Secure Transmission With Antenna Selection in MIMO Nakagami-m Fading Channels

Lifeng Wang, *Student Member, IEEE*, Maged Elkashlan, *Member, IEEE*, Jing Huang, *Member, IEEE*, Robert Schober, *Fellow, IEEE*, and Ranjan K. Mallik, *Fellow, IEEE*

***Abstract*—This paper considers transmit antenna selection (TAS) and receive generalized selection combining (GSC) for secure communication in the multiple-input–multiple-output wiretap channel, where confidential messages transmitted from an N_A-antenna transmitter to an N_B-antenna legitimate receiver are overheard by an N_E-antenna eavesdropper. We assume that the main channel and the eavesdropper's channel undergo Nakagami-m fading with fading parameters m_B and m_E, respectively. In order to assess the secrecy performance, we present a new unifying framework for the average secrecy rate and the secrecy outage probability. We first derive expressions for the probability density function and the cumulative distribution function of the signal-to-noise ratio with TAS/GSC, from which we derive exact expressions for the average secrecy rate and the secrecy outage probability. We then derive compact expressions for the asymptotic average secrecy rate and the asymptotic secrecy outage probability for two distinct scenarios: 1) the legitimate receiver is located close to the transmitter, and 2) the legitimate receiver and the eavesdropper are located close to the transmitter. For these scenarios, we present new closed-form expressions for several key performance indicators: 1) the capacity slope and the power offset of the asymptotic average secrecy rate, and 2) the secrecy diversity order and the secrecy array gain of the asymptotic secrecy outage probability. For the first scenario, we confirm that the capacity slope is one and the secrecy diversity order is $m_B N_B N_A$. For the second scenario, we confirm that the capacity slope and the secrecy diversity order collapse to zero.**

***Index Terms*—Diversity combining, average secrecy rate, Nakagami-m fading, physical layer security, secrecy outage probability.**

I. Introduction

SECURE transmission in wireless networks is confronted with increasing problems due to the rapid evolution of future wireless network architectures [1]–[3]. Mobile terminals are more vulnerable to eavesdropping than their fixed counterparts. Furthermore, the trend towards network densification and multi-layer deployments, as well as the development of decentralized wireless mesh networks pose great challenges to the implementation of higher-layer key distribution and management in practice [4], [5]. Physical layer security is an appealing alternative to resist various malicious abuses and security attacks. The initial work was pioneered by Wyner from an information-theoretic perspective [6]. Stimulated by the development of multiple-input multiple-output (MIMO) communications [7], physical layer security in MIMO wiretap channels has recently been addressed [8]–[11].

The basic concept behind physical layer security is to exploit characteristics of wireless channels for transmitting confidential messages [12]. In [13], secure connectivity of wireless random networks with multi-antenna transmission in Rayleigh fading channels was analyzed to show the connectivity improvement. In [14], the diversity-multiplexing tradeoff (DMT) for MIMO wiretap channel was analyzed. The close relationship between the multi-antenna secrecy communications and cognitive radio communications was explored in [15]. Transmit antenna selection (TAS) can be adopted to improve information security at low cost and complexity [16], [17]. In [17], the secrecy outage probability with receiver side antenna correlation was derived for Rayleigh fading channels. In [18], maximal-ratio combining (MRC) and selection combining (SC) were used to secure the communication in Nakagami-m fading channels. Secrecy mutual information in single-input multiple-output (SIMO) wiretap channels with Nakagami-m fading was examined in [19]. In [20], TAS with receive generalized selection combining (GSC) was applied to enable secure transmission over Rayleigh fading channels. In [21], the secrecy outage was analyzed in MISO wiretap channels when partial information of the eavesdropper's channel is known at the transmitter.

In this paper, we explore antenna selection to secure the transmission in wiretap channels. We consider the Nakagami-m fading environment due to its versatility in providing a good match to various empirically obtained measurement data [22]. Moreover, it includes Rayleigh fading as a special case [19]. At the transmitter side, TAS selects the optimal transmit antenna which maximizes the instantaneous signal-to-noise ratios (SNRs) at the legitimate receiver. Owing to the fact that the feedback requirements of TAS are considerably lower compared to the so-called closed-loop transmit diversity, it has been applied to the uplink of 4G long term evolution (LTE)

Manuscript received October 30, 2013; revised January 29, 2014, April 30, 2014, and July 25, 2014; accepted September 23, 2014. Date of publication September 23, 2014; date of current version November 7, 2014. The material in this paper was presented in part at the IEEE International Conference on Communications, Sydney, Australia, June 2014. The associate editor coordinating the review of this paper and approving it for publication was C. Yang.

L. Wang and M. Elkashlan are with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, UK (e-mail: lifeng.wang@qmul.ac.uk; maged.elkashlan@qmul.ac.uk).

J. Huang is with Qualcomm Technologies Inc., Santa Clara, CA 95051 USA (e-mail: jinghuang@qti.qualcomm.com).

R. Schober is with the Institute for Digital Communication, Friedrich-Alexander University of Erlangen-Nuremberg, Erlangen 91054, Germany (e-mail: schober@LNT.de).

R. K. Mallik is with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi 110 016, India (e-mail: rkmallik@ee.iitd.ernet.in).

Digital Object Identifier 10.1109/TWC.2014.2359877

and LTE-Advanced [23]. At the receiver side, GSC selects and combines the subset of receive antennas with the largest SNRs. This approach offers a performance/implementation tradeoff between MRC and SC [24], and reduces the power consumption and the cost of RF electronics at the receiver [25]. In non-identically distributed noise, GSC can outperform MRC [26]. It is also robust to channel estimation errors since the weak SNR antennas are eliminated [27]. Therefore, research efforts have been devoted to GSC. For example, the performance of GSC was examined for Rayleigh fading [28] and Nakagami-m fading [29]. In [30], [31], GSC in correlated Nakagami-m fading channels was considered. In [32], the high SNR performance of GSC was analyzed in various fading environments. In [33], approximations were presented for the high SNR performance of GSC in relay networks with Nakagami-m fading.

While the aforementioned literature [24]–[33] laid a solid foundation for the role of GSC in Nakagami-m fading, the impact of GSC on the wiretap channel in Nakagami-m fading has not been investigated yet and the secrecy performance of TAS/GSC in Nakagami-m fading channels is not well understood. In this paper, we address two eavesdropping scenarios: 1) Passive eavesdropping and 2) active eavesdropping. For passive eavesdropping, we characterize the secrecy outage probability as the fundamental security metric. For active eavesdropping, we characterize the average secrecy rate as the fundamental security metric. Our detailed contributions are as follows.

- We derive a new exact closed-form expression for the cumulative distribution function (CDF) of the SNR with the GSC. Although CDF expressions were presented in [24], [34] with the aid of the trapezoidal rule, they are not in closed-form and cannot be used to derive the CDF of the SNR with TAS/GSC. Hence, we derive new closed-form expressions for the CDF and the probability density function (PDF) of the SNR with TAS/GSC.
- We derive new exact closed-form expressions for the average secrecy rate and the secrecy outage probability using the new CDF and PDF of the SNR with TAS/GSC. Notably, we develop a new comprehensive analytical framework for the average secrecy rate. We accurately examine the impact of the antenna configuration and the channel fading conditions on the average secrecy rate.
- We derive new expressions for the average secrecy rate in the high SNR regime for two cases: 1) The legitimate receiver is located close to the transmitter, and 2) the legitimate receiver and the eavesdropper are located close to the transmitter. Based on the asymptotic average secrecy rate, we characterize the average secrecy rate in terms of the high SNR slope and high SNR power offset. We show that although the high SNR slope is unaffected by the network parameters, the high SNR power offset is dependent on the system parameters including transceiver antenna configuration and the fading parameters in the main and the eavesdropper's channels. We reach the interesting conclusion that a capacity ceiling is created when both the legitimate receiver and the eavesdropper are close to the transmitter.
- In contrast to the prior literature such as [16]–[20], we carefully investigate the impact of the locations of the legitimate receiver and the eavesdropper relative to the transmitter. As such, we derive new expressions for the secrecy outage probability in the high SNR regime for two important cases: 1) The legitimate receiver is located close to the transmitter, and 2) the legitimate receiver and the eavesdropper are located close to the transmitter. Based on the asymptotic secrecy outage probability, we characterize the secrecy outage probability in terms of the secrecy diversity order and the secrecy array gain. We show that when the legitimate receiver is close to the transmitter, the full secrecy diversity order is achieved and is entirely determined by the antenna configuration and the fading parameters in the main channel. The impact of the eavesdropper is only reflected in the secrecy array gain. We reach the interesting conclusion that the secrecy diversity order collapses to zero when both the legitimate receiver and the eavesdropper are close to the transmitter.

Notation: In this paper, $(\cdot)^T$ denotes the transpose operator, $\mathbf{I}_M$ denotes the $M \times M$ identity matrix, $\mathbf{0}_{M\times N}$ denotes the $M \times N$ zero matrix, $\mathbb{E}[\cdot]$ denotes the expectation operator, $F_\varphi(\cdot)$ denotes the CDF of random variable (RV) φ, $f_\varphi(\cdot)$ denotes the PDF of φ, $\mathrm{sgn}(\cdot)$ denotes the signum function, $o(\cdot)$ denotes the higher order terms, and $[x]^+ = \max\{x, 0\}$.

II. System Model

We consider a MIMO wiretap channel model which consists of a transmitter (Alice) with N_A antennas, a legitimate receiver (Bob) with N_B antennas, and an eavesdropper (Eve) with N_E antennas. The main channel (Alice-Bob) and the eavesdropper's channel (Alice-Eve) are assumed to undergo quasi-static Nakagami-m fading with fading parameters m_B and m_E, respectively. In the main channel, Alice selects a single transmit antenna among N_A antennas that maximizes the GSC output SNR at Bob, while Bob combines the L_B $(1 \le L_B \le N_B)$ strongest receive antennas. In the eavesdropper's channel, Eve combines the L_E $(1 \le L_E \le N_E)$ strongest receive antennas. The channel power gain from the pth transmit antenna to the l_Bth receive antenna at Bob is denoted as $|h_{p,l_B}|^2$ with $\mathbb{E}[|h_{p,l_B}|^2] = \Omega_1$, $p = 1, \cdots, N_A$, $l_B = 1, \cdots, N_B$. The channel power gain from the pth transmit antenna to the l_Eth receive antenna at Eve is denoted as $|g_{p,l_E}|^2$ with $\mathbb{E}[|g_{p,l_E}|^2] = \Omega_2$, $l_E = 1, \cdots, N_E$. Based on GSC, we arrange $\{|h_{p,(l_B)}|^2, 1 \le l_B \le N_B\}$ in descending order as $|h_{p,(1)}|^2 \ge |h_{p,(2)}|^2 \ge \cdots \ge |h_{p,(N_B)}|^2$, and $\{|g_{p,(l_E)}|^2, 1 \le l_E \le N_E\}$ in descending order as $|g_{p,(1)}|^2 \ge |g_{p,(2)}|^2 \ge \cdots \ge |g_{p,(N_E)}|^2$. The index of the optimal transmit antenna is determined as

$$p^* = \underset{1\le p\le N_A}{\arg\max} \left\{ \sum_{l_B=1}^{L_B} \left|h_{p,(l_B)}\right|^2 \right\}. \tag{1}$$

Secure transmission is achieved by encoding the confidential message block W into a codeword $\mathbf{x} = [x(1), \cdots, x(l), \cdots,$

$x(L)]$, where L is the length of $\mathbf{x}$. The codeword is subject to an average power constraint $\frac{1}{L}\sum_{l=1}^{L}\mathbb{E}[|x(l)|^2] \le P$. In the main channel, at time slot l, the received signal vector is given by

$$\mathbf{y}_B(l) = \mathbf{h}x(l) + \mathbf{n}_B(l), \tag{2}$$

where $\mathbf{h} = [h_{p^*,1}, h_{p^*,2}, \cdots, h_{p^*,N_B}]^T \in \mathcal{C}^{N_B\times 1}$ is the main channel vector between transmit antenna p^* at Alice and the N_B receive antennas at Bob, and $\mathbf{n}_B(l) \sim \mathcal{CN}_{N_B\times 1}(\mathbf{0}_{N_B\times 1}, \delta_B^2\mathbf{I}_{N_B})$ is the additive white Gaussian noise (AWGN) vector at Bob. We denote $\bar{\gamma}_B = \Omega_1\frac{P}{\delta_B^2}$ as the average SNR per antenna at Bob. Combining the subset of receive antennas with the largest SNRs at Bob results in the instantaneous SNR in the main channel as

$$\gamma_B = \sum_{l_B=1}^{L_B}\gamma_{(l_B)}^{B}, \tag{3}$$

where $\gamma_{(l_B)}^{B} = |h_{p^*,(l_B)}|^2\frac{P}{\delta_B^2}$. In the eavesdropper's channel, at time slot l, the received signal vector is given by

$$\mathbf{y}_E(l) = \mathbf{g}x(l) + \mathbf{n}_E(l), \tag{4}$$

where $\mathbf{g} = [g_{p^*,1}, g_{p^*,2}, \cdots, g_{p^*,N_E}]^T \in \mathcal{C}^{N_E\times 1}$ is the eavesdropper's channel vector between transmit antenna p^* at Alice and the N_E receive antennas at Eve, and $\mathbf{n}_E(l) \sim \mathcal{CN}_{N_E\times 1}(\mathbf{0}_{N_E\times 1}, \delta_E^2\mathbf{I}_{N_E})$ is the additive white Gaussian noise (AWGN) vector at Eve. We denote $\bar{\gamma}_E = \Omega_2\frac{P}{\delta_E^2}$ as the average SNR per antenna at Eve. Combining the subset of receive antennas with the largest SNRs at Eve results in the instantaneous SNR in the eavesdropper's channel as

$$\gamma_E = \sum_{l_E=1}^{L_E}\gamma_{(l_E)}, \tag{5}$$

where $\gamma_{(l_E)} = |g_{p^*,(l_E)}|^2\frac{P}{\delta_E^2}$.

III. New Statistical Properties

In this section, we derive new closed-form expressions for the PDF and the CDF of γ_B in the main channel, and the PDF and the CDF of γ_E in the eavesdropper's channel, which lay the foundation for extracting several key secrecy performance indicators, namely the high SNR slope, the high SNR power offset, the secrecy diversity order, and the secrecy array gain. These statistics are general in nature and as such are useful for determining the performance of other wireless systems with GSC.

A. CDF and PDF of the SNR in the Main Channel

Theorem 1: The expressions for the CDF and the PDF of γ_B are derived as

$$F_{\gamma_B}(x) = \left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A!\widetilde{\sum}\hbar_\rho x^{\theta_\rho}e^{-\eta_\rho x}, \tag{6}$$

$$f_{\gamma_B}(x) = \left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A!\widetilde{\sum}\hbar_\rho x^{\theta_\rho-1}e^{-\eta_\rho x}(\theta_\rho-\eta_\rho x), \tag{7}$$

where $\widetilde{\sum} \triangleq \sum_{\mathcal{S}_B}\sum_{\mathcal{S}_B^1}\cdots\sum_{\mathcal{S}_B^k}\cdots\sum_{\mathcal{S}_B^{|\mathcal{S}|}}$, $\mathcal{S}_B = \left\{\left(n_{\tau,1},\cdots,n_{\tau,|\mathcal{S}|}\right)\middle|\sum_{k=1}^{|\mathcal{S}|} n_{\tau,k} = N_A\right\}$, $|\mathcal{S}|$ is the cardinality of set $\mathcal{S}$, and $\mathcal{S}$ denotes a set of $(2m_B+1)$-tuples satisfying the condition

$$\mathcal{S} = \left\{ \left(n_{k,0}^{\Phi}\cdots, n_{k,m_B-1}^{\Phi}, n_{k,0}^{F},\cdots,n_{k,m_B}^{F}\right) \middle| \sum_{i=0}^{m_B-1} n_{k,i}^{\Phi} = L_B-1, \sum_{j=0}^{m_B} n_{k,j}^{F} = N_B-L_B\right\},$$

thereby $|\mathcal{S}| = \binom{m_B+L_B-2}{m_B-1}\binom{m_B+N_B-L_B}{m_B}$, $\mathcal{S}_B^k = \left\{\left(n_{\rho_k,0},\cdots,n_{\rho_k,m_BL_B+b_k^F}\right)\middle|\sum_{n=0}^{m_BL_B+b_k^F} n_{\rho_k,n} = n_{\tau,k}\right\}$, $k=1,\cdots,|\mathcal{S}|$, and $\hbar_\rho$, θ_ρ, and η_ρ are respectively given by

$$\hbar_\rho = \prod_{k=1}^{|\mathcal{S}|}\left(\left(a_k^{\Phi}a_k^{F}\frac{(n_1-1)!}{(L_B)^{n_1}}\right)^{n_{\tau,k}}\frac{\prod_{n=0}^{m_BL_B+b_k^F}\ell_n^{n_{\rho_k,n}}}{\prod_{n=0}^{m_BL_B+b_k^F}n_{\rho_k,n}!}\right),$$

$$\theta_\rho = \sum_{k=1}^{|\mathcal{S}|}\sum_{n=0}^{m_BL_B+b_k^F}\mu_n n_{\rho_k,n},\ \eta_\rho = \sum_{k=1}^{|\mathcal{S}|}\sum_{n=0}^{m_BL_B+b_k^F}\nu_n n_{\rho_k,n},$$

where $n_1 = b_k^{\Phi}+b_k^F+m_B$, a_k^{Φ}, a_k^F, ℓ_n, b_k^F, b_k^{Φ}, μ_n, and ν_n are defined in Appendix A.

Proof: The proof is given in Appendix A. ■

Theorem 2: In the high SNR regime with $\gamma_B \to \infty$, the asymptotic CDF of γ_B is given by

$$F_{\gamma_B}(x) = \frac{\left(L_B\binom{N_B}{L_B}\right)^{N_A}\left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_BN_BN_A}x^{m_BN_BN_A}}{((m_B-1)!(m_B!)^{N_B-L_B}(m_BN_B)!)^{N_A}} \times\left(\sum_{\mathcal{S}_B^{\Phi}}a_k^{\Phi}\frac{(b_k^{\Phi}+m_B(N_B-L_B)+m_B-1)!}{(L_B)^{b_k^{\Phi}+m_B(N_B-L_B)+m_B}}\right)^{N_A}, \tag{8}$$

where $\mathcal{S}_B^{\Phi} = \left\{\left(n_{k,0}^{\Phi},\cdots,n_{k,m_B-1}^{\Phi}\right)\middle|\sum_{i=0}^{m_B-1}n_{k,i}^{\Phi} = L_B-1\right\}$.

Proof: The proof is given in Appendix B. ■

B. CDF and PDF of the SNR in the Eavesdropper's Channel

Alice selects the strongest transmit antenna according to the channel power gains of the main channel, which corresponds to selecting a random transmit antenna for Eve. Hence, similar to

(59) given in Appendix A, the expressions for the CDF and the PDF of γ_E are respectively derived as

$$F_{\gamma_E}(x) = \frac{L_E}{(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=0}^{m_E L_E+b_k^F} a_k^\Phi a_k^F \frac{\left(b_k^\Phi+b_k^F+m_E-1\right)!}{(L_E)^{b_k^\Phi+b_k^F+m_E}}\ell_n x^{\mu_n}e^{-\nu_n x}, \tag{9}$$

$$f_{\gamma_E}(x) = \frac{L_E}{(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=1}^{m_E L_E+b_k^F} a_k^\Phi a_k^F \frac{\left(b_k^\Phi+b_k^F+m_E-1\right)!}{(L_E)^{b_k^\Phi+b_k^F+m_E}}\ell_n x^{\mu_n-1}e^{-\nu_n x}(\mu_n-\nu_n x), \tag{10}$$

where $\mathcal{S}_E$ denotes a set of $(2m_E+1)$-tuples satisfying the condition

$$\mathcal{S}_E = \left\{ \left(n_{k,0}^\Phi \cdots, n_{k,m_E-1}^\Phi, n_{k,0}^F, \cdots, n_{k,m_E}^F\right) \Big| \sum_{i=0}^{m_E-1} n_{k,i}^\Phi = L_E-1, \sum_{j=0}^{m_E} n_{k,j}^F = N_E-L_E \right\}.$$

All the parameters in (9) and (10) are identical to those in *Theorem 1* and are calculated accordingly.

IV. Average Secrecy Rate

In this section, we focus on the active eavesdropping scenario,[1] where the CSI of the eavesdropper's channel is also known at Alice. Following the wiretap channel in [11], [35], Alice encodes a message block W^k into a codeword X^n, and Eve receives Y_w^n from the output of its channel. The equivocation rate of Eve is $R_e = H(W^k|Y_w^n)/n$, which is the amount of ignorance that the eavesdropper has about a message W^k [11]. In the active eavesdropping scenario, Alice can adapt the achievable secrecy rate R such that $R \le R_e$ [11], [35]. Here, We focus on the maximum achievable secrecy rate $C_s = R_e$ [11], [35], which is characterized as [8], [11], [14], [35]

$$C_s = [C_B - C_E]^+, \tag{11}$$

where $C_B = \log_2(1+\gamma_B)$ is the capacity of the main channel and $C_E = \log_2(1+\gamma_E)$ is the capacity of the eavesdropper's channel. Since the CSI of eavesdropper's channel is available to Alice, Alice can transmit confidential messages at a rate C_s, to guarantee perfect secrecy.

In active eavesdropping scenario, the average secrecy rate is essentially a fundamental secrecy performance metric. We derive new exact and asymptotic expressions for the average secrecy rate. Based on the asymptotic expressions, we characterize the average secrecy rate in terms of the high SNR slope and the high SNR power offset, to explicitly capture the impact of arbitrary antennas and channel parameters on the average secrecy rate at high SNR [36].

[1]In this scenario, the eavesdropper is active [35]. Such a scenario 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 [12].

A. Exact Average Secrecy Rate

The average secrecy rate is the average of the secrecy rate C_s over γ_B and γ_E. As such, the exact average secrecy rate is given by

$$\bar{C}_s = \int_0^\infty\int_0^\infty C_s f_{\gamma_B}(x_1)f_{\gamma_E}(x_2)dx_1dx_2 = \int_0^\infty \underbrace{\left[\int_0^\infty C_s f_{\gamma_E}(x_2)dx_2\right]}_{\omega_1} f_{\gamma_B}(x_1)dx_1. \tag{12}$$

We first calculate ω_1 in (12) as

$$\omega_1 = \int_0^{x_1}\left(\log_2(1+x_1)-\log_2(1+x_2)\right)f_{\gamma_E}(x_2)dx_2. \tag{13}$$

Using integration by parts, and applying some algebra, we derive (13) as

$$\begin{aligned}\omega_1 &= \log_2(1+x_1)F_{\gamma_E}(x_1) - \left(\log_2(1+x_1)F_{\gamma_E}(x_1) - \frac{1}{\ln 2}\int_0^{x_1}\frac{1}{1+x_2}F_{\gamma_E}(x_2)dx_2\right)\\ &= \frac{1}{\ln 2}\int_0^{x_1}\frac{F_{\gamma_E}(x_2)}{1+x_2}dx_2.\end{aligned} \tag{14}$$

Substituting (14) into (12), and changing the order of integration, we obtain

$$\begin{aligned}\bar{C}_s &= \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_E}(x_2)}{1+x_2}\left[\int_{x_2}^\infty f_{\gamma_B}(x_1)dx_1\right]dx_2\\ &= \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_E}(x_2)}{1+x_2}\left(1-F_{\gamma_B}(x_2)\right)dx_2.\end{aligned} \tag{15}$$

Using the new statistical properties in Section III, we calculate (15) as

$$\begin{aligned}\bar{C}_s &= \frac{L_E}{\ln 2(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=0}^{m_E L_E+b_k^F} a_k^\Phi a_k^F \times \frac{\left(b_k^\Phi+b_k^F+m_E-1\right)!}{(L_E)^{b_k^\Phi+b_k^F+m_E}}\ell_n\\ &\quad\times\left[\int_0^\infty \frac{x_2^{\mu_n}}{1+x_2}e^{-\nu_n x_2}dx_2 - \left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A!\widetilde{\sum}\hbar_\rho \times\int_0^\infty\frac{x_2^{\mu_n+\theta_\rho}}{1+x_2}e^{-(\nu_n+\eta_\rho)x_2}dx_2\right]\\ &= \frac{L_E}{\ln 2(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=0}^{m_E L_E+b_k^F} a_k^\Phi a_k^F \times \frac{\left(b_k^\Phi+b_k^F+m_E-1\right)!}{(L_E)^{b_k^\Phi+b_k^F+m_E}}\ell_n\end{aligned}$$

$$\times \Bigg[\mu_n! \Psi(\mu_n+1, \mu_n+1; \nu_n) - \left(\frac{L_B}{(m_B-1)!} \binom{N_B}{L_B} \right)^{N_A} N_A! \widetilde{\sum} \hbar_\rho (\mu_n+\theta_\rho)! \times \Psi(\mu_n+\theta_\rho+1, \mu_n+\theta_\rho+1; \nu_n+\eta_\rho) \Bigg], \quad (16)$$

where $\Psi(\cdot,\cdot;\cdot)$ is the confluent hypergeometric function [37, eq. (9.211.4)]. Our new expression for the exact average secrecy rate in (16) applies to arbitrary numbers of antennas, arbitrary fading parameters, and arbitrary average SNRs.

B. Asymptotic Average Secrecy Rate

In order to explicitly examine the performance in the high SNR regime, we proceed to derive the asymptotic average secrecy rate. We take into account two realistic scenarios: 1) Bob is located close to Alice, which can be mathematically described as $\bar{\gamma}_B \to \infty$ for arbitrary $\bar{\gamma}_E$, and 2) Bob and Eve are located close to Alice, which can be mathematically described as $\bar{\gamma}_B \to \infty$ and $\bar{\gamma}_E \to \infty$.

To facilitate the analysis, we rewrite the CDF of γ_E as

$$F_{\gamma_E}(x) = 1 + \chi_{\gamma_E}(x), \quad (17)$$

where

$$\chi_{\gamma_E}(x) = \frac{L_E}{(m_E-1)!} \binom{N_E}{L_E} \sum_{\mathcal{S}_E} \sum_{n=1}^{m_E L_E + b_k^F} a_k^\Phi a_k^F \times \frac{\left(b_k^\Phi + b_k^F + m_E - 1\right)!}{(L_E)^{b_k^\Phi + b_k^F + m_E}} \ell_n x^{\mu_n} e^{-\nu_n x}.$$

1) $\bar{\gamma}_B \to \infty$: In this case, we introduce a new general form to derive the average secrecy rate in the following theorem.

Theorem 3: The asymptotic average secrecy rate is given by

$$\bar{C}_s^\infty = \Delta_1 + \Delta_2, \quad (18)$$

where

$$\Delta_1 = \frac{1}{\ln 2} \int_0^\infty \ln(x_1) f_{\gamma_B}(x_1) dx_1 \quad (19)$$

and

$$\Delta_2 = \frac{1}{\ln 2} \int_0^\infty \frac{\chi_{\gamma_E}(x_2)}{1+x_2} dx_2. \quad (20)$$

Proof: The proof is given in Appendix C. ■

Based on *Theorem 3*, we calculate the asymptotic average secrecy rate using the new statistical properties in Section III. Specifically, by substituting (7) into (19), and employing [37, eq. (4.352.1)], Δ_1 is derived as

$$\Delta_1 = \log_2(\bar{\gamma}_B) - \log_2(m_B) + \frac{1}{\ln 2} \times \left(\frac{L_B}{(m_B-1)!} \binom{N_B}{L_B} \right)^{N_A} N_A! \widetilde{\sum} \tilde{\hbar}_\rho \zeta_1, \quad (21)$$

where $\tilde{\hbar}_\rho = \hbar_\rho \left(\frac{m_B}{\bar{\gamma}_B}\right)^{-\theta_\rho}$ and

$$\zeta_1 = \begin{cases} 0, & \theta_\rho = 0, \tilde{\eta}_\rho = 0, \\ \ln(\tilde{\eta}_\rho) + C, & \theta_\rho = 0, \tilde{\eta}_\rho > 0, \\ -\frac{(\theta_\rho - 1)!}{(\tilde{\eta}_\rho)^{\theta_\rho}}, & \theta_\rho > 0, \tilde{\eta}_\rho > 0, \end{cases} \quad (22)$$

In (22), C is the Euler's constant [37, eq. (8.367.1)] and $\tilde{\eta}_\rho = \left(\frac{m_B}{\bar{\gamma}_B}\right)^{-1} \eta_\rho$. It is worth noting that $\tilde{\hbar}_\rho$ and $\tilde{\eta}_\rho$ are independent of $\bar{\gamma}_B$. We should also note that Δ_1 in (21) explicitly quantifies the impact of the main channel on the average secrecy rate.

Substituting χ_{γ_E} given in (17) into (20), we obtain Δ_2

$$\Delta_2 = \frac{L_E}{\ln 2 (m_E-1)!} \binom{N_E}{L_E} \sum_{\mathcal{S}_E} \sum_{n=1}^{m_E L_E + b_k^F} a_k^\Phi a_k^F \times \frac{\left(b_k^\Phi + b_k^F + m_E - 1\right)!}{(L_E)^{b_k^\Phi + b_k^F + m_E}} \ell_n \mu_n! \Psi(\mu_n+1, \mu_n+1, \nu_n), \quad (23)$$

which explicitly quantifies the impact of the eavesdropper's channel on the average secrecy rate.

Based on (18), (21), and (23), we derive the asymptotic average secrecy rate as

$$\bar{C}_s^\infty = \log_2(\bar{\gamma}_B) - \log_2(m_B) + \frac{1}{\ln 2} \left(\frac{L_B}{(m_B-1)!} \binom{N_B}{L_B} \right)^{N_A} \times N_A! \widetilde{\sum} \tilde{\hbar}_\rho \zeta_1 + \frac{L_E}{\ln 2 (m_E-1)!} \binom{N_E}{L_E} \sum_{\mathcal{S}_E} \sum_{n=1}^{m_E L_E + b_k^F} a_k^\Phi a_k^F \times \frac{\left(b_k^\Phi + b_k^F + m_E - 1\right)!}{(L_E)^{b_k^\Phi + b_k^F + m_E}} \ell_n \mu_n! \Psi(\mu_n+1, \mu_n+1, \nu_r). \quad (24)$$

Based on (24), we derive two key performance indicators that determine the average secrecy rate at high SNR, namely the high SNR slope and the high SNR power offset [36], [38]. The asymptotic average secrecy rate in (24) can be conveniently re-expressed as [36]

$$\bar{C}_s^\infty = S_\infty \left(\log_2(\bar{\gamma}_B) - \mathcal{L}_\infty \right), \quad (25)$$

where S_∞ is the high SNR slope in bits/s/Hz/(3 dB) and $\mathcal{L}_\infty$ is the high SNR power offset in 3 dB units. We note that the high SNR slope is also known as the maximum multiplexing gain or the number of degrees of freedom [7]. The high SNR power offset is a more intricate function which depends on the number of transmit and receive antennas, as well as the channel characteristics [36], [38].

The high SNR slope S_∞ is given by

$$S_\infty = \lim_{\bar{\gamma}_B \to \infty} \frac{\bar{C}_S^\infty}{\log_2(\bar{\gamma}_B)}. \quad (26)$$

Substituting (24) into (26), we obtain

$$S_\infty = 1. \quad (27)$$

From (27), we see that the eavesdropper's channel and the number of Bob's receive antennas have no impact on the high SNR slope S_∞.

The high SNR power offset $\mathcal{L}_\infty$ is given by

$$\mathcal{L}_\infty = \lim_{\bar{\gamma}_B \to \infty} \left(\log_2(\bar{\gamma}_B) - \frac{\bar{C}_S^\infty}{S_\infty} \right). \quad (28)$$

Substituting (24) and (27) into (28), we derive $\mathcal{L}_\infty$ as[2]

$$\mathcal{L}_\infty = \mathcal{L}_\infty^B(m_B, N_B, L_B, N_A) + \mathcal{L}_\infty^E(m_E, N_E, L_E, \bar{\gamma}_E), \quad (29)$$

where

$$\mathcal{L}_\infty^B(m_B, N_B, L_B, N_A) = \log_2(m_B) - \times \frac{1}{\ln 2} \left(\frac{L_B}{(m_B-1)!} \binom{N_B}{L_B} \right)^{N_A} N_A! \widetilde{\sum} \tilde{h}_\rho \zeta_1 \quad (30)$$

and

$$\mathcal{L}_\infty^E(m_E, N_E, L_E, \bar{\gamma}_E) = -\Delta_2. \quad (31)$$

In (30), $\mathcal{L}_\infty^B$ quantifies the contribution of the main channel to the high SNR power offset. In (31), $\mathcal{L}_\infty^E$ quantifies the contribution of the eavesdropper's channel to the high SNR power offset. We next examine special cases of $\mathcal{L}_\infty^B$ and $\mathcal{L}_\infty^E$ in which these expressions reduce to more simple forms.

Corollary 1: For the special case of Rayleigh fading, where $m_B = m_E = 1$, $\mathcal{L}_\infty^B$ in (30) reduces to

$$\mathcal{L}_\infty^B(1, N_B, L_B, N_A) = -\frac{1}{\ln 2} \left(L_B \binom{N_B}{L_B} \right)^{N_A} N_A! \widetilde{\sum} \tilde{h}_\rho \zeta_1 \quad (32)$$

and $\mathcal{L}_\infty^E$ in (31) reduces to

$$\mathcal{L}_\infty^E(1, N_E, L_E, \bar{\gamma}_E) = -\frac{1}{\ln 2} \binom{N_E}{L_E} \sum_{\mathcal{S}_E^F} \sum_{n=1}^{L_E} a_k^F \ell_n \mu_n! \times \Psi(\mu_n + 1, \mu_n + 1, \nu_n), \quad (33)$$

where $\mathcal{S}_E^F = \left\{ \left(n_{k,0}^F, n_{k,1}^F \right) \Big| \sum_{j=0}^{1} n_{k,j}^F = N_E - L_E \right\}$.

Corollary 2: For the special case of Rayleigh fading with TAS/MRC, where $m_B = m_E = 1$, $L_B = N_B$, and $L_E = N_E$, $\mathcal{L}_\infty^B$ in (30) reduces to

$$\mathcal{L}_\infty^B(1, N_B, N_B, N_A) = -\frac{1}{\ln 2} N_A! \sum_{\mathcal{S}_B^1} \frac{\prod_{n=1}^{N_B} \left(\frac{-1}{(n-1)!} \right)^{n_{\rho_1,n}}}{\prod_{n=0}^{N_B} n_{\rho_1,n}!} \beta, \quad (34)$$

where $\mathcal{S}_B^1 = \left\{ (n_{\rho_1,0}, \cdots, n_{\rho_1,N_B}) | \sum_{n=0}^{N_B} n_{\rho_1,n} = N_A \right\}$ and

$$\beta = \begin{cases} \ln(N_A) + C, & \theta_\rho = 0, \\ -\frac{(\theta_\rho - 1)!}{(N_A)^{\theta_\rho}}, & \theta_\rho > 0. \end{cases} \quad (35)$$

From (31), $\mathcal{L}_\infty^E$ reduces to

$$\mathcal{L}_\infty^E(1, N_E, N_E, \bar{\gamma}_E) = \frac{1}{\ln 2} \sum_{n=1}^{N_E} \left(\frac{1}{\bar{\gamma}_E} \right)^{n-1} \Psi\left(n, n, \frac{1}{\bar{\gamma}_E} \right). \quad (36)$$

[2]Here, we explicitly reveal the dependence of the high SNR power offset on $m_B, N_A, N_B, L_B, m_E, N_E, L_E, \bar{\gamma}_E$.

It is clear from (36) that L_∞^E is an increasing function of N_E. As such, when the number of antennas at Eve increases, the high SNR power offset also increases, which in turn decreases the average secrecy rate.

Corollary 3: For the special case of Rayleigh fading with TAS/SC, where $m_B = m_E = 1$, $L_B = 1$, and $L_E = 1$, $\mathcal{L}_\infty^B$ in (30) reduces to

$$\mathcal{L}_\infty^B(1, N_B, 1, N_A) = -\frac{1}{\ln 2} (N_B)^{N_A} N_A! \widetilde{\sum} \tilde{h}_\rho \times \operatorname{sgn}(\tilde{\eta}_\rho) \left(\ln(\tilde{\eta}_\rho) + C \right). \quad (37)$$

By applying [37, eq. (3.352.4)], $\mathcal{L}_\infty^E$ in (31) reduces to

$$\mathcal{L}_\infty^E(1, N_E, 1, \bar{\gamma}_E) = \frac{N_E}{\ln 2} \sum_{S_E^F} \frac{(N_E - 1)!}{\prod_{j=0}^{1} n_{k,j}^F!} (-1)^{n_{k,1}^F} \times \left(\frac{\operatorname{sgn}\left(n_{k,1}^F \right)}{n_{k,1}^F + 1} + 1 - \operatorname{sgn}\left(n_{k,1}^F \right) \right) \times \left(-e^{\frac{\left(n_{k,1}^F + 1 \right)}{\bar{\gamma}_E}} \operatorname{Ei}\left(-\frac{\left(n_{k,1}^F + 1 \right)}{\bar{\gamma}_E} \right) \right), \quad (38)$$

where $\mathcal{S}_E^F = \left\{ (n_{k,0}^F, n_{k,1}^F) | \sum_{j=0}^{1} n_{k,j}^F = N_E - 1 \right\}$ and $\operatorname{Ei}(\cdot)$ is the exponential integral function defined in [37, eq. (8.211.1)].

2) $\bar{\gamma}_B \to \infty$ and $\bar{\gamma}_E \to \infty$: In this case, the average secrecy rate can be easily obtained based on *Theorem 3*. We only need to further provide the asymptotic Δ_2 with $\bar{\gamma}_E \to \infty$. Observing Δ_1 in (21), the asymptotic Δ_2 is derived according to

$$\Delta_2 = -\left(\log_2(\bar{\gamma}_E) - \log_2(m_E) \right) - \Xi, \quad (39)$$

where

$$\Xi = \frac{1}{\ln 2} \frac{L_E}{(m_E - 1)!} \binom{N_E}{L_E} \sum_{\mathcal{S}_E} \sum_{n=1}^{m_E L_E + b_k^F} a_k^\Phi a_k^F \times \frac{\left(b_k^\Phi + b_k^F + m_E - 1 \right)!}{(L_E)^{b_k^\Phi + b_k^F + m_E}} \tilde{\ell}_n \times \left((1 - \operatorname{sgn}(\mu_n)) \times (C + \ln(\tilde{\nu}_n)) - \operatorname{sgn}(\mu_n) \frac{(\mu_n - 1)!}{(\tilde{\nu}_n)^{\mu_n}} \right). \quad (40)$$

In (40), $\tilde{\ell}_n = \ell_n \left(\frac{m_E}{\bar{\gamma}_E} \right)^{-\mu_n}$ and $\tilde{\nu}_n = \nu_n \left(\frac{m_E}{\bar{\gamma}_E} \right)^{-1}$. We should note that in (40), Ξ is independent of $\bar{\gamma}_E$.

Substituting (21) and (39) into (18), we derive the asymptotic average secrecy rate as

$$\bar{C}_s^\infty = \log_2 \left(\frac{\bar{\gamma}_B}{\bar{\gamma}_E} \right) - \log_2 \left(\frac{m_B}{m_E} \right) + \frac{1}{\ln 2} \left(\frac{L_B}{(m_B - 1)!} \binom{N_B}{L_B} \right)^{N_A} N_A! \widetilde{\sum} \tilde{h}_\rho \zeta_1 - \Xi. \quad (41)$$

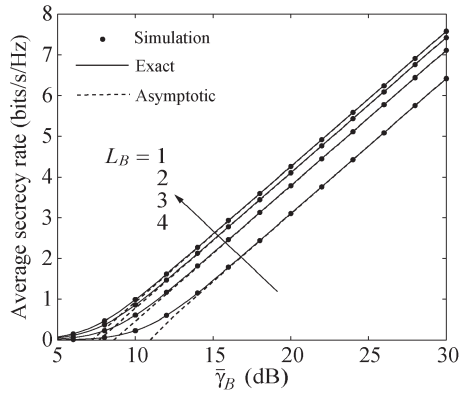

Fig. 1. Average secrecy rate for $N_A = 2$, $N_B = 4$, $N_E = 3$, $L_E = 2$, $m_B = m_E = 2$, and $\bar{\gamma}_E = 10$ dB.

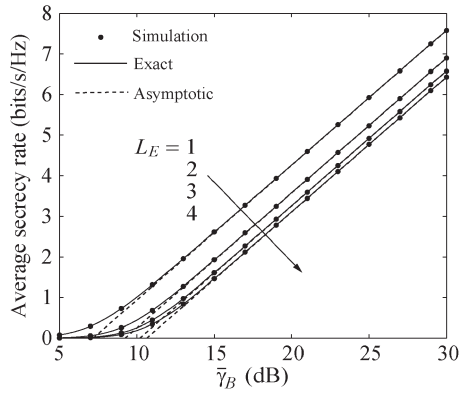

Fig. 2. Average secrecy rate for $N_A = 2$, $N_B = 4$, $N_E = 4$, $L_B = 2$, $m_B = m_E = 2$, and $\bar{\gamma}_E = 10$ dB.

From (41), we see that for a fixed ratio of $\bar{\gamma}_B$ and $\bar{\gamma}_E$, the average secrecy rate is a constant value at high SNR. According to (26), the high SNR slope S_∞ is zero. This new result shows that when the eavesdropper is located close to the transmitter, increasing the transmit power does not have an impact on the average secrecy rate.

C. Numerical Examples

Fig. 1 plots the average secrecy rate versus $\bar{\gamma}_B$ for different L_B. The exact curves are obtained from (16). Considering the scenario where Bob is located close to Alice, the asymptotic average secrecy rate curves are obtained from (24). We see that the exact curves are well-validated by Monte Carlo simulations[3] marked with '•'. We also see that the asymptotic curves well approximate the exact curves at high SNR. As suggested by (27), the high SNR slope is independent of L_B, which is also indicated by the parallel slopes of the asymptotes. The average secrecy rate increases with the number of selected antennas L_B. This is because $\mathcal{L}_\infty^B$ in (30) decreases with increasing L_B and accordingly the high SNR power offset $\mathcal{L}_\infty$ decreases. Notably, the performance difference diminishes for large L_B. This confirms that TAS/GSC provides a performance tradeoff between TAS/MRC and TAS/SC in MIMO wiretap channels.

Fig. 2 plots the average secrecy rate versus $\bar{\gamma}_B$ for different L_E. The parallel slopes of the asymptotes confirm that the high SNR slope is independent of L_E. The average secrecy rate decreases with the number of selected antennas L_E. This is due to the fact that $\mathcal{L}_\infty^E$ in (31) increases with L_E and accordingly the high SNR power offset $\mathcal{L}_\infty$ increases.

Fig. 3 plots the high SNR power offset for several cases. Here, (a) and (b) represent the impact of increasing Eve's antennas for different L_E, and (c) and (d) represent the impact of increasing Bob's antennas for different L_B. The power offset is obtained using (29). We see that the power offset increases with increasing N_E and L_E, which in turn decreases the average secrecy rate, as shown in (25). We also see that the power offset decreases with increasing N_B and L_B, which in turn increases the average secrecy rate.

[3]In this paper, Monte Carlo simulated results are numerically computed based on system parameters given in each figure, which validate the accuracy of our analytical results.

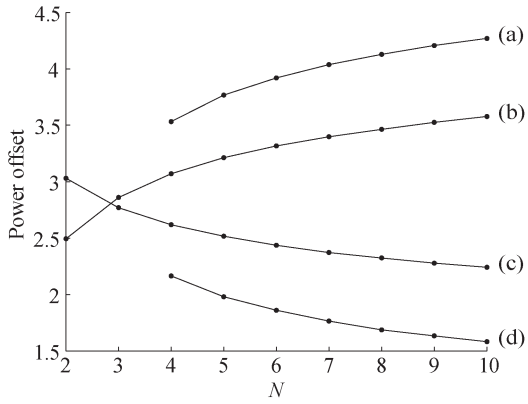

Fig. 3. High SNR power offset with $m_B = m_E = 2$ and $\bar{\gamma}_E = 10$ dB for four cases: (a) $N_A = 2$, $N_B = 4$, $N_E = N$, $L_B = 2$, $L_E = 4$, (b) $N_A = 2$, $N_B = 4$, $N_E = N$, $L_B = 2$, $L_E = 2$, (c) $N_A = 4$, $N_B = N$, $N_E = 3$, $L_B = 2$, $L_E = 2$, and (d) $N_A = 4$, $N_B = N$, $N_E = 3$, $L_B = 4$, $L_E = 2$.

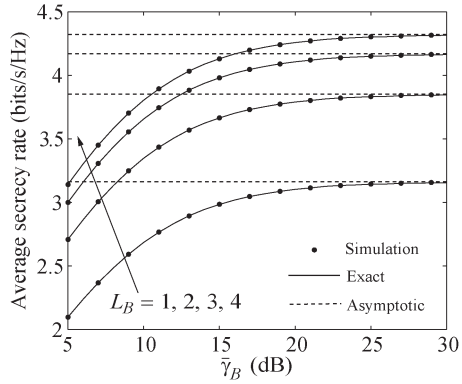

Fig. 4. Average secrecy rate for $N_A = 2$, $N_B = 4$, $N_E = 3$, $m_B = m_E = 2$, and $L_E = 2$.

Fig. 4 plots the average secrecy rate versus $\bar{\gamma}_B$ for different L_B. The exact curves are obtained from (16). Considering the scenario where Bob and Eve are located close to Alice, we set $\left.\frac{\bar{\gamma}_B}{\bar{\gamma}_E}\right|_{\text{dB}} = 10$ dB, and the asymptotic curves are obtained from (41). Observe that the average secrecy rate increases with increasing L_B. As predicted by (41), the average secrecy rate converges to a finite limit at high SNR, which proves that the high SNR slope collapses to zero.

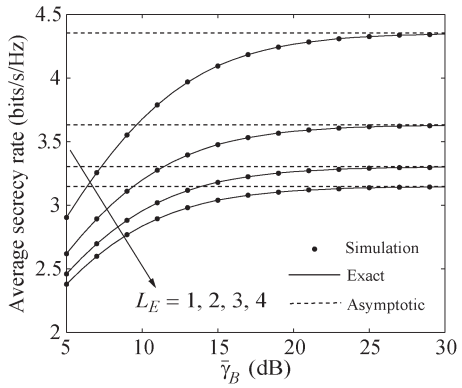

Fig. 5. Average secrecy rate for $N_A = 2$, $N_B = 4$, $N_E = 4$, $m_B = m_E = 2$, and $L_B = 2$.

Fig. 5 plots the average secrecy rate versus $\bar{\gamma}_B$ for different L_E. Here, we set $\left.\frac{\bar{\gamma}_B}{\bar{\gamma}_E}\right|_{\text{dB}} = 10$ dB. We see that the average secrecy rate decreases with increasing L_E. As reflected in (41), the average secrecy rate approaches a constant at high SNR.

V. Secrecy Outage Probability

In this section, we concentrate on passive eavesdropping scenario, where the CSI of the eavesdropper's channel is not known at Alice. In such a scenario, Alice has no choice but to encode the confidential data into codewords of a constant rate R_s [35], if $R_s \leq C_s$ (C_s has been defined in (11)), perfect secrecy can be achieved. Otherwise, if $R_s > C_s$, information-theoretic security is compromised. In other words, unlike the active eavesdropping scenario, perfect secrecy cannot be guaranteed in the passive eavesdropping scenario, since Alice has no information about the eavesdropper's channel. Motivated by this, we adopt the secrecy outage probability as a useful performance measure. We derive new closed-form expressions for the exact and the asymptotic secrecy outage probability. Based on the asymptotic expressions, we present two key performance indicators, namely the secrecy diversity order and the secrecy array gain.

A. Exact Secrecy Outage Probability

A secrecy outage is declared when the secrecy rate C_s is less than the expected secrecy rate R_s. As such, the secrecy outage probability is derived as

$$P_{out}(R_s) = \Pr(C_s < R_s) = \int_0^\infty f_{\gamma_E}(x_2) F_{\gamma_B}\left(2^{R_s}(1+x_2)-1\right) dx_2. \quad (42)$$

Substituting (6) and (10) into (42), and applying the binomial expansion [37, eq. (1.111)] and [37, eq. (3.351.3)], we obtain

$$P_{out}(R_s) = \frac{L_E}{(m_E-1)!}\binom{N_E}{L_E}\sum_{\mathcal{S}_E}\sum_{n=1}^{m_E L_E + b_k^F} a_k^\Phi a_k^F \times \frac{\left(b_k^\Phi + b_k^F + m_E - 1\right)!}{(L_E)^{b_k^\Phi + b_k^F + m_E}}\ell_n \times \left(\frac{L_B}{(m_B-1)!}\binom{N_B}{L_B}\right)^{N_A} N_A! \times \widetilde{\sum}\hbar_\rho \sum_{q=0}^{\theta_\rho}\binom{\theta_\rho}{q} 2^{R_s q}(2^{R_s}-1)^{\theta_\rho - q} e^{-\eta_\rho(2^{R_s}-1)} \times \left(\frac{\mu_n \Gamma(q+\mu_n)}{(\eta_\rho 2^{R_s}+\nu_n)^{q+\mu_n}} - \frac{\nu_n (q+\mu_n)!}{(\eta_\rho 2^{R_s}+\nu_n)^{q+\mu_n+1}}\right). \quad (43)$$

Our new expression for the exact secrecy outage probability in (43) applies to arbitrary numbers of antennas at Bob and Eve, arbitrary fading parameters, and arbitrary average SNRs in the main and eavesdropper's channels. As shown in [17], the probability of positive secrecy can be evaluated as $1 - P_{out}(0)$.

B. Asymptotic Secrecy Outage Probability

In this subsection, we turn our attention to the asymptotic secrecy outage probability. We consider the following two scenarios.

1) $\bar{\gamma}_B \to \infty$: In this case, Bob is located close to Alice. We substitute (8) and (10) into (42), and derive the asymptotic secrecy outage probability as

$$P_{out}^\infty(R_s) = (G_a \bar{\gamma}_B)^{-G_d} + o\left(\bar{\gamma}_B^{-G_d}\right), \quad (44)$$

where the secrecy diversity order is

$$G_d = m_B N_B N_A \quad (45)$$

and the secrecy array gain is

$$G_a = \left[\frac{L_E}{(m_E-1)!}\frac{\left(L_B\binom{N_B}{L_B}\right)^{N_A}(m_B)^{m_B N_B N_A}}{\left(\Gamma(m_B)(m_B!)^{N_B-L_B}(m_B N_B)!\right)^{N_A}} \times \binom{N_E}{L_E}\left(\sum_{\mathcal{S}_B^\Phi} a_k^\Phi \frac{\left(b_k^\Phi + m_B(N_B-L_B)+m_B-1\right)!}{(L_B)^{b_k^\Phi + m_B(N_B-L_B)+m_B}}\right)^{N_A} \times \sum_{\mathcal{S}_E}\sum_{n=1}^{m_E L_E + b_k^F} a_k^\Phi a_k^F \frac{\left(b_k^\Phi + b_k^F + m_E - 1\right)!}{(L_E)^{b_k^\Phi + b_k^F + m_E}}\ell_n \times \sum_{q=0}^{m_B N_B N_A}\binom{m_B N_B N_A}{q}\left(\Gamma(q+\mu_n)\mu_n - (q+\mu_n)!\right) \times \frac{2^{R_s q}\left(2^{R_s}-1\right)^{m_B N_B N_A - q}}{(\nu_n)^{q+\mu_n}}\right]^{-\frac{1}{m_B N_B N_A}}. \quad (46)$$

Based on (45) and (46), we find that the secrecy diversity order is entirely determined by the antenna configuration and the fading parameters in the main channel. The impact of the eavesdropper's channel is only reflected in the secrecy array gain.

In order to characterize the impact of GSC on the secrecy outage probability, we quantify the secrecy outage tradeoff between $L_B + l$ and L_B, $l = 1, \cdots, N_B - L_B$. From (45), we

confirm that $L_B + l$ and L_B have the same secrecy diversity order. As such, one can conclude that the SNR gap between $L_B + l$ and L_B is strictly determined by their respective secrecy array gains and is expressed as

$$\frac{G_a(L_B+l)}{G_a(L_B)} = \left[\frac{(m_B!)^l (L_B+l)\binom{N_B}{L_B+l}}{L_B \binom{N_B}{L_B}} \times \frac{\sum\limits_{S_B^{\Phi^l}} a_k^{\Phi^l} \frac{\left(b_k^{\Phi^l}+m_B(N_B-L_B-l)+m_B-1\right)!}{(L_B+l)^{b_k^{\Phi^l}+m_B(N_B-L_B-l)+m_B}}}{\sum\limits_{S_B^{\Phi}} a_k^{\Phi} \frac{\left(b_k^{\Phi}+m_B(N_B-L_B)+m_B-1\right)!}{(L_B)^{b_k^{\Phi}+m_B(N_B-L_B)+m_B}}} \right]^{-\frac{1}{m_B N_B}} \quad (47)$$

where $\mathcal{S}_B^{\Phi^l}$ satisfies the condition

$$\mathcal{S}_B^{\Phi^l} = \left\{ \left(n_{k,0}^{\Phi^l}, \cdots, n_{k,m_B-1}^{\Phi^l} \right) \Big| \sum_{i=0}^{m_B-1} n_{k,i}^{\Phi^l} = L_B + l - 1 \right\}.$$

Corollary 4: For the special case of Rayleigh fading, the secrecy diversity order in (45) reduces to $N_B N_A$ and the secrecy array gain in (46) reduces to

$$G_a = \left[\binom{N_E}{L_E} \frac{(2^{R_s}-1)^{N_B N_A}}{(L_B!)^{N_A} (L_B)^{N_A(N_B-L_B)}} \sum_{\mathcal{S}_E^F} \times \sum_{n=1}^{L_E} a_k^F \ell_n \sum_{q=0}^{N_B N_A} \binom{N_B N_A}{q} \left(\frac{2^{R_s}}{2^{R_s}-1} \right)^q \times \frac{(\Gamma(q+\mu_n)\mu_n - (q+\mu_n)!)}{(\nu_n)^{q+\mu_n}} \right]^{-\frac{1}{N_B N_A}}. \quad (48)$$

Based on (48), we confirm that $\frac{G_a(L_B+1)}{G_a(L_B)} > 1$. This proves that the secrecy array gain is an increasing function of L_B. It follows that the SNR gap between $L_B + l$ and L_B in (47) reduces to

$$\frac{G_a(L_B+l)}{G_a(L_B)} = \left[\frac{(L_B)^l L_B!}{(L_B+l)! \left(1+\frac{l}{L_B}\right)^{N_B-L_B-l}} \right]^{-\frac{1}{N_B}}. \quad (49)$$

Based on (49), we confirm that $\left(\frac{G_a(L_B+1+l)}{G_a(L_B+1)}\right) \Big/ \left(\frac{G_a(L_B+l)}{G_a(L_B)}\right) < 1$. This proves that the SNR gap is a decreasing function of L_B.

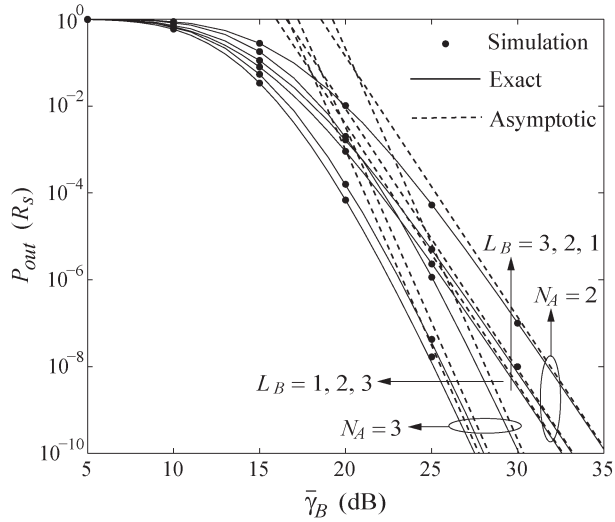

Fig. 6. Secrecy outage probability for $N_B = 3$, $N_E = 3$, $L_E = 2$, $m_B = 1$, $m_E = 2$, and $\bar{\gamma}_E = 10$ dB.

2) $\bar{\gamma}_B \to \infty$, $\bar{\gamma}_E \to \infty$: In this case, both Bob and Eve are located close to Alice. Based on (43), the asymptotic secrecy outage probability is derived as

$$P_{out}^{\infty}(R_s) = \lim_{\bar{\gamma}_B \to \infty, \bar{\gamma}_E \to \infty} P_{out}(R_s) = \frac{L_E}{(m_E-1)!} \binom{N_E}{L_E} \sum_{\mathcal{S}_E} \sum_{n=1}^{m_E L_E + b_k^F} a_k^{\Phi} a_k^F \times \tilde{\ell}_n \frac{\left(b_k^{\Phi}+b_k^F+m_E-1\right)!}{(L_E)^{b_k^{\Phi}+b_k^F+m_E}} \times \left(\frac{L_B}{(m_B-1)!} \binom{N_B}{L_B} \right)^{N_A} N_A! \times \widetilde{\sum} \tilde{\hbar}_\rho \left(\frac{m_B \bar{\gamma}_E}{m_E \bar{\gamma}_B} \right)^{\theta_\rho} \frac{2^{R_s \theta_\rho}}{\left(\tilde{\eta}_\rho 2^{R_s} \frac{m_B \bar{\gamma}_E}{m_E \bar{\gamma}_B} + \tilde{\nu}_n \right)^{\theta_\rho + \mu_n}} \times \left(\mu_n \Gamma(\theta_\rho + \mu_n) - \frac{\tilde{\nu}_n (\theta_\rho + \mu_n)!}{\tilde{\eta}_\rho 2^{R_s} \frac{m_B \bar{\gamma}_E}{m_E \bar{\gamma}_B} + \tilde{\nu}_n} \right). \quad (50)$$

For a fixed ratio of $\bar{\gamma}_B$ and $\bar{\gamma}_E$, (50) confirms that the secrecy outage probability approaches a constant at high SNR, which implies that the secrecy diversity order is zero. Once again, this result shows that increasing the transmit power does not have an impact on the secrecy outage probability.

C. Numerical Examples

Fig. 6 plots the secrecy outage probability versus $\bar{\gamma}_B$ for different L_B and N_A. The expected secrecy rate is $R_s = 1$ bit/s/Hz. The exact curves are obtained from (43). Considering Bob is located close to Alice, the asymptotic curves are obtained from (44). The exact curves are in precise agreement with the Monte Carlo simulations. We also see that the asymptotic curves accurately predict the secrecy diversity order and the secrecy array gain. According to (45), we see that the secrecy diversity order increases with N_A, which in

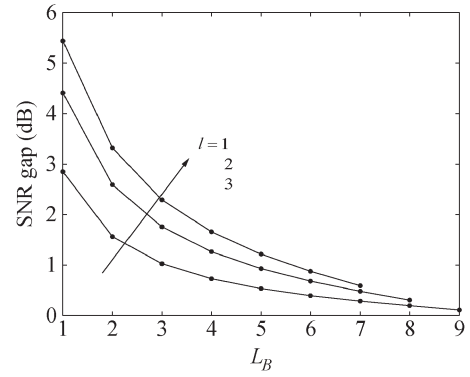

Fig. 7. SNR gap for $m_B = 2$ and $N_B = 10$.

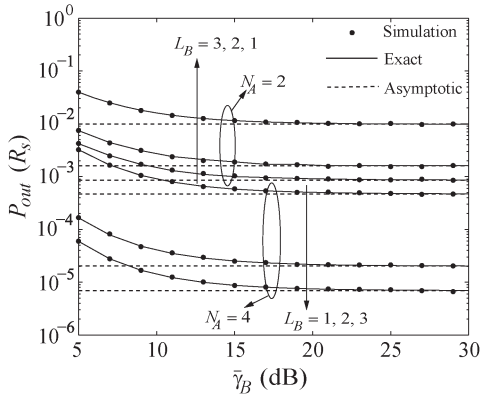

Fig. 8. Secrecy outage probability for $N_B = 3$, $N_E = 3$, $m_B = 1$, $m_E = 2$, and $L_E = 2$.

turn decreases the secrecy outage probability. We also see that the secrecy outage probability decreases with L_B, due to an increase in the secrecy array gain.

Fig. 7 plots the SNR gap versus L_B for different l. The SNR gap between $L_B + l$ and L_B is obtained from (47). The expected secrecy rate is $R_s = 1$ bit/s/Hz. On the one hand, the SNR gap increases with increasing l. This confirms that the secrecy array gain is an increasing function of L_B. On the other hand, the SNR gap decreases with increasing L_B. This shows that the SNR gap is a decreasing function of L_B.

Fig. 8 plots the secrecy outage probability versus $\bar{\gamma}_B$ for different L_B and N_A. The expected secrecy rate is $R_s = 1$ bit/s/Hz. The exact curves are obtained from (43). Considering both Bob and Eve are located close to Alice, we set $\left.\frac{\bar{\gamma}_B}{\bar{\gamma}_E}\right|_{\mathrm{dB}} = 10$ dB and the asymptotic curves are obtained from (50). Observe that the secrecy outage probability decreases with L_B and N_A. As suggested by (50), the secrecy outage probability approaches a constant at high SNR, which confirms that the secrecy diversity order is zero.

VI. Conclusion

We analyzed TAS/GSC for physical layer security in MIMO wiretap channels. In doing so, we derived new analytical expressions of the statistical properties on the SNR with TAS/GSC in Nakagami-m fading. With the aid of these results, we first presented new closed-form expressions for the exact and the asymptotic average secrecy rate. Using these expressions, we precisely characterized the high SNR slope and the high SNR power offset. We then presented new closed-form expressions for the exact and the asymptotic secrecy outage probability, which concisely characterized the secrecy diversity order and the secrecy array gain. Several key observations were drawn based on the locations of the legitimate receiver and the eavesdropper relative to the transmitter. We showed that a capacity ceiling and an outage floor were created when both the legitimate receiver and the eavesdropper were close to the transmitter. Massive MIMO [39] could be used to cope with this issue. Moreover, our results provide a useful analytical guideline for the more general scenarios of: 1) Cooperative jamming [40] to confound the eavesdroppers, 2) imperfect channel knowledge, and 3) multiple destinations and multiple eavesdroppers.

Appendix A
Proof of Theorem 1

We first present the PDF and the CDF of the SNR of a single branch in the main channel with Nakagami-m fading as [41]

$$f(x) = \frac{x^{m_B-1}}{(m_B-1)!}\left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B} e^{-\frac{m_B}{\bar{\gamma}_B}x} \tag{51}$$

and

$$F(x) = 1 - e^{-x\frac{m_B}{\bar{\gamma}_B}} \sum_{j=0}^{m_B-1} \frac{\left(x\frac{m_B}{\bar{\gamma}_B}\right)^j}{j!}, \tag{52}$$

respectively. The marginal moment generating function (MGF) of (51) is given by [24]

$$\Phi(s,x) = \left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B} \sum_{i=0}^{m_B-1} \frac{x^i e^{-\left(s+\frac{m_B}{\bar{\gamma}_B}\right)x}}{i!\left(s+\frac{m_B}{\bar{\gamma}_B}\right)^{m_B-i}}. \tag{53}$$

As shown in [24], [34], the MGF expression for the SNR γ after GSC is expressed as

$$\Phi_\gamma(s) = L_B\binom{N_B}{L_B}\int_0^\infty e^{-sx} f(x) \times \left(\Phi(s,x)\right)^{L_B-1}\left(F(x)\right)^{N_B-L_B} dx. \tag{54}$$

Here, the MGF is defined as $\Phi_\gamma(s) = \mathbb{E}[e^{-\gamma s}]$. In order to evaluate the integral in (54), we will rewrite $\left(\Phi(s,x)\right)^{L_B-1}$ and $\left(F(x)\right)^{N_B-L_B}$.

Based on (53), using the multinomial theorem [42], we rewrite $\left(\Phi(s,x)\right)^{L_B-1}$ as

$$\left(\Phi(s,x)\right)^{L_B-1} = \left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B(L_B-1)} \sum_{\mathcal{S}_B^\Phi} a_k^\Phi \times \left(s+\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^\Phi - m_B(L_B-1)} x^{b_k^\Phi} e^{-c_k^\Phi x}, \tag{55}$$

where $\mathcal{S}_B^{\Phi} = \left\{ \left(n_{k,0}^{\Phi}, \cdots, n_{k,m_B-1}^{\Phi} \right) \Big| \sum_{i=0}^{m_B-1} n_{k,i}^{\Phi} = L_B - 1 \right\}$, $a_k^{\Phi} = \frac{(L_B-1)!}{\prod_{i=0}^{m_B-1} n_{k,i}^{\Phi}!} \prod_{i=0}^{m_B-1} \left(\frac{1}{i!}\right)^{n_{k,i}^{\Phi}}$, $b_k^{\Phi} = \sum_{i=0}^{m_B-1} n_{k,i}^{\Phi} i$, and $c_k^{\Phi} = (L_B - 1)\left(s + \frac{m_B}{\bar{\gamma}_B}\right)$.

Based on (52), we proceed to employ the multinomial theorem to express $(F(x))^{N_B - L_B}$ as

$$(F(x))^{N_B-L_B} = \sum_{\mathcal{S}_B^F} a_k^F \left(\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^F} x^{b_k^F} e^{-c_k^F x}, \tag{56}$$

where $\mathcal{S}_B^F = \left\{ \left(n_{k,0}^F, \cdots, n_{k,m_B}^F \right) \Big| \sum_{j=0}^{m_B} n_{k,j}^F = N_B - L_B \right\}$, $a_k^F = \frac{(N_B-L_B)!}{\prod_{j=0}^{m_B} n_{k,j}^F!} \prod_{j=0}^{m_B-1} \left(\frac{-1}{j!}\right)^{n_{k,j+1}^F}$, $b_k^F = \sum_{j=0}^{m_B-1} j n_{k,j+1}^F$, and $c_k^F = \frac{m_B}{\bar{\gamma}_B} \sum_{j=1}^{m_B} n_{k,j}^F$.

Substituting (51), (55), and (56) into (54), and applying [37, eq. (3.351.3)], $\Phi_\gamma(s)$ is derived as

$$\begin{aligned}\Phi_\gamma(s) =& \frac{L_B}{(m_B-1)!}\binom{N_B}{L_B} \\ &\times \left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B L_B} \sum_{\mathcal{S}_B^{\Phi}} \sum_{\mathcal{S}_B^F} a_k^{\Phi} a_k^F \left(\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^F} \\ &\times \frac{\Gamma\left(b_k^{\Phi}+b_k^F+m_B\right)\left(s+\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^{\Phi}-m_B(L_B-1)}}{\left(s+c_k^{\Phi}+c_k^F+\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^{\Phi}+b_k^F+m_B}}. \end{aligned} \tag{57}$$

Let $F_\gamma(x)$ denote the CDF of γ, the Laplace transform of $F_\gamma(x)$ is given by $\mathcal{L}[F_\gamma(x)] = \Phi_\gamma(s)/s$ [25]. Therefore, the Laplace transform of the CDF of γ is

$$\begin{aligned}\mathcal{L}[F_\gamma(x)] =& \frac{L_B}{(m_B-1)!}\binom{N_B}{L_B} \\ &\times \left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B L_B} \sum_{\mathcal{S}_B^{\Phi}} \sum_{\mathcal{S}_B^F} a_k^{\Phi} a_k^F \left(\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^F} \\ &\times \frac{\Gamma\left(b_k^{\Phi}+b_k^F+m_B\right)}{(L_B)^{b_k^{\Phi}+b_k^F+m_B}} \frac{\left(s+\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^{\Phi}-m_B(L_B-1)}}{s\left(s+\frac{c_k^F}{L_B}+\frac{m_B}{\bar{\gamma}_B}\right)^{b_k^{\Phi}+b_k^F+m_B}}. \end{aligned} \tag{58}$$

Using a partial fraction expansion [37, eq. (2.102)], we can rewrite (58) in an equivalent form. Then, taking the inverse Laplace transform of $\mathcal{L}[F_\gamma(x)]$ to obtain

$$\begin{aligned}F_\gamma(x) = \frac{L_B}{(m_B-1)!}\binom{N_B}{L_B} \sum_{\mathcal{S}} \sum_{n=0}^{m_B L_B + b_k^F} a_k^{\Phi} a_k^F \\ \times \frac{\Gamma\left(b_k^{\Phi}+b_k^F+m_B\right)}{(L_B)^{b_k^{\Phi}+b_k^F+m_B}} \ell_n x^{\mu_n} e^{-\nu_n x}, \end{aligned} \tag{59}$$

where $\mathcal{S}$ denotes

$$\mathcal{S} = \left\{ \left(n_{k,0}^{\Phi} \cdots, n_{k,m_B-1}^{\Phi}, n_{k,0}^F, \cdots, n_{k,m_B^F}^F \right) \Big| \sum_{i=0}^{m_B-1} n_{k,i}^{\Phi} = L_B - 1, \sum_{j=0}^{m_B} n_{k,j}^F = N_B - L_B \right\},$$

and we define ℓ_n as

$$\ell_n = \begin{cases} \left(\frac{m_B}{\bar{\gamma}_B}\right)^{\mu_n} \left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F + 1\right)^{-n_1} & n = 0 \\ \left(\frac{m_B}{\bar{\gamma}_B}\right)^{\mu_n} \left(\Upsilon_1 + \Upsilon_2 - \frac{1-\mathrm{sgn}\left(c_k^F\right)}{(n-1)!}\right) & 1 \le n \le m_B(L_B-1) - b_k^{\Phi} \\ \left(\frac{m_B}{\bar{\gamma}_B}\right)^{\mu_n} \left(\Upsilon_3 + \Upsilon_4 - \frac{1-\mathrm{sgn}\left(c_k^F\right)}{(n-1)!}\right) & m_B(L_B-1) - b_k^{\Phi} < n \le m_B L_B + b_k^F \end{cases} \tag{60}$$

with $n_1 = b_k^{\Phi} + b_k^F + m_B$,

$$\begin{aligned}\Upsilon_1 =& -\frac{\mathrm{sgn}\left(c_k^F\right)}{(n-1)!}\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F + 1\right)^{-n_1}, \\ \Upsilon_2 =& \frac{\mathrm{sgn}\left(c_k^F\right)}{(n-1)!}(-1)^{1-n_2} \sum_{l=1}^{n_1} \binom{l-n_2-1}{l-1} \\ &\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F + 1\right)^{-(n_1-l+1)} \left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F\right)^{n_2-l}, \\ \Upsilon_3 =& -\frac{\mathrm{sgn}\left(c_k^F\right)}{(n_2-1)!}\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F + 1\right)^{-(n_1-n_2+1)}, \\ \Upsilon_4 =& \frac{\mathrm{sgn}\left(c_k^F\right)}{(n_2-1)!} \sum_{l=1}^{m_B(L_B-1)-b_k^{\Phi}} (-1)^{l+1} \\ &\binom{n_1-n_2+l-1}{l-1}\left(\frac{1}{L_B}\sum_{j=1}^{m_B} n_{k,j}^F\right)^{-(n_1-n_2+l)}, \end{aligned}$$

where $n_2 = n - m_B(L_B-1) + b_k^{\Phi}$. In (59), we also have

$$\mu_n = \begin{cases} 0 & n = 0 \\ n-1 & 1 \le n \le m_B(L_B-1) - b_k^{\Phi} \\ n - \mathrm{sgn}\left(c_k^F\right) & \\ \quad \left(m_B(L_B-1) - b_k^{\Phi}\right) - 1 & m_B(L_B-1) - b_k^{\Phi} < n \le m_B L_B + b_k^F \end{cases}$$

and

$$\nu_n = \begin{cases} 0 & n = 0 \\ \frac{m_B}{\bar{\gamma}_B} & 1 \le n \le m_B(L_B-1) - b_k^{\Phi} \\ \left(\frac{c_k^F}{L_B} + \frac{m_B}{\bar{\gamma}_B}\right) & m_B(L_B-1) - b_k^{\Phi} < n \le m_B L_B + b_k^F \end{cases}$$

The CDF of γ_B with TAS and GSC is given by $F_{\gamma_B} = (F_\gamma(x))^{N_A}$. Based on (59), and employing the multinomial theorem, we derive the CDF of γ_B as (6). Taking the derivative of the CDF in (6), we obtain the PDF of γ_B as (7).

APPENDIX B
PROOF OF THEOREM 2

We start with the asymptotic CDF for the SNR of a single branch of the main channel. In the high SNR regime with $\bar{\gamma}_B \to \infty$, applying the Taylor series expansion truncated to the kth order given by $e^x = \sum_{j=0}^{k} \frac{x^j}{j!} + o(x^k)$ in (52), we obtain

$$F(x) = 1 - e^{-x\frac{m_B}{\bar{\gamma}_B}} \left(e^{x\frac{m_B}{\bar{\gamma}_B}} - \frac{\left(x\frac{m_B}{\bar{\gamma}_B}\right)^{m_B}}{m_B!} - o\left(\left(x\frac{m_B}{\bar{\gamma}_B}\right)^{m_B}\right)\right)$$
$$= \frac{\left(x\frac{m_B}{\bar{\gamma}_B}\right)^{m_B}}{m_B!} + o(x^{m_B}). \quad (61)$$

Substituting (51), (55), and (61) into (54) yields

$$\Phi_\gamma(s) = \frac{L_B}{(m_B-1)!(m_B!)^{N_B-L_B}} \times \binom{N_B}{L_B}\left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B N_B} \sum_{\mathcal{S}_B^\Phi} a_k^\Phi \times \frac{\left(b_k^\Phi + m_B(N_B-L_B)+m_B-1\right)!}{(L_B)^{b_k^\Phi + m_B(N_B-L_B)+m_B}\left(s+\frac{m_B}{\bar{\gamma}_B}\right)^{m_B N_B}}. \quad (62)$$

It is shown in Appendix A that $\mathcal{L}[F_\gamma(x)] = \Phi_\gamma(s)/s$. Taking the inverse Laplace transform of $\mathcal{L}[F_\gamma(x)]$, F_γ is derived as

$$F_\gamma(x) = \frac{L_B}{(m_B-1)!(m_B!)^{N_B-L_B}}\binom{N_B}{L_B} \times \left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B N_B} \sum_{\mathcal{S}_B^\Phi} a_k^\Phi \frac{\left(b_k^\Phi + m_B(N_B-L_B)+m_B-1\right)!}{(L_B)^{b_k^\Phi + m_B(N_B-L_B)+m_B}} \times \left(\left(\frac{m_B}{\bar{\gamma}_B}\right)^{-m_B N_B} - \sum_{n=1}^{m_B N_B} \frac{\left(\frac{m_B}{\bar{\gamma}_B}\right)^{-(m_B N_B - n+1)}}{(n-1)!} x^{n-1} e^{-\frac{m_B}{\bar{\gamma}_B}x}\right). \quad (63)$$

Still employing the Taylor series expansion truncated to the kth order given by $e^x = \sum_{j=0}^{k} \frac{x^j}{j!} + o(x^k)$ in (63), we rewrite (63) as

$$F_\gamma(x) = \frac{L_B\binom{N_B}{L_B}\left(\frac{m_B}{\bar{\gamma}_B}\right)^{m_B N_B} x^{m_B N_B}}{(m_B-1)!(m_B!)^{N_B-L_B}(m_B N_B)!} \times \sum_{\mathcal{S}_B^\Phi} a_k^\Phi \frac{\left(b_k^\Phi + m_B(N_B-L_B)+m_B-1\right)!}{(L_B)^{b_k^\Phi + m_B(N_B-L_B)+m_B}}. \quad (64)$$

Based on (64), the asymptotic expression for the CDF of γ_B is $F_{\gamma_B}(x) = (F_\gamma(x))^{N_A}$ and the final expression is shown in (8).

APPENDIX C
PROOF OF THEOREM 3

Substituting (14) into (12), we rewrite the average secrecy rate as

$$\bar{C}_s = \frac{1}{\ln 2}\int_0^\infty \left[\int_0^{x_1} \frac{F_{\gamma_E}(x_2)}{1+x_2}dx_2\right] f_{\gamma_B}(x_1)dx_1. \quad (65)$$

Substituting (17) into (65), we transform (65) as

$$\bar{C}_s = \underbrace{\frac{1}{\ln 2}\int_0^\infty \ln(1+x_1) f_{\gamma_B}(x_1)dx_1}_{\omega_2} + \underbrace{\frac{1}{\ln 2}\int_0^\infty \int_0^{x_1} \frac{\chi_{\gamma_E}(x_2)}{1+x_2} f_{\gamma_B}(x_1)dx_2dx_1}_{\omega_3}. \quad (66)$$

In the high SNR regime with $\bar{\gamma}_B \to \infty$, $\ln(1+x_1) \approx \ln(x_1)$, thereby the asymptotic expression for ω_2 can be written as Δ_1 in (19). Changing the order of integration in ω_3, we rewrite

$$\omega_3 = \frac{1}{\ln 2}\int_0^\infty \frac{\chi_{\gamma_E}(x_2)}{1+x_2}\int_{x_2}^\infty f_{\gamma_B}(x_1)dx_1dx_2 = \frac{1}{\ln 2}\int_0^\infty \frac{\chi_{\gamma_E}(x_2)}{1+x_2}\left(1 - F_{\gamma_B}(x_2)\right)dx_2. \quad (67)$$

According to (8), when $\bar{\gamma}_B \to \infty$, $F_{\gamma_B}(x_2) \approx 0$. Hence, the asymptotic expression for ω_3 can be expressed as Δ_2 in (20). Based on (19), (20), and (66), we derive the asymptotic expression for the average secrecy rate as (18).

REFERENCES

[1] 3GPP TS 36.300, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), Overall description: Stage 2," Mar. 2013, version 11.5.0. [Online]. Available: www.3gpp.org

[2] R. Pabst *et al.*, "Relay-based deployment concepts for wireless and mobile broadband radio," *IEEE Commun. Mag.*, vol. 42, no. 9, pp. 80–89, Sep. 2004.

[3] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[4] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[5] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[6] A. D. Wyner, "The wire-tap channel," *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[7] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[8] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT*, 2007, pp. 2466–2470.

[9] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[10] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

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

[12] 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.

[13] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[14] M. Yuksel and E. Erkip, "Diversity–Multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, Mar. 2011.
[15] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.
[16] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.
[17] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.
[18] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wire-tap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
[19] M. Z. I. Sarkar and T. Ratnarajah, "On the secrecy mutual information of Nakagami-m fading SIMO channel," in *Proc. IEEE ICC*, May 2010, pp. 1–5.
[20] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wire-tap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.
[21] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.
[22] A. Lodhi, F. Said, M. Dohler, and A. H. Aghvami, "Closed-form symbol error probabilities of STBC and CDD MC-CDMA with frequency-correlated subcarriers over Nakagami-m fading channels," *IEEE Trans. Veh. Technol.*, vol. 57, no. 2, pp. 962–973, Mar. 2008.
[23] N. B. Mehta, S. Kashyap, and A. F. Molisch, "Antenna selection in LTE: From motivation to specification," *IEEE Commun. Mag.*, vol. 50, no. 10, pp. 144–150, Oct. 2012.
[24] A. Annamalai and C. Tellambura, "A new approach to performance evaluation of generalized selection diversity receivers in wireless channels," in *Proc. IEEE VTC*, 2001, pp. 2309–2313.
[25] X. Cai and G. B. Giannakis, "Performance analysis of combined transmit selection diversity and receive generalized selection combining in Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 1980–1983, Nov. 2004.
[26] I. Ahmed, A. Nasri, R. Schober, and R. K. Mallik, "Asymptotic performance of generalized selection combining in generic noise and fading," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 916–922, Apr. 2012.
[27] M.-S. Alouini and M. K. Simon, "An MGF-based performance analysis of generalized selection combining over Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 401–415, Mar. 2000.
[28] M. Win and J. Winters, "Virtual branch analysis of symbol error probability for hybrid selection/maximal-ratio combining in Rayleigh fading," *IEEE Trans. Commun.*, vol. 49, no. 11, pp. 1926–1934, Nov. 2001.
[29] Y. Ma and C. C. Chai, "Unified error probability analysis for generalized selection combining in Nakagami fading channels," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 11, pp. 2198–2210, Nov. 2000.
[30] R. K. Mallik and M. Z. Win, "Analysis of hybrid selection/maximal-ratio combining in correlated Nakagami fading," *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1372–1383, Aug. 2002.
[31] X. Zhang and N. C. Beaulieu, "Performance analysis of generalized selection combining in generalized correlated Nakagami-m fading," *IEEE Trans. Commun.*, vol. 54, no. 11, pp. 2103–2112, Nov. 2006.
[32] Y. Ma, Z. Wang, and S. Pasupathy, "Asymptotic performance of hybrid-selection/maximal-ratio combining over fading channels," *IEEE Trans. Commun.*, vol. 54, no. 5, pp. 770–777, May 2006.
[33] S.-I. Chu, "Performance of amplify-and-forward cooperative diversity networks with generalized selection combining over Nakagami-m fading channels," *IEEE Commun. Lett.*, vol. 16, no. 5, pp. 634–637, May 2012.
[34] Y. Ma and S. Pasupathy, "Efficient performance evaluation for generalized selection combining on generalized fading channels," *IEEE Trans. Wireless Commun.*, vol. 3, no. 1, pp. 29–34, Jan. 2004.
[35] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[36] 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.
[37] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.
[38] S. Jin, M. R. 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.
[39] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.
[40] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.
[41] D. B. da Costa and S. Aissa, "Cooperative dual-hop relaying systems with beamforming over Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3950–3954, Aug. 2009.
[42] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*. New York, NY, USA: Addison-Wesley, 1989.

Lifeng Wang (S'12) received the M.S. degree in electronic engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2012. He is currently working toward the Ph.D. degree in electronic engineering with Queen Mary University of London, London, U.K.

His research interests include physical layer security, millimeter-wave communications, and 5G HetNets.

Maged Elkashlan (M'06) received the Ph.D. degree in electrical engineering from The University of British Columbia, Vancouver, Canada, in 2006. From 2007 to 2011, he was with the Wireless and Networking Technologies Laboratory, Commonwealth Scientific and Industrial Research Organization, Clayton, Australia. During this time, he held an adjunct appointment at the University of Technology, Sydney, Australia. In 2011, he joined the School of Electronic Engineering and Computer Science, Queen Mary University of London, London, U.K., as an Assistant Professor. He also holds visiting faculty appointments at the University of New South Wales, Sydney, Australia, and Beijing University of Posts and Telecommunications, Beijing, China. His current research interests include distributed information processing, security, cognitive radio, and 5G HetNets.

Dr. Elkashlan is an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the IEEE COMMUNICATIONS LETTERS. He also serves as the Lead Guest Editor for the special issue on "Green Media: The Future of Wireless Multimedia Networks" of the *IEEE Wireless Communications Magazine* and for the special issue on "Millimeter Wave Communications for 5G" of the *IEEE Communications Magazine* and the Guest Editor for the special issue on "Energy Harvesting Communications" of the *IEEE Communications Magazine* and for the special issue on "Location Awareness for Radios and Networks" of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. His research has won several academic awards, including Best Paper Awards at IEEE ICC 2014, CHINACOM 2014, and IEEE VTC-Spring 2013. He received the Exemplary Reviewer Certificate of the IEEE COMMUNICATIONS LETTERS in 2012.

Jing Huang (S'10–M'13) received the B.S. degree in communication engineering from Jilin University, Changchun, China, in 2006, the M.S. degree in communications and information systems from Beijing University of Posts and Telecommunications, Beijing, China, in 2009, and the Ph.D. degree in electrical and computer engineering from the University of California, Irvine, CA, USA, in 2013.

He was an Intern at Broadcom Corporation, Sunnyvale, CA, during the spring and summer of 2012. He is currently with Qualcomm Technologies Inc., Santa Clara, CA. His research interests include cooperative communications, applied signal processing, and radio resource management in wireless networks.

Robert Schober (S'98–M'01–SM'08–F'10) was born in Neuendettelsau, Germany, in 1971. He received the Diplom (Univ.) and Ph.D. degrees in electrical engineering from the University of Erlangen-Nuremberg (FAU), Erlangen, Germany, in 1997 and 2000, respectively. From May 2001 to April 2002, he was a Postdoctoral Fellow at the University of Toronto, Toronto, Canada, sponsored by the German Academic Exchange Service (DAAD). Since May 2002, he has been with The University of British Columbia (UBC), Vancouver, Canada, where he is currently a Full Professor. Since January 2012, he has been also an Alexander von Humboldt Professor and the Chair for Digital Communication at FAU, Erlangen, Germany. His research interests fall into the broad areas of communication theory, wireless communications, and statistical signal processing.

Dr. Schober is a Fellow of The Canadian Academy of Engineering and The Engineering Institute of Canada. He is currently the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS. He was a recipient of several awards for his work, including the 2002 Heinz Maier-Leibnitz Award of the German Science Foundation (DFG), the 2004 Innovations Award of the Vodafone Foundation for Research in Mobile Communications, the 2006 UBC Killam Research Prize, the 2007 Friedrich Wilhelm Bessel Research Award of the Alexander von Humboldt Foundation, the 2008 Charles McDowell Award for Excellence in Research from UBC, a 2011 Alexander von Humboldt Professorship, and a 2012 NSERC E.W.R. Steacie Fellowship. He was also a recipient of the best paper awards from the German Information Technology Society (ITG); the European Association for Signal, Speech and Image Processing (EURASIP); IEEE WCNC 2012; IEEE Globecom 2011; IEEE ICUWB 2006; the International Zurich Seminar on Broadband Communications; and European Wireless 2000.

Ranjan K. Mallik (S'88–M'93–SM'02–F'12) received the B.Tech. degree from the Indian Institute of Technology, Kanpur, India, in 1987 and the M.S. and Ph.D. degrees from the University of Southern California, Los Angeles, CA, USA, in 1988 and 1992, respectively, all in electrical engineering. From August 1992 to November 1994, he was a Scientist at the Defence Electronics Research Laboratory, Hyderabad, India, working on missile and EW projects. From November 1994 to January 1996, he was a Faculty Member of the Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology, Kharagpur, India. From January 1996 to December 1998, he was with the faculty of the Department of Electronics and Communication Engineering, Indian Institute of Technology, Guwahati, India. Since December 1998, he has been with the faculty of the Department of Electrical Engineering, Indian Institute of Technology, Delhi, New Delhi, India, where he is currently a Professor. His research interests are in diversity combining and channel modeling for wireless communications, space-time systems, cooperative communications, multiple-access systems, power line communications, difference equations, and linear algebra.

Dr. Mallik is a member of the IEEE Communications, IEEE Information Theory, and IEEE Vehicular Technology Societies; the American Mathematical Society; and the International Linear Algebra Society. He is a Fellow of the Indian National Academy of Engineering; the Indian National Science Academy; The National Academy of Sciences, India (Allahabad); the Indian Academy of Sciences, Bangalore; The World Academy of Sciences; The Institution of Engineering and Technology, U.K.; and The Institution of Electronics and Telecommunication Engineers, India. He is a Life Member of the Indian Society for Technical Education and an Associate Member of The Institution of Engineers (India). He is an Area Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He has been a recipient of the Hari Om Ashram Prerit Dr. Vikram Sarabhai Research Award in the field of Electronics, Telematics, Informatics, and Automation and the Shanti Swarup Bhatnagar Prize in Engineering Sciences. He is a member of Eta Kappa Nu.