Secure Transmission in MIMO Wiretap Channels Using General-Order Transmit Antenna Selection with Outdated CSI

Secure Transmission in MIMO Wiretap Channels Using General-Order Transmit Antenna Selection with Outdated CSI

Yuzhen Huang, Fawaz S. Al-Qahtani, *Member*, *IEEE*, Trung Q. Duong, *Senior Member*, *IEEE*, and Jinlong Wang, *Senior Member*, *IEEE*

***Abstract*—In this paper, we propose general-order transmit antenna selection to enhance the secrecy performance of multiple-input multiple-output multi-eavesdropper channels with the outdated channel state information (CSI) at the transmitter. To evaluate the effect of outdated CSI on the secure transmission of the system, we investigate the secrecy performance for two practical scenarios, i.e., Scenario I: the eavesdropper's CSI is not available at the transmitter, and Scenario II: the eavesdropper's CSI is available at the transmitter. For Scenario I, we derive exact and asymptotic closed-form expressions for the secrecy outage probability in Nakagami-*m* fading channels. In addition, we also derive the probability of non-zero secrecy capacity and the ε-outage secrecy capacity, respectively. Simple asymptotic expressions for the secrecy outage probability reveal that the secrecy diversity order is reduced when CSI is outdated at the transmitter, and is independent of the number of antennas at each eavesdropper N_{E}, fading parameter of the eavesdropper's channel m_{E}, and the number of eavesdroppers M. For Scenario II, we make a comprehensive analysis of the average secrecy capacity obtained by the system. Specifically, new closed-form expressions for the exact and asymptotic average secrecy capacity are derived, which are valid for general systems with arbitrary number of antennas, number of eavesdroppers and fading severity parameters. Resorting to these results, we also determine the high signal-to-noise ratio power offset to explicitly quantify the impacts of the main channel and the eavesdropper's channel on the average secrecy capacity.**

***Index Terms*—MIMO wiretap channel, physical layer security, transmit antenna selection, Nakagami-*m* fading.**

I. Introduction

INFORMATION transmission security has become a prominent frontier in wireless communications due to the broadcast nature of the wireless propagation environment. In conventional communication systems, various cryptographic schemes have been designed and applied to guarantee the information transmission security in the upper layers assuming an error-free link in the physical layer [1]. However, traditional cryptographic schemes based on complex mathematical functions have become increasingly unreliable when the computational ability of eavesdropper becomes more powerful [2]. Based on this important observation, from the information-theoretic point of perspective, physical layer security has been introduced to strengthen the secure transmission of wireless communications. The key idea behind physical layer security is to exploit different characteristics between the main channel and the eavesdropper's channel [3]. The author in [4] first introduced the concept of the wiretap channel and demonstrated that perfect security can be achieved when the quality of the eavesdropper's channel is inferior to that of the main channel.

In an effort to further improve physical layer security, a number of works have suggested the idea of incorporating the multiple antenna technique into wireless communication systems (see [5]–[8] and references therein). In [5], the authors considered a general system model with each node being equipped with multiple antennas and analyzed the secrecy capacity of the Gaussian multi-antenna wiretap channel. In [6], the secrecy performance metrics with maximum ratio combining (MRC) scheme were examined in independent Rayleigh fading channels. In [7], the authors investigated the confidential communication in slow non-selection correlated Rayleigh fading channel, and evaluated the effect of antenna correlation on the secrecy performance such as the probability of positive secrecy capacity and the secure outage probability, respectively. In [8], transmit antenna selection (TAS) was proposed to enhance physical layer security in multiple-input multiple-output (MIMO) wiretap channels, and the secrecy capacity of the MIMO wiretap channel was characterized in non-identical Nakagami-*m* fading channels. The authors in [9], [10] investigated the secrecy performance of MIMO wiretap channels using transmit antenna selection with receive generalized selection combining (TAS/GSC) in Rayleigh and Nakagami-*m* fading, respectively. While these prior works have significantly improved our understanding on the impact of multiple antennas on the security performance of the wiretap channels, the key limitations of these aforementioned works are that they all assume perfect channel state information (CSI) of the main channel at the transmitter and only a single eavesdropper. Assuming Nakagami-*m* fading, a recent work [11] analyzed the effect of outdated CSI on the secrecy outage performance of multiple-input single-output (MISO) wiretap channels with transmit antenna selection. However,

This work was supported by the National Science Foundation of China (No. 61401508). The work of F. S. Al-Qahtani was partially supported by JSREP grant 3-039-2-010 from the Qatar National Research Fund (a member of Qatar Foundation). The work of T. Q. Duong was partially funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2013.13.

Yuzhen Huang and Jinlong Wang are with the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China (e-mail: yzh_huang@sina.com; wjl543@sina.com).

Fawaz Al-Qahtani is with the Department of Electrical and Computer Engineering, Texas A&M University at Qatar, Doha, Qatar (e-mail: fawaz.al-qahtani@qatar.tamu.edu).

Trung Q. Duong is with Queen's University Belfast, Belfast BT7 1NN, U.K. (e-mail: trung.q.duong@qub.ac.uk).

one major drawback of [11] is that both legitimate receiver and eavesdropper are equipped with a single antenna, and hence the received diversity gain has not been understood well. In addition, [12] also investigated the effect of outdated CSI on the secrecy outage performance of MIMO wiretap channels using transmit antenna selection with receive maximum ratio combining in Rayleigh fading environments. However, it only considered a single eavesdropper and neglected the impact of channel fading severity on the secrecy performance of the MIMO wiretap channels.

Different from all previous works, we propose a general-order transmit antenna selection with receive maximum ratio combining (TAS/MRC) for secure data transmission in MIMO wiretap channels with multiple eavesdroppers in independent and non-identical Nakagami-*m* fading. To make our analysis more general, we take into account the realistic scenario of only outdated CSI at the transmitter. Specifically, the motivations of adopting general-order transmit antenna selection not the best transmit antenna selection are given as follows:

- The ranking of transmit channels may be inaccurate due to the unreliable pilot signals, which are used to predict CSI for diversity combining and antenna selection.
- Since only subset of CSI is sufficient to decide on the suitable transmit antenna to satisfy a target quality of service, hence, this selection criterion can reduce processing complexity at the receiver.
- The best transmit channel may be unavailable or occupied by other service requirements. Therefore, a possible solution is to use other than the best channel in order to avoid service interruption.

In doing so, to evaluate the effect of outdated CSI on the secrecy performance of MIMO wiretap channels, we consider two practical eavesdropping scenarios. That is, Scenario I (i.e., passive eavesdropping): the transmitter has no knowledge of CSI about the eavesdropper's link, and Scenario II (i.e., active eavesdropping): the CSI of the eavesdropper's link is available at the transmitter[1]. For Scenario I, due to the unavailable of the eavesdropper's CSI, we investigate the secrecy performance in terms of the secrecy outage probability. For Scenario II, we take into account of the average secrecy capacity as the principal secrecy performance, since the transmitter adapts its transmission rate based on the global CSI to achieve perfect secrecy. The main contributions of the paper are summarized as follows:

- *Scenario I:* We first derive new exact closed-form expressions for the probability of non-zero secrecy capacity and secrecy outage probability, and also provide an approximated expression for the ε-outage secrecy capacity of MIMO wiretap channels, which provide an efficient means to evaluate the impact of key system parameters on the secrecy performance of MIMO wiretap channels.
- *Scenario I:* To gain further insights, an asymptotic and secrecy diversity analysis are carried out in the high signal-to-noise ratio (SNR) regime. Based on the derived asymptotic results, we find that the secrecy diversity order is significantly affected by the outdated CSI and is independent of the parameters related with the eavesdropper.
- *Scenario II:* We derive a new exact closed-form expression for the average secrecy capacity in independent and non-identical Nakagami-*m* fading channels, which are very general and are applicable to MIMO wiretap channels with arbitrary number of eavesdroppers, number of antennas at each receiver, and fading severity parameters.
- *Scenario II:* To evaluate the effect of the main channel and the eavesdropper's channel on the average secrecy capacity, we derive a new compact expression for the average secrecy capacity in the high SNR regime, which facilitates the characterization of the high SNR power offset, and demonstrates that the high slope is one and is independent of all system parameters.

[1]Scenario II is particularly applicable in the multicast and unicast networks where the users play dual roles as legitimate receivers for some signals and eavesdroppers for others. The scenario has been broadly adopted in the published works [13], [14].

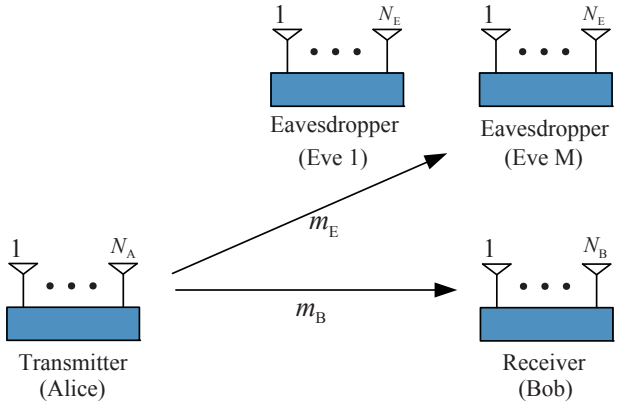

Fig. 1. System model.

The paper is organized as follows. The system model is introduced in Section II. Section III formulates the problem and presents a set of new analytical expressions for the key secrecy performance. In Section IV, we provide numerical results and discussions. Finally, Section VI concludes the paper and summarizes the findings.

Notations: We use bold lower case letters to denote vectors and lower case letters to denote scales, respectively. The probability density function (PDF) and the cumulative distribution function (CDF) of a random variable (RV) X are denoted as $f_X(\cdot)$ and $F_X(\cdot)$, respectively. The symbol $\|\cdot\|_F$ denotes the Frobenius norm, and $\mathrm{E}[\cdot]$ stands for the expectation operator.

II. System Model

Let us consider a MIMO wiretap channel as illustrated in Fig. 1, which consists of a transmitter (Alice), a legitimate receiver (Bob), and M eavesdroppers (Eve). The number of transmit antennas at Alice is represented as N_{A}, and the number of receive antennas at Bob and each Eve are denoted as N_{B} and N_{E}, respectively. We assume that the corresponding CSI of the main channel and the eavesdropper's channel is known to Bob and Eve, respectively. Without loss of generality, the main channel and eavesdropper's channel are assumed to be quasi-static fading channel with independent

non-identical distributed block Nakagami-*m* fading, so that the channel coefficients keep constant during the coherence time of the channel. The overall general-order TAS/MRC scheme is carried out in two phases [11], [12].

- **TAS Phase**: Since Alice has only a single radio frequency (RF) chain, it has to send the pilot sequence one by one for the channel estimation at Bob. We assume that Bob can perfectly estimate the CSI corresponding to each transmit antenna[2]. After that, Bob selects a transmit antenna associated with the kth best instantaneous SNR, and feeds back the corresponding antenna index to Alice. The feedback information can be represented by a binary vector with $B = \lceil \log N_{\mathrm{A}} \rceil$ bits.
- **Transmission Phase**: During the information transmission, the CSI corresponding to the kth optimal antenna should be estimated again for decoding at Bob. Using the pilot tones in the data frame, Bob can obtain the accurate CSI of the main channel and subsequently feed back the instantaneous SNR of the main channel to Alice for wiretap code construction.

Noteworthy, unlike the conventional general-order TAS/MRC scheme without secrecy consideration, Bob also need to feed back the received SNR value to Alice for wiretap code construction, in addition to the kth optimal transmit antenna index. In the following, the detail selection of transmit antenna will be discussed[3].

Let $\mathbf{h}_{i\mathrm{B}}(t) \in \mathbb{C}^{N_{\mathrm{B}} \times 1}$ be the channel vector between the ith transmit antenna at Alice and Bob at time t, and its entries follow independent and identically distributed Nakagami-*m* fading with fading severity parameter m_{B}. Employing MRC scheme, the instantaneous received SNR between the ith transmit antenna of Alice and Bob is given by

$$\widehat{\gamma}_{i\mathrm{B}} = \frac{P_{\mathrm{A}}}{\sigma^2} \|\mathbf{h}_{i\mathrm{B}}(t)\|^2, \tag{1}$$

where P_{A} denotes the transmit power at Alice and σ^2 denotes the noise variance at each receive antenna. In this paper, the general-order TAS criterion used is to select the kth highest post-processing SNR for Bob, which is entirely determined by the CSI of the main channel. As such, the index of the selected antenna, k, is given by

$$k = k^{\mathrm{th}} \arg\max_{1 \le i \le N_{\mathrm{A}}} \left(\widehat{\gamma}_{i\mathrm{B}}\right), \tag{2}$$

where $k^{\mathrm{th}} \arg\max(\cdot)$ denotes to select the kth optimal antenna. As a result, the instantaneous SNRs of the main channel and the mth eavesdropper channel can be, respectively, given by

$$\widehat{\gamma}_{(k\mathrm{B})} = \frac{P_{\mathrm{A}}}{\sigma^2} \|\mathbf{h}_{k\mathrm{B}}(t)\|^2 \tag{3}$$

and

$$\gamma_{m\mathrm{E}} = \frac{P_{\mathrm{A}}}{\sigma^2} \|\mathbf{h}_{mk\mathrm{E}}(t)\|^2, \tag{4}$$

where $m \in \{1, \ldots, M\}$, and $\mathbf{h}_{mk\mathrm{E}}$ is the $N_{\mathrm{E}} \times 1$ channel vector between the selected kth transmit antenna at Bob and the mth Eve, its entries follow independent and identically distributed Nakagami-*m* fading with fading severity parameter m_{E}[4]. Without loss of generality, we assume that there are no cooperation between eavesdroppers[5]. That is to say, secure data transmission between Alice and Bob can be achieved under the condition of the quality of main channel is larger than that of any eavesdropper's channel. Hence, the end-to-end instantaneous SNR of the eavesdropper's channel is represented as

$$\gamma_{\mathrm{E}} = \max_{1 \le m \le M} \gamma_{m\mathrm{E}}. \tag{5}$$

According to [14], the achievable secrecy rate of MIMO wiretap channels with multiple eavesdroppers is given by

$$C_{\mathrm{S}} = \begin{cases} C_{\mathrm{B}} - C_{\mathrm{E}}, \widehat{\gamma}_{(k\mathrm{B})} > \gamma_{\mathrm{E}} \\ 0, \qquad\quad \widehat{\gamma}_{(k\mathrm{B})} \le \gamma_{\mathrm{E}} \end{cases}, \tag{6}$$

where $C_{\mathrm{B}} = \log\left(1 + \widehat{\gamma}_{(k\mathrm{B})}\right)$ and $C_{\mathrm{E}} = \log\left(1 + \gamma_{\mathrm{E}}\right)$ are the achievable instantaneous rates at Bob and Eve, respectively.

Please note, in practical systems, the general-order **TAS phase** may exceed the coherent time of the channel. As a result, the main channel may have already changed the moment when Alice receives the feedback of the kth optimal antenna index due to the time-varying nature of the wireless channel. In this case, the kth optimal antenna is selected based on the outdated CSI, i.e., $\mathbf{h}_{i\mathrm{B}}(t-\tau) \in \mathbb{C}^{N_{\mathrm{B}} \times 1}$, which denotes the τ time-delayed version of the current CSI, i.e., $\mathbf{h}_{i\mathrm{B}}(t)$. Without loss of generality, we assume that $\gamma_{(k\mathrm{B})} = \frac{P_{\mathrm{A}}}{\sigma^2} \|\mathbf{h}_{k\mathrm{B}}(t-\tau)\|^2$ denotes the time-delayed version of the current SNR $\widehat{\gamma}_{(k\mathrm{B})}$. Hence, the relationship between $\gamma_{(k\mathrm{B})}$ and $\widehat{\gamma}_{(k\mathrm{B})}$ can be modeled as [15]–[17]

$$\widehat{\gamma}_{(k\mathrm{B})} = \sqrt{\rho}\gamma_{(k\mathrm{B})} + \sqrt{1-\rho}\omega, \tag{7}$$

where $|\omega|^2$ is Gamma-distributed random variable with same variance $\gamma_{(k\mathrm{B})}$, and ρ is the correlation coefficient between $\gamma_{(k\mathrm{B})}$ and $\widehat{\gamma}_{(k\mathrm{B})}$. For Jake's autocorrelation model, we have $\rho = [J_0(2\pi f \tau)]^2$, where f represents the maximum Doppler frequency, and $J_0(\cdot)$ is the zeroth-order Bessel function of the first kind [18, Eq. (8.411)]. In addition, an important issue is the construction of wiretap code in the case of time-delayed feedback. To construct the corresponding wiretap code, Bob has to feed back the current SNR value $\widehat{\gamma}_{(k\mathrm{B})}$ to Alice during the **Transmission Phase**. We assume that the feedback of $\widehat{\gamma}_{(k\mathrm{B})}$ is perfect, which is also adopted in [12]. Thus, Alice will use the main channel capacity of $C_{\mathrm{B}} = \log\left(1 + \widehat{\gamma}_{(k\mathrm{B})}\right)$ to construct the wiretap code and transmit the signal at the antenna selected based on $\mathbf{h}_{i\mathrm{B}}(t-\tau)$.

In the proposed MIMO wiretap channels, we consider two practical eavesdropping scenarios, i.e., Scenario I and Scenario II. For Scenario I and Scenario II, we take into consideration

[2]In practice, when the kth best instantaneous SNR is found, the estimation process by Bob can be terminated due to the fact that the general-order TAS is adopted in this work.

[3]To avoid the overhead of antenna selection and make analysis more tractable, we propose an antenna selection based on the CSI of the main channel.

[4]Noteworthy, we assume that the eavesdroppers are located in close proximity to each other with same fading severity parameter m_{E} and average powers.

[5]Please note, if maximal ratio combining scheme between eavesdroppers is adopted, the corresponding PDF and CDF of γ_{E} are still Gamma distribution. Thus, by following similar derivations for non-cooperation, the desired results can be easily obtained.

of the secrecy outage probability and the average secrecy capacity, respectively, as the secrecy performance metrics of interests. In the following sections, we will provide a detailed analysis of these secrecy performance metrics.

III. Secrecy Performance

In this section, we present a comprehensive investigation on the secrecy performance of MIMO wiretap channels with multiple eavesdroppers described in the previous section.

A. Preliminaries

Before delving into the details, we first present a set of statistical properties of $\widehat{\gamma}_{(k\mathrm{B})}$ and γ_{E}, which will be frequently invoked in the subsequent derivations.

Lemma 1. *The exact PDF and CDF of $\widehat{\gamma}_{(k\mathrm{B})}$ are given by*

$$f_{\widehat{\gamma}_{(k\mathrm{B})}}(x) = k\binom{N_{\mathrm{A}}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^n\Phi_{\mathrm{B}}}{\Gamma(m_{\mathrm{B}}N_{\mathrm{B}})}\sum_{i=0}^{\phi_{\mathrm{B}}}\binom{\phi_{\mathrm{B}}}{i} \times \frac{\Gamma(\phi_{\mathrm{B}}+m_{\mathrm{B}}N_{\mathrm{B}})}{\Gamma(m_{\mathrm{B}}N_{\mathrm{B}}+i)}\left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^{m_{\mathrm{B}}N_{\mathrm{B}}+i}\frac{\rho^i(1-\rho)^{\phi_{\mathrm{B}}-i}}{\xi^{m_{\mathrm{B}}N_{\mathrm{B}}+\phi_{\mathrm{B}}+i}} \times x^{m_{\mathrm{B}}N_{\mathrm{B}}+i-1}e^{-\frac{\alpha m_{\mathrm{B}}}{\xi\overline{\gamma}_{\mathrm{B}}}x} \tag{8}$$

and

$$F_{\widehat{\gamma}_{(k\mathrm{B})}}(x) = k\binom{N_{\mathrm{A}}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^n\Phi_{\mathrm{B}}}{\Gamma(m_{\mathrm{B}}N_{\mathrm{B}})}\sum_{i=0}^{\phi_{\mathrm{B}}}\binom{\phi_{\mathrm{B}}}{i} \times \Gamma(\phi_{\mathrm{B}}+m_{\mathrm{B}}N_{\mathrm{B}})\frac{\rho^i(1-\rho)^{\phi_{\mathrm{B}}-i}}{\xi^{\phi_{\mathrm{B}}}\alpha^{m_{\mathrm{B}}N_{\mathrm{B}}+i}} \times \left\{1-e^{-\frac{\alpha m_{\mathrm{B}}x}{\xi\overline{\gamma}_{\mathrm{B}}}}\sum_{m=0}^{m_{\mathrm{B}}N_{\mathrm{B}}+i-1}\frac{x^m}{m!}\left(\frac{\alpha m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}\xi}\right)^m\right\}, \tag{9}$$

where $\overline{\gamma}_{\mathrm{B}} = \mathrm{E}[\gamma_{i\mathrm{B}}]$ is the average SNR of the main channel, $\alpha = N_{\mathrm{A}}+n-k+1$, $\xi = 1+(N_{\mathrm{A}}+n-k)(1-\rho)$, $\phi_{\mathrm{B}} = \sum_{q=1}^{N_{\mathrm{B}}m_{\mathrm{B}}-1} n_q$, and

$$\Phi_{\mathrm{B}} = \sum_{n_1=0}^{N_{\mathrm{A}}+n-k}\sum_{n_2=0}^{n_1}\cdots\sum_{n_{N_{\mathrm{B}}m_{\mathrm{B}}-1}=0}^{n_{N_{\mathrm{B}}m_{\mathrm{B}}-2}}\frac{(N_{\mathrm{A}}+n-k)!}{n_{N_{\mathrm{B}}m_{\mathrm{B}}-1}!} \times \prod_{t=1}^{N_{\mathrm{B}}m_{\mathrm{B}}-1}\frac{(t!)^{n_{t+1}-n_t}}{(n_{t-1}-n_t)!} \tag{10}$$

with $n_0 = N_{\mathrm{A}}+n-k$ and $n_{N_{\mathrm{B}}m_{\mathrm{B}}} = 0$.

Proof: See Appendix A. ∎

Lemma 2. *The exact PDF and CDF of γ_{E} are given by*

$$f_{\gamma_{\mathrm{E}}}(x) = M\sum_{v=0}^{M-1}\binom{M-1}{v}\frac{(-1)^v\Phi_{\mathrm{E}}}{\Gamma(N_E m_E)} \times \left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}m_{\mathrm{E}}+\phi_{\mathrm{E}}}x^{\phi_{\mathrm{E}}+N_{\mathrm{E}}m_{\mathrm{E}}-1}e^{-\frac{(1+v)m_{\mathrm{E}}x}{\overline{\gamma}_{\mathrm{E}}}} \tag{11}$$

and

$$F_{\gamma_{\mathrm{E}}}(x) = \sum_{v=0}^{M}\binom{M}{v}(-1)^v\Phi_{\mathrm{E}}\left(\frac{m_{\mathrm{E}}x}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}}e^{-\frac{vm_{\mathrm{E}}x}{\overline{\gamma}_{\mathrm{E}}}}, \tag{12}$$

where $\overline{\gamma}_{\mathrm{E}} = \mathrm{E}[\gamma_{m\mathrm{E}}]$ represents the average SNR of the eavesdropper's channel, $\phi_{\mathrm{E}} = \sum_{q=1}^{N_{\mathrm{E}}m_{\mathrm{E}}-1} m_q$, and

$$\Phi_{\mathrm{E}} = \sum_{m_1=0}^{v}\sum_{m_2=0}^{m_1}\cdots\sum_{m_{N_{\mathrm{E}}m_{\mathrm{E}}-1}=0}^{m_{N_{\mathrm{E}}m_{\mathrm{E}}-2}}\frac{v!}{m_{N_{\mathrm{E}}m_{\mathrm{E}}-1}!} \times \prod_{p=1}^{N_{\mathrm{E}}m_{\mathrm{E}}-1}\frac{(p!)^{m_{p+1}-m_p}}{(m_{p-1}-m_p)!} \tag{13}$$

with $m_0 = v$ and $m_{N_{\mathrm{E}}m_{\mathrm{E}}} = 0$.

Proof: The proof can be found in [16]. ∎

B. Scenario I: CSI of the eavesdropper's channel is not available at Alice

In this subsection, we concentrate on the scenario, which Alice has no knowledge of CSI about the eavesdropper's channel. Under this scenario, we investigate three important metrics to evaluate the secrecy performance of the considered system, i.e., the probability of non-zero secrecy capacity, the secrecy outage probability, and the ε-outage secrecy capacity.

1) Probability of Non-Zero Secrecy Capacity: According to [1], the probability of non-zero secrecy capacity of the proposed model is given by

$$\Pr(C_{\mathrm{S}}>0) = \Pr\left(\widehat{\gamma}_{(k\mathrm{B})}>\gamma_{\mathrm{E}}\right) = \int_0^\infty\int_0^x f_{\widehat{\gamma}_{(k\mathrm{B})}}(x)\,f_{\gamma_{\mathrm{E}}}(y)\,dydx. \tag{14}$$

Then, by substituting (8) and (11) into (14), and utilizing the equation [18, Eq. (3.351.3)], the exact closed-form expression for the probability of non-zero secrecy capacity can be derived as (15) after some simple mathematical manipulations.

To the best of the authors' knowledge, (15) is a new closed-form expression and is valid for general scenarios with arbitrary SNR, arbitrary numbers of eavesdroppers, and arbitrary numbers of antennas. Notably, in the following three special cases, the derived expression for (15) can be reduced to the foregone results.

- Case 1: When the best antenna selection ($k = N_{\mathrm{A}}$), a single antenna at Alice ($N_{\mathrm{A}} = 1$), a single eavesdropper ($M = 1$), Rayleigh fading ($m_{\mathrm{B}} = m_{\mathrm{E}} = 1$) is considered, (15) becomes to [5, Eq. (3)] under the condition of perfect CSI at Alice.
- Case 2: When the best antenna selection ($k = N_{\mathrm{A}}$) and a single eavesdropper ($M = 1$) is considered, (15) can be reduced to [8, Eq. (16)] under the condition of perfect CSI at Alice.
- Case 3: When the best antenna selection ($k = N_{\mathrm{A}}$), a single eavesdropper ($M = 1$), and Rayleigh fading ($m_{\mathrm{B}} = m_{\mathrm{E}} = 1$) is considered, (15) becomes to [12, Eq. (21)] under the condition of imperfect CSI at Alice.

This demonstrates the validation of our analysis and the generality of our result.

$$\Pr\left(C_{\mathrm{S}}>0\right)=k\binom{N_{\mathrm{A}}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^{n}\Phi_{\mathrm{B}}}{\Gamma\left(m_{\mathrm{B}}N_{\mathrm{B}}\right)}\sum_{i=0}^{\phi_{\mathrm{B}}}\binom{\phi_{\mathrm{B}}}{i}\frac{\Gamma\left(\phi_{\mathrm{B}}+m_{\mathrm{B}}N_{\mathrm{B}}\right)}{\Gamma\left(m_{\mathrm{B}}N_{\mathrm{B}}+i\right)}\left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^{m_{\mathrm{B}}N_{\mathrm{B}}+i}\frac{\rho^{i}(1-\rho)^{\phi_{\mathrm{B}}-i}}{\xi^{m_{\mathrm{B}}N_{\mathrm{B}}+\phi_{\mathrm{B}}+i}}$$
$$\times\sum_{v=0}^{M}\binom{M}{v}(-1)^{v}\Phi_{\mathrm{E}}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}}\Gamma\left(m_{\mathrm{B}}N_{\mathrm{B}}+i+\phi_{\mathrm{E}}\right)\left(\frac{\alpha m_{\mathrm{B}}}{\xi\overline{\gamma}_{\mathrm{B}}}+\frac{vm_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{-(m_{\mathrm{B}}N_{\mathrm{B}}+i+\phi_{\mathrm{E}})}\tag{15}$$

$$P_{\mathrm{out}}\left(R_{\mathrm{S}}\right)=k\binom{N_{\mathrm{A}}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^{n}\Phi_{\mathrm{B}}}{\Gamma\left(m_{\mathrm{B}}N_{\mathrm{B}}\right)}\sum_{i=0}^{\phi_{\mathrm{B}}}\binom{\phi_{\mathrm{B}}}{i}\Gamma\left(\phi_{\mathrm{B}}+m_{\mathrm{B}}N_{\mathrm{B}}\right)\frac{\rho^{i}(1-\rho)^{\phi_{\mathrm{B}}-i}}{\xi^{\phi_{\mathrm{B}}}\alpha^{m_{\mathrm{B}}N_{\mathrm{B}}+i}}$$
$$\times\left\{1-Me^{-\frac{\alpha m_{\mathrm{B}}\left(2^{R_{\mathrm{S}}}-1\right)}{\xi\overline{\gamma}_{\mathrm{B}}}}\sum_{v=0}^{M-1}\binom{M-1}{v}\frac{(-1)^{v}\Phi_{\mathrm{E}}}{\Gamma\left(N_{E}m_{E}\right)}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}m_{\mathrm{E}}+\phi_{\mathrm{E}}}\sum_{m=0}^{m_{\mathrm{B}}N_{\mathrm{B}}+i-1}\left(\frac{\alpha m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}\xi}\right)^{m}\right.$$
$$\left.\times\sum_{u=0}^{m}\binom{m}{u}2^{uR_{S}}\left(2^{R_{S}}-1\right)^{m-u}\frac{\Gamma\left(u+\phi_{\mathrm{E}}+N_{\mathrm{E}}m_{\mathrm{E}}\right)}{\Gamma\left(m+1\right)}\left[\frac{\alpha m_{\mathrm{B}}2^{R_{\mathrm{S}}}}{\xi\overline{\gamma}_{\mathrm{B}}}+\frac{(1+v)\,m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right]^{-(u+\phi_{\mathrm{E}}+N_{\mathrm{E}}m_{\mathrm{E}})}\right\}\tag{17}$$

2) Secrecy Outage Probability: The secrecy outage probability is defined as the probability that the secrecy capacity falls below a predefined rate R_{S}. Mathematically, it is given by $P_{\mathrm{out}}\left(R_{\mathrm{S}}\right)=\Pr\left(C_{\mathrm{S}}<R_{\mathrm{S}}\right)$, which can be further expanded as

$$P_{\mathrm{out}}\left(R_{\mathrm{S}}\right)=\underbrace{\Pr\left(C_{\mathrm{S}}<R_{\mathrm{S}}|\,\widehat{\gamma}_{(k\mathrm{B})}>\gamma_{\mathrm{E}}\right)\Pr\left(\widehat{\gamma}_{(k\mathrm{B})}>\gamma_{\mathrm{E}}\right)}_{I_{1}}+\underbrace{\Pr\left(\widehat{\gamma}_{(k\mathrm{B})}<\gamma_{\mathrm{E}}\right)}_{I_{2}},\tag{13}$$

where I_1 and I_2 are represented as

$$I_{1}=\int_{0}^{\infty}\int_{y}^{2^{R_{\mathrm{S}}}(1+y)-1}f_{\widehat{\gamma}_{(k\mathrm{B})}}\left(x\right)f_{\gamma_{\mathrm{E}}}\left(y\right)dxdy\tag{14}$$

and

$$I_{2}=\int_{0}^{\infty}\int_{0}^{y}f_{\widehat{\gamma}_{(k\mathrm{B})}}\left(x\right)f_{\gamma_{\mathrm{E}}}\left(y\right)dxdy.\tag{15}$$

Now, by substituting (14) and (15) into (13), we have

$$P_{\mathrm{out}}\left(R_{\mathrm{S}}\right)=\int_{0}^{\infty}\int_{0}^{2^{R_{\mathrm{S}}}(1+y)-1}f_{\widehat{\gamma}_{(k\mathrm{B})}}\left(x\right)f_{\gamma_{\mathrm{E}}}\left(y\right)dxdy$$
$$=\int_{0}^{\infty}F_{\widehat{\gamma}_{(k\mathrm{B})}}\left(2^{R_{\mathrm{S}}}\left(1+y\right)-1\right)f_{\gamma_{\mathrm{E}}}\left(y\right)dy.\tag{16}$$

Then, by utilizing the equation [18, Eq. (3.351.3)] and performing some simple mathematical manipulations, the closed-form expression for secrecy outage probability is derived as (17). For the special case of a single antenna at Bob ($N_{\mathrm{B}}=1$), a single eavesdropper with single antenna ($N_{\mathrm{E}}=1$ and $M=1$), (17) reduces to [11, Eq. (19)]. In addition, when perfect CSI at Alice ($\rho=1$), the best antenna selection ($k=N_{\mathrm{A}}$) and a single eavesdropper $M=1$ is considered, (17) reduces to [8, Eq. (28)]. Furthermore, (17) can also be reduced to [19, Eq. (10)] with $\rho=1$, $M=1$, $N_{\mathrm{A}}=N_{\mathrm{B}}=1$ and $m_{\mathrm{A}}=m_{\mathrm{B}}=1$. On the other hand, when $\rho\neq1$, (17) reduces to [12, Eq. (15)] with $k=N_{\mathrm{A}}$, $M=1$ and $m_{\mathrm{A}}=m_{\mathrm{B}}=1$. These observations also prove the generality of our analysis.

Although the exact closed-form expression for secrecy outage probability is obtained, it is difficult to achieve more insights from (17). Hence, in order to get more insights, we turn our attention to the asymptotic secrecy outage probability in the high SNR regime, i.e., $\overline{\gamma}_{\mathrm{B}}\to\infty$. We find it convenient to give a separate treatment for the following two cases of interest. Case 1: perfect feedback, i.e., $\rho=1$, and Case 2: delayed feedback, i.e., $\rho\neq1$.

Theorem 1. *Based on* (17)*, the secrecy outage probability at the high SNR regime can be approximated as*

$$P_{\mathrm{out}}^{\infty}\left(R_{\mathrm{S}}\right)=\begin{cases}\vartheta_{1}\overline{\gamma}_{\mathrm{B}}^{-m_{\mathrm{B}}N_{\mathrm{B}}}, & \rho\neq1\\ \vartheta_{2}\overline{\gamma}_{\mathrm{B}}^{-km_{\mathrm{B}}N_{\mathrm{B}}}, & \rho=1\end{cases},\tag{18}$$

where

$$\vartheta_{1}=kM\binom{N_{\mathrm{A}}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^{n}\Phi_{\mathrm{B}}m_{\mathrm{B}}^{m_{\mathrm{B}}N_{\mathrm{B}}}(1-\rho)^{\phi_{\mathrm{B}}}}{\Gamma\left(m_{\mathrm{B}}N_{\mathrm{B}}+1\right)\xi^{m_{\mathrm{B}}N_{\mathrm{B}}+\phi_{\mathrm{B}}}}$$
$$\times\frac{\Gamma\left(\phi_{\mathrm{B}}+m_{\mathrm{B}}N_{\mathrm{B}}\right)}{\Gamma\left(m_{\mathrm{B}}N_{\mathrm{B}}\right)}\sum_{v=0}^{M-1}\binom{M-1}{v}\frac{(-1)^{v}\Phi_{\mathrm{E}}}{\Gamma\left(N_{\mathrm{E}}m_{\mathrm{E}}\right)}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}m_{\mathrm{E}}}$$
$$\times\Gamma\left(\phi_{\mathrm{E}}+N_{\mathrm{E}}m_{\mathrm{E}}\right)\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}}\sum_{m=0}^{m_{\mathrm{B}}N_{\mathrm{B}}}\binom{m_{\mathrm{B}}N_{\mathrm{B}}}{m}(-1)^{m_{\mathrm{B}}N_{\mathrm{B}}-m}$$
$$\times2^{mR_{\mathrm{S}}}\Psi\left(\phi_{\mathrm{E}}+N_{\mathrm{E}}m_{\mathrm{E}},\phi_{\mathrm{E}}+N_{\mathrm{E}}m_{\mathrm{E}}+m+1;\frac{(1+v)\,m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)\tag{19}$$

and

$$\vartheta_{2}=\binom{N_{\mathrm{A}}}{k}\frac{Mm_{\mathrm{B}}^{kN_{\mathrm{B}}m_{\mathrm{B}}}}{\left[(N_{\mathrm{B}}m_{\mathrm{B}})!\right]^{k}}\sum_{v=0}^{M-1}\binom{M-1}{v}\frac{(-1)^{v}\Phi_{\mathrm{E}}}{\Gamma\left(N_{\mathrm{E}}m_{\mathrm{E}}\right)}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}m_{\mathrm{E}}}$$
$$\times\Gamma\left(N_{\mathrm{E}}m_{\mathrm{E}}+\phi_{\mathrm{E}}\right)\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}}\sum_{n=0}^{kN_{\mathrm{B}}m_{\mathrm{B}}}\binom{kN_{\mathrm{B}}m_{\mathrm{B}}}{n}(-1)^{kN_{\mathrm{B}}m_{\mathrm{B}}-n}$$
$$\times2^{nR_{\mathrm{S}}}\Psi\left(N_{\mathrm{E}}m_{\mathrm{E}}+\phi_{\mathrm{E}},N_{\mathrm{E}}m_{\mathrm{E}}+\phi_{\mathrm{E}}+n+1;\frac{(1+v)\,m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right),\tag{20}$$

where $\Psi\left(\cdot,\cdot;\cdot\right)$ *is the confluent hypergeometric function of the second kind [18, Eq. (9.211.4)].*

Proof: See Appendix B. ■

From Theorem 1, we present the following corollary.

Corollary 1. *With the proposed antenna selection algorithm, the achievable secrecy diversity order and the secrecy array gain of MIMO wiretap channels are given respective by*

$$G_{\mathrm{d}} = \begin{cases} m_{\mathrm{B}} N_{\mathrm{B}}, & \rho \neq 1 \\ k m_{\mathrm{B}} N_{\mathrm{B}}, & \rho = 1 \end{cases} \tag{21}$$

and

$$G_{\mathrm{a}} = \begin{cases} \vartheta_1^{-\frac{1}{m_{\mathrm{B}} N_{\mathrm{B}}}}, & \rho \neq 1 \\ \vartheta_2^{-\frac{1}{k m_{\mathrm{B}} N_{\mathrm{B}}}}, & \rho = 1 \end{cases}. \tag{22}$$

Proof: By expressing the asymptotic secrecy outage probability as $P_{\mathrm{out}}^{\infty}(R_{\mathrm{S}}) = (G_{\mathrm{a}} \overline{\gamma}_{\mathrm{B}})^{-G_{\mathrm{d}}}$, the achievable secrecy diversity order and array gain can be easily obtained. ■

Based on Corollary 1, we summarize the following remarks to provide insights into the use of general-order TAS/MRC scheme in the main channel under Nakagami-*m* fading channels.

Remark 1: When there is no feedback delay, the maximum secrecy outage diversity gain of MIMO wiretap channels with general-order TAS/MRC scheme is $k m_{\mathrm{B}} N_{\mathrm{B}}$. However, for the case of delayed feedback, the secrecy outage diversity gain reduces to $m_{\mathrm{B}} N_{\mathrm{B}}$. Please note that whether there exists feedback delay or not, the secrecy outage diversity gain of MIMO wiretap channels is entirely independent of the parameter of the eavesdropper's channel.

Remark 2: The number of antennas N_E, the number of eavesdroppers M, and the fading severity parameter m_{E} have no impact on the secrecy outage diversity. However, there affect the secrecy performance of MIMO wiretap channels by reducing the secrecy outage SNR gain.

Remark 3: To characterize the performance loss when the number of antennas at Eve N_{E} or the number of eavesdroppers M increases to $N_{\mathrm{E}}+1$ and $M+1$, we define the following ratio of secrecy array gain as

$$\left.\frac{G_{\mathrm{a}}(N_{\mathrm{E}}+1)}{G_{\mathrm{a}}(N_{\mathrm{E}})}\right|_{\mathrm{dB}} = \begin{cases} \frac{10}{m_{\mathrm{B}} N_{\mathrm{B}}} \log_{10}\left(\frac{\vartheta_1(N_{\mathrm{E}}+1)}{\vartheta_1(N_{\mathrm{E}})}\right), & \rho \neq 1 \\ \frac{10}{k m_{\mathrm{B}} N_{\mathrm{B}}} \log_{10}\left(\frac{\vartheta_2(N_{\mathrm{E}}+1)}{\vartheta_2(N_{\mathrm{E}})}\right), & \rho = 1 \end{cases} \tag{23}$$

and

$$\left.\frac{G_{\mathrm{a}}(M+1)}{G_{\mathrm{a}}(M)}\right|_{\mathrm{dB}} = \begin{cases} \frac{10}{m_{\mathrm{B}} N_{\mathrm{B}}} \log_{10}\left(\frac{\vartheta_1(M+1)}{\vartheta_1(M)}\right), & \rho \neq 1 \\ \frac{10}{k m_{\mathrm{B}} N_{\mathrm{B}}} \log_{10}\left(\frac{\vartheta_2(M+1)}{\vartheta_2(M)}\right), & \rho = 1 \end{cases}. \tag{24}$$

Hence, by using (19) and (20) together with (23) and (24), the SNR gap can be easily evaluated when increasing the number of antennas N_{E} and the number of eavesdroppers M.

3) ε-Outage Secrecy Capacity: For a typical delay-limited wireless communications system scenario, ε-outage secrecy capacity is an appropriate metric to evaluate the secrecy performance of MIMO wiretap channels. The ε-outage secrecy capacity is defined as the largest secrecy rate $R_{\mathrm{S,max}}$ such that the outage probability is equal to ε. Mathematically, it can be expressed as

$$C_{\mathrm{out}}(\varepsilon) = R_{\mathrm{S,max}}, \tag{25}$$

where $P_{\mathrm{out}}(R_{\mathrm{S,max}}) = \varepsilon$. Hence, substituting (17) into (25), the outage secrecy capacity of MIMO wiretap channels with general-order TAS/MRC can be easily obtained by numerical evaluation.

Alternatively, to avoid using numerical root-finding, we can apply Gaussian approximation to find a tight expression for the ε-outage secrecy capacity of the system. Firstly, the t-th moment of $\widehat{\gamma}_{(k\mathrm{B})}$ and γ_{E} are respective given as (26) and

$$\begin{aligned} \mathrm{E}\left[\gamma_{\mathrm{E}}^{t}\right] &= \int_0^{\infty} x^t f_{\gamma_{\mathrm{E}}}(x)\, dx \\ &= M \sum_{v=0}^{M-1} \binom{M-1}{v} \frac{(-1)^v \Phi_{\mathrm{E}}}{\Gamma(N_{\mathrm{E}} m_{\mathrm{E}})} \left(\frac{\overline{\gamma}_{\mathrm{E}}}{m_{\mathrm{E}}}\right)^t \frac{\Gamma(t+\phi_{\mathrm{E}}+N_{\mathrm{E}} m_{\mathrm{E}})}{(1+v)^{t+\phi_{\mathrm{E}}+N_{\mathrm{E}} m_{\mathrm{E}}}}. \end{aligned} \tag{27}$$

Resorting to [20], the capacity of the main channel can be expanded in Taylor series in terms of the expected value of the effective SNR as

$$\begin{aligned} C_{\mathrm{B}}\left(\widehat{\gamma}_{(k\mathrm{B})}\right) &= \log_2\left(1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]\right) \\ &\quad + \log_2 e \sum_{m=1}^{\infty} (-1)^{m-1} \frac{\left(\widehat{\gamma}_{(k\mathrm{B})} - \mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]\right)^m}{m\left(1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]\right)^m}. \end{aligned} \tag{28}$$

Then, the expectation of C_{B} is approximated as

$$\mathrm{E}[C_{\mathrm{B}}] \approx \log_2\left(1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]\right) - \frac{\log_2 e \cdot \mathrm{D}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]}{2\left(1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]\right)^2}, \tag{29}$$

where $\mathrm{D}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]$ is the variance of $\widehat{\gamma}_{(k\mathrm{B})}$. Furthermore, by expanding C_{B}^2 in Taylor series about the expected SNR and applying the expectation operator, the second moment of the capacity of the main channel can be approximated as

$$\begin{aligned} \mathrm{E}\left[C_{\mathrm{B}}^2\right] &= \left[\log_2\left(1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]\right)\right]^2 \\ &\quad + \frac{\mathrm{D}\left[\widehat{\gamma}_{(k\mathrm{B})}\right] \log_2 e}{\left(1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]\right)^2} \log_2\left(\frac{e}{1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]}\right). \end{aligned} \tag{30}$$

Then, according to (29) and (30), the variance of the capacity of the main channel is given by

$$\mathrm{D}[C_{\mathrm{B}}] \approx \frac{(\log_2 e)^2 \cdot \mathrm{D}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]}{\left(1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]\right)^2} - \frac{(\log_2 e)^2 \cdot \mathrm{D}^2\left[\widehat{\gamma}_{(k\mathrm{B})}\right]}{4\left(1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]\right)^4}. \tag{31}$$

Similarly, by substituting the corresponding parameters into (29) and (31), we can get the expectation and variance of C_{E}, respectively. When $C_{\mathrm{B}} > C_{\mathrm{E}}$, secrecy capacity C_{S} is also a Gaussian variable due to the fact that it is a linear combination of the two independent Gaussian variables. Hence, we have $\mathrm{E}[C_{\mathrm{S}}] = \mathrm{E}[C_{\mathrm{B}}] - \mathrm{E}[C_{\mathrm{E}}]$ and $\mathrm{D}[C_{\mathrm{S}}] = \mathrm{D}[C_{\mathrm{B}}] + \mathrm{D}[C_{\mathrm{E}}]$. Thus, a gaussian approximation of the CDF of the secrecy capacity is

$$F_{C_{\mathrm{S}}}(x) \approx 1 - \frac{1}{2}\mathrm{erfc}\left(\frac{x - \mathrm{E}[C_{\mathrm{B}}]}{\sqrt{2\mathrm{D}[C_{\mathrm{B}}]}}\right), \tag{32}$$

where $\mathrm{erfc}\left(\cdot\right)$ is the complementary error function. Then, according to the definition of the ε-outage secrecy capacity, and utilizing (32), we have

$$C_{\mathrm{out}}\left(\varepsilon\right) \approx \log_2 e\left[\ln\left(\frac{\mu_{\mathrm{B}}}{\mu_{\mathrm{E}}}\right) - \frac{\sigma_{\mathrm{B}}^2}{2\mu_{\mathrm{B}}^2} + \frac{\sigma_{\mathrm{E}}^2}{2\mu_{\mathrm{E}}^2}\right] + \sqrt{2}\log_2 e\left[\frac{\sigma_{\mathrm{B}}^2}{\mu_{\mathrm{B}}^2} - \frac{\sigma_{\mathrm{B}}^2}{4\mu_{\mathrm{B}}^4} + \frac{\sigma_{\mathrm{E}}^2}{\mu_{\mathrm{E}}^2} - \frac{\sigma_{\mathrm{E}}^2}{4\mu_{\mathrm{E}}^4}\right]^{\frac{1}{2}} \mathrm{erfc}^{-1}\left(2-2\varepsilon\right), \tag{33}$$

where $\mu_{\mathrm{B}} = 1+\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}\right]$, $\mu_{\mathrm{E}} = 1+\mathrm{E}\left[\gamma_{\mathrm{E}}\right]$, $\sigma_{\mathrm{B}}^2 = \mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}^2\right] - \mathrm{E}^2\left[\widehat{\gamma}_{(k\mathrm{B})}\right]$, and $\sigma_{\mathrm{E}}^2 = \mathrm{E}\left[\gamma_{\mathrm{E}}^2\right] - \mathrm{E}^2\left[\gamma_{\mathrm{E}}\right]$.

C. Scenario II: CSI of the eavesdropper's channel is available at Alice

In this subsection, we consider the scenario, where Alice has knowledge of CSI about the eavesdropper's channel. Different to Scenario I, the average secrecy capacity is taken as the principal secrecy performance metric, since Alice can adapt transmission rate according to both CSI of the main channel and eavesdropper's channel to achieve perfect secure transmission.

1) Average Secrecy Capacity: By recalling the definition of the achieved secrecy rate defined in (6), we have

$$C_{\mathrm{S}} = \int_0^\infty \int_z^\infty \left[\log_2\left(1+x\right) - \log_2\left(1+z\right)\right] \times f_{\gamma_{\mathrm{E}}}\left(z\right) f_{\widehat{\gamma}_{(k\mathrm{B})}}\left(x\right) dzdx. \tag{34}$$

To evaluate the above integrals, we adopt the same steps developed in [21]. First, we evaluate the inner integral by applying integration by parts, and after applying some algebraic manipulations, the average secrecy capacity can be represented as follows:

$$C_{\mathrm{S}} = \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_{\mathrm{E}}}\left(z\right)}{1+z}\left[\int_z^\infty f_{\widehat{\gamma}_{(k\mathrm{B})}}\left(x\right)dx\right]dz. \tag{35}$$

By inserting (8) and (12) into (35), and performing some simple mathematical manipulations, the closed-form expression for average secrecy capacity can be found as (36).

2) Asymptotic Average Secrecy Capacity: To capture the impact of key system parameters on the average secrecy capacity, we proceed to analyze the asymptotic average secrecy capacity of the system in the high SNR regime. In doing so, we provide two novel metrics to characterize the asymptotic average secrecy capacity, i.e., the high SNR slope and the high SNR power offset.

Before delving into the detail analysis of the asymptotic average secrecy capacity, we first rewrite the CDF of γ_{E} as $F_{\gamma_{\mathrm{E}}}\left(x\right) = 1 - \lambda_{\gamma_{\mathrm{E}}}\left(x\right)$, where

$$\lambda_{\gamma_{\mathrm{E}}}\left(x\right) = \sum_{v=1}^{M}\binom{M}{v}(-1)^{v+1}\Phi_{\mathrm{E}}\left(\frac{m_{\mathrm{E}}x}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}} e^{-\frac{vm_{\mathrm{E}}x}{\overline{\gamma}_{\mathrm{E}}}}. \tag{37}$$

Then, taking into consideration (37), the average secrecy capacity can be re-expressed as

$$C_{\mathrm{S}} = \frac{1}{\ln 2}\int_0^\infty \left[\int_0^x \frac{1-\lambda_{\gamma_{\mathrm{E}}}\left(z\right)}{1+z}dz\right] f_{\widehat{\gamma}_{(k\mathrm{B})}}\left(x\right)dx = \varpi_1 - \varpi_2, \tag{38}$$

where

$$\varpi_1 = \frac{1}{\ln 2}\int_0^\infty \ln\left(1+x\right) f_{\widehat{\gamma}_{(k\mathrm{B})}}\left(x\right)dx \tag{39}$$

and

$$\varpi_2 = \frac{1}{\ln 2}\int_0^\infty \int_0^x \frac{\lambda_{\gamma_{\mathrm{E}}}\left(z\right)}{1+z} f_{\widehat{\gamma}_{(k\mathrm{B})}}\left(x\right)dzdx. \tag{40}$$

Next, we derive ϖ_1 and ϖ_2 in the high SNR regime, respectively. When $x \to \infty$, we have $\ln\left(1+x\right) \approx \ln x$. Hence, by substituting the PDF of $\widehat{\gamma}_{(k\mathrm{B})}$ and utilizing [18, Eq. (4.352.1)], we have

$$\varpi_1^\infty = \frac{k}{\ln 2}\binom{N_{\mathrm{A}}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^n}{\Gamma\left(m_{\mathrm{B}}N_{\mathrm{B}}\right)}\Phi_{\mathrm{B}} \times \sum_{i=0}^{\phi_{\mathrm{B}}}\binom{\phi_{\mathrm{B}}}{i}\Gamma\left(\phi_{\mathrm{B}}+m_{\mathrm{B}}N_{\mathrm{B}}\right)\frac{\rho^i(1-\rho)^{\phi_{\mathrm{B}}-i}}{\xi^{\phi_{\mathrm{B}}}\alpha^{m_{\mathrm{B}}N_{\mathrm{B}}+i}} \times \left[\psi\left(m_{\mathrm{B}}N_{\mathrm{B}}+i\right) + \ln\left(\frac{\xi}{\alpha m_{\mathrm{B}}}\right)\right] + \log_2\overline{\gamma}_{\mathrm{B}}, \tag{41}$$

where $\psi\left(\cdot\right)$ is the digamma function [22].

Similarly, according to [21, Eq. (19)], the asymptotic expression for ϖ_2 is derived as

$$\varpi_2^\infty = \frac{1}{\ln 2}\int_0^\infty \frac{\lambda_{\gamma_{\mathrm{E}}}\left(x\right)}{1+x}dx = \frac{1}{\ln 2}\sum_{v=1}^{M}\binom{M}{v}(-1)^{v+1}\Phi_{\mathrm{E}}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}} \times \Gamma\left(\phi_{\mathrm{E}}+1\right)\Psi\left(\phi_{\mathrm{E}}+1, \phi_{\mathrm{E}}+1; \frac{vm_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right). \tag{42}$$

Finally, substituting (41) and (42) into (38), the asymptotic average secrecy capacity of MIMO wiretap channels is derived as (43).

As the conventional non-secrecy network, we also analyze the high SNR slope and the high SNR power offset to gain the characterization of the average secrecy capacity in the high SNR regime. To facilitate the asymptotic analysis, we use the following general form to express the average secrecy capacity as

$$C_{\mathrm{S}}^\infty = \mathcal{S}_\infty\left(\log_2\overline{\gamma}_{\mathrm{B}} - \mathcal{L}_\infty\right), \tag{44}$$

where $\mathcal{S}_\infty$ denotes the high SNR slope in bits/s/Hz (3dB) and $\mathcal{L}_\infty$ is the high SNR power offset in 3dB units.

According to [23]–[25], the high SNR slope is given by

$$\mathcal{S}_\infty = \lim_{\overline{\gamma}_{\mathrm{B}}\to\infty}\frac{C_{\mathrm{S}}^\infty}{\log_2\overline{\gamma}_{\mathrm{B}}}. \tag{45}$$

Substituting (43) into (45) and performing some mathematical manipulations, we have

$$\mathcal{S}_\infty = 1. \tag{46}$$

This result demonstrates that the key parameters, such as the number of antennas, the number of eavesdroppers, correlation coefficient, and fading severity parameters, have no impact on the high SNR slope.

$$\mathrm{E}\left[\widehat{\gamma}_{(k\mathrm{B})}^{t}\right] = \int_0^\infty x^t f_{\widehat{\gamma}_{(k\mathrm{B})}}(x)\,dx$$
$$= k\binom{N_\mathrm{A}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^n\Phi_\mathrm{B}}{\Gamma(m_\mathrm{B}N_\mathrm{B})}\sum_{i=0}^{\phi_\mathrm{B}}\binom{\phi_\mathrm{B}}{i}\frac{\Gamma(\phi_\mathrm{B}+m_\mathrm{B}N_\mathrm{B})}{\Gamma(m_\mathrm{B}N_\mathrm{B}+i)}\left(\frac{\overline{\gamma}_\mathrm{B}}{m_\mathrm{B}}\right)^t\frac{\rho^i(1-\rho)^{\phi_\mathrm{B}-i}\Gamma(t+m_\mathrm{B}N_\mathrm{B}+i)}{\xi^{\phi_\mathrm{B}-t}\alpha^{t+m_\mathrm{B}N_\mathrm{B}+i}} \quad (26)$$

$$C_\mathrm{S} = \frac{1}{\ln 2}k\binom{N_\mathrm{A}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^n\Phi_\mathrm{B}}{\Gamma(m_\mathrm{B}N_\mathrm{B})}\sum_{i=0}^{\phi_\mathrm{B}}\binom{\phi_\mathrm{B}}{i}\Gamma(\phi_\mathrm{B}+m_\mathrm{B}N_\mathrm{B})\frac{\rho^i(1-\rho)^{\phi_\mathrm{B}-i}}{\xi^{\phi_\mathrm{B}}\alpha^{m_\mathrm{B}N_\mathrm{B}+i}}\sum_{m=0}^{m_\mathrm{B}N_\mathrm{B}+i-1}\frac{1}{m!}\left(\frac{\alpha m_\mathrm{B}}{\overline{\gamma}_\mathrm{B}\xi}\right)^m$$
$$\times\sum_{v=0}^{M}\binom{M}{v}(-1)^v\Phi_\mathrm{E}\left(\frac{m_\mathrm{E}}{\overline{\gamma}_\mathrm{E}}\right)^{\phi_\mathrm{E}}\Gamma(\phi_\mathrm{E}+m+1)\,\Psi\left(\phi_\mathrm{E}+m+1,\phi_\mathrm{E}+m+1;\left(\frac{vm_\mathrm{E}}{\overline{\gamma}_\mathrm{E}}+\frac{\alpha m_\mathrm{B}}{\xi\overline{\gamma}_\mathrm{B}}\right)\right) \quad (36)$$

$$C_\mathrm{S}^\infty = \log_2\overline{\gamma}_\mathrm{B} + \frac{1}{\ln 2}k\binom{N_\mathrm{A}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^n}{\Gamma(m_\mathrm{B}N_\mathrm{B})}\Phi_\mathrm{B}\sum_{i=0}^{\phi_\mathrm{B}}\binom{\phi_\mathrm{B}}{i}\Gamma(\phi_\mathrm{B}+m_\mathrm{B}N_\mathrm{B})\frac{\rho^i(1-\rho)^{\phi_\mathrm{B}-i}}{\xi^{\phi_\mathrm{B}}\alpha^{m_\mathrm{B}N_\mathrm{B}+i}}$$
$$\times\left[\psi(m_\mathrm{B}N_\mathrm{B}+i)+\ln\left(\frac{\xi}{\alpha m_\mathrm{B}}\right)\right]-\frac{1}{\ln 2}\sum_{v=1}^{M}\binom{M}{v}(-1)^{v+1}\Phi_\mathrm{E}\left(\frac{m_\mathrm{E}}{\overline{\gamma}_\mathrm{E}}\right)^{\phi_\mathrm{E}}\Gamma(\phi_\mathrm{E}+1)\,\Psi\left(\phi_\mathrm{E}+1,\phi_\mathrm{E}+1;\frac{vm_\mathrm{E}}{\overline{\gamma}_\mathrm{E}}\right) \quad (43)$$

Now, we turn our attention to the high SNR power offset. Mathematically, it can be expressed as

$$\mathcal{L}_\infty = \lim_{\overline{\gamma}_\mathrm{B}\to\infty}\left(\log_2\overline{\gamma}_\mathrm{B} - \frac{C_\mathrm{S}^\infty}{\mathcal{S}_\infty}\right). \quad (47)$$

It is noted that (47) definitely characterizes the effect of the main channel and the eavesdropper's channel on the average secrecy capacity. Hence, substituting (43) and (46) into (47), we have

$$\mathcal{L}_\infty = \mathcal{L}_\infty(N_\mathrm{A},N_\mathrm{B},m_\mathrm{B},\rho) + \mathcal{L}_\infty(M,N_\mathrm{E},m_\mathrm{E}), \quad (48)$$

where

$$\mathcal{L}_\infty(N_\mathrm{A},N_\mathrm{B},m_\mathrm{B},\rho) = -\frac{k}{\ln 2}\binom{N_\mathrm{A}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^n\Phi_\mathrm{B}}{\Gamma(m_\mathrm{B}N_\mathrm{B})}$$
$$\times\sum_{i=0}^{\phi_\mathrm{B}}\binom{\phi_\mathrm{B}}{i}\Gamma(\phi_\mathrm{B}+m_\mathrm{B}N_\mathrm{B})\frac{\rho^i(1-\rho)^{\phi_\mathrm{B}-i}}{\xi^{\phi_\mathrm{B}}\alpha^{m_\mathrm{B}N_\mathrm{B}+i}}$$
$$\times\left[\psi(m_\mathrm{B}N_\mathrm{B}+i)+\ln\left(\frac{\xi}{\alpha m_\mathrm{B}}\right)\right] \quad (49)$$

and

$$\mathcal{L}_\infty(M,N_\mathrm{E},m_\mathrm{E}) = \varpi_2^\infty. \quad (50)$$

From the above analysis, we highlight that the positive effect of the key parameters related with the main link, i.e., N_A, N_B, m_B, and ρ, on the average secrecy capacity can be quantitatively evaluated through $\mathcal{L}_\infty(N_\mathrm{A},N_\mathrm{B},m_\mathrm{B},\rho)$. On the other hand, the negative effect of the key parameters related with the eavesdropper's link, i.e., M, N_E, and m_E, on the average secrecy capacity can be characterized by $\mathcal{L}_\infty(M,N_\mathrm{E},m_\mathrm{E})$.

IV. Numerical Results

In this section, representative numerical simulations are provided to examine the joint impacts of the correlation coefficient, the number of antennas, the number of eavesdroppers, and the fading parameters on the secrecy performance. Without loss of generality, we set the predefined rate $R_\mathrm{S} = 1$ and average Eve's SNR $\overline{\gamma}_\mathrm{E} = 5\mathrm{dB}$ in the following simulations. As shown in both the figures, the analytical results are in exact agreement with the Monte Carlo simulation results and the asymptotic curves match very well with the exact curves in the high SNR regime, which corroborates the accuracy of our derivation.

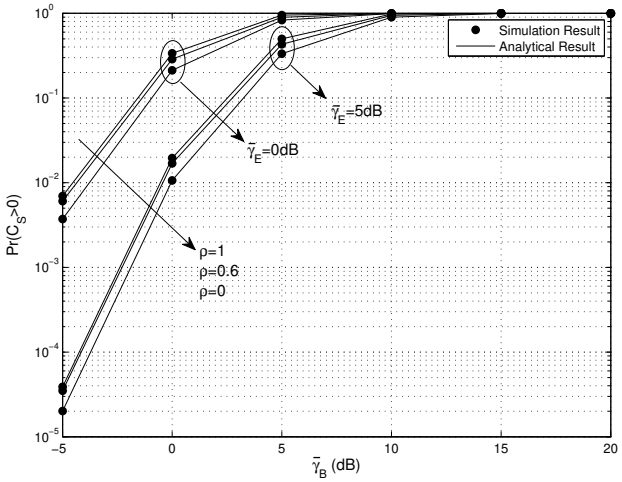

Fig. 2. The probability of non-zero secrecy capacity versus $\overline{\gamma}_\mathrm{B}$ for $N_\mathrm{A} = N_\mathrm{B} = N_\mathrm{E} = 2$, $m_\mathrm{B} = m_\mathrm{E} = 2$, $k = 2$, and $M = 2$.

Fig. 2 shows the probability of non-zero secrecy capacity of MIMO wiretap channels with different average Bob's SNR $\overline{\gamma}_\mathrm{B}$. It is observed that when the average Eve's SNR $\overline{\gamma}_\mathrm{E}$ is fixed, high feedback delay, i.e., small ρ, slightly degrades $\Pr(C_\mathrm{S} > 0)$. Moreover, we obtain a counter-intuitive phenomenon from the figure, that is even the average SNR of Eve's link is higher than that of Bob's link, a non-zero secrecy capacity also exists.

Fig. 3 examines the impact of antenna diversity and cor-

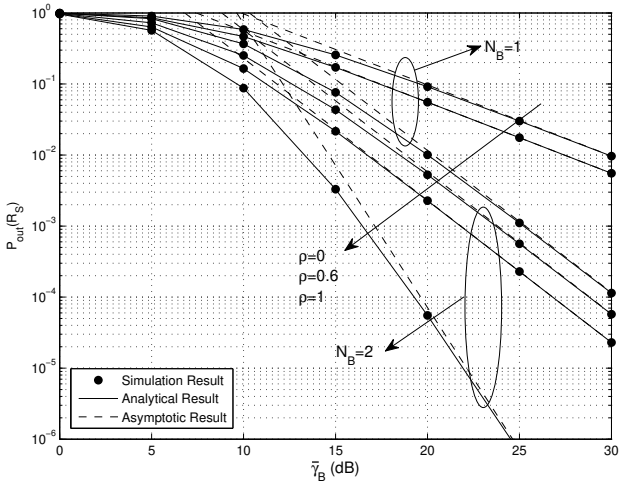

Fig. 3. The secrecy outage probability versus $\overline{\gamma}_{\rm B}$ for $N_{\rm A}=2$, $N_{\rm E}=1$, $m_{\rm B}=1$, $m_{\rm E}=2$, $k=2$, and $M=2$.

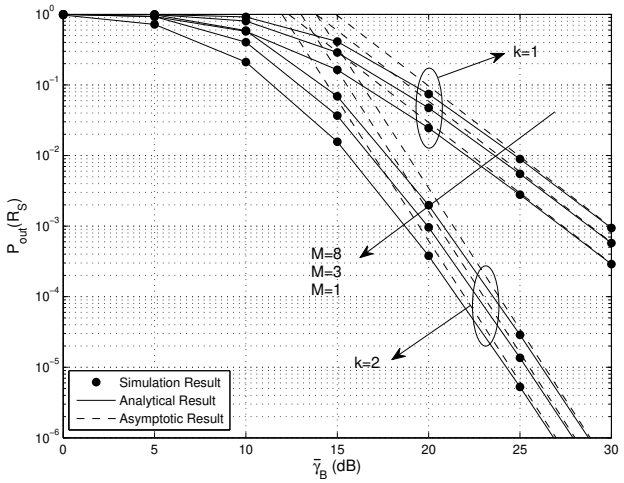

Fig. 4. The secrecy outage probability versus $\overline{\gamma}_{\rm B}$ for $N_{\rm A}=2$, $N_{\rm B}=N_{\rm E}=1$, $m_{\rm B}=m_{\rm E}=2$, and $\rho=1$.

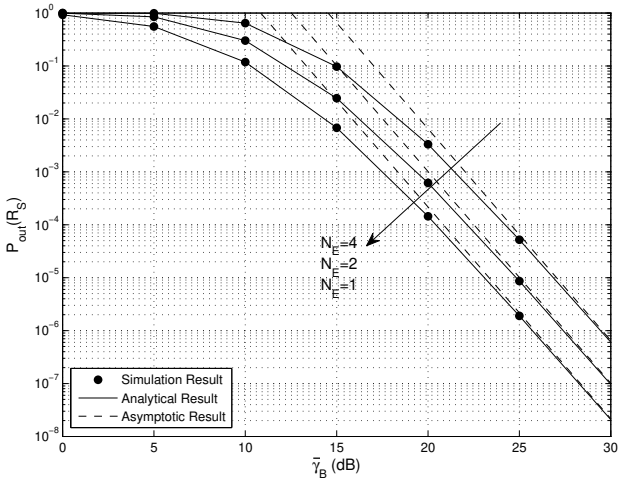

Fig. 5. The secrecy outage probability versus $\overline{\gamma}_{\rm B}$ for $N_{\rm A}=N_{\rm B}=2$, $m_{\rm B}=m_{\rm E}=1$, $k=2$, $M=2$, and $\rho=1$.

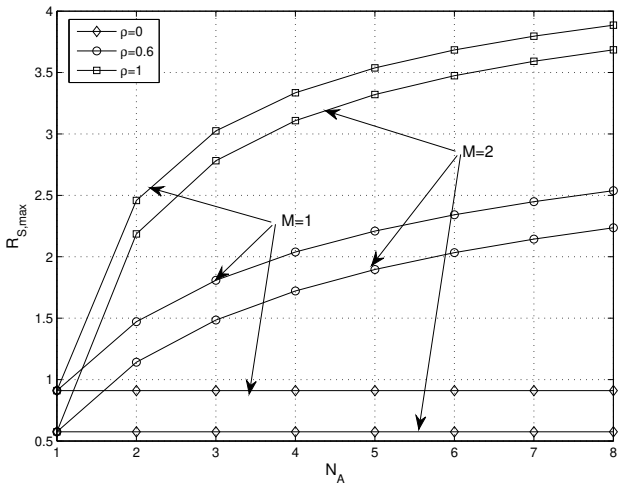

Fig. 6. The ε-outage secrecy capacity versus $N_{\rm A}$ for $\varepsilon=0.01$, $\overline{\gamma}_{\rm B}=20$dB, $\overline{\gamma}_{\rm E}=5$dB, $N_{\rm A}=N_{\rm B}=2$, and $m_{\rm B}=m_{\rm E}=1$

relation coefficient on the secrecy outage probability of the system. The exact and asymptotic results are obtained from (17) and (18), respectively. We observe that increasing $N_{\rm B}$ has significant impact on the secrecy outage probability of the considered system. This is due to the fact increasing $N_{\rm B}$ provides additional diversity order to the considered system with feedback delay or not. In addition, as will be seen, when $\rho=1$, the full diversity order can be achieved, i.e., 4 and 2 for $N_{\rm B}=2$ and $N_{\rm B}=1$, respectively. However, when $\rho\neq 1$, the diversity order will be reduced to 2 and 1.

Figs. 4 and 5 present the impact of numbers of Eve M and numbers of Eve's antenna $N_{\rm E}$ on the secrecy outage probability of the system, respectively. As shown in both figures, increasing M or $N_{\rm E}$ does not influence the achievable diversity order as indicated by the parallel slopes of the asymptotes. However, the secrecy outage performance of the system will be degraded by increasing M or $N_{\rm E}$ due to the reduction of the array gain. In addition, increasing the antenna selection parameter k can significantly improve the secrecy outage probability of the system.

Fig. 6 illustrates the ε-outage secrecy capacity of the system with different $N_{\rm A}$. As can be readily observed, $R_{\rm S,max}$ can be improved by increasing the number of antennas $N_{\rm A}$ at transmitter. Furthermore, an intuitive result that the ε-outage secrecy capacity of the system improves when feedback delay is reduced, i.e., when ρ increases from 0 to 1. In particular, increasing $N_{\rm A}$ has no impact on the ε-outage secrecy capacity when the CSI is completely outdated, i.e., $\rho=0$. This phenomenon is consistent with the result observed in [26].

Fig. 7 depicts the average secrecy capacity versus $\overline{\gamma}_{\rm B}$ for different feedback delay ρ and the number of antennas at Eve $N_{\rm E}$ in Nakagami-*m* fading channels. It is shown in this figure that the average secrecy capacity decreases with increasing $N_{\rm E}$, since increasing $N_{\rm E}$ results in the increment of the high power offset $\mathcal{L}_\infty$. Moreover, the higher feedback delay, i.e, small ρ, significantly degrades the average secrecy capacity. In addition, in Fig. 8, we evaluate the impact of antenna selection parameter k on the average secrecy capacity. From the figure, antenna selection parameter k has a positive impact on the secrecy performance, that is, increasing k results in

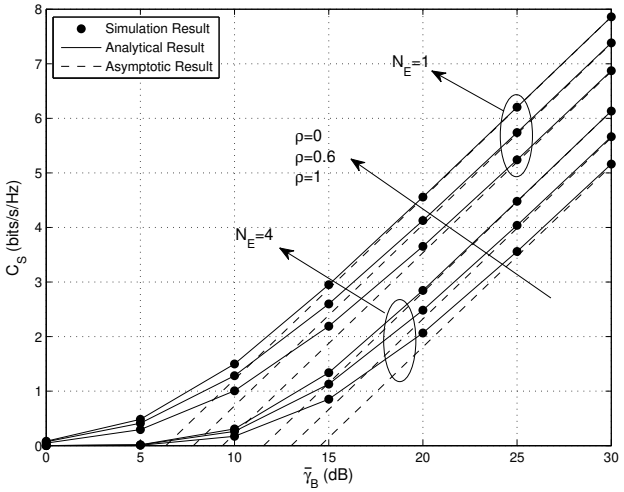

Fig. 7. The average secrecy capacity versus $\overline{\gamma}_{\rm B}$ for $N_{\rm A}=2$, $N_{\rm B}=1$, $m_{\rm B}=m_{\rm E}=1$, $k=2$, and $M=2$.

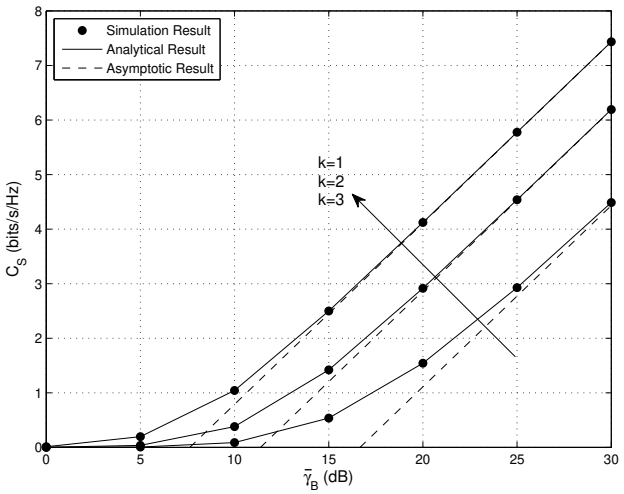

Fig. 8. The average secrecy capacity versus $\overline{\gamma}_{\rm B}$ for $N_{\rm A}=3$, $N_{\rm B}=1$, $N_{\rm E}=2$, $m_{\rm B}=m_{\rm E}=1$, $M=2$, and $\rho=1$.

the increment of the average secrecy capacity owing to the achievement of more diversity gain and coding gain.

Fig. 9 shows the effect of the number of antenna at Bob $N_{\rm B}$ and the number of eavesdroppers M on the average secrecy capacity. As illustrated in the figure, we can see that the average secrecy capacity is improved as increasing $N_{\rm B}$. This is due to the fact increasing $N_{\rm B}$ brings about additional power gains via MRC at Bob. Furthermore, increasing M also reduces the average secrecy capacity. In addition, an interesting phenomenon that the secrecy capacity slope keeps the same under any parameter configurations can be obtained, which is valid for the result as in (46).

V. Conclusions

In this paper, we have investigated the effect of outdated CSI on the secrecy performance of MIMO wiretap channels with multiple eavesdroppers in non-identical Nakagami-*m* fading. Specifically, two practical scenarios were considered, i.e., Scenario I: Alice has no knowledge of CSI about the

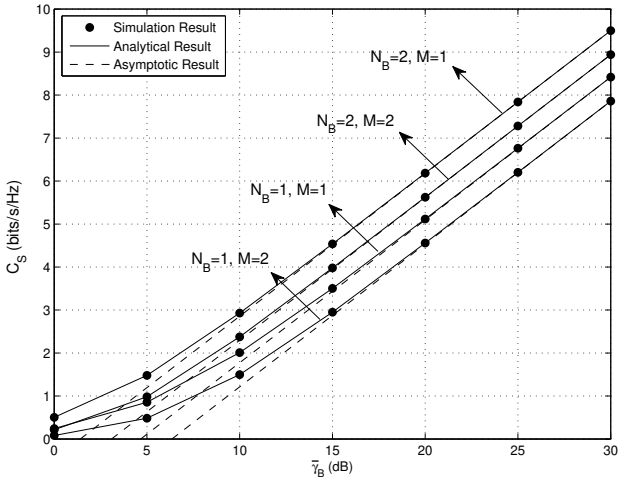

Fig. 9. The average secrecy capacity versus $\overline{\gamma}_{\rm B}$ for $N_{\rm A}=2$, $N_{\rm E}=1$, $m_{\rm B}=m_{\rm E}=1$, $k=2$, and $\rho=1$.

eavesdropper's channel, and Scenario II: Alice has knowledge of CSI about the eavesdropper's channel. For Scenario I, we have derived closed-form expressions for the probability of non-zero secrecy capacity, the secrecy outage probability, and the ε-outage secrecy capacity of the considered system with general-order TAS/MRC scheme, which provide fast and efficient means to evaluate the secrecy performance of the system. Moreover, simple and informative high SNR approximations for the secrecy outage probability was derived, which enables us to gain further insights into the impact of key parameters on the secrecy performance. The findings of this paper suggest that the full diversity order, i.e., $km_{\rm B}N_{\rm B}$, can be achieved under the case of perfect CSI. However, when the CSI is outdated, the diversity order is reduced to $m_{\rm B}N_{\rm B}$, which means the transmitter diversity disappears. For Scenario II, we also provided the exact and asymptotic closed-form expressions for the average secrecy capacity, which make us easily to characterize the effect of the main channel and the eavesdropper's channel on the average capacity through the high SNR power offset. In addition, an un-intuitional result that the high SNR slope is independent of all system parameters was observed.

Appendix A
Proof of Lemma 1

According to [27], the PDF of $\gamma_{(k{\rm B})}$ is given by

$$f_{\gamma_{(k{\rm B})}}=k\binom{N_{\rm A}}{k}\left[F_{\gamma_{i{\rm B}}}(x)\right]^{k-1}\left[1-F_{\gamma_{i{\rm B}}}(x)\right]^{N_{\rm A}-k}f_{\gamma_{i{\rm B}}}(x)\,, \tag{51}$$

where

$$f_{\gamma_{i{\rm B}}}(x)=\left(\frac{m_{\rm B}}{\overline{\gamma}_{\rm B}}\right)^{N_{\rm B}m_{\rm B}}\frac{x^{N_{\rm B}m_{\rm B}-1}}{\Gamma(N_{\rm B}m_{\rm B})}e^{-\frac{m_{\rm B}x}{\overline{\gamma}_{\rm B}}} \tag{52}$$

and

$$F_{\gamma_{i{\rm B}}}(x)=1-e^{-\frac{m_{\rm B}x}{\overline{\gamma}_{\rm B}}}\sum_{k=0}^{N_{\rm B}m_{\rm B}-1}\frac{x^k}{k!}\left(\frac{m_{\rm B}}{\overline{\gamma}_{\rm B}}\right)^k. \tag{53}$$

$$f_{\widehat{\gamma}_{(k\mathrm{B})}}(x) = k\binom{N_\mathrm{A}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}\frac{(-1)^n\Phi_\mathrm{B}}{\Gamma(m_\mathrm{B}N_\mathrm{B})(1-\rho)}\left(\frac{m_\mathrm{B}}{\overline{\gamma}_\mathrm{B}}\right)^{\phi_\mathrm{B}+m_\mathrm{B}N_\mathrm{B}+1}\left(\frac{x}{\rho}\right)^{\frac{m_\mathrm{B}N_\mathrm{B}-1}{2}} \times e^{-\frac{xm_\mathrm{B}}{(1-\rho)\overline{\gamma}_\mathrm{B}}}\underbrace{\int_0^\infty z^{\phi_\mathrm{B}+\frac{m_\mathrm{B}N_\mathrm{B}-1}{2}}e^{-z\left[\frac{m_\mathrm{B}}{(1-\rho)\overline{\gamma}_\mathrm{B}}+\frac{(N_\mathrm{A}+n-k)m_\mathrm{B}}{\overline{\gamma}_\mathrm{B}}\right]}I_{m_\mathrm{B}N_\mathrm{B}-1}\left(\frac{2m_\mathrm{B}\sqrt{\rho xz}}{(1-\rho)\overline{\gamma}_\mathrm{B}}\right)dz}_{\Delta_1} \quad (57)$$

$$\Delta_1 = \frac{\Gamma(\phi_\mathrm{B}+m_\mathrm{B}N_\mathrm{B})}{\Gamma(m_\mathrm{B}N_\mathrm{B})}\frac{(1-\rho)\overline{\gamma}_\mathrm{B}}{m_\mathrm{B}\sqrt{\rho x}}e^{\frac{\rho m_\mathrm{B}x}{2\overline{\gamma}_\mathrm{B}\xi(1-\rho)}}\left[\frac{m_\mathrm{B}\xi}{\overline{\gamma}_\mathrm{B}(1-\rho)}\right]^{-\phi_\mathrm{B}-\frac{m_\mathrm{B}N_\mathrm{B}}{2}}M_{-\phi_\mathrm{B}-\frac{m_\mathrm{B}N_\mathrm{B}}{2},\frac{m_\mathrm{B}N_\mathrm{B}-1}{2}}\left(\frac{\rho m_\mathrm{B}x}{\overline{\gamma}_\mathrm{B}\xi(1-\rho)}\right) \quad (58)$$

Considering the relation between $\gamma_{(k\mathrm{B})}$ and $\widehat{\gamma}_{(k\mathrm{B})}$, the PDF of $\widehat{\gamma}_{(k\mathrm{B})}$ can be derived as

$$f_{\widehat{\gamma}_{(k\mathrm{B})}}(x) = \int_0^\infty f_{\widehat{\gamma}_{(k\mathrm{B})}|\gamma_{(k\mathrm{B})}}(x|\,z)\,f_{\gamma_{(k\mathrm{B})}}(z)\,dz, \quad (54)$$

where

$$f_{\widehat{\gamma}_{(k\mathrm{B})}|\gamma_{(k\mathrm{B})}}(x|\,z) = \frac{f_{\widehat{\gamma}_{i\mathrm{B}},\gamma_{i\mathrm{B}}}(x,z)}{f_{\gamma_{i\mathrm{B}}}(z)}. \quad (55)$$

Correspondingly, the joint PDF of $\widehat{\gamma}_{i\mathrm{B}}$ and $\gamma_{i\mathrm{B}}$ is given by [17]

$$f_{\widehat{\gamma}_{i\mathrm{B}},\gamma_{i\mathrm{B}}}(x,z) = \left(\frac{m_\mathrm{B}}{\overline{\gamma}_\mathrm{B}}\right)^{m_\mathrm{B}N_\mathrm{B}+1}\frac{(xz/\rho)^{\frac{m_\mathrm{B}N_\mathrm{B}-1}{2}}}{\Gamma(m_\mathrm{B}N_\mathrm{B})(1-\rho)} \times e^{-\left(\frac{x+z}{1-\rho}\right)\frac{m_\mathrm{B}}{\overline{\gamma}_\mathrm{B}}}I_{m_\mathrm{B}N_\mathrm{B}-1}\left(\frac{2m_\mathrm{B}\sqrt{\rho xz}}{(1-\rho)\overline{\gamma}_\mathrm{B}}\right), \quad (56)$$

where $I_n(\cdot)$ is the n-th modified Bessel function of the first kind [18, Eq. (8.406.1)].

By combining (51)-(56) and utilizing the multinomial theorem, the PDF of $\widehat{\gamma}_{(k\mathrm{B})}$ is expanded as (57). Resorting to [18, Eq. (6.643.2)] and performing some simple mathematical manipulations, Δ_1 is derived as (58), where $M_{a,b}(\cdot)$ is the Whittaker-M function [18, Eq. (9.220.2)], which can be reexpressed in terms of the polynomial as

$$M_{a,b}(z) = e^{\frac{z}{2}}\sum_{k=0}^{-b-a-\frac{1}{2}}C_k^{-b-a-\frac{1}{2}}z^{b+k+\frac{1}{2}}\frac{\Gamma(2b+1)}{\Gamma(2b+k+1)}. \quad (59)$$

To this end, the desired PDF of $\widehat{\gamma}_{(k\mathrm{B})}$ is given by (8) with the help of (59). Obviously, the CDF of $\widehat{\gamma}_{(k\mathrm{B})}$ can be derived by integrating the PDF of $\widehat{\gamma}_{(k\mathrm{B})}$.

APPENDIX B
PROOF OF THEOREM 1

When $\rho = 1$ and $\overline{\gamma}_\mathrm{B} \to \infty$, the PDF of $\gamma_{(k\mathrm{B})}$ can be approximated as

$$f_{\gamma_{(kB)}} \approx k\binom{N_\mathrm{A}}{k}\left(\frac{m_\mathrm{B}}{\overline{\gamma}_\mathrm{B}}\right)^{kN_\mathrm{B}m_\mathrm{B}}\frac{x^{kN_\mathrm{B}m_\mathrm{B}-1}}{[\Gamma(N_\mathrm{B}m_\mathrm{B})]^k(N_\mathrm{B}m_\mathrm{B})^{k-1}}. \quad (60)$$

Then, substituting (60) into (16) and utilizing [18, Eq. (9.211.4)], the asymptotic secrecy outage probability result can be derived as (18) after some mathematical manipulations.

On the other hand, when $\rho \neq 1$ and $\overline{\gamma}_\mathrm{B} \to \infty$, we have

$$f_{\widehat{\gamma}_{(k\mathrm{B})}}(x) \approx k\binom{N_\mathrm{A}}{k}\sum_{n=0}^{k-1}\binom{k-1}{n}(-1)^n\Phi_\mathrm{B} \times \left(\frac{m_\mathrm{B}}{\overline{\gamma}_\mathrm{B}}\right)^{m_\mathrm{B}N_\mathrm{B}}\frac{\Gamma(\phi_\mathrm{B}+m_\mathrm{B}N_\mathrm{B})(1-\rho)^{\phi_\mathrm{B}}}{[\Gamma(m_\mathrm{B}N_\mathrm{B})]^2\xi^{m_\mathrm{B}N_\mathrm{B}+\phi_\mathrm{B}}}x^{m_\mathrm{B}N_\mathrm{B}-1}. \quad (61)$$

By following the similar lines, the approximated result for the secrecy outage probability under the case of outdated CSI can be easily obtained after some mathematical manipulations.

REFERENCES

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

[2] R. Liu and W. Trappe, *Securing Communications at the Physical Layer*. New York: Springer, 2010.

[3] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Commun. Mag.*, vol. 19, no. 1, pp. 40-47, Feb. 2012.

[4] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journ.*, vol. 54, pp. 1355-1387, 1975.

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

[6] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509-511, May 2011.

[7] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing security in correlated channel with maximal ratio combining diversity," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6745-6751, Dec. 2012.

[8] N. Yang, P. L. Yeoh, 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, Jan. 2013.

[9] N. Yang, P. L. Yeoh, 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, Sep. 2013.

[10] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-*m* channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054-6067, Nov. 2014.

[11] N. S. Ferdinand, D. B. da. Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864-867, May 2013.

[12] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K. K. Wong, "Secrecy performance analysis for TAS-MRC system with imperfect feedback," *IEEE Trans. Inf. Forensics Security*, accepted for publication, in 2015.

[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[14] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[15] Y. Huang, F. Al-Qahtani, C. Zhong, Q. Wu, J. Wang, and H. Alnuweiri, "Performance analysis of multiuser multiple antenna relaying networks with co-channel interference and feedback delay," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 59-73, Jan. 2014.
[16] N. S. Ferdinand, N. Rajatheva, and M. Latva-aho, "Effects of feedback delay in partial relay selection over Nakagami-*m* fading channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1620-1634, May 2012.
[17] M. K. Simon and M.-S. Alouini, *Digital Communications over Fading Channels: A Unified Approach to Performance Analysis*, 1st ed., New York: John Wiley and Sons, 2000.
[18] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.
[19] V. U. Prabhu and M. R. D.Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853-860, Sep. 2011.
[20] J. Pérez, J. Ibánez, L. Vielva, and I. Santamaria, "Closed-form approximation for the outage capacity of orthogonal STBC," *IEEE Commun. Lett.*, vol. 9, no. 11, pp. 961-963, Nov. 2005.
[21] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247-258, Feb. 2014.
[22] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*, 9th ed. New York, NY, USA: Dover, 1970.
[23] A. Lozano, A. Tulino, and S. Verdú, "High-SNR power offset in multiantenna communication," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4134-4151, Dec. 2005.
[24] S. Jin, M. McKay, C. Zhong, and K.-K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2204-2224, May 2010.
[25] R. H. Y. Louie, M. R. McKay, and I. B. Collings, "New performance results for multiuser optimum combining in the presence of Rician fading," *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2348-2358, Aug. 2009.
[26] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.
[27] R. M. Radaydeh and M.-S. Alouini, "On the performance of arbitrary transmit selection for threshold-based receive MRC with and without co-channel interference," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3177-3191, Nov. 2011.

Yuzhen Huang received his B.S. degree in Communications Engineering, and Ph.D. degree in Communications and Information Systems from College of Communications Engineering, PLA University of Science and Technology, in 2008 and 2013 respectively. He has been with College of Communications Engineering, PLA University of Science and Technology since 2013, and currently as an Assistant Professor. His research interests focus on channel coding, MIMO communications systems, cooperative communications, physical layer security, and cognitive radio systems. He has published nearly 20 research papers in international journals and conferences such as IEEE TCOM, IEEE TVT, IEEE CL, WCNC, etc. He and his coauthors has been awarded a Best Paper Award at the WCSP 2013. He received an IEEE COMMUNICATIONS LETTERS exemplary reviewer certificate for 2014.

Fawaz S. Al-Qahtani (M'10) received the B.Sc. in electrical engineering from King Fahad University of Petroleum and Minerals (KFUPM), Saudi Arabia in 2000 and his M.Sc. in Digital Communication Systems from Monash University, Australia in 2005, and Ph.D. degree in Electrical and Computer Engineering, RMIT University, Australia. Since May 2010, he has been with Texas A&M University at Qatar, where he is an assistant research scientist. His research interests are digital communications, channel modeling, applied signal processing, MIMO communication systems, cooperative communications, cognitive radio systems, and physical layer security.

Trung Q. Duong (S'05, M'12, SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, mm-waves communications, and localization for radios and networks. He is the author or co-author of 170 technical papers published in scientific journals and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE COMMUNICATIONS LETTERS, IET COMMUNICATIONS, WILEY TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES. He has also served as the Guest Editor of the special issue on some major journals including IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS MAGAZINE, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014.

Jinlong Wang (SM'13) received the B.S. degree in mobile communications, M.S. degree and Ph.D. degree in communications engineering and information systems from Institute of Communications Engineering, Nanjing, China, in 1983, 1986 and 1992, respectively. Since 1979, Dr. Wang has been with the Institute of Communications Engineering, PLA University of Science and Technology, where he is currently a Full Professor and the Head of Institute of Communications Engineering. He has published over 100 papers in refereed mainstream journals and reputed international conferences and has been granted over 20 patents in his research areas. His current research interests are the broad area of digital communications systems with emphasis on cooperative communication, adaptive modulation, multiple-input-multiple-output systems, soft defined radio, cognitive radio, green wireless communications, and game theory.

Dr. Wang also has served as the Founding Chair and Publication Chair of International Conference on Wireless Communications and Signal Processing (WCSP) 2009, a member of the Steering Committees of WCSP2010-2012, a TPC member for several international conferences and a reviewer for many famous journals. He currently is the vice-chair of the IEEE Communications Society Nanjing Chapter and is an IEEE Senior Member.