\right|} \\ &= \log\left(\prod_{i=1}^{N_{\rm B}}(1+\alpha/\lambda_i)\right), \end{aligned} \tag{38}$$

where λ_i, $1 \leq i \leq N_{\rm B}$, represent the eigenvalues of $\mathbf{V}_1^H\left(\mathbf{G}^H\mathbf{G}\right)^{-1}\mathbf{V}_1$.

From (38), we have

$$I(\mathbf{u};\hat{\mathbf{y}}_{\rm ZF}) > \log\left(\prod_{i=1}^{N_{\rm B}}\alpha/\lambda_i\right). \tag{39}$$

Let $\delta_{\min}$ be the smallest eigenvalue of $\frac{1}{N_{\rm E}}\mathbf{G}^H\mathbf{G}$. Then $1/\delta_{\min}$ is the largest eigenvalue of $\left(\frac{1}{N_{\rm E}}\mathbf{G}^H\mathbf{G}\right)^{-1}$. According to [15, Th. 8, pp. 69], we have

$$\prod_{i=1}^{N_{\rm B}}\lambda_i N_{\rm E} < \delta_{\min}^{-N_{\rm B}}. \tag{40}$$

Based on (39) and (40), we have

$$I(\mathbf{u};\hat{\mathbf{y}}_{\rm ZF}) > N_{\rm B}\log\alpha N_{\rm E}\delta_{\min}. \tag{41}$$

As $N_{\rm A}$ and $N_{\rm E} \to \infty$, according to Marčenko-Pastur law, $\delta_{\min} \overset{a.s.}{\to} (1-\sqrt{\beta_1})^2$ [13, Eq. 1.10], (41) reduces to

$$\frac{I(\mathbf{u};\hat{\mathbf{y}}_{\rm ZF})}{N_{\rm B}} > \log\frac{P_{\rm u}(1-\sqrt{\beta_1})^2}{\gamma\beta_3} \tag{42}$$

almost surely.

By substituting (37) and (42) into (36), as $N_{\rm A}$, $N_{\rm B}$ and $N_{\rm E} \to \infty$ with fixed β_1, β_2 and β_3,

$$\frac{\hat{R}_{\text{S, ZF}}}{N_{\rm B}} < \Phi\left(P_{\rm u},\, \beta_2\right) - \log\frac{P_{\rm u}(1-\sqrt{\beta_1})^2}{\gamma\beta_3},$$

almost surely. ■

References

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

[2] C. E. Shannon, "Communication theory of secrecy systems," *Confidential report*, 1946.

[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] 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.

[5] 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.

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

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

[8] ——, "Secure transmission with multiple antennas Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[9] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483–1486, 2013.

[10] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

[12] 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.

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

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

[15] H. Lütkepohl, *Handbook of matrices*. John Wiley and Sons, 1996.