Artificial Noise Generated in MIMO Scenario: Optimal Power Design

On parle pas de la structure de décodage à Eve

Yan Zhu, Yongkai Zhou, Shivani Patel, Xiao Chen, Liang Pang, and Zhi Xue

***Abstract*—In wireless communication, the transmitter (Alice) can send artificial noise (AN) to interfere with the eavesdropper (Eve). This letter considers the AN MIMO scenario, i.e., both Alice and the legitimate receiver (Bob) are equipped with multiple antennas. A closed-form expression for the lower bound of secrecy capacity is obtained. It is proved that water-filling is the optimal power allocation scheme. An efficient iterative algorithm is proposed to find the optimal power distribution ratio between information and AN so that maximum secrecy capacity can be achieved. Simulation results show that the proposed algorithm converges fast, and multiple antennas can improve the secrecy capacity to some extent compared to the AN MISO case.**

***Index Terms*—AN MIMO scenario, artificial noise, power allocation, power distribution ratio, secrecy capacity.**

Lower bound of SC ontained

I. Introduction

A malicious intruder can easily overhear messages transmitted between two nodes because of the open characteristics of the wireless communication. Traditional security problems involve three parties: a transmitter (Alice), a legitimate receiver (Bob) and a passive eavesdropper (Eve). Wyner [1] first studied the wiretap channel and introduced the notion of secrecy capacity. After that, Csiszar and Korner [2] extended the work to non-degraded discrete memoryless broadcast channel. They showed that if Bob's channel is more capable than Eve's, perfect secrecy can be achieved. Recently, secrecy capacity in MIMO (multiple-input and multiple-output) wiretap channel and fading channel was also studied in [5] and [6].

The method of adopting artificial noise (AN) to increase the secrecy capacity was first proposed by Goel and Negi [3], [4]. In their model, Alice utilizes multiple transmitting antennas or cooperates with the helper nodes to generate the AN. This degrades Eve's channel, without affecting Bob, by injecting the AN into the null space of Bob's channel. Alice's transmitting signal design is of key importance, and one design parameter is the ratio of power distributed between the information bearing signal and the AN, denoted as ϕ. This parameter has a great impact on the secrecy capacity, Cs.

Manuscript received April 30, 2013; revised June 16, 2013; accepted July 16, 2013. Date of publication July 31, 2013; date of current version August 14, 2013. This work was supported in part by the Natural Science Foundation of China (NSFC) under Grants 60932003 and 61271220. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Negar Kiyavash.

Y. Zhu, Y. Zhou, X. Chen, L. Pang, and Z. Xue are with the Department of Electronic Engineering, Shanghai Jiaotong University, Shaghai, China (e-mail: topbestzy1983@sjtu.edu.cn; ssmailzyk@sjtu.edu.cn; chenxiao@sjtu.edu.cn; cyclone0000@sjtu.edu.cn; zxue@sjtu.edu.cn).

S. Patel is with the Department of Electronic Engineering, The Ohio State University, Columbus, OH 43210 USA (e-mail: patel.1311@osu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LSP.2013.2276042

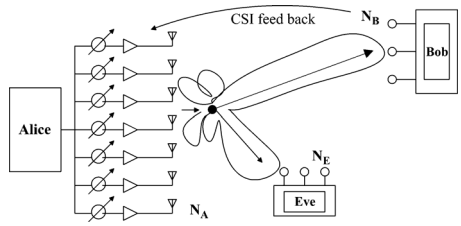

Fig. 1. AN generated in MIMO scenario.

A lot of optimization work has been done on the AN MISO scenario, i.e., Bob is equipped with only one antenna. In [7], closed-form of Cs is derived, so the optimal ϕ^* can be obtained analytically in this case. [8] proposed an optimum power allocation strategy between transmitted information and AN to guarantee a given outage probability of secrecy.

As for the AN MIMO scenario (see Fig. 1), in which Bob is also equipped with multiple antennas, no practical optimal design is available yet. In the AN MIMO case, another factor, the power allocation for the multiple information symbols, denoted as $\mathbf{\Sigma}$, also has to be considered, and this complicates the problem. Although Goel *et al.* have proposed the water-filling scheme for $\mathbf{\Sigma}$ in their original AN paper [3], they did not prove whether it is the optimal power allocation. In [9]–[11], optimal ϕ was obtained by pre-specifying a fixed SINR or fixed rate for Bob. However, they did not consider the random characteristics of Eve's channel condition. [12] proposed a modified water-filling algorithm for MIMO spatial multiplexing and applied it to MIMO wiretap channel. They assigned an optimal power to achieve a fixed information rate, R_b, and used the remaining power for sending AN. However, not all of the rate, R_b, can be guaranteed as secure.

In this letter, we first adopt the results of the random matrix theory [14] to obtain the closed-form expression for the secrecy capacity, Cs. Based on such an expression, it is proved that water-filling is still the optimal power allocation scheme in AN MIMO scenario. An efficient iterative algorithm is then proposed to find the optimal power distribution ratio ϕ^* between information and AN so that maximum Cs can be achieved.

The letter is organized as follows. The system model will be described in Section II. Section III and Section IV will then focus on the secrecy capacity and optimal parameter design. Simulation results will be presented in Section V, and the conclusion will be given in Section VI.

Notation: Bold symbols in capital letter and small letter denote matrices and vectors, respectively. $\mathbb{C}^N$ is the N-dimension vector space over the complex field. $(\cdot)^\dagger$ denotes the conjugate transpose and $(x)^+ = \max\{0, x\}$. $|\cdot|$ is the determinant of a square matrix. $E_{\boldsymbol{G}}(\cdot)$ stands for the expectation over the random variate $\boldsymbol{G}$.

II. System Model

Passive eavesdropper

Suppose Alice and Bob are equipped with N_A ($N_A \geq 2$) and N_B ($N_B \geq 1$) antennas respectively. Eve will have N_E ($N_E \geq 1$) antennas for eavesdropping on the transmission signal between Alice and Bob. It is assumed that the channel between Alice and Bob is known to all parties, but they do not hold information about the CSI of Eve.

The total transmission power of Alice is P_A, in which a proportion of ϕ ($0 \leq \phi \leq 1$) is allocated to the information signal, with others left for AN. That is, $P_{info} = \phi \cdot P_A$ and $P_{AN} = (1-\phi) \cdot P_A$.

As shown in Fig. 1, Alice adopts multiple antennas to send both information signal and artificial noise. At time period k, the signal received by Bob is

uncorrelated MIMO channel. Here, no spatial correlation

$$\boldsymbol{y}_b(k) = \boldsymbol{H}_{ab} \cdot \boldsymbol{x}(k) + \boldsymbol{n}_b(k) \tag{1}$$

where $\boldsymbol{x}$ is the signal transmitted by Alice and $\boldsymbol{n}_b$ is the Gaussian noise at Bob. $\boldsymbol{H}_{ab}$ denotes the channel between Alice and Bob, which is an $N_B \times N_A$ matrix with rank $r_{\boldsymbol{H}}$. The singular value decomposition (SVD) of $\boldsymbol{H}_{ab}$ is $\boldsymbol{H}_{ab} = \boldsymbol{U}\Lambda\boldsymbol{V}^\dagger$, with singular values $\lambda_1, \lambda_2, \ldots, \lambda_{r_H}$ of descending order.

Similarly, the received signal at Eve is given by:

$$\boldsymbol{y}_e(k) = \boldsymbol{G}_{ae} \cdot \boldsymbol{x}(k) + \boldsymbol{n}_e(k) \tag{2}$$

where $\boldsymbol{n}_e$ is the Gaussian noise at Eve. $\boldsymbol{G}_{ae}$ is the channel between Alice and Eve, and it is unknown to Alice or Bob. Therefore, the entries of $\boldsymbol{G}_{ae}$ are modeled as independent zero-mean complex circularly symmetric Gaussian random variables. In the following part, when there is no ambiguity, the time factor k will be omitted for simplicity; $\boldsymbol{G}_{ae}$ and $\boldsymbol{H}_{ab}$ will be abbreviated as $\boldsymbol{G}$ and $\boldsymbol{H}$, respectively.

The transmitted signal $\mathbf{x}$ can be decomposed into the information part and the AN part:

SVD precoding
No SVD decoding (cfr 6)

$$\begin{aligned} \boldsymbol{x} &= \boldsymbol{s} + \boldsymbol{w} \\ &= \boldsymbol{V}_r \cdot \boldsymbol{u} + \boldsymbol{W} \cdot \boldsymbol{z}. \end{aligned} \tag{3}$$

According to the beamforming scheme by [3], $(\mathbf{V}_r, \mathbf{W})$ forms an orthogonal basis of $\mathbb{C}^{N_A}$. $\mathbf{V}_r$ is composed of the first r ($1 \leq r \leq r_{\mathbf{H}}$) column vectors of $\mathbf{V}$, the SVD unitary matrix; $\mathbf{W}$ spans the null space of $\mathbf{H}^\dagger$, with size $N_A \times (N_A - r)$·r is the number of dimensions allocated to the information signals, while the remaining $N_A - r$ dimensions are left for AN.

$\mathbf{u}$ is the information symbol vector. Alice can choose a certain power allocation $\boldsymbol{\Sigma}_r = diag(\rho_1, \rho_2, \ldots, \rho_r)$ for these information symbols, with $\sum_{i=1}^{r} \rho_i = 1$ so that

$$E(\mathbf{u}\mathbf{u}^\dagger) = P_{info} \cdot \boldsymbol{\Sigma}_r = \phi \cdot P_A \cdot diag(\rho_1, \rho_2, \ldots, \rho_r) \tag{4}$$

$\mathbf{z}$ is the AN vector of length $N_A - r$, and the elements of $\mathbf{z}$ are chosen to be i.i.d. complex Gaussian random variables. Therefore, the AN power is evenly distributed to each of the AN symbols,

$$E(\mathbf{z}\mathbf{z}^\dagger) = \frac{P_{AN}}{N_A - r} \cdot \mathbf{I}_{N_A - r} = \frac{(1-\phi)P_A}{N_A - r} \cdot \boldsymbol{I}_{N_A - r}. \tag{5}$$

By substituting (3) for $\boldsymbol{x}$, Equation (1) and (2) can be further expanded as

$$\begin{aligned} \mathbf{y}_b &= \mathbf{H} \cdot (\mathbf{V}_r \cdot \mathbf{u} + \mathbf{W} \cdot \mathbf{z}) + \mathbf{n_b} \\ &= \mathbf{H} \cdot \mathbf{V}_r \cdot \mathbf{u} + \mathbf{n}_b \end{aligned} \tag{6}$$

$$\mathbf{y}_e = \mathbf{G} \cdot \mathbf{V}_r \cdot \mathbf{u} + \mathbf{G} \cdot \mathbf{W} \cdot \mathbf{z} + \mathbf{n}_e. \tag{7}$$

III. Secrecy Capacity and Optimal Power Design

In this section, we will study the design of two key parameters:

1) ϕ, the *power distribution ratio* between Info. and AN;
2) $\boldsymbol{\Sigma}_r$, the *power allocation* for the r MIMO Info. symbols.

for Alice in the MIMO AN model, so that maximum secrecy capacity between Alice and Bob can be achieved. An efficient iterative algorithm combined with water-filling power allocation will be proposed to find the optimal ϕ^*.

A. Secrecy Capacity and Optimal Power Allocation, $\boldsymbol{\sigma}_r^*$

Based on the work of [5] and [3], the lower bound on secrecy capacity can be calculated in terms of Equation (6) and Equation (7).

$$Cs = \left(Cs_1 - \overline{Cs_2}\right)^+ \tag{8}$$

$$\begin{aligned} Cs_1 &= \log_2 \left| \mathbf{I} + \frac{\mathbf{H}\mathbf{V}_r E(\mathbf{u}\mathbf{u}^\dagger)\mathbf{V}_r^\dagger \mathbf{H}^\dagger}{\sigma_n^2} \right| \\ &= \sum_{i=1}^{r} \log_2 \left(1 + \frac{\lambda_i^2 \rho_i \cdot \phi P_A}{\sigma_n^2}\right) \end{aligned} \tag{9}$$

$$\begin{aligned} Cs_2 &\leq E_{\mathbf{G}} \log_2 \left| \frac{\mathbf{G}\mathbf{V}_r E(\mathbf{u}\mathbf{u}^\dagger)\mathbf{V}_r^\dagger \mathbf{G}^\dagger + \mathbf{G}\mathbf{W}E(\mathbf{z}\mathbf{z}^\dagger)\mathbf{W}^\dagger\mathbf{G}^\dagger}{\mathbf{G}\mathbf{W}E(\mathbf{z}\mathbf{z}^\dagger)\mathbf{W}^\dagger\mathbf{G}^\dagger} \right| \\ &= E_{\substack{\mathbf{G}_1, \\ \mathbf{G}_2}} \log_2 \left| \frac{P_{info} \cdot \mathbf{G}_1 \boldsymbol{\Sigma}_r {\mathbf{G}_1}^\dagger + \frac{P_{AN}}{N_A - r}\mathbf{G}_2 {\mathbf{G}_2}^\dagger}{\frac{P_{AN}}{N_A - r}\mathbf{G}_2 {\mathbf{G}_2}^\dagger} \right| \end{aligned} \tag{10}$$

Consideration: No noise @Eve

(a) holds because the worst case situation, $\mathbf{n}_e \to 0$, is considered. $\mathbf{G}$ can be normalized to have identity covariance because it appears in both the numerator and the denominator. We denote $\mathbf{G}_1 = \mathbf{G}\mathbf{V}_r$ and $\mathbf{G}_2 = \mathbf{G}\mathbf{W}$. Note that due to the orthonormality of $(\mathbf{V}_r, \mathbf{W})$, $\mathbf{G}_1$ and $\mathbf{G}_2$ also have circularly symmetric i.i.d. complex unit Gaussian distributed elements. Cs_2 can be further approximated as

$$\begin{aligned} Cs_2 &\overset{(b)}{\leq} E_{\mathbf{G}_2} \log_2 \left| \frac{P_{info} \cdot \mathbb{E}_{\mathbf{G}_1}(\mathbf{G}_1 \boldsymbol{\Sigma}_r {\mathbf{G}_1}^\dagger) + \frac{P_{AN}}{N_A - r}\mathbf{G}_2 {\mathbf{G}_2}^\dagger}{\frac{P_{AN}}{N_A - r}\mathbf{G}_2 {\mathbf{G}_2}^\dagger} \right| \\ &\overset{(c)}{=} N_E \cdot \log_2 \frac{\phi(N_A - r)}{1 - \phi} + \frac{1}{ln2} \frac{\left.\frac{\mathrm{d}\left|\boldsymbol{\Omega}(t, \frac{(1-\phi)}{\phi(N_A - r)})\right|}{\mathrm{d}t}\right|_{t=0}}{\prod_{i=1}^{N_E}(N_A - r - i)!} \\ &\quad - \frac{1}{ln2} \sum_{i=0}^{N_E - 1} \psi(N_A - r - i) = \overline{Cs_2} \end{aligned} \tag{11}$$

where $\psi(\cdot)$ is Euler's digamma function, and $\boldsymbol{\Omega}(t, \gamma)$ is an $N_E \times N_E$ Hankel matrix whose entry is explained in the Appendix. (b) holds due to the concavity of logarithm function, and the derivation of (c) is available in the Appendix.

$\overline{Cs_2}$ in (11) is the upper bound of the information tapped by Eve. Therefore, Cs in (8) is the minimum guaranteed secrecy capacity that can be ensured in this scenario, and its closed-form expression is available via Equation (8)–(11). Note that in (11), $\overline{Cs_2}$ is irrelevant to the power distribution of the information symbols, $\boldsymbol{\Sigma}_r$. Therefore, given a fixed SNR for Alice, the optimal $\boldsymbol{\Sigma}_r$ for Cs_1 also results in maximized Cs. On the other hand, it is a well-known result that water-filling power distribution maximizes the MIMO channel capacity (Cs_1) when the

CSI is available at the transmitter [13]. Therefore, we have the following proposition:

Proposition 3.1: For a fixed SNR at Bob, Cs is maximized by water-filling power allocation $\mathbf{\Sigma}_{wf} = diag(\rho_1, \rho_2, \ldots, \rho_r)$, which is given by

$$\rho_i = \frac{P_i}{P_{info}} = \left(\frac{1}{\gamma_0} - \frac{1}{SNR \cdot \lambda_i^2}\right)^+, i = 1 \ldots r$$
$$with \quad \sum_{i=1}^{r} \left(\frac{1}{\gamma_0} - \frac{1}{SNR \cdot \lambda_i^2}\right)^+ = 1 \qquad (12)$$

where $SNR = \phi \cdot SNR_0$, with SNR_0 corresponding to the SNR when all power is allocated to information signals (i.e., $\phi = 1$).

Algorithm for Optimal Power Distribution Ratio, ϕ^*

A closed-form expression for Cs is available in terms of Equation (8)–(11). Therefore, the optimal ϕ can be obtained by numerical methods such as one dimension search or differential analysis. The power allocation $\mathbf{\Sigma}_r$, however, is related to the SNR at Bob and in turn depends on ϕ. The loop optimization between $\mathbf{\Sigma}_r^*$ and ϕ^* complicates the problem. Still, we have a fairly simple yet effective algorithm to find the optimal ϕ^*:

Algorithm 1 Algorithm for ϕ^* with a given r

1: $\phi(0) = 1, n = 1$; //ϕ is set to 1 initially

2: **while** not converged **do**

3: $\mathbf{\Sigma}_r(n-1) = waterfilling(\phi(n-1))$;

4: $\phi(n) = arg \max_{\phi} \{Cs(\mathbf{\Sigma}_r(n-1))\}$;

5: $n = n + 1$

6: **end while**

7: $\phi^* = \phi(n); \mathbf{\Sigma}_r^* = waterfilling(\phi(n))$;

8: $Cs^* = Cs(\phi^*, \mathbf{\Sigma}_r^*)$

The basic idea for Alg. 1 is to alternatively fix ϕ and $\mathbf{\Sigma}_r$ to obtain new ϕ and $\mathbf{\Sigma}_r$, thus iteratively approximating ϕ^*. In order to show the effectiveness of Algorithm 1, we have the following proposition.

Proposition 3.2: In Alg. 1, $Cs(\phi(n), \mathbf{\Sigma}_r(n)) \geq Cs(\phi(n-1), \mathbf{\Sigma}_r(n-1))$

Proof: $\mathbf{\Sigma}_r(n)$ is the water-filling solution for SNR under $\phi(n)$ (Alg. 1, step 3), and thus is the optimal power allocation for $Cs(\phi(n))$ by Prop. (3.1). Therefore,

$$Cs(\phi(n), \mathbf{\Sigma}_r(n)) \geq Cs(\phi(n), \mathbf{\Sigma}_r(n-1))$$

$\phi(n)$ is the optimal argument for Cs under the power allocation $\mathbf{\Sigma}_r(n-1)$ (Alg. 1, step 4). Therefore,

$$Cs(\phi(n), \mathbf{\Sigma}_r(n-1)) \geq Cs(\phi(n-1), \mathbf{\Sigma}_r(n-1)).$$

Hence, $Cs(n) \geq Cs(n-1)$ is proved. ■

By Proposition 3.2, Cs always increases during each round of iteration. Hence, Alg. 1 can indeed approach the optimal ϕ^*. As for the convergence criteria, some precision requirement can be set on ϕ or Cs, for example, $|\phi(n) - \phi(n-1)| < 0.005$.

prob:
Na > Ne + r
Nb = Ne is assumed, i.e. same capabilities bw Bob and Eve

TABLE I
ITERATION RESULTS FOR ALG. 1

Round No. i	ϕ	$\mathbf{\Sigma}_r$	$Cs(bit)$
0	0	[0.41 0.34 0.24]	0
1	0.324	[0.58 0.35 0.08]	0.348
2	0.284	[0.61 0.35 0.04]	0.441
3	0.271	[0.63 0.35 0.02]	0.445
4	0.266	[0.63 0.35 0.02]	0.446

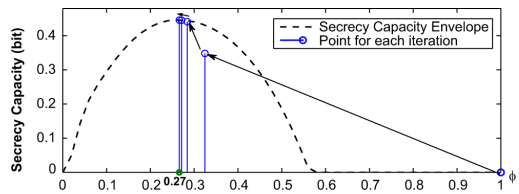

Fig. 2. Illustration of the process to find the optimal ϕ^*.

IV. Discussion and Extension

A. Constraints on Antenna Numbers

Compared to the MISO AN model analysed in [7], there are some size constraints on the number of antennas for Alice, Bob and Eve in the MIMO case. First, as can be seen from Equation(10), to avoid $|\boldsymbol{G}_2\boldsymbol{G}_2^\dagger| = 0$, $N_A \geq r + N_E$ has to be ensured. Second, for Eve's antenna number (N_E), it is related to an assumption on the capability of Eve. $N_E = N_B$ is typically assumed meaning that Eve has the same capability as Bob. N_E can also be considered as the number of colluding eavesdroppers, each equipped with one antenna.

B. The Choice of the Information Dimension, r

The number of dimensions allocated for information symbols, r, plays a key role in the AN MIMO scenario. As was discussed in [4], the secrecy capacity, Cs, does not necessarily grow linearly with the number of receive dimensions, and thus behaves differently from the usual MIMO capacity. The optimal design would be to iterate r through 1 to $r_{\boldsymbol{H}}$, and choose r^* according to the highest $Cs(r)$ obtained by Algorithm 1.

V. Simulation Results

Simulation scenario is set up according to Fig. 1. First, the optimal design of ϕ and $\mathbf{\Sigma}_r$ is analysed. Parameters are set as: $N_A = 6$, $N_B = r = 3$, $N_E = 3$, $SNR_0 = 2$, and ϕ is set to 0 initially. Alg. 1 is taken to find the optimal ϕ^*, and the convergence criteria is set as $|\phi(n) - \phi(n-1)| < 0.005$. The iteration results for each round are shown in Table I.

As can be seen from the results, it takes only 5 iterations to search the optimal ϕ^*, and it is even faster in high SNR condition. The detailed process is shown in Fig. 2 to best illustrate the effectiveness of the algorithm. The dotted line is the envelope for Cs under different ϕ, while the stemmed points are the results for each round. It finally converges to the optimal value.

Next, the impact of multiple antennas on the MIMO AN scenario is studied. Parameters are set as: $N_A = 10$, $SNR_0 = 5.0$. First, we study how Cs and ϕ^* vary with the number of dimensions, r, allocated for information symbols. In this case, $N_E = 4$, $N_B = 6$, and r varies from 1 to N_B.

From Fig. 3(a), it can be seen that multiple antennas for Bob can greatly improve the secrecy capacity, and $r = 5$ achieves the best performance. When $r = 6$, no dimensions are left for AN, and the model degenerates to a typical MIMO wiretap channel.

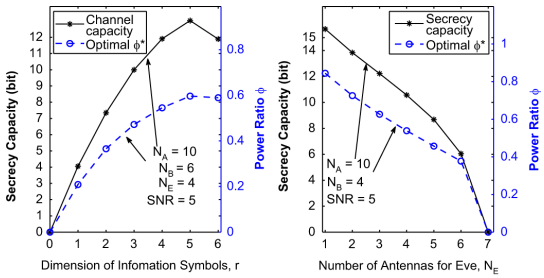

Fig. 3. The Impact of Multiple Antennas on Cs and ϕ^*.

Fig. 3(b) shows how Cs and ϕ^* adapt to cope with an Eve of different capabilities (N_E). This time, N_B is fixed to 4, and N_E varies from 1 to 7. Secrecy capacity drops drastically with the increase of N_E. When N_E exceeds the size constraint in Section IV-A($N_E \geq 7$ for this case), Cs drops to zero. The optimal power distribution ratio (ϕ^*) also decreases so that more proportion of the power should be assigned to AN in order to resist a more powerful eavesdropper.

VI. Conclusion

In this letter, artificial noise (AN) generation in MIMO scenario was studied. A closed-form expression for the minimum guaranteed secrecy capacity (Cs) was obtained. It was proved that water-filling is the optimal power allocation for this MIMO AN model. An efficient iterative algorithm was proposed to distribute the proportion of Alice's transmission power between information and AN so that maximum Cs can be achieved. Simulation results showed that the proposed algorithm converged quickly to the optimal solution and multiple antennas can improve the secrecy capacity to some extent.

Appendix
Derivation of $\overline{Cs_2}$, (11)

$$
\begin{aligned}
Cs_2 \leq & E_{\boldsymbol{G}_2} log_2 \left| \frac{P_{info} \cdot \mathbb{E}_{\boldsymbol{G}_1}(\boldsymbol{G}_1 \boldsymbol{\Sigma}_r \boldsymbol{G}_1{}^\dagger) + \frac{P_{AN}}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2{}^\dagger}{\frac{P_{AN}}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2{}^\dagger} \right| \\
= & E_{\boldsymbol{G}_2} log_2 \left| \frac{P_{info} \cdot \sum_{i=1}^{r} \mathbb{E}_{\boldsymbol{g}_i}(\rho_i \boldsymbol{g}_i \boldsymbol{g}_i{}^\dagger) + \frac{P_{AN}}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2{}^\dagger}{\frac{P_{AN}}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2{}^\dagger} \right| \\
= & E_{\boldsymbol{G}_2} log_2 \left| \frac{P_{info} \cdot \sum_{i=1}^{r} (\rho_i \cdot \boldsymbol{I}_{N_A - r}) + \frac{P_{AN}}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2{}^\dagger}{\frac{P_{AN}}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2{}^\dagger} \right| \\
\overset{(b)}{=} & E_{\boldsymbol{G}_2} log_2 \left| \frac{P_{info} \cdot \boldsymbol{I}_{N_A - r} + \frac{P_{AN}}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2{}^\dagger}{\frac{P_{AN}}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2{}^\dagger} \right| \\
= & E_{\boldsymbol{G}_2} log_2 \left| \phi \boldsymbol{I} + \frac{1 - \phi}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2^\dagger \right| \\
& - E_{\boldsymbol{G}_2} log_2 \left| \frac{1 - \phi}{N_A - r} \boldsymbol{G}_2 \boldsymbol{G}_2^\dagger \right| \\
\overset{(c)}{=} & N_E \cdot log_2 \frac{\phi (N_A - r)}{1 - \phi} + \frac{1}{ln2} \frac{\left. \frac{\mathrm{d} \left| \boldsymbol{O}_{mega}(t, \frac{(1-\phi)}{\phi (N_A - r)}) \right|}{\mathrm{d}t} \right|_{t=0}}{\prod_{i=1}^{N_E} (N_A - r - i)!} \\
& - \frac{1}{ln2} \sum_{i=0}^{N_E - 1} \psi(N_A - r - i) = \overline{Cs_2}
\end{aligned}
$$

in (a), $\boldsymbol{g}_i (1 \leq i \leq r)$ is the ith column vector of $\boldsymbol{G}_1$, and its entries are i.i.d. complex random Gaussian variables with zero mean and unit covariance. (b) holds due to $\sum \rho_i = 1$ for $\boldsymbol{\Sigma}_r$. $\boldsymbol{G}_2 \boldsymbol{G}_2^\dagger$ is a $\mathcal{W}_{N_E}(N_A - r, \boldsymbol{I})$ Wishart matrix, and the result of (c) is obtained by the random matrix formulas shown below, which is listed in [14].

For a central Wishart matrix $\boldsymbol{W} \sim \mathcal{W}_m(n, \boldsymbol{I})$, with $n \geq m$,

$$\mathbb{E}[\log_e \det \boldsymbol{W}] = \sum_{i=0}^{m-1} \psi(n - i) \tag{13}$$

$$\mathbb{E}\left[e^{t \log_e \det(I + \gamma \boldsymbol{W})} \right] = \frac{|\boldsymbol{\Omega}(t, \gamma)|}{\prod_{i=1}^{m} (n - i)!} \tag{14}$$

where $\psi(\cdot)$ is Euler's digamma function, and $\boldsymbol{\Omega}(t, \gamma)$ is a $m \times m$ Hankel matrix whose (i, k)th entry is

$$
\begin{aligned}
\boldsymbol{\Omega}_{i,k} = & \\
& \frac{\pi}{\Gamma(-t) sin(\pi(d - 1 + t))} \left(\frac{\gamma^{-d} (d-1)!}{\Gamma(1 + d + t)} {}_1F_1(d, 1 + d + t, \frac{1}{\gamma}) \right. \\
& \left. \frac{\gamma^t \Gamma(-t)}{\Gamma(1 - d - t)}_1 F_1(-t, 1 - d - t, \frac{1}{\gamma}) \right)
\end{aligned}
$$

with ${}_1F_1(\cdot)$ the confluent hypergeometric function and with $d = n - m + i + k + 1$.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J*, vol. 54, pp. 1355–1387, 1975.

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

[3] R. Negi and S. Goel, "Secret communication using artificial noise," *Proc. VTC Fall 2005*, vol. 3, pp. 1501–1506, Sep. 2005.

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

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, pp. 4961–4972, Aug. 2011.

[6] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2470–2492, Jun. 2008.

[7] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[8] N. R. Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[9] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *IEEE Int. Conf. on ICASSP 2009*, Apr. 2009, pp. 2437–2440.

[10] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *IEEE Int. Conf. SPAWC 2009*, Jun. 2009, pp. 344–348.

[11] A. Mukherjee and A. L. Swindlehurst, "Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[12] A. Mukherjee and A. L. Swindlehurst, "Modified waterfilling algorithms for MIMO spatial multiplexing with asymmetric CSI," *IEEE Wireless Commun. Lett.*, vol. 1, no. 2, pp. 89–92, Apr. 2012.

[13] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[14] A. M. Tunilo and S. Verdu, *Random Matrix Theory and Wireless Communications*. Boston, MA, USA: Now, 2004.