Ergodic Lower Bound and Optimal Power Allocation for Secrecy-Capacity-Optimization-Artificial-Noise in MIMO Wireless System

Yebo Gu(✉), Zhilu Wu, and Zhendong Yin

School of Electronics and Information Engineering,
Harbin Institute of Technology, Harbin, China
16B305002@hit.edu.cn

Abstract. The transmission security problem is considered in this paper. A new artificial noise is added into transmitted signal to improve the secrecy performance of the system. A expression for the ergodic lower bound of SCO-AN system is derived. Based on the expression, optimal power distribution for SCO-AN system is studied. Moreover, optimal ratio of power distribution can be calculated. Moreover, the influence of channel estimation error is considered. As a result, it is necessary to generate more SCO-AN if the channel information error is considered.

Keywords: Artificial noise · Transmission security · Secrecy capacity · SCO-AN · Power distribution

1 Introduction

The transmission security of information is fundamental problems in wireless communication [1]. Wireless communication is useless unless a secure transmission of information is guaranteed. The foundation of the physical layer security (PLS) was proposed in [3]. Wyner introduced wiretap channel model which contains an information transmitter, a receiver, and an eavesdropper. Later in 2003, Csiszár and Körner considered common conditions of the model and studied the transmission of broadcasting information [4].

[5] introduces the Artificial noise (AN). AN is orthogonal to receiver's channel, so AN will not reduce ability of the receiver's channel to obtain information. Meanwhile, AN reduces the capable performance of eavesdropper's channel.

Based on AN, SCO-AN is introduced in [6]. [6] studies the issues in the secure communication of fading channels. A expression for secrecy capacity in fading channels which adds SCO-AN is derived.

Q. Guo et al. (Eds.): WiSATS 2021, LNICST 410, pp. 742–748, 2022.
https://doi.org/10.1007/978-3-030-93398-2_64

The main contribution is summarized as follows: This paper creatively uses statistical knowledge to find the objective function for SCO-AN under ideal conditions, and finds the optimal power distribution coefficient under ideal conditions. We reach crucial conclusion: the secrecy capacity of the legitimate channel depends entirely on the partition of power and the number of receiving antennas. On the contrary, the allocation objective function is not related to power at all.

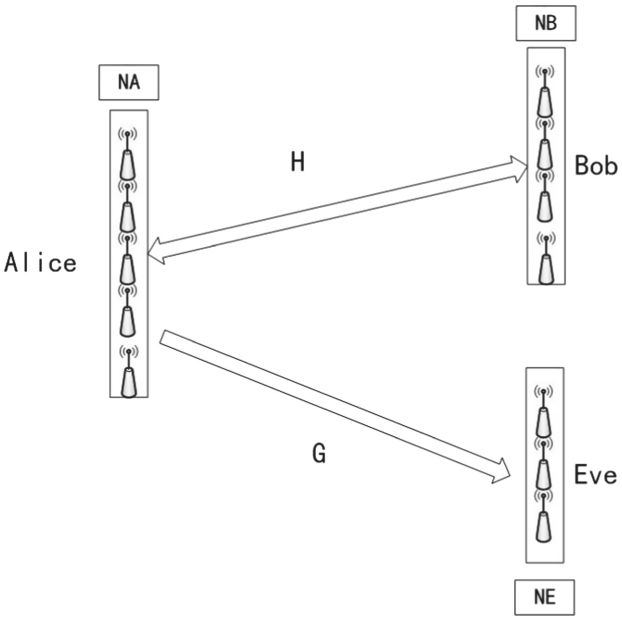

Fig. 1. Wiretap communication system model

According to the previously obtained expression for ergodic secrecy capacity, the optimal power distribution ratio of SCO-AN communication system is investigated. We consider the imperfect channel information as well. The expression for ergodic secrecy capacity with channel information error is derived. We conclude that once the channel estimation error increases, SCO-AN should be generate to more power.

2 System Model

Secure communication system over a multiple access wiretap channel is shown in Fig. 1. Alice is the signal transmitter. Bob is the receiver who equipped N_B antennas. Eve is the eavesdropper who equipped with N_E antennas. To facilitate discussion, we assumed that $N_A > N_E$, which means that the transmitter will have more freedom to assign the transmitted signal to SCO-AN. In the next

section, we assume that N_E is a large number to apply the strong law of large numbers. If N_E is a large number and $N_A < N_E$, the study in Sect. 3 will be invalid. Eve is a passive eavesdropper. So:

$$y_{B1} = \mathbf{H}\mathbf{x} + n, \tag{1}$$

$$y_{E1} = \mathbf{G}\mathbf{x} + e, \tag{2}$$

Bob receives the signal y_{B1}, Eve receives the signal y_{E1}. $\mathbf{H}$ denotes legitimate channel, $\mathbf{G}$ is eavesdropping channel; $\mathbf{x}$ is the transmitted signal. n and e are AWGN. In this paper,

The SCO-AN designs as follows: $W = [\mathbf{p}_1 \ \ \mathbf{P}_2]$ is a $N_A \times N_B$ matrix, where $\mathbf{p}_1 = \mathbf{H}^{\dagger}/\|\mathbf{H}\|$. x is a $N_A \times 1$ vector, and $\mathbf{x} = \mathbf{p}_1\mathbf{u} + \mathbf{P}_2\mathbf{v}$. $\mathbf{u}$ is transmitting signal. The power of $\mathbf{u}$ is σ_u^2. So:

$$y_{B1} = \mathbf{H}\mathbf{p}_1\mathbf{u} + \mathbf{H}\mathbf{P}_2\mathbf{v} + n = \|\mathbf{H}\|\,\mathbf{u} + \mathbf{H}_1\mathbf{v} + n, \tag{3}$$

$$y_{E1} = \mathbf{G}\mathbf{p}_1\mathbf{u} + \mathbf{G}\mathbf{P}_2\mathbf{v} + e = \mathbf{G}_1\mathbf{u} + \mathbf{G}_2\mathbf{v} + e, \tag{4}$$

where $\mathbf{H}_1 = \mathbf{H}\mathbf{W}_2$, $\mathbf{G}_1 = \mathbf{G}\mathbf{w}_1$ and $\mathbf{G}_2 = \mathbf{G}\mathbf{w}_2$.

The transmission power P, so $P = \sigma_u^2 + (N_A - 1)\sigma_v^2$. The percentage of signal is ϕ. Therefore,

$$\sigma_u^2 = \phi P, \tag{5}$$

$$\sigma_v^2 = (1 - \phi)P/(N_A - 1), \tag{6}$$

according to (5) and (6), Alice could change the power allocation strategy by changing ϕ.

3 SCO-AN: Optimal Power Allocation

3.1 Ergodic Lower Bound of Secrecy Capacity

The boundaries of SCO-AN are determined by $\mathbf{H}$ and $\mathbf{G}$. The legitimate channel capacity is:

$$\begin{aligned} C_A &= E_1\{\log_2(1 + \frac{\sigma_u^2\|\mathbf{H}\|^2}{\sigma_v^2\|\mathbf{H}\|^2})\} \\ &= E_1\{\log_2(1 + \frac{\sigma_u^2}{\sigma_v^2})\} \\ &= E_1\{\log_2(1 + \frac{\phi P}{(1-\phi)P/(N_A - 1)})\} \\ &= E_1\{\log_2(1 + \frac{\phi(N_A - 1)}{(1-\phi)})\}, \end{aligned} \tag{7}$$

From (7), we see the receiver's channel capacity is entirely unrelated to the transmitted power. It is an exciting discovery that the receiver's channel capacity only

relates to the power partition coefficient of ϕ. The receiver's channel capacity is easy to adjust.

Next, the eavesdropping channel capacity will be discussed.

The upper bound of the eavesdropping channel capacity is:

$$\begin{aligned} C_B &= E_{h,\mathbf{G}_1,\mathbf{G}_2}\{\log_2 \left| I + \sigma_u^2 \mathbf{G}_1 \mathbf{G}_1^\dagger (\sigma_v^2 \mathbf{G}_2 \mathbf{G}_2^\dagger)^{-1} \right|\} \\ &= E_{h,\mathbf{G}_1,\mathbf{G}_2}\{\log_2(1 + \frac{N_A - 1}{r-1} \mathbf{G}_1^\dagger (\mathbf{G}_2 \mathbf{G}_2^\dagger)^{-1} \mathbf{G}_1\}, \end{aligned} \tag{8}$$

r is defined as ϕ^{-1}. In (8), $\mathbf{G}_2\mathbf{G}_2^\dagger$ is invertible so the assumption of $N_A > N_E$ is guaranteed.

As we know, the secrecy capacity is $C = [C_1 - C_2]^+$ and $[a]^+$ means $\max\{0, \alpha\}$. The ergodic secrecy capacity is:

$$\begin{aligned} C_B = \frac{1}{\ln 2}[E_h\{\log_2(1 + \frac{r * N_A - 1}{(r-1)}) - \sum_{n=0}^{r*N_A-1} \binom{r * N_A - 1}{k} \frac{r * N_A - 1}{r+1} \\ \times D(k+1, r * N_A - 1 - k) \times F_1(1, k+1; N_A; \frac{r - r * N_A}{r+1})\}], \end{aligned} \tag{9}$$

in the following sections, the above expressions leads us to get the optimal power allocation.

3.2 Infinite N_A Analysis

This subsection discusses the ergodic secrecy capacity lower bound when N_A approaches infinity asymptotically. Here, $\lim_{N_C \to \infty} \mathbf{G}_2\mathbf{G}_2^\dagger/(N_C - 1) = I$. So we can rewrite (9) as:

$$\lim_{N_A \to \infty} C_B = \lim_{N_A \to \infty} E_{\mathbf{G}_1,\mathbf{G}_2}\{\log_2 \left(1 + \frac{1}{r-1} \mathbf{G}_1^\dagger (\frac{\mathbf{G}_2\mathbf{G}_2^\dagger}{N_A - 1})^{-1} \mathbf{G}_1\right)\} = e_k(r+1) \sum_{n=1}^{N_E} E_k(r+1), \tag{10}$$

the gain of Rayleigh fading channel among N_E non-colluding eavesdroppers obey an exponential distribution. So $\|\mathbf{G}_1\|^2$ obeys a Gamma distribution with parameters $(N_E, 1)$.

When N_A approaches infinity asymptotically, so

$$C = E_h\{\log_2(1 + \frac{\phi(N_A - 1)}{(1-\phi)})\} - e_k(r+1) \sum_{n=1}^{N_E} E_k(r+1) \tag{11}$$

3.3 The Optimal Allocation

We study the case where N_A approaches infinity asymptotically. It then follows that $N_E = 1$. (13) gives $dC_B \backslash dz = 0$. Substituting $N_E = 1$ in the expression of C_B in (11) and taking its derivative with respect to z gives

$$\begin{aligned} dC_B/dz &= (e_k(r+1)E_1(r-1) - \exp(r-1)E_x(r+1))/\ln 2 \\ &= (e_k(r+1)e_k(r+1) - (r+1)^{-1})\Big/\ln 2. \end{aligned} \tag{12}$$

The solution to (12) is $r = 1.8$. Therefore when N_A approaches infinity asymptotically.

Hence, for sufficiently large N_A, the optimal $\phi = 0.55$. We can see that there is no significance difference in the optimal power distribution between the case where N_A takes its smallest possible value and the case where N_A approaches infinity asymptotically.

4 Results and Discussion

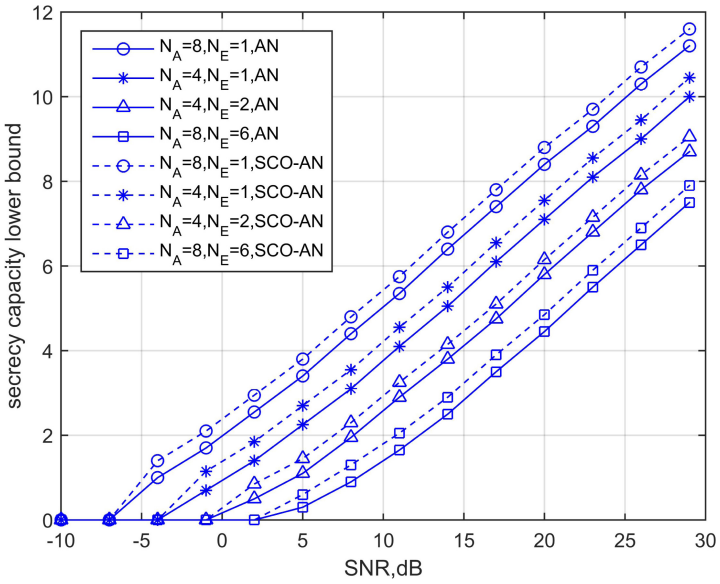

Fig. 2. The lower bound of secrecy capacity versus SNR with different numbers of antennas

Figure 2 shows the variation of C calculated using (9) with the optimal ϕ. The solid lines show the system's secrecy capacity (SC), which uses SCO-AN. The dash lines show the SC, which uses AN. The variation of SCO-AN and AN have

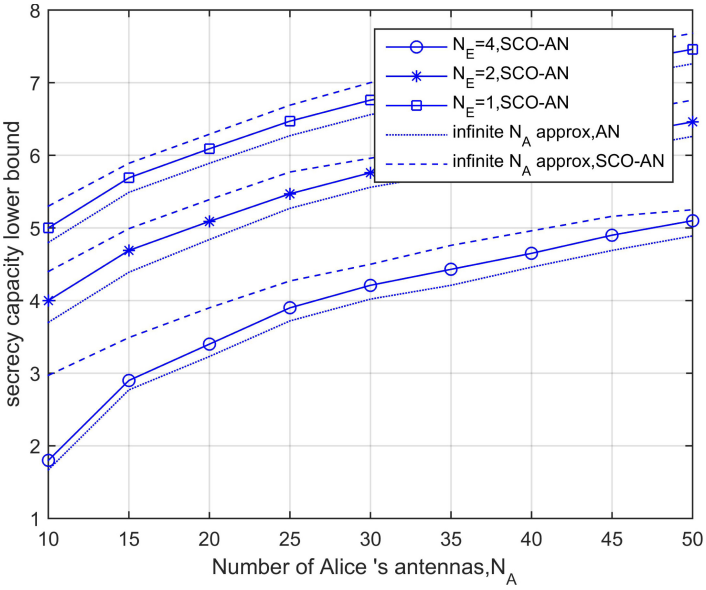

Fig. 3. The SC versus SNR with different numbers of eavesdropper's antennas and infinite N_A

similar behaviour. Furthermore, C increases with N_A when SNR is from -10 dB to 30 dB. C decreases with N_E as well. C reduced to closer to zero when the SNR is small.

The dashed line in Fig. 3 denotes the approximations of C in (11) as N_A approaches infinity. The dotted line denotes the approximations of SC of AN as N_A approaches infinity. Figure 3 shows that SC is correlated with N_A and N_E. The SC increases with an increasing of N_A. The infinite N_A lower bound of secrecy capacity for SCO-AN is always greater than that of secrecy capacity for AN. When the N_A approaches infinite asymptotically, the secrecy capacity of AN is the smallest. The secrecy capacity decreases with a increase of N_E.

5 Conclusion

This paper has explored and discussed the power distribution coefficients between the transmitted signal and SCO-AN under ideal conditions. The expression of secrecy capacity is obtained. We then prove the secrecy capacity for SCO-AN is always greater than that of secrecy capacity for AN. The optimal power allocation ratio is computed. In comparison with AN, SCO-AN has better secrecy performance when presented with less power for extra artificial noise. It then follows that SCO-AN is a better option for artificial noise than AN. This paper also considers the channel estimation error on power allocation. The result of this paper provides a much-valued help to the design of a secure wireless communication system.

References

1. Hashem, T., Hasan, R.: Method and system for secure transmission of information. US (2004)
2. Barros, J., Rodrigues, M.R.D.: Secrecy capacity of wireless channels. In: 2006 IEEE International Symposium on Information Theory, pp. 356–360. IEEE (2006)
3. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
4. Csiszar, I., Korner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**(3), 339–348 (2003)
5. Negi, R., Goel, S.: Secret communication using artificial noise. In: IEEE Vehicular Technology Conference (2005)
6. Yebo, G., Zhilu, W., Yin, Z., et al.: The secrecy capacity optimization artificial noise: a new type of artificial noise for secure communication in MIMO system. IEEE Access **7**, 58353–58360 (2019)
7. Oggier, F., Hassibi, B.: The secrecy capacity of the MIMO wiretap channel. IEEE Trans. Inf. Theory **57**(8), 4961–4972 (2011)
8. Gopala, P.K., Lai, L., El Gamal, H.: On the secrecy capacity of fading channels. IEEE Trans. Inf. Theory **54**(10), 4687–4698 (2008)
9. Mahdavifar, H., Vardy, A.: Achieving the secrecy capacity of wiretap channels using polar codes. IEEE Trans. Inf. Theory **57**(10), 6428–6443 (2011). 1628–1631
10. Khisti, A., Wornell, G.W.: Secure transmission with multiple antennas: the MIMOME channel. IEEE Trans. Inf. Theory (to be published). http://allegro.mit.edu/pubs/posted/journal/2008-khisti-wornell-it.pdf2547-2553
11. Ekrem, E., Ulukus, S.: The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. IEEE Trans. Inf. Theory **57**(4), 2083–2114 (2011)
12. Gao, H., Smith, P.J., Clark, M.V.: Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels. IEEE Trans. Commun. **46**(5), 666–672 (1998)