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

Chongjun Ouyang, Zeliang Ou, Lu Zhang, Hongwen Yang and Xin Zhang
Wireless Theories and Technologies Lab
Beijing University of Posts and Telecommunications
Beijing, China
{DragonAim, ouzeliang, zhangl_96, yanghong, zhangxin}@bupt.edu.cn

***Abstract*—This paper studies the secrecy performance of multiple-input multiple-output (MIMO) wiretap channels, also termed as multiple-input multiple-output multiple-eavesdropper (MIMOME) channels, under transmit antenna selection (TAS) and BPSK/QPSK modulations. In the main channel between the transmitter and the legitimate receiver, a single transmit antenna is selected to maximizes the instantaneous Signal to Noise Ratio (SNR) at the receiver. At the receiver and the eavesdropper, selection combination (SC) is utilized. By assuming Rayleigh flat fading, we first derive the closed-form approximated expression for the ergodic secrecy rate when the channel state information of the eavesdropper (CSIE) is available at the transmitter. Next, analytical formulas for the approximated and asymptotic secrecy outage probability (SOP) are also developed when CSIE is unavailable. Besides theoretical derivations, simulation results are provided to demonstrate the approximation precision of the derived results. Furthermore, the asymptotic results reveal that the secrecy diversity order degrades into 0 due to the finite-alphabet inputs, which is totally different from that driven by the Gaussian inputs.**

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

I. Introduction

Physical layer (PHY) security has become a pivotal and pervasive concern in wireless communications due to its remarkable performance in information security enhancement. Different from the traditional cryptographic techniques [1], physical layer security utilizes the inherent characteristics of wireless channels to ensure reliable transmission. In recent years, there has been an increasing interest in multiple-input multiple-output (MIMO) wiretap channels, also referred to as multiple-input multiple-output multiple-eavesdropper (MIMOME) channels, where multiple antennas are deployed at the transmitter, the legitimate receiver and the eavesdropper.

The secrecy capacity of MIMOME channels has been investigated in [2], [3] from an information-theoretic perspective. Later, theses works were further extended to large-scale systems in [4] to declare the significant improvements of transmission security and reliability in massive MIMOME channels compared to the small-scale one. Nevertheless, the deployment of multiple antennas will result in high hardware cost since each antenna should be connected with an expensive Radio-Frequency (RF) chain. To settle this challenge, antenna selection (AS) [5] can be applied into the MIMO wiretap channels, which can alleviate the requirement on RF chains by selecting a subset of antennas to transceive signals.

In the past years, many researches on antenna-selection-aided MIMOME channels were presented [6]–[10]. For example, Yang *et al.*, in [6] and [7] derived closed-form expressions for the secrecy outage probability (SOP) in MIMOME channels under transmit antenna selection (TAS) with or without the impact of antenna correlation, respectively. Zhu *et al.*, in [8] studied the probability of zero secrecy capacity for two TAS schemes depending on the availability of the eavesdropper's channel state information (CSI). Later, the achievable secrecy performance of MIMO wiretap channels in the presence of imperfect CSI was analyzed in [9]. In contrast to the explicit analysis in [6]–[9], Asaad *et al.*, in [10] proposed asymptotically approximated results for both the average secrecy rate and the SOP in the limit of large-scale MIMOME systems under the norm-based TAS protocol. However, all these aforementioned works focused on the Gaussian input assumption. In fact, an important scenario which is necessary to be investigated when moving towards a practical implementation is the case where the channel inputs are constrained by finite constellation size.

Motivated by this, the works in [11] and [12] firstly studied the impacts of standard constellations on the achievable secrecy rates of Gaussian wiretap channels. Recently, most literatures about the MIMOME channels driven by finite-alphabet inputs focused on optimal precoding schemes [13], [14], artificial noise (AN) design [15], [16] or the joint precoding and AN design [17], while previous studies have not yet treated the TAS-aided MIMOME channels with finite-alphabet inputs in detail. Consequently, there is an urgent need to address the secrecy performance in TAS-aided MIMOME channels with inputs drawn form discrete constellations.

This paper detailedly analyzed the secrecy performance for MIMOME channels with transmit antenna selection and finite-alphabet inputs. To the best of our knowledge, this is the first time to propose a comprehensive theoretical analysis for the TAS-aided MIMOME channels with finite-alphabet inputs. For simplicity, assume that the modulation mode is BPSK/QPSK and the channel side information of the legitimate receiver (CSIL) is available at the transmitter. Closed-form approximated expressions for the ergodic secrecy rate and secrecy outage probability are respectively formulated in

two scenarios: 1) For Scenario A: the eavesdropper's channel side information is unavailable at the transmitter (NCSIE), and 2) For Scenario B: the eavesdropper's channel side information (CSIE) is available. In each scenario, the derivations meet accurately the results given via numerical simulations. Finally, we set the Signal to Noise Ratio (SNR) of the main channel to infinity and derive the asymptotic secrecy outage probability. On the basis of the asymptotic SOP, we demonstrate that the secrecy diversity order [6] for the finite-alphabet inputs is totally different with that driven by Gaussian inputs due to the constraint imposed by the discrete signaling inputs.

The remaining parts of this manuscript is structured as follows: Section II describes the system model. In Section III, the ergodic secrecy rate and secrecy outage probability of the MIMOME channel are investigated. The simulation results and corresponding analysis are shown in Section IV. Finally, Section V concludes the paper.

II. System Model

In this paper, we consider a MIMO wiretap channel, where the transmitter, the legitimate receiver and the eavesdropper are equipped with $N_{\rm A}$, $N_{\rm B}$ and $N_{\rm E}$ antennas, respectively. Let $\mathbf{H}_{\rm B}$ and $\mathbf{H}_{\rm E}$ denote the main channel and the eavesdropper's channel, both of which are suffering independent and identical distributed (i.i.d.) Rayleigh flat fading with Gaussian noise. For the sake of brevity, suppose that the elements in the channel matrix $\mathbf{H}_{\rm B} \in \mathbb{C}^{N_{\rm B}\times N_{\rm A}}$ and $\mathbf{H}_{\rm E} \in \mathbb{C}^{N_{\rm E}\times N_{\rm A}}$ are i.i.d. complex Gaussian random variables following $\mathcal{CN}(0,1)$.

Then, consider single antenna selection at the transmitter and selection combination (SC) at the legitimate receiver, which is a typical scenario declared in [6]. As a result, a single transmit/receive antenna pair between the transmitter and the legitimate receiver is selected to maximize the instantaneous SNR at the legitimate receiver. Consequently, the index of the selected antenna at the transmitter is given by

$$\beta^* = \underset{1\le\alpha\le N_{\rm B},1\le\beta\le N_{\rm A}}{\operatorname{argmax}} |h_{{\rm B},\alpha,\beta}|, \tag{1}$$

where $h_{{\rm B},\alpha,\beta}$ represents the element in $\mathbf{H}_{\rm B}$ located in the α-th row and β-th line. Therefore, the magnitude of the main channel is $|f_{\rm AB}| = \max_{1\le\alpha\le N_{\rm B}} |h_{{\rm B},\alpha,\beta^*}|$. Furthermore, we assume that the eavesdropper also performs the SC to receive the secret message, thus the magnitude of the eavesdropper's channel is given by $|f_{\rm AE}| = \max_{1\le\xi\le N_{\rm E}} |h_{{\rm E},\xi,\beta^*}|$, where $h_{{\rm E},\xi,\beta}$ represents the element in $\mathbf{H}_{\rm E}$.

A. Main channel

After the antenna selection and SC, the received signal at the legitimate receiver can be written as

$$y_{\rm B} = \sqrt{\bar{\gamma}_{\rm b}} f_{\rm AB} x + n_{\rm B}, \tag{2}$$

where x is the transmitted symbol constrained by finite alphabet with unit power, such as BPSK, $\bar{\gamma}_{\rm b}$ is the average per-antenna SNR of the main channel and $n_{\rm B} \in \mathcal{CN}(0,1)$ is the additive white Gaussian noise (AWGN). Let $\gamma_{\rm b}$ denote the instantaneous SNR at the legitimate receiver, then its probability density function (PDF) is given by

$$f_{\rm b}(\gamma_{\rm b}) = N_{\rm A} N_{\rm B} \left(1 - {\rm e}^{-\frac{\gamma_{\rm b}}{\bar{\gamma}_{\rm b}}}\right)^{N_{\rm A}N_{\rm B}-1} {\rm e}^{-\frac{\gamma_{\rm b}}{\bar{\gamma}_{\rm b}}} \frac{1}{\bar{\gamma}_{\rm b}}. \tag{3}$$

B. Eavesdropper's channel

The received signal at the eavesdropper is written as

$$y_{\rm E} = \sqrt{\bar{\gamma}_{\rm e}} f_{\rm AE} x + n_{\rm E}, \tag{4}$$

where $\bar{\gamma}_{\rm e}$ is the average per-antenna SNR of the eavesdropper's channel and $n_{\rm E} \in \mathcal{CN}(0,1)$ is the additive complex Gaussian noise. Since the eavesdropper only utilizes the antenna corresponding to the largest SNR, the PDF of the instantaneous SNR $\gamma_{\rm e}$ is

$$f_{\rm e}(\gamma_{\rm e}) = N_{\rm E} \left(1 - {\rm e}^{-\frac{\gamma_{\rm e}}{\bar{\gamma}_{\rm e}}}\right)^{N_{\rm E}-1} {\rm e}^{-\frac{\gamma_{\rm e}}{\bar{\gamma}_{\rm e}}} \frac{1}{\bar{\gamma}_{\rm e}}. \tag{5}$$

C. Achievable Secrecy Rate

Since QPSK is the superposition of two orthogonal BPSK modulations, it is sufficient to consider BPSK. Moreover, Shannon formula $\log_2(1+{\rm SNR})$ can not be used for the input signals do not follow the Gaussian distribution. Assume that the transmitted data stream are i.i.d. zero-mean binary symbols with equal probabilities, the input-output mutual information (MI) in terms of the SNR γ under BPSK modulation over AWGN channels is formulated as [19]

$$\mathcal{I}(\gamma) = 1 - \int_{-\infty}^{+\infty} \frac{1}{\sqrt{2\pi}} {\rm e}^{-\frac{u^2}{2}} \log_2\left(1 + {\rm e}^{-2\sqrt{\gamma}u - 2\gamma}\right) {\rm d}u, \tag{6}$$

Therefore, the achievable secrecy rate of the wiretap channel with BPSK modulation is given by [20]

$$C_{\rm s} = \mathcal{I}_{\rm s}(\gamma_{\rm b},\gamma_{\rm e}) = \begin{cases} \mathcal{I}(\gamma_{\rm b}) - \mathcal{I}(\gamma_{\rm e}), & \gamma_{\rm b} > \gamma_{\rm e} \\ 0, & \gamma_{\rm b} \le \gamma_{\rm e} \end{cases} \tag{7}$$

III. Secrecy Performance Analysis

This section will investigate the secrecy performance of the MIMOME channel under TAS in detail. In the followings, consider two scenarios stated before depending on whether the CSIE is available or not, and propose corresponding performance measurement metric for these cases respectively.

A. CSIE

When the CSIE is available, the ergodic secrecy rate, is usually utilized to measure the secrecy performance of the wiretap channel [20], which is formulated as follows:

$$\begin{aligned} \bar{C}_{\rm s} =& \mathbb{E}\left[\mathcal{I}_{\rm s}(\gamma_{\rm b},\gamma_{\rm e})\right] \\ =& \int_0^{+\infty}\int_0^{+\infty} \mathcal{I}_{\rm s}(\gamma_{\rm b},\gamma_{\rm e}) f_{\rm b}(\gamma_{\rm b}) f_{\rm e}(\gamma_{\rm e}) {\rm d}\gamma_{\rm b}{\rm d}\gamma_{\rm e} \\ =& \int_0^{+\infty}\int_{\gamma_{\rm e}}^{+\infty} \left(\mathcal{I}(\gamma_{\rm b}) - \mathcal{I}(\gamma_{\rm e})\right) f_{\rm b}(\gamma_{\rm b}) f_{\rm e}(\gamma_{\rm e}) {\rm d}\gamma_{\rm b}{\rm d}\gamma_{\rm e}. \end{aligned} \tag{8}$$

Nevertheless, due to the complexity of the expression for the MI in Equ. (6), the exact value for the ergodic secrecy rate is hard to calculate. Fortunately, there exists a closed-form

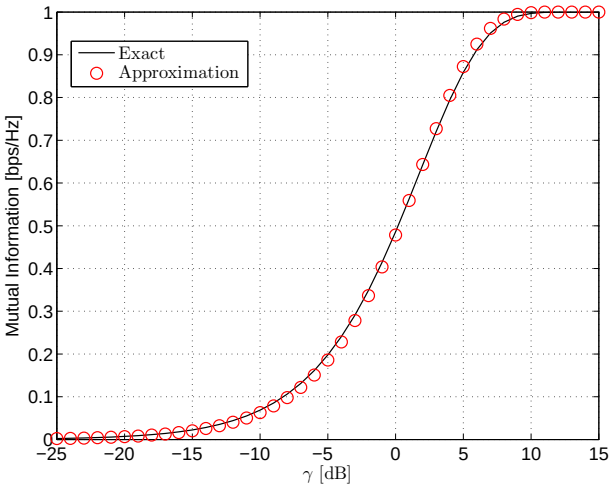


Fig. 1. Comparison of exact and approximated MI of BPSK. The exact and approximated results are calculated by Equ. (6) and Equ. (9), respectively.

approximated formula for the MI, with a compact form, which is written as:

$$\mathcal{I}(\gamma) \approx 1 - \mathrm{e}^{-\phi\gamma}, \tag{9}$$

where $\phi = 0.6507$. To examine the approximation precision of Equ. (9), Fig. 1 compares the exact and approximated input-ouput MI of BPSK in terms of the SNR. As can be seen from this figure, the approximation effect is fantastic for all SNR ranges. Additionally, as γ tending to be 0 or $+\infty$, $\left(1-\mathrm{e}^{-\phi\gamma}\right)$ will tend to be 0 or 1, which can accord with practice. In summary, these facts indicate that it is accurate enough to estimate the exact secrecy rate using this formula, which is given by

$$C_{\mathrm{s}} = \mathcal{I}_{\mathrm{s}}(\gamma_{\mathrm{b}}, \gamma_{\mathrm{e}}) \approx \begin{cases} \mathrm{e}^{-\phi\gamma_{\mathrm{e}}} - \mathrm{e}^{-\phi\gamma_{\mathrm{b}}}, & \gamma_{\mathrm{b}} > \gamma_{\mathrm{e}} \\ 0, & \gamma_{\mathrm{b}} \le \gamma_{\mathrm{e}}. \end{cases} \tag{10}$$

Substituting Equ. (10) into Equ. (8), the expression for the approximated ergodic secrecy rate can be developed, that is

$$\begin{aligned} \bar{C}_{\mathrm{s}} &\approx \int_0^{+\infty}\int_{\gamma_{\mathrm{e}}}^{+\infty} \left(\mathrm{e}^{-\phi\gamma_{\mathrm{e}}} - \mathrm{e}^{-\phi\gamma_{\mathrm{b}}}\right) f_{\mathrm{b}}(\gamma_{\mathrm{b}}) f_{\mathrm{e}}(\gamma_{\mathrm{e}}) \mathrm{d}\gamma_{\mathrm{b}}\mathrm{d}\gamma_{\mathrm{e}} \\ &= \underbrace{\int_0^{+\infty}\int_{\gamma_{\mathrm{e}}}^{+\infty} \mathrm{e}^{-\phi\gamma_{\mathrm{e}}} f_{\mathrm{b}}(\gamma_{\mathrm{b}}) f_{\mathrm{e}}(\gamma_{\mathrm{e}}) \mathrm{d}\gamma_{\mathrm{b}}\mathrm{d}\gamma_{\mathrm{e}}}_{\Psi_1} \\ &\quad - \underbrace{\int_0^{+\infty}\int_{\gamma_{\mathrm{e}}}^{+\infty} \mathrm{e}^{-\phi\gamma_{\mathrm{b}}} f_{\mathrm{b}}(\gamma_{\mathrm{b}}) f_{\mathrm{e}}(\gamma_{\mathrm{e}}) \mathrm{d}\gamma_{\mathrm{b}}\mathrm{d}\gamma_{\mathrm{e}}}_{\Psi_2}. \end{aligned} \tag{11}$$

Using Equ. (3) and Equ. (5), the approximated ergodic secrecy rate can be derived as

$$\begin{aligned} \bar{C}_{\mathrm{s}} \approx & \sum_{k=0}^{N_{\mathrm{A}}N_{\mathrm{B}}-1}\sum_{j=0}^{N_{\mathrm{E}}-1} \frac{N_{\mathrm{A}}N_{\mathrm{B}}N_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{e}}} \binom{N_{\mathrm{A}}N_{\mathrm{B}}-1}{k} \binom{N_{\mathrm{E}}-1}{j} \\ & \times \frac{(-1)^{k+j}}{\phi + \frac{j+1}{\bar{\gamma}_{\mathrm{e}}} + \frac{k+1}{\bar{\gamma}_{\mathrm{b}}}} \left(\frac{1}{k+1} - \frac{1}{k+1+\phi\bar{\gamma}_{\mathrm{b}}}\right). \end{aligned} \tag{12}$$

We first look into Ψ_1 and apply [21, Equ. (1.111)] for the binomial expansion into Equ. (3) and Equ. (5), then Ψ_1 can be written as

$$\begin{aligned} \Psi_1 =& \frac{N_{\mathrm{A}}N_{\mathrm{B}}N_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{b}}\bar{\gamma}_{\mathrm{e}}} \int_0^{+\infty} \left(1-\mathrm{e}^{-\frac{\gamma_{\mathrm{e}}}{\bar{\gamma}_{\mathrm{e}}}}\right)^{N_{\mathrm{E}}-1} \mathrm{e}^{-\frac{\gamma_{\mathrm{e}}}{\bar{\gamma}_{\mathrm{e}}}} \mathrm{e}^{-\phi\gamma_{\mathrm{e}}} \mathrm{d}\gamma_{\mathrm{e}} \\ & \times \int_{\gamma_{\mathrm{e}}}^{+\infty} \left(1-\mathrm{e}^{-\frac{\gamma_{\mathrm{b}}}{\bar{\gamma}_{\mathrm{b}}}}\right)^{N_{\mathrm{A}}N_{\mathrm{B}}-1} \mathrm{e}^{-\frac{\gamma_{\mathrm{b}}}{\bar{\gamma}_{\mathrm{b}}}} \mathrm{d}\gamma_{\mathrm{b}} \\ =& \sum_{k=0}^{N_{\mathrm{A}}N_{\mathrm{B}}-1}\sum_{j=0}^{N_{\mathrm{E}}-1} \frac{N_{\mathrm{A}}N_{\mathrm{B}}N_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{b}}\bar{\gamma}_{\mathrm{e}}} \binom{N_{\mathrm{A}}N_{\mathrm{B}}-1}{k} \binom{N_{\mathrm{E}}-1}{j} \\ & \times \underbrace{\int_0^{+\infty} \mathrm{e}^{-\left(\phi+\frac{j+1}{\bar{\gamma}_{\mathrm{e}}}\right)\gamma_{\mathrm{e}}} \mathrm{d}\gamma_{\mathrm{e}} \int_{\gamma_{\mathrm{e}}}^{+\infty} \mathrm{e}^{-\left(\frac{j+1}{\bar{\gamma}_{\mathrm{b}}}\right)\gamma_{\mathrm{b}}} \mathrm{d}\gamma_{\mathrm{b}}}_{\Psi_3(j,k)}, \end{aligned} \tag{13}$$

in which $\Psi_3(j,k)$ is easy to solve for it only contains exponential functions. On the other hand, Ψ_2 can be also calculated following the similar steps as Ψ_1. Next, substituting Ψ_1 and Ψ_2 into Equ. (11) and performing some basic mathematical manipulations, the final result in Equ. (12) can be derived.

This subsection has detailedly investigated the scenario when CSIE is available at the transmitter and the approximated closed-form expression for the ergodic secrecy rate is derived. The next subsection, therefore, moves on to discuss the situation when the transmitter knows nothing about the CSIE.

B. NCSIE

When the CSI of the eavesdropper is unknown at the transmitter, the secrecy rate defined in Equ. (7) is not achievable [20]. Under this circumstance, the secrecy performance is usually measured by the secrecy outage probability (SOP), which is defined as

$$P_{\mathrm{out}}(R_{\mathrm{s}}) = \Pr(C_{\mathrm{s}} < R_{\mathrm{s}}), \tag{14}$$

where $R_{\mathrm{s}} \ge 0$ represents the preset secrecy rate. According to the definition of SOP, it is clear that SOP denotes the probability that the achievable secrecy rate is less than a predetermined secrecy transmission rate, below which secure transmission is not guaranteed.

1) Probability of non-zero secrecy: Before explaining the general SOP (for $R_{\mathrm{s}} > 0$), we first examine the condition of positive secrecy rate i.e., the probability of taking positive values for the secrecy rate C_{s}. On the basis of Equ. (7) and Equ. (14), the probability of non-zero secrecy rate is formulated as

$$\begin{aligned} \Pr(C_{\mathrm{s}} > 0) &= 1 - P_{\mathrm{out}}(0) = \Pr(\gamma_{\mathrm{b}} > \gamma_{\mathrm{e}}) \\ &= \int_0^{+\infty}\int_{\gamma_{\mathrm{e}}}^{+\infty} f_{\mathrm{b}}(\gamma_{\mathrm{b}}) f_{\mathrm{e}}(\gamma_{\mathrm{e}}) \mathrm{d}\gamma_{\mathrm{b}}\mathrm{d}\gamma_{\mathrm{e}}. \end{aligned} \tag{15}$$

By substituting Equ. (3) and Equ. (5) into Equ. (15) and calculating the resultant integrals on the basis of [21, Equ.

(3.432.1)], the closed-form expression for the probability of positive secrecy rate can be obtained, namely

$$\Pr\left(C_{\mathrm{s}}>0\right)=\sum_{k=0}^{N_{\mathrm{A}}N_{\mathrm{B}}-1}\sum_{j=0}^{N_{\mathrm{E}}-1}\frac{(-1)^{k+j}}{(k+1)\,\bar{\gamma}_{\mathrm{e}}}\frac{N_{\mathrm{A}}N_{\mathrm{B}}N_{\mathrm{E}}}{\frac{j+1}{\bar{\gamma}_{\mathrm{e}}}+\frac{k+1}{\bar{\gamma}_{\mathrm{b}}}}\times\binom{N_{\mathrm{A}}N_{\mathrm{B}}-1}{k}\binom{N_{\mathrm{E}}-1}{j}. \tag{16}$$

2) General secrecy outage probability: On the basis of the definition of the secrecy rate and the secrecy outage probability, the expression of the SOP is given by

$$\begin{aligned}P_{\mathrm{out}}\left(R_{\mathrm{s}}\right)=&\Pr\left(C_{\mathrm{s}}<R_{\mathrm{s}}|\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)\Pr\left(\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)\\&+\Pr\left(C_{\mathrm{s}}<R_{\mathrm{s}}|\gamma_{\mathrm{b}}<\gamma_{\mathrm{e}}\right)\Pr\left(\gamma_{\mathrm{b}}<\gamma_{\mathrm{e}}\right).\end{aligned} \tag{17}$$

By Equ. (7), C_{s} is 0 when $\gamma_{\mathrm{b}}<\gamma_{\mathrm{e}}$; on the other hand, the preset R_{s} is positive, thus $\Pr\left(C_{\mathrm{s}}<R_{\mathrm{s}}|\gamma_{\mathrm{b}}<\gamma_{\mathrm{e}}\right)$ equals to 1. As a result, the SOP can be simplified as

$$\begin{aligned}P_{\mathrm{out}}\left(R_{\mathrm{s}}\right)=&\Pr\left(C_{\mathrm{s}}<R_{\mathrm{s}}|\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)\\&\times\Pr\left(\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)+\Pr\left(\gamma_{\mathrm{b}}<\gamma_{\mathrm{e}}\right).\end{aligned} \tag{18}$$

In Equ. (18), the final results for both $\Pr\left(\gamma_{\mathrm{b}}<\gamma_{\mathrm{e}}\right)$ and $\Pr\left(\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)$ can be directly obtained using Equ. (16). Next, let us turn to the term $\Pr\left(C_{\mathrm{s}}<R_{\mathrm{s}}|\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)$. On the basis of [20], $\Pr\left(C_{\mathrm{s}}<R_{\mathrm{s}}|\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)$ can be expressed as

$$\begin{aligned}&\Pr\left(C_{\mathrm{s}}<R_{\mathrm{s}}|\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)\\=&\frac{1}{\Theta}\int_{0}^{+\infty}\int_{\gamma_{\mathrm{e}}}^{\mathcal{I}^{-1}(R_{\mathrm{s}}+\mathcal{I}(\gamma_{\mathrm{e}}))}f_{\mathrm{b}}\left(\gamma_{\mathrm{b}}\right)f_{\mathrm{e}}\left(\gamma_{\mathrm{e}}\right)\mathrm{d}\gamma_{\mathrm{b}}\mathrm{d}\gamma_{\mathrm{e}}\\=&\frac{1}{\Theta}\underbrace{\int_{0}^{+\infty}\int_{0}^{\mathcal{I}^{-1}(R_{\mathrm{s}}+\mathcal{I}(\gamma_{\mathrm{e}}))}f_{\mathrm{b}}\left(\gamma_{\mathrm{b}}\right)f_{\mathrm{e}}\left(\gamma_{\mathrm{e}}\right)\mathrm{d}\gamma_{\mathrm{b}}\mathrm{d}\gamma_{\mathrm{e}}}_{\Psi_4}\\&-\frac{1}{\Theta}\underbrace{\int_{0}^{+\infty}\int_{0}^{\gamma_{\mathrm{e}}}f_{\mathrm{b}}\left(\gamma_{\mathrm{b}}\right)f_{\mathrm{e}}\left(\gamma_{\mathrm{e}}\right)\mathrm{d}\gamma_{\mathrm{b}}\mathrm{d}\gamma_{\mathrm{e}}}_{\Psi_5},\end{aligned} \tag{19}$$

where $\Theta=\Pr\left(\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)$ and $\mathcal{I}^{-1}\left(\cdot\right)$ denotes the inverse function of $\mathcal{I}\left(\cdot\right)$. Note that $\Psi_5=1-\Pr\left(\gamma_{\mathrm{b}}>\gamma_{\mathrm{e}}\right)$ which can be simply solved by Equ. (16). As for Ψ_4, the approximated formula $\left(1-\mathrm{e}^{-\phi\gamma}\right)$ can be utilized to simplify its calculation, since the inverse function of $\mathcal{I}\left(\gamma\right)$ is difficult to derive. Consequently,

$$\Psi_4\approx\int_{0}^{+\infty}\int_{0}^{-\ln\left(\mathrm{e}^{-\phi\gamma_{\mathrm{e}}}-R_{\mathrm{s}}\right)/\phi}f_{\mathrm{b}}\left(\gamma_{\mathrm{b}}\right)f_{\mathrm{e}}\left(\gamma_{\mathrm{e}}\right)\mathrm{d}\gamma_{\mathrm{b}}\mathrm{d}\gamma_{\mathrm{e}} \tag{20}$$

We substitute Equ. (3) and Equ. (5) into Equ. (20) and expand the PDF by the binomial expansion. After some lines of derivation, the approximated result for Ψ_4 is given by

$$\begin{aligned}&\Psi_4\approx\\&1-\sum_{k=0}^{N_{\mathrm{A}}N_{\mathrm{B}}-1}\sum_{j=0}^{N_{\mathrm{E}}-1}\frac{(-1)^{k+j}}{k+1}\frac{N_{\mathrm{A}}N_{\mathrm{B}}N_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{e}}\phi}\binom{N_{\mathrm{A}}N_{\mathrm{B}}-1}{k}\\&\times\binom{N_{\mathrm{E}}-1}{j}\left(-R_{\mathrm{s}}\right)^{v_k}\mathrm{B}\left(u_j,1\right){}_2F_1\left(-v_k,u_j;u_j+1;\frac{1}{R_{\mathrm{s}}}\right),\end{aligned} \tag{21}$$

in which $v_k=\frac{1+k}{\bar{\gamma}_{\mathrm{b}}\phi}$ and $u_j=\frac{1+j}{\bar{\gamma}_{\mathrm{e}}\phi}$. Besides, $\mathrm{B}\left(\cdot,\cdot\right)$ and ${}_2F_1\left(\cdot,\cdot;\cdot;\cdot\right)$ denote the Beta function [21, Equ. (8.380)] and Gauss hypergeometric function [21, Equ. (9.100)], respectively. Afterwards, substituting the results of Ψ_4 and Ψ_5 into Equ. (19) and performing some mathematical manipulations, the approximated expression of the SOP can be obtained, which is exhibited on the top of next page.

Let R_{s} and $\bar{\gamma}_{\mathrm{e}}$ be fixed, and the secrecy outage probability will tend to be 0 as $\bar{\gamma}_{\mathrm{b}}\to+\infty$ when the input signals follow Gaussian distribution [6], for the channel capacity of the main channel can increase monotonically without any limitation. In contrast with the Gaussian inputs, the maximal input-output MI of the main channel is a constant for the digital-modulation systems due to the constraint of finite constellation size. Next, we still take BPSK as an example and evaluate the asymptotic SOP when $\bar{\gamma}_{\mathrm{b}}\to+\infty$. By Equ. (6), the MI for the main channel will tend to be 1 as $\bar{\gamma}_{\mathrm{b}}$ rises up, thus the asymptotic SOP can be written as

$$\begin{aligned}\mathrm{P}_{\mathrm{out}}^{\infty}\left(R_{\mathrm{s}}\right)&=\Pr\left(1-\mathcal{I}\left(\gamma_{\mathrm{e}}\right)<R_{\mathrm{s}}\right)=\Pr\left(\gamma_{\mathrm{e}}>\mathcal{I}^{-1}\left(1-R_{\mathrm{s}}\right)\right)\\&=1-\left(1-\mathrm{e}^{-\frac{\mathcal{I}^{-1}(1-R_{\mathrm{s}})}{\bar{\gamma}_{\mathrm{e}}}}\right)^{N_{\mathrm{E}}}.\end{aligned} \tag{23}$$

Since $\mathcal{I}^{-1}\left(\cdot\right)$ is hard to solve, the approximated expression $\left(1-\mathrm{e}^{-\phi\gamma}\right)$ can be used to approximate the final result, thus the asymptotic SOP can be estimated as

$$\mathrm{P}_{\mathrm{out}}^{\infty}\left(R_{\mathrm{s}}\right)\approx1-\left(1-R_{\mathrm{s}}^{\frac{1}{0.6507\bar{\gamma}_{\mathrm{e}}}}\right)^{N_{\mathrm{E}}}. \tag{24}$$

As can be seen from Equ. (24), $\bar{\gamma}_{\mathrm{b}}$, N_{A} and N_{B} have no impact on the the asymptotic SOP. Nevertheless, on the basis of [6], the asymptotic SOP for Gaussian inputs when $\bar{\gamma}_{\mathrm{b}}\to+\infty$ is

$$\mathrm{P}_{\mathrm{out}}^{\infty}\left(R_{\mathrm{s}}\right)=\left(A\bar{\gamma}_{\mathrm{b}}\right)^{-G}+o\left(\bar{\gamma}_{\mathrm{b}}^{-G}\right), \tag{25}$$

where A is only related with $\bar{\gamma}_{\mathrm{e}}$ and N_{E}, $o\left(\cdot\right)$ denotes higher order terms and $G=N_{\mathrm{A}}N_{\mathrm{B}}$. According to [6], G is termed as secrecy diversity order, which represents the slope of the SOP curve. On the basis of our asymptotic result, the secrecy diversity order for finite-alphabet inputs has degraded from $N_{\mathrm{A}}N_{\mathrm{B}}$ into 0 for $\mathrm{P}_{\mathrm{out}}^{\infty}\left(R_{\mathrm{s}}\right)$ is irrelevant to $\bar{\gamma}_{\mathrm{b}}$, which is totally different from the scenario of Gaussian inputs. It is clear that the maximal MI for the main channel is a constant related with the modulation modes, which has nothing to do with $\bar{\gamma}_b$ due to the limitation of finite constellation size. And this is just the reason why $\mathrm{P}_{\mathrm{out}}^{\infty}\left(R_{\mathrm{s}}\right)$ is unaffected by $\bar{\gamma}_b$, causing the secrecy diversity order to be 0.

IV. Simulation Results

In this section, numerical and simulation results derived in the preceding sections are given. As stated before, there is no closed-form expression for the ergodic secrecy rate, thus Monte-Carlo simulations with a large number of trials are utilized to approach the exact value, which will be used to examine the feasibility and validity of the former derivations.

Let us fix $N_{\mathrm{B}}=3$, $N_{\mathrm{E}}=2$ and increase N_{A} from 1 to 16. Besides, the average SNR at the eavesdropper is set

$$\Pr\left(C_{\rm s} < R_{\rm s}\right) \approx 1 - \sum_{k=0}^{N_{\rm A}N_{\rm B}-1} \sum_{j=0}^{N_{\rm E}-1} \frac{(-1)^{k+j+v_k}}{k+1} \frac{N_{\rm A}N_{\rm B}N_{\rm E}}{\bar{\gamma}_{\rm e}\phi} \binom{N_{\rm A}N_{\rm B}-1}{k} \binom{N_{\rm E}-1}{j} R_{\rm s}^{v_k} {\rm B}\left(u_j, 1\right) {}_2F_1\left(-v_k, u_j; u_j+1; \frac{1}{R_{\rm s}}\right) \tag{22}$$

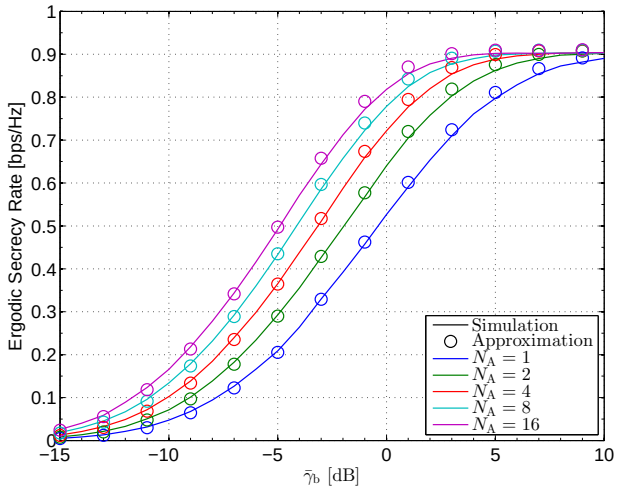


Fig. 2. Simulated and approximated (○) ergodic secrecy capacity versus $\bar{\gamma}_{\rm b}$ for $N_{\rm B}=3$, $N_{\rm E}=2$ and $\bar{\gamma}_{\rm e}=-10$ dB.

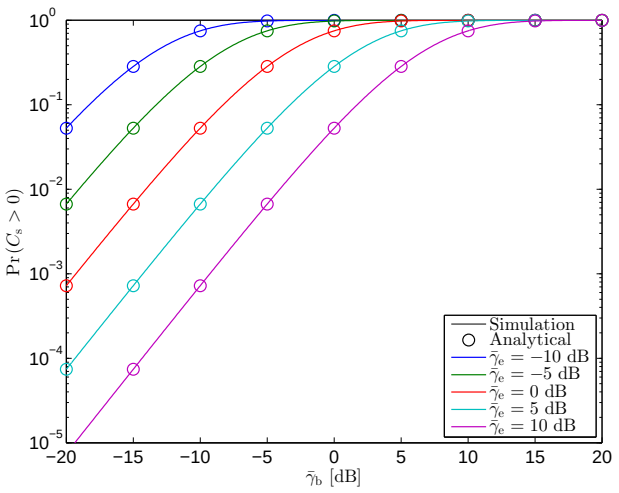
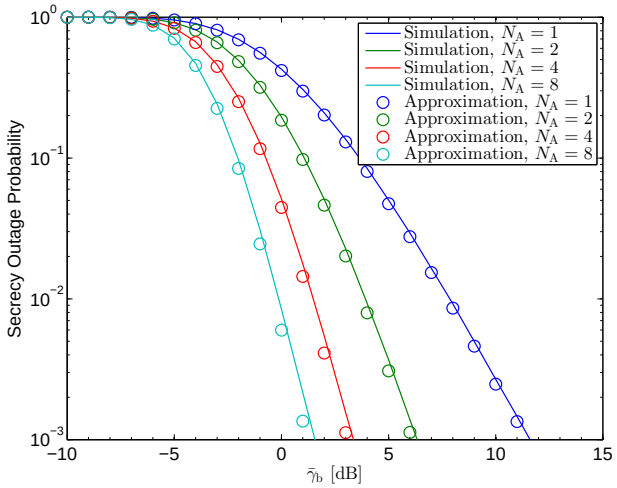
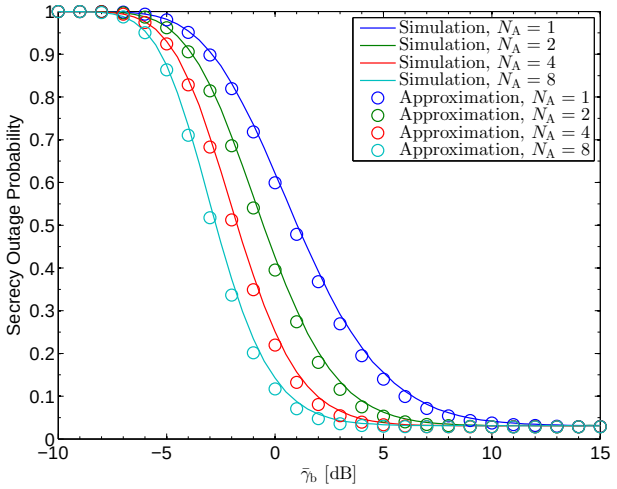


Fig. 3. Simulated and analytical probability of non-zero secrecy capacity versus $\bar{\gamma}_{\rm b}$ for $N_{\rm A}=3$, $N_{\rm B}=N_{\rm E}=2$.



(a) $R_{\rm s}=0.5$ bps/Hz, $\bar{\gamma}_{\rm e}=-10$ dB



(b) $R_{\rm s}=0.5$ bps/Hz, $\bar{\gamma}_{\rm e}=-6$ dB

Fig. 4. Simulated and approximated secrecy outage secrecy versus $\bar{\gamma}_{\rm b}$ for $N_{\rm B}=3$, $N_{\rm E}=2$.

to be $\bar{\gamma}_{\rm e}=-10$ dB as $\bar{\gamma}_{\rm b}$ ranges between -15 dB and 10 dB. Fig. 2 presents the results of simulated and approximated ergodic secrecy rate, obtained by Monte-Carlo experiments and Equ. (12) respectively. As shown in Fig. 2, the curves denoting the simulated results nearly coincide with the circles denoting the approximated results, which suggests that the former derivation about the ergodic secrecy rate in Section III-A is correct. In addition, the coincidence of the curves also indicates that the approximated formula of the MI for BPSK serves as a efficient tool that can be utilized to simplify some derivations. Finally, comparing the curves for different $N_{\rm A}$, it can be observed that the larger the $N_{\rm A}$, the more secrecy transmission rate the antenna selection system can achieve even though the total number of the RF chains is fixed.

Next, let us turn to the scenario when the CSI of the eavesdropper is unavailable at the transmitter. In the following part, the simulation and numerical results for the probability of non-zero secrecy rate will be presented first, then we will turn to the secrecy outage probability. Fig. 3 compares the simulated and analytical probability of non-zero secrecy rate versus $\bar{\gamma}_{\rm b}$. The analytical results are calculated by Equ. (16) and the simulated results are obtained by Monte-Carlo experiments. To approach the exact probability of non-zero secrecy rate, the Monte-Carlo experiments consist of 10^7 trails. It can be seen form Fig. 3 that the analytical results meet accurately with the simulation results, which further verifies

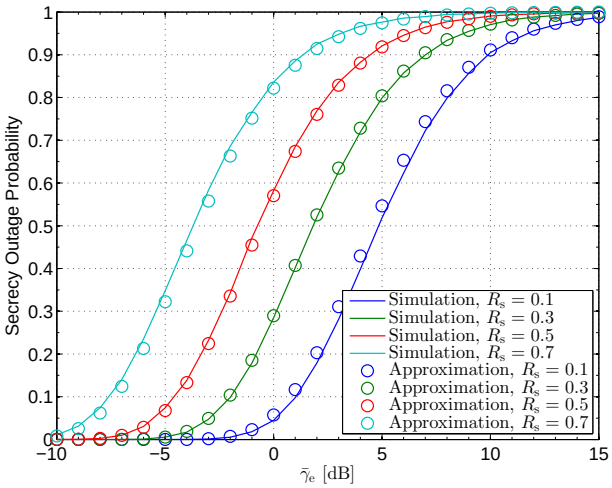


Fig. 5. Simulated and approximated limit secrecy outage secrecy versus $\bar{\gamma}_e$ for $\bar{\gamma}_b = 30$ dB, $N_E = N_B = 2$ and $N_A = 5$.

the former derivation. Furthermore, the probability decreases with the increment of $\bar{\gamma}_e$ but increases as $\bar{\gamma}_b$ rises up, which suggests the active and passive effect of the legitimate receiver and the eavesdropper in the wiretap channel. Note that the approximated formula of the mutual information is not utilized during the derivation of the probability of non-zero secrecy capacity, thus the derived results just represent the exact values of the probability.

Then, Fig. 4 provides the simulated and approximated results for the secrecy outage probability in terms of γ_b as N_A increases from 1 to 8 and γ_e ranges between -10 dB and -6 dB. As shown in Fig. 4(a) and Fig. 4(b), the approximated SOP, calculated by Equ. (22), agrees well with the simulated results, which supports our approximate derivations in Section III-B. As explained in the previous section, the SOP can not tend to be 0 with the increment of $\bar{\gamma}_b$ due to the limitation of finite-alphabet inputs, and this phenomenon can be clearly observed from Fig. 4(b). Overall, taken the results in Fig. 2 and Fig. 4 together, it makes sense to apply the approximation expression $\left(1 - e^{-0.6507\gamma}\right)$ into the estimation of secrecy performance for wiretap channel with BPSK/QPSK modulations.

As stated before, the SOP can not decrease continuously with the increment of $\bar{\gamma}_b$ when $\bar{\gamma}_e$ is fixed. To further explore the asymptotic behavior of the wiretap channel, Fig. 5 plots the asymptotic SOP versus $\bar{\gamma}_e$. Moreover, $\bar{\gamma}_b$ is fixed to 30 dB to make sure the mutual information of the main channel reaches 1. As can be seen from this graph, the asymptotic SOP will increase as $\bar{\gamma}_e$ rises up. In addition, the approximated results and the simulated results nearly equal to each other, which verifies the validity of the deduction.

V. Conclusion

This paper detailedly analyzes the secrecy performance of antenna-selection-aided MIMOME channels under BPSK/QPSK modulations. Approximated expressions for the ergodic secrecy rate and SOP are proposed and discussed in the situations when the CSIE is available or unavailable. Simulation shows that the approximated results indicated high precision and can serve as the estimation in the practical wiretap channel. Additionally, discussion about the SOP suggests that the finite alphabet input is the main limitation of the security and reliability in digital-modulation systems.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Technol. J.*, vol. 28, pp. 656–715, 1949.

[2] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennaspart II: the MIMOME wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[4] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Magazine*, vol. 53, no. 6, pp. 21–27, 2015.

[5] A. F. Molisch and M. Z. Win, "MIMO systems with antenna selection," *IEEE Microwave Magazine*, vol. 5, no. 1, pp. 46-56, 2004.

[6] N. Yang, P. L. Yeoh, M. Elkashlan, et al. "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144-154, 2013.

[7] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. on Inf. Forensics and Security*, vol. 8, no. 1, pp. 254–259, 2013.

[8] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," *IEEE Trans. on Vehicular Technology*, vol. 65, no. 1, pp. 214–225, 2016.

[9] F. S. Al-Qahtani, Y. Huang, S. Hessien, et al. "Secrecy analysis of MIMO wiretap channels with low-complexity receivers under imperfect channel estimation," *IEEE Trans. Inf. Forensics and Security*, vol. 12, no. 2, pp. 257–270, 2017.

[10] S. Asaad, A. Bereyhi, A. M. Rabiei, et al. "Optimal Transmit Antenna Selection for Massive MIMO Wiretap Channels," *IEEE J. Sel. Areas Commun.*, vol. 36, no.4, pp. 817–828, 2018.

[11] G. D. Raghava and B. S. Rajan, "Secrecy capacity of the Gaussian wiretap channel with finite complex constellation input," *arXiv preprint arXiv:1010.1163*, 2010.

[12] Z. Li, R. Yates and W. Trappe, "Achieving secret communication for fast Rayleigh fading channels," in *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792–2799, 2010.

[13] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Vehicular Technology*, vol. 61, no. 6, pp. 2599–2612, 2012.

[14] Y. Wu, J.-B. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3614–3628, 2017.

[15] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, Ming Zhao, and Jing Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, 2013.

[16] K. Cao, Y. Cai, Y. Wu, and W. Yang, "Cooperative jamming for secure communication with finite alphabet inputs," *IEEE Commun. Lett.*, vol. 21, no. 9, pp. 2025–2028, 2017.

[17] S. R. Aghdam, S. Rezaei, and T. M. Duman, "Joint precoder and artificial noise design for MIMO wiretap channels with finite-alphabet inputs based on the cut-off rate," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3913-3923, 2017.

[18] F. Wu, R. Zhang, L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Vehicular Technology*, vol. 65, no. 1, pp. 467–471, 2016.

[19] P. Yang, Y. Wu, and H. Yang, "Capacity of Nakagami-m fading channel with BPSK/QPSK modulations," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 564–567, 2017.

[20] 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.

[21] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed., Academic, San Diego, C.A., 2007.