Ergodic Secrecy Rate of Antenna-Selection-Aided MIMOME Channels with BPSK/QPSK Modulations

Chongjun Ouyang, Student Member, IEEE, Zeliang Ou, Student Member, IEEE, Pei Yang, Student Member, IEEE, Lu Zhang, Student Member, IEEE, Xin Zhang, Member, IEEE, and Hongwen Yang, Member, IEEE

Abstract—This paper analyzes transmit antenna selection (TAS) under Rayleigh flat fading for BPSK/QPSK modulations in multiple-input multiple-output wiretap channels, also termed as multiple-input multiple-output multiple-eavesdropper (MIMOME) channels. In our protocol, a single antenna is selected to transmit the secret message and selection combing (SC) or maximal-ratio combing (MRC) is utilized at the legitimate receiver or the eavesdropper. Novel closed-form expressions for the ergodic secrecy rates are derived to approximate the exact values, which hold high precision and compact forms. Besides theoretical derivations, simulations are provided to demonstrate the feasibility and validity of the proposed formulas.

Index Terms—MIMOME channel, physical layer security, transmit antenna selection, BPSK/QPSK

I. INTRODUCTION

Achievable secrecy rate [1] serves as a significant performance measurement metric in wiretap fading channels, which characterizes the limitation of the transmission security and reliability. Recent developments in transmit-antenna-selection-aided (TAS-aided) multiple-input multiple-output MIMO (MIMOME) systems have heightened the need for analysis of the secrecy transmission rate in multiple-input multiple-output (MIMO) wiretap channels.

The works in [2] analyzed the secrecy outage probability (SOP), the probability when the instantaneous secrecy rate is lower than a preset value, of the multiple-input single-output multiple-eavesdropper (MISOME) channels when single transmit antenna is activated and maximal-ratio combing (MRC) is used at the eavesdropper. Later, Yang et al., in [3] and [4] derived closed-form expressions for the SOP in TAS-aided MIMOME channels with or without the impact of antenna correlation when selection combing (SC) or maximal-ratio combing (MRC) is adopted at the legitimate receiver and the eavesdropper, and these works were further extended to receive generalized selection combining in [5]. Nevertheless, all these aforementioned researches are based on Gaussian inputs assumption, and a more practical scenario, when the inputs are drawn from discrete constellations, has not been investigated in detail. Additionally, most studies in the field of secrecy rate analysis only focused on the SOP, thus they have paid less attention on the ergodic secrecy rate (ESR), which is also an important performance metric in wiretap fading channels.

In this paper, we comprehensively study the ergodic secrecy rate under BPSK/QPSK modulations in TAS-aided MIMOME channels, assuming that the secret messages suffer from Rayleigh flat fading. At the transmitter, a single antenna is activated to maximize the instantaneous Signal to Noise Ratio (SNR) at the receiver. Moreover, selection combing (SC) or maximal-ratio combing (MRC) is utilized at the legitimate receiver and the eavesdropper. Consequently, four scenarios, including SC/SC at the receiver/eavesdropper, SC/MRC at the receiver/eavesdropper, MRC/SC at the receiver/eavesdropper and MRC/MRC at the receiver/eavesdropper, are considered, and corresponding closed-form expressions are developed to approximate the exact ESR, which possess high precision and compact forms. Furthermore, simulation results are offered to confirm our derivations.

II. SYSTEM MODEL

Consider a MIMOME channel, where the transmitter, the legitimate receiver and the eavesdropper are equipped with $N_A$, $N_B$ and $N_E$ antennas, respectively. As stated before, the transmitter selects a single antenna, and the diversity techniques adopted at the legitimate receiver and the eavesdropper possesses four combination modes: 1) SC/SC, 2) SC/MRC, 3) MRC/SC and 4) MRC/MRC, which are also the four classic schemes ever discussed in [6]. Notably, suppose that the fading type is independent identically distributed (i.i.d.) Rayleigh flat fading in both the main and eavesdropper channel. Besides, we assume that the main channel and the eavesdropper channel suffer independent fading.

A. Main Channel

For the main channel with SC, the probability density function (PDF) of the received SNR at the legitimate receiver is given by

$$f_{b}^{\text{SC}} (\gamma_b) = N_A N_B \left(1 - e^{-\frac{\gamma_b}{\gamma}}\right) N_A N_B^{-1} e^{-\frac{\gamma_b}{\gamma}} \frac{1}{\gamma_b}, \quad (1)$$

in which $\gamma_b$ denotes the average per-antenna SNR at the legitimate receiver. Furthermore, for the main channel with MRC, the PDF of the received SNR is expressed as

$$f_{b}^{\text{MRC}} (\gamma_b) = \frac{N_A N_B^{-1} e^{-\frac{\gamma_b}{\gamma}}}{\Gamma (N_B) \gamma^n B} \left(1 - e^{-\frac{\gamma_b}{\gamma}} \sum_{n=0}^{N_B-1} \frac{\gamma_b^n}{n! \gamma_B^n} \right)^{N_A-1}. \quad (2)$$

M. Ouyang, M. Ou, M. Yang, M. Zhang, M. Zhang and M. Yang are with the Wireless Theories and Technologies Lab, Beijing University of Posts and Telecommunications, Beijing, 100876, China (e-mail: {DragonAin, ouzeliang, yp, zhangl_966, zhangxin, yanghong}@bupt.edu.cn)

M. Ouyang, M. Ou, M. Yang, Ms. Zhang, M. Zhang and M. Yang are with the Wireless Theories and Technologies Lab, Beijing University of Posts and Telecommunications, Beijing, 100876, China (e-mail: {DragonAin, ouzeliang, yp, zhangl_966, zhangxin, yanghong}@bupt.edu.cn)
B. Eavesdropper's Channel

For the eavesdropper's channel with SC, the PDF of the received SNR at the eavesdropper is given by

\[ f_{e}^{SC}(\gamma_{e}) = \frac{\gamma_{E}^{N_{E}-1}}{\Gamma(N_{E})} e^{-\frac{\gamma_{E}}{\gamma_{e}}} \]  

(3)

where \( \overline{\gamma}_{e} \) represents the average per-antenna SNR at the eavesdropper. Additionally, for the eavesdropper's channel with MRC, the PDF of the received SNR can be written as

\[ f_{e}^{MRC}(\gamma_{e}) = \frac{\gamma_{E}^{N_{E}-1} e^{-\frac{\gamma_{E}}{\gamma_{e}}}}{\Gamma(N_{E})} \]  

(4)

C. Achievable Secrecy Rate

Since QPSK is the superposition of two orthogonal BPSK modulations, it is sufficient to consider BPSK. Moreover, Shannon formula \( \log_{2}(1 + \text{SNR}) \) can not be used because the input signals do not follow the Gaussian distribution. Assume that the transmitted data stream are i.i.d. zero-mean binary information (MI) in terms of the SNR under BPSK modulation over additive white Gaussian noise (AWGN) channels is formulated as [6]

\[ I(\gamma) = 1 - \int_{-\infty}^{+\infty} \frac{1}{\sqrt{2\pi} \sigma} e^{-\frac{(\gamma - \overline{\gamma})^{2}}{2\sigma^{2}}} d\gamma \]  

(5)

From Equ. (5), the achievable secrecy rate of the wiretap channel with BPSK modulation is given by [1]

\[ C_{s} = I_{s}(\gamma_{b}, \gamma_{e}) = \begin{cases} I(\gamma_{b}) - I(\gamma_{e}) , & \gamma_{b} > \gamma_{e} \\ 0 , & \gamma_{b} \leq \gamma_{e} \end{cases} \]  

(6)

III. Ergodic Secrecy Rate

The ergodic secrecy rate is usually utilized to measure the secrecy performance of the wiretap fading channel, which is formulated as follows:

\[ \overline{C}_{s} = \int_{0}^{+\infty} \int_{\gamma_{e}}^{+\infty} (I(\gamma_{b}) - I(\gamma_{e})) f_{b}(\gamma_{b}) f_{e}(\gamma_{e}) d\gamma_{b} d\gamma_{e} \]

\[ = \int_{0}^{+\infty} \int_{\gamma_{e}}^{+\infty} (I(\gamma_{b}) - I(\gamma_{e})) f_{b}(\gamma_{b}) f_{e}(\gamma_{e}) d\gamma_{b} d\gamma_{e} \]  

(7)

Nevertheless, due to the complexity of the expression for the MI in Equ. (5), the exact value for the ergodic secrecy rate is intractable.

Fortunately, there exists a closed-form approximated formula for the MI, with a compact form, which is written as [7]

\[ I(\gamma) \approx 1 - e^{-\vartheta \gamma} \]  

(8)

where \( \vartheta = 0.6507 \). As \( \gamma \) tending to be 0 or \(+\infty\), \( 1 - e^{-\vartheta \gamma} \) will tend to be 0 or 1, which can accord with practice. Moreover, its approximation precision will be further examined in Section 11 by simulations. On the basis of Equ. (8), the exact secrecy rate can be estimated as

\[ C_{s} = I_{s}(\gamma_{b}, \gamma_{e}) \approx \begin{cases} e^{-\vartheta \gamma_{e}} - e^{-\vartheta \gamma_{b}} , & \gamma_{b} > \gamma_{e} \\ 0 , & \gamma_{b} \leq \gamma_{e} \end{cases} \]  

(9)

A. SC/SC

Lemma 1. The approximated ergodic secrecy rate under the SC/SC mode can be derived as

\[ \overline{C}_{s} \approx \sum_{k=0}^{N_{A}N_{B}-1} \frac{N_{A}N_{B}N_{E}}{\gamma_{e}} \left( \frac{N_{A}N_{B} - 1}{k} \right) \left( \frac{N_{E} - 1}{j} \right) \times \frac{(-1)^{k+j}}{\vartheta + \frac{k+1}{\gamma_{e}} + \frac{k+j}{\gamma_{b}}} \]  

(10)

Proof. Substituting Equ. (9) into Equ. (7), the expression for the approximated ergodic secrecy rate can be developed, that is

\[ \overline{C}_{s} \approx \int_{0}^{+\infty} \int_{\gamma_{e}}^{+\infty} e^{-\vartheta \gamma_{b}} f_{b}(\gamma_{b}) f_{e}(\gamma_{e}) d\gamma_{b} d\gamma_{e} \]

\[ = \int_{0}^{+\infty} \int_{\gamma_{e}}^{+\infty} e^{-\vartheta \gamma_{b}} f_{b}(\gamma_{b}) f_{e}(\gamma_{e}) d\gamma_{b} d\gamma_{e} \]  

(11)

We first look into \( \Psi_{1} \) and apply [8 Equ. (1.111)] for the binomial expansion into Equ. (11) and Equ. (3), then \( \Psi_{1} \) can be written as

\[ \Psi_{1} = \sum_{k=0}^{N_{A}N_{B}-1} \sum_{j=0}^{N_{E}-1} \frac{N_{A}N_{B}N_{E}}{\gamma_{e}} \left( \frac{N_{A}N_{B} - 1}{k} \right) \left( \frac{N_{E} - 1}{j} \right) \times \frac{(-1)^{k+j}}{\vartheta + \frac{k+1}{\gamma_{e}} + \frac{k+j}{\gamma_{b}}} \]  

(12)

in which \( \Psi_{3}(j,k) \) is easy to solve for it only contains exponential functions. Additionally, \( \Psi_{2} \) can also be calculated following the similar steps as \( \Psi_{1} \). Next, substituting \( \Psi_{1} \) and \( \Psi_{2} \) into Equ. (11) and performing some basic mathematical manipulations, the final result in Equ. (10) can be derived. \( \square \)

B. SC/MRC

Lemma 2. The approximated ergodic secrecy rate under the SC/MRC mode can be derived as

\[ \overline{C}_{s} \approx \sum_{k=0}^{N_{A}N_{B}-1} \left( \frac{N_{A}N_{B} - 1}{k} \right) \left( \frac{-1)^{k} N_{A}N_{B}}{\vartheta \gamma_{e} + \gamma_{b}(k+1)} + 1 \right)^{N_{E}} \times \left( \frac{1}{k+1} - \frac{1}{k+1 + \vartheta \gamma_{b}} \right) \]  

(13)
Proof. Substituting Eq. (9) into Eq. (7), the expression for the approximated ergodic secrecy rate can be developed, that is

\[ C_s \approx \int_0^{\infty} \int_{N_e}^{\infty} \left( e^{-\theta_\gamma e} - e^{-\theta_\gamma b} \right) f_b^{SC} (\gamma_b) f_e^{MRC} (\gamma_e) d\gamma_b d\gamma_e \]

\[ = \int_0^{\infty} \int_{N_e}^{\infty} e^{-\theta_\gamma e} f_b^{SC} (\gamma_b) f_e^{MRC} (\gamma_e) d\gamma_b d\gamma_e \]

\[ - \int_0^{\infty} \int_{N_e}^{\infty} e^{-\theta_\gamma b} f_b^{SC} (\gamma_b) f_e^{MRC} (\gamma_e) d\gamma_b d\gamma_e. \]

By continuously using the binomial expansion in [8, Eq. (1.111)], we can calculate \( \Psi_1 \) as

\[ \Psi_1 = \frac{N_A N_B}{\Gamma (N_e) \bar{\gamma}_b \bar{\gamma}_e N_e} \int_0^{\infty} \int_{N_e}^{\infty} e^{-\frac{2}{\gamma_e} - \theta_\gamma e N_e - 1} d\gamma_e \\
\times \int_{N_e}^{\infty} \left( 1 - e^{-\frac{2}{\gamma_b} N_e N_B - b} \right) d\gamma_b \\
= \sum_{k=0}^{N_B N_B - 1} \frac{N_A N_B}{\Gamma (N_e) \bar{\gamma}_b \bar{\gamma}_e N_e} \left( N_A N_B - 1 \right) \frac{\bar{\gamma}_b}{k + 1} \int_0^{\infty} e^{-\left( \frac{1}{\gamma_e} + \frac{k + 1}{\gamma_b} \right) \gamma_e N_e - 1} d\gamma_e, \] 

in which \( \Psi_1 (j, k) \) can be calculated by [8, Eq. (3.326.2)]. Additionally, \( \Psi_2 \) can be also solved similar as \( \Psi_1 \). Next, substituting \( \Psi_1 \) and \( \Psi_2 \) into Eq. (14) and performing some basic mathematical manipulations, the final result in Eq. (13) can be derived.

C. MRC/SC

Lemma 3. The approximated ergodic secrecy rate under the MRC/SC mode can be derived as

\[ \bar{C}_s \approx \sum_{j=0}^{N_e - 1} \left( \frac{N_e - 1}{j} \right) \left( \frac{(-1)^j N_e}{1 + j + \theta_\gamma e} \right) \left( \frac{1}{1 + j + \theta_\gamma e} \right) \]

\[ \times \left[ 1 - \sum_{k=0}^{N_A - 1} \left( \frac{(-1)^k N_A}{\Gamma (N_B)} \right) \left( \frac{N_A - 1}{k} \right) \right] \]

\[ \times \left[ \prod_{\gamma_e=0}^{N_B - 1} \left( i_{\gamma_e - 1} \right) \left( \frac{1}{i_{\gamma_e}} \right) \right] \]

\[ \times \Gamma \left( \theta_{\phi_0 + N_B} \right) \left( \frac{\theta + 1}{\gamma_e} + \frac{k + 1}{\gamma_b} \right)^{\phi_0 + N_B - 1}, \]

where \( \phi_0 = \sum_{\gamma_e=0}^{N_B - 1} i_{\gamma_e}, i_0 = k, \) and \( i_{N_B} = 0. \)

Proof. Substituting Eq. (9) into Eq. (7), the expression for the approximated ergodic secrecy rate can be developed, that is

\[ \bar{C}_s \approx \int_0^{\infty} \int_{N_e}^{\infty} \left( e^{-\theta_\gamma e} - e^{-\theta_\gamma b} \right) f_b^{MRC} (\gamma_b) f_e^{SC} (\gamma_e) d\gamma_b d\gamma_e \]

\[ = \int_0^{\infty} f_b^{MRC} (\gamma_b) \int_0^{\infty} e^{-\theta_\gamma b} f_e^{MRC} (\gamma_e) d\gamma_e \]

\[ - \int_0^{\infty} e^{-\theta_\gamma b} f_b^{MRC} (\gamma_b) \int_0^{\infty} f_e^{SC} (\gamma_e) d\gamma_e. \]
In Eq. (20), \( \Psi_1 \) can be simplified by applying \([8]\) Eq. (1.111) to expand the binomial and \([9]\) Eq. (9)] to expand the resultant polynomial. We then apply \([8]\) Eq. (3.351.1) and \([8]\) Eq. (3.326.2) to solve the resultant integral. Then, \( \Psi_1 \) can be written as

\[
\Psi_1 = \frac{1}{(1 + \theta \gamma_b)^N_B} \left[ 1 - \sum_{j=0}^{N_E-1} \sum_{k=0}^{N_A-1} \frac{(-1)^k N_A}{j!} \Gamma(N_B) \prod_{u=1}^{N_A-1} \left( \sum_{i_u=0}^{i_u-1} \left( \frac{\gamma_b}{1 + \phi_u + \gamma_b + j} \frac{1}{i_u} \left( \frac{1}{u} \right) \right) \right)^{i_u-i_{u+1}} \right] \times \frac{\Gamma(\phi_u + N_B + j)}{\left( \theta + \gamma_b \frac{1}{\gamma_b} \right)^{\phi_u + N_B + j}}.
\]

Later, \( \Psi_2 \) can be solved with the similar method as \( \Psi_1 \). Next, substituting \( \Psi_1 \) and \( \Psi_2 \) into Eq. (20), the final result in Eq. (19) can be derived after some basic manipulations. \( \square \)

IV. SIMULATION

In this part, numerical and simulated results are presented to corroborate the accuracy of our derived results. All these results are based on BPSK, and the simulated results are obtained by Monte-Carlo experiments.

Fig. 1 firstly examines the approximation precision of Eq. (8). The exact and approximated results over AWGN channels are calculated by Eq. (5) and Eq. (8), respectively. As can be seen from Fig. 1, the approximation effect is fantastic for all SNR ranges. Besides, this graph also compares the simulated and approximated ESR in terms of \( \gamma_b \) for selected values of \( \gamma_e \). As Fig. 1 shows, the approximation for SC/SC, MRC/SC, SC/MRC, MRC/MRC can all meet tightly with the simulation. In addition, the ESR cannot tend to be infinity with the increment of \( \gamma_b \), which is due to the constraint of finite-alphabet inputs. Besides, it can be seen from this graph that the ESR is higher for smaller \( \gamma_e \), which suggests the passive effect of the eavesdropper in wiretap channels. Fig. 2a moves to explore the relationship between \( N_A \) and the ESR. As it shows, the larger the \( N_A \), the higher the ESR, demonstrating the security enhancement via transmit antenna selection. As for the approximation precision, the analytical results match well with the simulations. Finally, Fig. 3b provides the simulated and approximated ESR for different values of \( N_B \). As explained earlier, the eavesdropper forces a negative influence on the transmission security, and this can be observed from the above graph where larger \( N_B \) corresponds to lower ESR.

V. CONCLUSION

This paper develops novel closed-form approximate formulas of the ergodic secrecy rate in TAS-aided MIMOME channels under BPSK modulation. Numerical experiments show that our derivations can meet tightly with the empirical results, which suggests that our approximation provides a simple and numerically efficient way to calculate the ESR of the TAS-aided MIMOME channels.

REFERENCES

[1] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, “Wireless information-theoretic security” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, 2008.
[2] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, “Performance of transmit antenna selection physical layer security schemes,” IEEE Signal Process. Lett., vol. 19, no. 6, pp. 372–375, 2012.
[3] N. Yang, P. L. Yoo, M. Elkashlan, R. Schober, and I. B. Collings, “Transmit antenna selection for security enhancement in MIMO wiretap channels,” IEEE Trans. Commun., vol. 61, no. 1, pp. 144-154, 2013.
[4] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, “Physical layer security of TAS/MRC with antenna correlation,” IEEE Trans. Inf. Forensics and Security, vol. 8, no. 1, pp. 254–259, 2013.
[5] N. Yang, P. L. Yoo, M. Elkashlan, R. Schober, and J. Yuan, “MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining,” IEEE Commun. Lett., vol. 17, no. 9, pp. 1754–1757, 2013.
[6] S. G. Wilson, Digital modulation and coding, Prentice-Hall, Inc., 1995.
[7] P. Yang, Y. Wu, L. Jin, and H. Yang, “Sum Capacity for Single-Cell Multi-User Systems with M-Ary Inputs,” Entropy, vol. 19, no. 9, pp. 497, 2017.
[8] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series and Products, 7th ed., Academic, San Diego, CA., 2007.
[9] S. Choi and Y.-C. Ko, “Performance of selection MIMO systems with generalized selection criterion over Nakagami-m fading channels,” 
IEICE Trans. Commun., vol. E89-B, no. 12, pp. 3467–3470, 2006.