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., \( N_E < N_A \). Several channel models have been considered to generalize the idea of AN. When the number of Bob’s antennas \( N_B = 1 \), [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 \( N_E \leq N_A - N_B \).
- 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 \( \mathbf{B}^{-1} \), respectively. \( |\mathbf{B}| \) denotes the determinant of \( \mathbf{B} \). Let \( \{X_n, X\} \) be defined on the same probability space. We write \( X_n \xrightarrow{a.s.} X \) 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 \( 0_{m \times n} \). We write \( \approx \) for equality in definition. A circularly symmetric complex Gaussian random variable \( x \) with variance \( \sigma^2 \) is defined as \( x \sim \mathcal{C}(0, \sigma^2) \).

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 \( \lim_{x \to \infty} \frac{|f(x)|}{|g(x)|} = 0 \). We use the standard asymptotic notation \( f(x) = \Omega(g(x)) \) when \( \lim_{x \to \infty} \frac{|f(x)|}{|g(x)|} = \infty \). [\( x \)] 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.
where $u \sim V = Z$ represent the channels from Alice to Bob and Alice to Eve. $H$ and $G$ are assumed to be independent (i.e., all terminals are not co-located) and have i.i.d. entries $\sim \mathcal{N}_C(0, 1)$. 

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

$$V = [V_1, Z],$$

where $V_1$ represents the matrix with the first $N_B$ columns of $V$. Using the AN scheme [6], Alice transmits

$$x = V_1 u + Zv = V \begin{bmatrix} u \\ v \end{bmatrix},$$

where $u$ is the secret data vector and $v$ is the artificial noise. Gaussian input alphabets are assumed, i.e., both $u \in \mathbb{C}^{N_A \times 1}$ and $v \in \mathbb{C}^{(N_A - N_B) \times 1}$ are mutually independent Gaussian vectors with i.i.d. entries $\sim \mathcal{N}_C(0, \sigma_u^2)$ and $\mathcal{N}_C(0, \sigma_v^2)$, respectively.

The signals received by Bob and Eve are given by

$$z = HV_1 u + HZv + n_B = HV_1 u + n_B,$$

$$y = GV_1 u + GZv + n_E,$$

where $n_B$ and $n_E$ are additive white Gaussian noise vectors at Bob and Eve, respectively, with i.i.d. entries $\sim \mathcal{N}_C(0, \sigma_B^2)$ and $\mathcal{N}_C(0, \sigma_E^2)$.

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

Since $V$ is unitary, the total transmission power $||x||^2$ is

$$||x||^2 = \begin{bmatrix} u \\ v \end{bmatrix}^H V^H V \begin{bmatrix} u \\ v \end{bmatrix} = ||u||^2 + ||v||^2.$$

We set the average transmit power constraints $P_u$ and $P_v$:

$$P_u = \mathbb{E} \left( ||u||^2 \right) = \sigma_u^2 N_B,$$

$$P_v = \mathbb{E} \left( ||v||^2 \right) = \sigma_v^2 (N_A - N_B).$$

We define Bob’s and Eve’s SNRs as

$$\text{SNR}_B \triangleq \frac{\sigma_u^2}{\sigma_B^2},$$

$$\text{SNR}_E \triangleq \frac{\sigma_v^2}{\sigma_E^2}.$$

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

- Alice only knows $H$.
- Eve knows $H, G, Z$ and $V_1$.

Different from [6], we assume no upper bound on $N_E$.

To simplify our analysis, we define three system parameters:

- $\alpha \triangleq \frac{\sigma_u^2}{\sigma_E^2}$ (SNR$_E$)
- $\beta \triangleq \frac{\sigma_v^2}{\sigma_B^2}$ (AN power fraction)
- $\gamma \triangleq \frac{\sigma_v^2}{\sigma_E^2}$ (Eve-to-Bob noise-power ratio)

If $\gamma > 1$, we say Eve has a degraded channel. Note that $\text{SNR}_B = \alpha \gamma$. For convenience, we fix $\sigma_E^2 = 1$, thus $P_v = \sigma_B^2 N_B$.

To evaluate the asymptotic secrecy rate, we assume

- $N_A/N_E \rightarrow \beta_1$
- $N_A/N_B \rightarrow \beta_2$
- $N_B/N_E \rightarrow \beta_3$

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:

$$C_S \triangleq \max_{\hat{p}(u)} \left\{ I(\hat{u}; z) - I(\hat{u}; y) \right\},$$

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

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

$$\hat{C}_S \triangleq \max_{\hat{p}(u)} \left\{ I(\hat{u}; z|H) - I(\hat{u}; y|H, G) \right\},$$

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

Since closed form expressions for $C_S$ and $\hat{C}_S$ are not always available (except for Theorem 1), we often resort to lower bounds given by

$$C_S \geq I(u; z) - I(u; y) \triangleq R_S,$$

$$\hat{C}_S \geq I(u; z|H) - I(u; y|H, G) \triangleq R_S,$$

assuming Gaussian input alphabets, i.e., $v$ and $u$ are mutually independent Gaussian vector with i.i.d. entries $\mathcal{N}_C(0, \sigma_v^2)$ and $\mathcal{N}_C(0, \sigma_u^2)$, respectively.

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

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

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.

Finally, we define

$$N_{\max} \triangleq \max \left\{ N_E, N_A - N_B \right\},$$

$$N_{\min} \triangleq \min \left\{ N_E, N_A - N_B \right\}.$$

B. Non-zero Average Secrecy Capacity

We provide some analytical insights relating $R_S$ and $\hat{C}_S$ to $N_A$, $N_B$, $N_E$, $\alpha$, $\beta$, and $\gamma$. We first derive an upper bound on $I(u; y|H, G)$.

Lemma 1:

$$I(u; y|H, G) \leq N_E \log(1 + \alpha N_B) - \Theta(N_{\min}, N_{\max}, \alpha \beta) + \Theta(N_{\min}, N_{\max}, \alpha \beta/(1 + \alpha N_B))$$

$$= (N_E - N_{\min}) \log \alpha N_B + O \left( \frac{1}{\alpha} \right) + O \left( \frac{1}{N_B} \right).$$

Proof: See Appendix A.
Lemma 1 reveals the following relation between $C_S$ and $R_S$.

**Theorem 1:** If $N_E \leq N_A - N_B$, as $\alpha, \beta \to \infty$, then

$$C_S = R_S.$$  \hfill (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 $R_S > 0$ 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 $R_S$, without any limitation on $N_E$.

**Theorem 2:**

$$R_S \geq \Theta(N_B, N_A, \alpha \gamma) + \Theta(N_{\text{min}}, N_{\text{max}}, \alpha \beta) - N_E \log(1 + \alpha N_B) - \Theta(N_{\text{min}}, N_{\text{max}}, \alpha \beta/(1 + \alpha N_B)) \triangleq \bar{R}_{\text{LB}},$$  \hfill (15)

**Proof:** See Appendix C.

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

**Corollary 1:** If $\beta_2 \to 1$, $\lim_{N_B \to \infty} \bar{R}_S/N_B > 0$ when

$$N_E < N_A + \frac{N_B (\log \gamma - 1 + \Theta(P_u))}{\log P_u - \log \gamma},$$  \hfill (16)

where

$$\Theta(P_u) = \sqrt{\frac{1 + 4P_u}{2P_u}} - 1 + 2 \tanh^{-1} \left( \frac{1}{\sqrt{1 + 4P_u}} \right).$$  \hfill (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 $N_E < N_A$ in [6], since the second term in (16) can be increased by $\gamma$.

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

**C. Non-zero Instantaneous Secrecy Capacity**

We now analyze the instantaneous secrecy rate $R_S$ as a random variable depending on the random matrices $G$ and $H$. 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 $N_B, N_A - N_B$ and $N_E \to \infty$ with fixed $\beta_1, \beta_2$ and $\beta_3$, $R_S \to \Phi(P_u, \beta_2) - \Phi(P_u/(\gamma \beta_3), \beta_1) + \Phi(P_u/(\gamma \beta_3), \beta_1 - \beta_3)$, where

$$\Phi(x, y) \triangleq y \log \left( 1 + x - \frac{1}{4} \frac{\mathcal{F}(x, y)}{x} \right) - \frac{\mathcal{F}(x, y)}{4x} + \log \left( 1 + xy - \frac{1}{4} \frac{\mathcal{F}(x, y)}{x} \right),$$  \hfill (18)

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

**Corollary 2:** Under the same assumptions of Theorem 3, if $N_E \geq N_A$ (i.e., $\beta_1 \leq 1$), as $P_u \to \infty$, the maximum $\bar{R}_S$ is achieved when

$$N_B = \min \left\{ \max \left\{ \left[ N_A - \frac{N_E}{1 + \gamma} \right], 1 \right\}, N_A - 1 \right\}.$$  \hfill (20)

**Proof:** Available in the journal version.

Corollary 2 reveals the relationship between the maximum $\bar{R}_S$, $N_A$ and $\gamma$ for given $N_A$ and $N_E$: the larger the channel degradation $\gamma$ is, the smaller the null space size $N_A - N_B$ is required.

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

The results for general $\beta$ and $\beta_1$ 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 $\alpha$ 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 $N_A$, $N_B$, $\alpha$, $\beta$, and $\gamma$ 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 $\hat{y}$ be a processed form of $y$. Thanks to the data processing inequality, we have

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

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

$$R_S \leq \hat{R}_S. \quad (22)$$

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 $\beta$.

In particular, if $N_E \geq N_A$, $G$ has a left inverse, denoted by $G^1$, then the interference term $GZv$ can be removed by multiplying $y$ by $W = HG^1$, i.e.,

$$W y = H V_1 u + W_{NE} \triangleq S_{ZF}. \quad (23)$$

Note that if $N_E < N_A$, ZF processing is not applicable.

**Theorem 4:** Let $\hat{R}_{S, ZF} \triangleq I(u; z) - I(u; \hat{y}_{ZF})$. As $N_A$, $N_B$ and $N_E \to \infty$ with fixed $\beta_1$, $\beta_2$ and $\beta_3$,

$$\frac{\hat{R}_{S, ZF}}{N_B} < \Phi(P_k, \beta_3) - \log \frac{P_k(1 - \sqrt{\beta_1})^2}{\gamma \beta_3}, \quad (24)$$

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

**Proof:** See Appendix E.

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

**Corollary 3:** Under the same assumptions of Theorem 4, $R_S/N_B \to 0$ if

$$N_E = \left[ \left\{ \frac{\exp(\Phi(P_k, \beta_3))}{\alpha} \right\} + \sqrt{N_A} \right]^2. \quad (25)$$

**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 $H$ and $G$ are mutually independent, $I(u; y)$ can be expressed as a function of these independent random entries. This allows us to take two steps to compute the expected value of $I(u; y)$: we first compute $I(u; y|G)$ given $H$, then compute $E_H[I(u; y|G)|H]$. The advantage is that for $H$, $V = [V_1, Z]$ is a fixed unitary matrix. Then, using [14, Th. 1], $GV_1$ and $GZ$ are mutually independent complex Gaussian random matrices with i.i.d. entries $\sim N_C(0, 1)$.

Let $G_1 = GV_1$, $G_2 = GZ$, $W_1 = G_1 G_1^H$ and $W_2 = G_2 G_2^H$. According to [11], we have

$$I(u; y|G) = E_{G_1, G_2} \left( \log \frac{|I_{N_0} + \sigma^2_{G_1} | W_1 + \sigma^2_{G_2} | W_2 |}{|I_{N_0} + \sigma^2_{G_1} + \sigma^2_{G_2} |} \right)$$

$$\geq \log \frac{|I_{N_0} + \sigma^2_{G_1} | W_1 + \sigma^2_{G_2} | W_2 |}{|I_{N_0} + \sigma^2_{G_1} + \sigma^2_{G_2} |}.$$  

$$= E_{G_1, G_2} \left( \log \frac{|I_{N_0} + \sigma^2_{G_1} | W_1 + \sigma^2_{G_2} W_2 |}{|I_{N_0} + \sigma^2_{G_1} + \sigma^2_{G_2} W_2 |} \right) + N_E \log \frac{\sigma^2_G}{\sigma^2_G} + N_B \sigma^2_W, \quad (26)$$

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

Note that $|I + G_2 G_2^H| = |I + G_2^H G_2|$ and define

$$W = \begin{cases} G_2 G_2^H & \text{if } N_E \leq N_A - N_B \\ G_2^H G_2 & \text{if } N_E > N_A - N_B \end{cases}$$

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

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

$$E_{G_2} \left( \log \frac{|I_{N_{min}} + \alpha \beta | W_{N_{max}} |}{|I_{N_{min}} + \alpha \beta | W_{N_{max}} |} \right)$$

$$= \Theta(N_{min}, N_{max}, \alpha \beta/(1 + \alpha N_B)) - \Theta(N_{min}, N_{max}, \alpha \beta)$$

(27)

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

From (26) and (27), we have

$$I(u; y|H, G) = E_H[I(u; y|G)|H]$$

$$\leq N_E \log(1 + \alpha N_B) - \Theta(N_{min}, N_{max}, \alpha \beta)$$

$$+ \Theta(N_{min}, N_{max}, \alpha \beta/(1 + \alpha N_B))$$

$$= (N_E - N_{min}) \log \alpha N_B + O \left( \frac{1}{\alpha} \right) + O \left( \frac{1}{\beta} \right).$$

**B. Proof of Theorem 1**

If $N_E \leq N_A - N_B$, from Lemma 1 and (10), as $\alpha$ and $\beta \to \infty$,

$$\hat{R}_S = I(u; z|H). \quad (28)$$
Moreover, we have
\[ \hat{C}_S \leq \max_{\mu (u)} \{ I(u; z; H) \} = I(u; z; H). \]  
(29)

The last equation holds since the input \( u \) is a circularly symmetric complex Gaussian random vector [11, Th. 1]. Based on (28) and (29), as \( \alpha \) and \( \beta \to \infty \), we have
\[ \hat{R}_S = \hat{C}_S. \]

**C. Proof of Theorem 2**

Since \((HV_1) (HV_1)^H = HH^H\), using [11, Th. 2] and [12, Th. 1], we have
\[ I(u; z; H) = E_H \left( \log \left| I_{N_B} + \alpha \gamma HH^H \right| \right) = \Theta(N_B, N_A, \alpha \gamma). \]  
(30)

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

From Lemma 1 and (30), we obtain
\[ \hat{R}_S \geq \Theta(N_B, N_A, \alpha \gamma) + \Theta(N_{\min}, N_{\max}, \alpha \beta) \]
\[ - N_E \log(1 + \alpha N_B) - \Theta(N_{\min}, N_{\max}, \alpha \beta/(1 + \alpha N_B)), \]  
(31)

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

**D. Proof of Corollary 1**

If \( \beta \to 1 \), according to [11], we have
\[ \lim_{N_B \to \infty} \frac{I(u; z; H)}{N_B} = \log P_B - 1 + \gamma (P_a), \]  
(32)

where \( \gamma (P_a) \) is given in (17).

From Lemma 1, we have
\[ \lim_{N_B \to \infty} \frac{I(u; z; H, G)}{N_B} \leq \lim_{N_B \to \infty} \frac{N_E - N_{\min}}{N_B} \log P_B \gamma. \]  
(33)

Moreover, if \( \beta \to 1 \), we have
\[ N_{\min} = N_A - N_B. \]  
(34)

Based on (32), (33) and (34), \[ \lim_{\gamma \to \infty} \hat{R}_S/N_B \geq 0 \] if
\[ N_E < N_A + N_B \log (\gamma - 1 + \gamma (P_a)). \]  
(35)

**E. Proof of Theorem 4**

We recall that
\[ \hat{R}_S^{ZF} = I(u; z) - I(u; \hat{y}_{ZF}). \]  
(36)

According to [13, Eq. 1.14], we have
\[ \lim_{N_B \to \infty} \frac{I(u; z)}{N_B} \xrightarrow{a.s.} \Phi(P_a, \beta_2), \]  
(37)

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

Moreover, since \( W = HG^\dagger \), we have
\[ I(u; \hat{y}_{ZF}) = \log \left| \frac{\sigma^2 (HV_1) (HV_1)^H + \sigma^2 W W^H}{\sigma^2 E E^H} \right| = \log \left( \frac{I_{N_B} + \sigma^2 V^H \gamma (GHG)^{-1} V_1}{\sigma^2 \gamma V^H (GHG)^{-1} V_1} \right) = \log \left( \prod_{i=1}^{N_B} \frac{1}{1 + \alpha/\lambda_i} \right), \]  
(38)

where \( \lambda_i, 1 \leq i \leq N_B \), represent the eigenvalues of
\( V_i^H (GHG)^{-1} V_1 \).

From (38), we have
\[ I(u; \hat{y}_{ZF}) > \log \left( \prod_{i=1}^{N_B} \frac{\alpha}{\lambda_i} \right) \]  
(39)

Let \( \delta_{\min} \) be the smallest eigenvalue of \( \frac{1}{N_B} GHG \). Then
\[ 1/\delta_{\min} \] is the largest eigenvalue of \( \frac{1}{N_B} GHG \). According to [15, Th. 8, pp. 69], we have
\[ \prod_{i=1}^{N_B} \lambda_i N_E < \delta_{\min}^{-1}. \]  
(40)

Based on (39) and (40), we have
\[ I(u; \hat{y}_{ZF}) > N_B \log \alpha N_B \delta_{\min}. \]  
(41)

As \( N_A \) and \( N_F \to \infty \), according to Marčenko-Pastur law, \( \delta_{\min} \to 1/\sqrt{\beta_3} \) [13, Eq. 1.10], (41) reduces to
\[ \frac{I(u; \hat{y}_{ZF})}{N_B} > \log \frac{P_\alpha (1 - \sqrt{\beta_3})^2}{\gamma \beta_3} \]  
(42)

almost surely.

By substituting (37) and (42) into (36), as \( N_A, N_B \) and \( N_E \to \infty \) with fixed \( \beta_1, \beta_2 \) and \( \beta_3 \),
\[ \hat{R}_S^{ZF} < \Phi(P_a, \beta_2) - \log \frac{P_\alpha (1 - \sqrt{\beta_3})^2}{\gamma \beta_3}, \]  
(43)

almost surely.

**REFERENCES**


