Correspondence

Physical Layer Security of TAS/MRC With Antenna Correlation

Nan Yang, Himal A. Suraweera, Iain B. Collings, and Chau Yuen

***Abstract*—We analyze the impact of antenna correlation on secrecy performance of multiple-input multiple-output wiretap channels where transmitter employs transmit antenna selection while receiver and eavesdropper perform maximal-ratio combining with arbitrary correlation. New closed-form expressions are derived for the exact and asymptotic (high signal-to-noise ratio in transmitter–receiver channel) secrecy outage probability.**

***Index Terms*—Antenna correlation, multiple-input multiple-output wiretap channel, physical layer security, transmit antenna selection.**

I. Introduction

Due to the broadcast nature of wireless medium and the resulting security vulnerabilities such as eavesdropping, physical (PHY) layer security has emerged as an indispensable strategy to augment secrecy in wireless communications networks [1]. The pivotal principle behind this novel strategy is to exploit the spatio-temporal characteristics of wireless channels to facilitate secure data transmission [2]. In early studies such as [3], perfect secrecy in wiretap channels was shown to be achieved when the channel between the transmitter and the eavesdropper is a degraded version of the channel between the transmitter and the receiver. This necessitates the channel state information (CSI) of both channels at the transmitter to ensure secure communications. In practice, the eavesdropper's channel knowledge may not be known at the transmitter such that perfect secrecy cannot be guaranteed. In this passive eavesdropping case, the secrecy outage probability is adopted as a useful and intuitive metric to evaluate security [2].

Motivated by the next generation wireless standards with multi-antenna nodes, PHY layer security in multiple-input multiple-output (MIMO) wiretap channels has recently been studied (see, e.g., [4] and reference therein). For the practical case of passive eavesdropping, maximal-ratio combining (MRC) was applied at the receiver and the eavesdropper in [5] to increase secrecy capacity. In [6], the secrecy outage probability was compared between MRC and selection combining (SC) at the eavesdropper. In [7] and [8], the secrecy performance metrics with transmit antenna selection (TAS) were examined in independent Rayleigh and Nakagami-m fading channels, respectively. To the best of authors' knowledge, however, very limited attention has been directed to the antenna correlation effect on secrecy (e.g., [6] considered a limited antenna correlation model which only applies to two antennas at the eavesdropper). The findings in this direction are crucial for system designers since antenna correlation is unavoidable in many practical situations [9]–[11]. We note that secrecy capacity increases with the signal-to-noise ratio (SNR) of the main channel and decreases with the SNR of the eavesdropper's channel. Therefore, the correlation features that increase (or decrease) the performance of both channels have non trivially predictable effects on the secrecy performance of the system.

In this paper, we completely characterize the impact of antenna correlation on the secrecy performance of the wiretap channel with multiple antennas at the transmitter, receiver, and eavesdropper. The adoption of this model relaxes some restrictions imposed in the existing literature on the number of antennas at the receiver (e.g., single antenna [7]) and the eavesdropper (e.g., dual antennas [6]). In our model, the transmitter side experiences independent fading which is applicable due to spatially separated antennas, e.g., at a base station. At the receiver side and the eavesdropper side, we assume an arbitrary antenna correlation model. This model has the ability to mimic a wide range of antenna correlation conditions often experienced in practice, such as uniform correlation [10], exponential correlation [11], and correlation models constructed from measured channels (e.g., [9]). The special case of full correlation is also included in our analysis as one extreme end. At the transmitter, TAS is adopted to enhance physical layer security with low feedback overhead [7] while MRC is applied at the receiver and at the eavesdropper.

For the considered wiretap channel in this paper, we examine the two following, fundamental and interesting questions: "*1) What is the impact of antenna correlation at the receiver/eavesdropper on secrecy?*" and "*2) Which correlation has a higher dominance on secrecy?*" In order to address these questions completely, new closed-form expressions are derived for the exact secrecy outage probability and the probability of positive secrecy. Our new expressions encompass the results for independent fading in [5]–[7] as special cases. Moreover, for the considered scenarios, we derive a new compact expression for the asymptotic secrecy outage probability, which characterizes the secrecy performance with high average SNR over the main channel. The asymptotic expressions explicitly show how the secrecy outage diversity order and the secrecy outage array gain vary depending on the correlation parameters, the number of antennas, and the average SNRs. Notably, we show that for the low average SNR of the main channel, higher correlation at the eavesdropper brings greater performance improvement than higher correlation at the receiver. For the medium and high average SNR of the main channel, higher correlation at the eavesdropper imposes less performance degradation than higher correlation at the receiver.

II. System and Channel Model

Consider a wiretap channel where the transmitter (Alice), the receiver (Bob), and the eavesdropper (Eve) are equipped with N_{A}, N_{B}, and N_{E} antennas, respectively. We concentrate on passive eavesdropping, where the CSI of the eavesdropper's channel is not available at Alice. A quasi-static Rayleigh fading model is assumed for the main channel and the eavesdropper's channel, where the fading coefficients remain fixed during a transmission block but vary independently from block to block. Also, the main channel and the eavesdropper's channel are assumed to be independent of each other. To perform secure transmission, Alice encodes the message block $\mathbf{m}$ into the codeword $\mathbf{x} =$

Manuscript received May 02, 2012; revised August 02, 2012; accepted September 29, 2012. Date of publication October 09, 2012; date of current version January 03, 2013. This work was supported in part by a CSIRO OCE postdoctoral fellowship and in part by the International Design Center (Grant IDG31100102 Grant IDD11100101). The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yao-Win (Peter) Hong.

N. Yang and I. B. Collings are with the Wireless and Networking Technologies Laboratory, CSIRO ICT Centre, Marsfield, NSW 2122, Australia (e-mail: jonas.yang@csiro.au; iain.collings@csiro.au).

H. A. Suraweera and C. Yuen are with the Singapore University of Technology and Design, Singapore 138682 (e-mail: himalsuraweera@sutd.edu.sg; yuenchau@sutd.edu.sg).

Digital Object Identifier 10.1109/TIFS.2012.2223681

$[x(1), \cdots, x(l), \cdots, x(L)]$, where L is the length of $\mathbf{x}$. This codeword is subject to an average power constraint $\sum_{l=1}^{L} \mathbb{E}[|x(l)|^2]/L \leq P$, where $\mathbb{E}[\cdot]$ denotes the expectation.

Applying the TAS/MRC protocol in this MIMO wiretap channel, the strongest antenna amongst $N_{\rm A}$ antennas at Alice is selected to maximize the instantaneous SNR of the main channel. Since MRC is adopted at Bob, the strongest antenna refers to the transmit antenna providing the highest instantaneous SNR at Bob. In this protocol, only the strongest antenna index is fed back from Bob and Alice. As such, the strongest antenna for Bob is entirely determined by the CSI of the main channel and thus, corresponds to a random transmit antenna for Eve. This is due to the assumption that the main channel and the eavesdropper's channel are assumed to be mutually independent. It follows that Eve is not able to exploit the multiantenna diversity from Alice. We consider MRC at Bob and Eve.[1] Therefore, the index of the selected strongest antenna, n^*, is determined as

$$n^* = \underset{1 \leq n \leq N_{\rm A}}{\arg\max} \left\| \mathbf{\Phi}_{\rm B}^{\frac{1}{2}} \mathbf{h}_{n{\rm B}} \right\|, \tag{1}$$

where $\mathbf{\Phi}_{\rm B}$ denotes the $N_{\rm B} \times N_{\rm B}$ antenna correlation matrix at Bob, $\mathbf{h}_{n{\rm B}}$ denotes the $N_{\rm B} \times 1$ channel vector between the nth transmit antenna at Alice and the $N_{\rm B}$ antennas at Bob with independent identically distributed (i.i.d.) Rayleigh fading entries, and $\| \cdot \|$ denotes the Euclidean norm. With this strongest antenna, the main channel vector is written as $\mathbf{h}_{\rm B} \triangleq \mathbf{h}_{n^*{\rm B}}$. We further denote $\mathbf{\Phi}_{\rm E}$ as the $N_{\rm E} \times N_{\rm E}$ antenna correlation matrix at Eve, and denote $\mathbf{h}_{n{\rm E}}$ as the $N_{\rm E} \times 1$ channel vector between the nth transmit antenna at Alice and the $N_{\rm E}$ antennas at Eve with i.i.d. Rayleigh fading entries. As such, the eavesdropper's channel vector is written as $\mathbf{h}_{\rm E} \triangleq \mathbf{h}_{n^*{\rm E}}$. The distinct real eigenvalues of $\mathbf{\Phi}_{\rm B}$ are denoted as $\phi_1, \phi_2, \cdots, \phi_b$ with multiplicities $\beta_1, \beta_2, \cdots, \beta_b$, respectively, where $\sum_{i=1}^{b} \beta_i = N_{\rm B}$. The distinct real eigenvalues of $\mathbf{\Phi}_{\rm E}$ are denoted as $\varphi_1, \varphi_2, \cdots, \varphi_\epsilon$ with multiplicities $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_\epsilon$, respectively, where $\sum_{u=1}^{\epsilon} \varepsilon_u = N_{\rm E}$.

In the main channel, the received signal vector at Bob at time l is given by $\mathbf{y}(l) = \mathbf{\Phi}_{\rm B}^{1/2} \mathbf{h}_{\rm B} x(l) + \mathbf{n}_{\rm B}$, where $\mathbf{n}_{\rm B}$ is the $N_{\rm B} \times 1$ additive white Gaussian noise (AWGN) vector at Bob satisfying $\mathbb{E}[\mathbf{n}_{\rm B}\mathbf{n}_{\rm B}^\dagger] = \mathbf{I}_{N_{\rm B}} \sigma_{\rm B}^2$, $\sigma_{\rm B}^2$ is the noise variance at each receive antenna, $(\cdot)^\dagger$ denotes the conjugate transpose operation, and $\mathbf{I}_m$ denotes the $m \times m$ identity matrix. Applying MRC, Bob multiplies the received signal vector by the conjugate transpose of a $N_{\rm B} \times 1$ weight vector $\mathbf{w}_{\rm B} = \mathbf{\Phi}_{\rm B}^{1/2} \mathbf{h}_{\rm B} / \| \mathbf{\Phi}_{\rm B}^{1/2} \mathbf{h}_{\rm B} \|$. This results in a single scalar symbol $y(l)$ given by

$$y(l) = \mathbf{w}_{\rm B}^\dagger \mathbf{y}(l) = \left\| \mathbf{\Phi}_{\rm B}^{\frac{1}{2}} \mathbf{h}_{\rm B} \right\| x(l) + \mathbf{w}_{\rm B}^\dagger \mathbf{n}_{\rm B}. \tag{2}$$

Based on (2), the instantaneous SNR of the main channel is given by $\gamma_{\rm B} = \| \mathbf{\Phi}_{\rm B}^{1/2} \mathbf{h}_{\rm B} \|^2 P / \sigma_{\rm B}^2$. In the eavesdropper's channel, Eve receives the signal vector from Alice and performs MRC at time l, resulting in

$$z(l) = \left\| \mathbf{\Phi}_{\rm E}^{\frac{1}{2}} \mathbf{h}_{\rm E} \right\| x(l) + \mathbf{w}_{\rm E}^\dagger \mathbf{n}_{\rm E}, \tag{3}$$

where $\mathbf{w}_{\rm E} = \mathbf{\Phi}_{\rm E}^{1/2} \mathbf{h}_{\rm E} / \| \mathbf{\Phi}_{\rm E}^{1/2} \mathbf{h}_{\rm E} \|$ is a $N_{\rm E} \times 1$ weight vector at Eve, $\mathbf{n}_{\rm E}$ is the $N_{\rm E} \times 1$ AWGN vector at Eve which satisfies $\mathbb{E}[\mathbf{n}_{\rm E}\mathbf{n}_{\rm E}^\dagger] = \mathbf{I}_{N_{\rm E}} \sigma_{\rm E}^2$, and $\sigma_{\rm AE}^2$ is the noise variance at each receive antenna. According to (3), the instantaneous SNR of the eavesdropper's channel is given by $\gamma_{\rm E} = \| \mathbf{\Phi}_{\rm E}^{1/2} \mathbf{h}_{\rm E} \|^2 P / \sigma_{\rm E}^2$.

In this system, the capacity of the main channel is given by $R_{\rm B} = \log_2(1+\gamma_{\rm B})$ and the capacity of the eavesdropper's channel is given by $R_{\rm E} = \log_2(1+\gamma_{\rm E})$. According to [2], the secrecy capacity is defined as $C_S = [R_{\rm B} - R_{\rm E}]^+$ for $R_{\rm B} > R_{\rm E}$, where $[x]^+$ denotes $\max\{0, x\}$. Here, the secrecy capacity is strictly positive. In TAS/MRC, Alice has no CSI about the main channel since Bob only feeds back the strongest antenna index to Alice. For passive eavesdropping, Alice and Bob have no CSI about the eavesdropper's channel. Therefore, Alice sets a constant code rate R. If $C_S > R$, the codewords with rate R guarantee perfect secrecy. Otherwise, if $C_S < R$, Eve can eavesdrop on data, thereby perfect secrecy is compromised. This mandates the use of secrecy outage probability as a useful and practical secrecy performance metric [2], [5]–[7]. Specifically, secrecy outage probability is the probability that either there is an outage between Alice and Bob (i.e., the conventional outage probability where the message is not decodable at Bob) or Eve can eavesdrop on data such that perfect secrecy is compromised.

[1]We note that [6] considered comparing MRC and SC at Eve. We do not consider SC in this paper since MRC always outperforms SC.

III. Secrecy With Antenna Correlation

In this section, we derive two important secrecy metrics, namely the secrecy outage probability and the probability of positive secrecy.[2] We commence our analysis by presenting the statistics of $\gamma_{\rm B}$ and $\gamma_{\rm E}$. With the aid of [12, Eq. (11)], the PDF of $\gamma_{\rm E}$ is given by

$$f_{\gamma_{\rm E}}(\gamma) = \sum_{u=1}^{\epsilon} \sum_{v=1}^{\varepsilon_u} \frac{\varpi_{u,v} e^{-\frac{\gamma}{\varphi_u \overline{\gamma}_{\rm E}}}}{\Gamma(v)(\varphi_u \overline{\gamma}_{\rm E})^v} \gamma^{v-1}. \tag{4}$$

In (4), $\varpi_{u,v}$ is the correlation coefficient at Eve, which is defined as [13, Eq. (12)]

$$\varpi_{u,v} = \frac{(-1)^{\varepsilon_u}}{\varphi_u^{\varepsilon_u}} \sum_{\tau(u,v)} \prod_{w=1, w \neq u}^{\epsilon} \binom{\varepsilon_w + q_w + 1}{q_w} \frac{\varphi_w^{q_w}}{\left(1 - \frac{\varphi_w}{\varphi_u}\right)^{\varepsilon_w + q_w}}, \tag{5}$$

where $\tau(u,v)$ denotes a set of ϵ-tuples such that $\tau(u,v) = \{(q_1, \cdots, q_\epsilon) : q_w \in N_q, q_u = 0, \sum_{w=1}^{\epsilon} q_w = \varepsilon_u - v\}$, with N_q signifying the set of nonnegative integers. Using [12, Eq. (12)], the CDF of $\gamma_{\rm B}$ can be expressed as

$$F_{\gamma_{\rm B}}(\gamma) = \left(1 - \sum_{i=1}^{b} \sum_{j=1}^{\beta_i} \sum_{k=0}^{j-1} \frac{\varpi_{i,j}}{k!} e^{-\frac{\gamma}{\phi_i \overline{\gamma}_{\rm B}}} \left(\frac{\gamma}{\phi_i \overline{\gamma}_{\rm B}} \right)^k \right)^{N_{\rm A}}. \tag{6}$$

In (6), $\varpi_{i,j}$ is the correlation coefficient at Bob, which is defined as [13, Eq. (12)]

$$\varpi_{i,j} = \frac{(-1)^{\beta_i}}{\phi_i^{\beta_i}} \sum_{\tau(i,j)} \prod_{m=1, m \neq i}^{b} \binom{\beta_m + p_m + 1}{p_m} \frac{\phi_m^{p_m}}{\left(1 - \frac{\phi_m}{\phi_i}\right)^{\beta_m + p_m}}, \tag{7}$$

where $\tau(i,j)$ denotes a set of b-tuples such that $\tau(i,j) = \{(p_1, \cdots, p_b) : p_m \in N_p, p_i = 0, \sum_{m=1}^{b} p_m = \beta_i - j\}$, with N_p signifying the set of nonnegative integers. In (4) and (6), we have $\overline{\gamma}_{\rm B} = P/\sigma_{\rm B}^2$, and $\overline{\gamma}_{\rm E} = P/\sigma_{\rm E}^2$. Expanding the binomial and the resultant polynomial in (6), we rewrite the CDF of $\gamma_{\rm B}$ as

$$F_{\gamma_{\rm B}}(\gamma) = 1 - \sum_{n=1}^{N_{\rm A}} \binom{N_{\rm A}}{n} (-1)^{n-1} \sum_{i=1}^{b} \sum_{j=1}^{\beta_i} \sum_{k=0}^{j-1} \sum_{S_m \in \mathcal{S}} \frac{n!}{\prod_{m=1}^{J} s_m!} \times \prod_{1 \leq m \leq J} \left(\frac{\varpi_{i,j}}{k!} \right)^{s_m} \frac{e^{-\frac{s_m \gamma}{\phi_i \overline{\gamma}_{\rm B}}}}{(\phi_i \overline{\gamma}_{\rm B})^{k s_m}} \gamma^{k s_m}, \tag{8}$$

where $\mathcal{S} = \{S_m | \sum_{m=1}^{J} s_m = n\}$ with nonnegative integers $\{s_m\}$ and $J = \sum_{i=1}^{b} \sum_{j=1}^{\beta_i} j$.

[2]In this paper, our focus is to quantify the achievable level of secrecy rather than the actual code design.

A. Secrecy Outage Probability

The secrecy outage probability is defined as $P_{\rm out}(R_S) = \Pr(C_S < R_S)$, where $R_S > 0$ is the predetermined secrecy rate. We proceed to rewrite $P_{\rm out}(R_S)$ as

$$P_{\rm out}(R_S) = \underbrace{\Pr(C_S < R_S | \gamma_{\rm B} > \gamma_{\rm E})}_{\hbar_1} \Pr(\gamma_{\rm B} > \gamma_{\rm E}) + \underbrace{\Pr(\gamma_{\rm B} < \gamma_{\rm E})}_{\hbar_2}, \quad (9)$$

where $\hbar_1$ is derived as

$$\hbar_1 = \frac{1}{\Pr(\gamma_{\rm B} > \gamma_{\rm E})} \times \int_0^{\infty} \int_{\gamma_{\rm E}}^{2^{R_S}(1+\gamma_{\rm E})-1} f_{\gamma_{\rm E}}(\gamma_{\rm E}) f_{\gamma_{\rm B}}(\gamma_{\rm B}) d\gamma_{\rm B} d\gamma_{\rm E}, \quad (10)$$

and $\hbar_2$ is derived as

$$\hbar_2 = \int_0^{\infty} \int_0^{\gamma_{\rm E}} f_{\gamma_{\rm E}}(\gamma_{\rm E}) f_{\gamma_{\rm B}}(\gamma_{\rm B}) d\gamma_{\rm B} d\gamma_{\rm E}. \quad (11)$$

Using (10) and (11) into (9), $P_{\rm out}(R_S)$ is derived as

$$\begin{aligned} P_{\rm out}(R_S) &= \int_0^{\infty} \int_0^{2^{R_S}(1+\gamma_{\rm E})-1} f_{\gamma_{\rm E}}(\gamma_{\rm E}) f_{\gamma_{\rm B}}(\gamma_{\rm B}) d\gamma_{\rm B} d\gamma_{\rm E} \\ &= \int_0^{\infty} f_{\gamma_{\rm E}}(\gamma_{\rm E}) F_{\gamma_{\rm B}}\left(2^{R_S}(1+\gamma_{\rm E})-1\right) d\gamma_{\rm E}. \end{aligned} \quad (12)$$

Substituting (4) and (8) into (12) and solving the resultant integrals with the help of [14, Eq. (3.326.2)] yields

$$\begin{aligned} P_{\rm out}(R_S) = 1 - &\sum_{n=1}^{N_{\rm A}} \binom{N_{\rm A}}{n} (-1)^{n-1} \\ &\times \sum_{i=1}^{b} \sum_{j=1}^{\beta_i} \sum_{k=0}^{j-1} \sum_{S_m \in \mathcal{S}} \frac{n!}{\prod_{m=1}^{J} s_m!} \\ &\times \prod_{1 \le m \le J} \left(\frac{\varpi_{i,j}}{k!(\phi_i \overline{\gamma}_{\rm B})^k} \right)^{s_m} e^{-\frac{s_m(2^{R_S}-1)}{\phi_i \overline{\gamma}_{\rm B}}} \sum_{q=0}^{k s_m} \binom{k s_m}{q} \\ &\times (2^{R_S}-1)^{k s_m - q} 2^{R_S q} \sum_{u=1}^{\epsilon} \sum_{v=1}^{\varepsilon_u} \frac{\Gamma(q+v)\varpi_{u,v}}{\Gamma(v)(\varphi_u \overline{\gamma}_{\rm E})^v} \\ &\times \left(\frac{2^{R_S} s_m}{\phi_i \overline{\gamma}_{\rm B}} + \frac{1}{\varphi_u \overline{\gamma}_{\rm E}} \right)^{-(q+v)}. \end{aligned} \quad (13)$$

The secrecy outage probability expression in (13) is derived in closed-form and applies to arbitrary numbers of antennas, arbitrary average SNRs, and generalized antenna correlation.

We note that (13) is useful to calculate other secrecy metrics. We first evaluate the probability of positive secrecy. In wiretap channels, positive secrecy is achievable when $R_{\rm B} > R_{\rm E}$. As such, the probability of positive secrecy is evaluated as

$$\Pr(C_S > 0) = \Pr(\gamma_{\rm B} > \gamma_{\rm E}) = 1 - P_{\rm out}(0). \quad (14)$$

Setting $R_S = 0$ in (13), a new closed-form expression for the probability of positive secrecy is derived as

$$\begin{aligned} \Pr(C_S > 0) = &\sum_{n=1}^{N_{\rm A}} \binom{N_{\rm A}}{n} (-1)^{n-1} \sum_{i=1}^{b} \sum_{j=1}^{\beta_i} \sum_{k=0}^{j-1} \sum_{S_m \in \mathcal{S}} \frac{n!}{\prod_{m=1}^{J} s_m!} \\ &\times \prod_{1 \le m \le J} \left(\frac{\varpi_{i,j}}{k!(\phi_i \overline{\gamma}_{\rm B})^k} \right)^{s_m} \sum_{u=1}^{\epsilon} \sum_{v=1}^{\varepsilon_u} \frac{\Gamma(k s_m + v)}{\Gamma(v)} \\ &\times \frac{\varpi_{u,v}}{(\varphi_u \overline{\gamma}_{\rm E})^v} \left(\frac{s_m}{\phi_i \overline{\gamma}_{\rm B}} + \frac{1}{\varphi_u \overline{\gamma}_{\rm E}} \right)^{-(k s_m + v)}. \end{aligned} \quad (15)$$

Second, based on (13) we obtain the ε-outage secrecy capacity as $C_{\rm out}(\varepsilon) = R_{S,\max}$, where $P_{\rm out}(R_{S,\max}) = \varepsilon$. This specifies the maximum secrecy rate $R_{S,\max}$ when the secrecy outage probability is less than ε.

We next derive the asymptotic secrecy outage probability $P_{\rm out}^{\infty}(R_S)$ to characterize the behavior of secrecy outage probability when the average SNR of the main channel is sufficiently high,[3] i.e., $\overline{\gamma}_{\rm B} \to \infty$. Here, $\overline{\gamma}_{\rm B} \to \infty$ corresponds to the scenario where Bob is located much closer to Alice than Eve, which is a practical scenario of interest. The asymptotic result will enable us to explicitly examine the impact of antenna correlation on the secrecy performance in terms of the secrecy outage diversity order and the secrecy outage array gain. The secrecy outage diversity order, which is the slope of the secrecy outage probability curve, describes how fast the secrecy outage probability decreases with average SNR. The secrecy outage array gain, which is the horizontal shift of the secrecy outage probability curve, describes the SNR advantage of a secrecy outage probability curve relative to the reference curve with the same secrecy outage diversity order. To this end, the first nonzero order expansion $F_{\gamma_{\rm B}}^{\infty}(\gamma)$ is derived. With the aid of the Maclaurin series expansion from [14, Eq. (1.211.1)], we retain the first nonzero order term and discard the higher order terms, which results in

$$\begin{aligned} F_{\gamma_{\rm B}}^{\infty}(\gamma) = &\left(\sum_{i=1}^{b} \sum_{j=1}^{\beta_i} \sum_{k=0}^{j-1} \binom{N_{\rm B}}{k} \frac{(-1)^{N_{\rm B}-k+1} \varpi_{i,j}}{(N_{\rm B}-k)! k! \phi_i^{N_{\rm B}}} \right)^{N_{\rm A}} \\ &\times \left(\frac{\gamma}{\overline{\gamma}_{\rm B}} \right)^{N_{\rm A} N_{\rm B}} + o\left(\overline{\gamma}_{\rm B}^{-N_{\rm A} N_{\rm B}} \right), \end{aligned} \quad (16)$$

where $o(\cdot)$ denotes the higher order terms, i.e., $f(x) = o(g(x))$ as $x \to x_0$ if $\lim_{x \to x_0} (f(x)/g(x)) = 0$. Substituting (16) and (4) into (9) and using [14, Eq. (3.326.2)], the asymptotic secrecy outage probability is derived as

$$P_{\rm out}^{\infty}(R_S) = (\Theta \overline{\gamma}_{\rm B})^{-\Delta} + o\left(\overline{\gamma}_{\rm B}^{-\Delta} \right), \quad (17)$$

where $\Delta = N_{\rm A} N_{\rm B}$ and Θ is given by

$$\begin{aligned} \Theta = &\frac{1}{2^{R_S}-1} \left(\sum_{i=1}^{b} \sum_{j=1}^{\beta_i} \sum_{k=0}^{j-1} \binom{N_{\rm B}}{k} \frac{(-1)^{N_{\rm B}-k+1} \varpi_{i,j}}{(N_{\rm B}-k)! k! \phi_i^{N_{\rm B}}} \right)^{-\frac{1}{N_{\rm B}}} \\ &\times \left(\sum_{l=0}^{\Delta} \delta(\Delta) \sum_{u=1}^{\epsilon} \sum_{v=1}^{\varepsilon_u} \frac{\Gamma(l+v)}{\Gamma(v)} \varpi_{u,v} \varphi_u^l \right)^{-\frac{1}{\Delta}}, \end{aligned} \quad (18)$$

[3] When $\overline{\gamma}_{\rm E} \to \infty$, the probability of successful eavesdropping will go to one. As such, we omit this case in this paper.

where $\delta(\Delta) = \binom{\Delta}{l}(2^{R_S}\overline{\gamma}_{\rm E}/(2^{R_S}-1))^l$. Based on (17), we confirm that the secrecy outage diversity order of $N_{\rm A}N_{\rm B}$ is achieved. It is evident that correlation has no impact of the secrecy outage diversity order but affects the secrecy outage array gain. By observing (18), we see that larger $\varpi_{i,j}$ and $\varpi_{u,v}$ lead to a lower Θ. This indicates that increasing antenna correlation will increases secrecy outage probability in the high SNR regime.

B. Special Correlation Models

Next we examine independent fading and two special correlation models: uniform and exponential correlation. The uniform correlation matrix is defined as $\mathbf{\Phi}_{\rm UNI} = [\rho^{\sigma}]$ where $\rho \in (0,1)$, $\sigma = 0$ if $i = j$ and $\sigma = 1$ otherwise. This model can provide suitable representations for closely spaced antennas on other than linear array configurations and for a trio of equidistant antennas forming an equilateral triangle in the space [15]. The exponential correlation matrix is defined as $\mathbf{\Phi}_{\rm EXP} = [\rho^{|i-j|}]$ and describes the scenario of reception from equi-spaced antennas [11]. Specifically, we characterize the performance gap between these cases as a simple ratio of their secrecy outage array gains.

1) Independent Fading: In this case, we have $b = 1$ with $\beta_i = N_{\rm B}$ for Bob and $\epsilon = 1$ with $\varepsilon_u = N_{\rm E}$ for Eve. We simplify $\varpi_{i,j}$ and $\varpi_{u,v}$ using [12, Eq. (23)] and then apply the simplified $\varpi_{i,j}$ and $\varpi_{u,v}$ into (13) and (17) to obtain the exact and asymptotic secrecy outage probability with independent fading, respectively. In this case, we note that the exact result with $N_{\rm A} = 1$ is equivalent to [5, Eq. (6)], the exact result with $N_{\rm A} = N_{\rm B} = 1$ is equivalent to [6, Eq. (10)], and the exact result with $N_{\rm B} = 1$ is equivalent to [7, Eq. (9)].

2) Uniform Correlation: In this special case, we have $\phi_1 = 1 + (N_{\rm B}-1)\rho_{\rm B}$ with $\beta_1 = 1$ and $\phi_2 = 1-\rho_{\rm B}$ with $\beta_2 = N_{\rm B}-1$ for Bob, and $\varphi_1 = 1+(N_{\rm E}-1)\rho_{\rm E}$ with $\varepsilon_1 = 1$ and $\varphi_2 = 1-\rho_{\rm E}$ with $\varepsilon_2 = N_{\rm E}-1$ for Eve, where $\rho_{\rm B}$ and $\rho_{\rm E}$ denote the correlation parameters of the main channel and the eavesdropper's channel, respectively. Substituting the simplified $\varpi_{i,j}$ and $\varpi_{u,v}$, given in [12, Eq. (22)], into (13) and (17), we obtain the exact and asymptotic secrecy outage probability with uniform correlation, respectively. The performance gap between uniform correlation and independent fading is characterized as

$$\frac{\Theta_{\rm UNI}}{\Theta_{\rm IND}} = \left(\frac{\sum_{l=0}^{\Delta}\delta(\Delta)\Gamma(l+N_{\rm E})}{(-1)^{\Delta+N_{\rm A}}\theta^{N_{\rm A}}\Gamma(N_{\rm E})\sum_{l=0}^{\Delta}\delta(\Delta)(\tau_1-\tau_2)}\right)^{\frac{1}{\Delta}}, \tag{19}$$

where $\Theta_{\rm UNI}$ and $\Theta_{\rm IND}$ denote the secrecy outage array gain of uniform correlation and independent fading, respectively, $\theta = (1/\phi_1(\phi_1-\phi_2)^{N_{\rm B}-1}) - \sum_{j=1}^{N_{\rm B}-1}\sum_{k=0}^{j-1}\binom{N_{\rm B}}{k}((-1)^k\phi_1^{N_{\rm B}-j-1}/\phi_2^{N_{\rm B}-1}(\phi_1-\phi_2)^{N_{\rm B}-j})$, $\tau_1 = (\Gamma(l+1)\varphi_1^{l+N_{\rm E}-1}/(\varphi_1-\varphi_2)^{N_{\rm E}-1})$, and $\tau_2 = \sum_{v=1}^{N_{\rm E}-1}(\Gamma(l+v)\varphi_1^{N_{\rm E}-v-1}\varphi_2^{l+1}/\Gamma(v)(\varphi_1-\varphi_2)^{N_{\rm E}-v})$.

3) Exponential Correlation: In this special case, we have $b = N_{\rm B}$ and $\beta_i = 1$ for Bob, and $\epsilon = N_{\rm E}$ and $\varepsilon_u = 1$ for Eve. Inserting the simplified $\varpi_{i,j}$ and $\varpi_{u,v}$, as given in [12, Eq. (20)], into (13) and (17), the exact and asymptotic secrecy outage probability with exponential correlation are obtained, respectively. The performance gap between exponential correlation and independent fading is characterized as

$$\frac{\Theta_{\rm EXP}}{\Theta_{\rm IND}} = \left(\frac{\left(\prod_{i=1}^{N_{\rm B}}\phi_i\right)^{N_{\rm A}}\sum_{l=0}^{\Delta}\delta(\Delta)\Gamma(l+N_{\rm E})}{\Gamma(N_{\rm E})\sum_{l=0}^{\Delta}\delta(\Delta)\Gamma(l+1)\sum_{u=1}^{N_{\rm E}}\chi}\right)^{\frac{1}{\Delta}}, \tag{20}$$

where $\Theta_{\rm EXP}$ denotes the secrecy outage array gain of exponential correlation and $\chi = \prod_{w=1,w\neq u}^{N_{\rm E}}(\varphi_u^{l+N_{\rm E}-1}/(\varphi_u-\varphi_w))$.

C. Impact of Full Correlation

We now consider the case where the $N_{\rm B}$ antennas and/or the $N_{\rm E}$ antennas at Eve are fully correlated, i.e., correlation matrices become rank-one and can be written as $\mathbf{\Phi}_{\rm B} = \mathbf{1}_{N_{\rm B}\times N_{\rm B}}$ and $\mathbf{\Phi}_{\rm E} = \mathbf{1}_{N_{\rm E}\times N_{\rm E}}$. The fully correlated case enables the examination of the effect of correlation on the secrecy performance at one extreme end (other being independent fading). Since we consider passive eavesdropping where the Eve's channel knowledge is not available at Alice, it is important for the system designers to understand the secrecy performance of the worst possible correlation scenario.

Using [16, Eq. (13)], the PDF of $\gamma_{\rm E}$ is given by

$$f_{\gamma_{\rm E_{FC}}}(\gamma) = \frac{e^{-\frac{\gamma}{N_{\rm E}\overline{\gamma}_{\rm E}}}}{N_{\rm E}\overline{\gamma}_{\rm E}}. \tag{21}$$

Correspondingly, the CDF of $\gamma_{\rm B}$ is given by

$$F_{\gamma_{\rm B_{FC}}}(\gamma) = 1 - \sum_{n=1}^{N_{\rm A}}\binom{N_{\rm A}}{n}(-1)^{n-1}e^{-\frac{n\gamma}{N_{\rm B}\overline{\gamma}_{\rm B}}}. \tag{22}$$

In the high SNR regime with $\overline{\gamma}_{\rm B_{FC}} \to \infty$, we express the first nonzero order expansion of $F_{\gamma_{\rm B_{FC}}}(\gamma)$ as

$$F^{\infty}_{\gamma_{\rm B_{FC}}}(\gamma) = \left(\frac{\gamma}{N_{\rm B}\overline{\gamma}_{\rm B}}\right)^{N_{\rm A}} + o\left(\overline{\gamma}_{\rm B}^{-N_{\rm A}}\right). \tag{23}$$

We next focus on three cases depending on fully correlation exists either at Bob or at Eve or at both, as follows:

Case 1) $N_{\rm E}$ *antennas are fully correlated*. We substitute (8) and (21) into (9) and derive the exact secrecy outage probability as

$$\begin{aligned} P_{\rm out}(R_S) = & 1 - \sum_{n=1}^{N_{\rm A}}\binom{N_{\rm A}}{n}(-1)^{n-1} \\ & \times \sum_{i=1}^{b}\sum_{j=1}^{\beta_i}\sum_{k=0}^{j-1}\sum_{S_m\in\mathcal{S}}\frac{n!}{\prod_{m=1}^{J}s_m!} \\ & \times \prod_{1\le m\le J}\left(\frac{\varpi_{i,j}}{k!(\phi_i\overline{\gamma}_{\rm B})^k}\right)^{s_m} e^{-\frac{s_m(2^{R_S}-1)}{\phi_i\overline{\gamma}_{\rm B}}} \\ & \times \sum_{q=0}^{ks_m}\binom{ks_m}{q}\frac{(2^{R_S}-1)^{ks_m-q}2^{R_S q}\Gamma(q+1)}{N_{\rm E}\overline{\gamma}_{\rm E}\left(\frac{2^{R_S}s_m}{\phi_i\overline{\gamma}_{\rm B}}+\frac{1}{N_{\rm E}\overline{\gamma}_{\rm E}}\right)^{q+1}}. \end{aligned} \tag{24}$$

As $\overline{\gamma}_{\rm B} \to \infty$, the asymptotic secrecy outage probability is derived as

$$P^{\infty}_{\rm out}(R_S) = (\Theta_1\overline{\gamma}_{\rm B})^{-\Delta_1} + o\left(\overline{\gamma}_{\rm B}^{-\Delta_1}\right), \tag{25}$$

where $\Delta_1 = N_{\rm A}N_{\rm B}$ and Θ is given by

$$\begin{aligned} \Theta_1 = & \frac{1}{2^{R_S}-1}\left(\sum_{i=1}^{b}\sum_{j=1}^{\beta_i}\sum_{k=0}^{j-1}\binom{N_{\rm B}}{k}\frac{(-1)^{N_{\rm B}-k+1}\varpi_{i,j}}{(N_{\rm B}-k)!k!\phi_i^{N_{\rm B}}}\right)^{-\frac{1}{N_{\rm B}}} \\ & \times \left(\sum_{l=0}^{\Delta_1}\delta(\Delta_1)\Gamma(l+1)N_{\rm E}^{l}\right)^{-\frac{1}{\Delta_1}}. \end{aligned} \tag{26}$$

Case 2) $N_{\rm B}$ *antennas are fully correlated*. We apply (4) and (22) into (9), which yields the exact secrecy outage probability as

$$P_{\rm out}(R_S) = 1 - \sum_{n=1}^{N_{\rm A}} \binom{N_{\rm A}}{n} (-1)^{n-1} e^{-\frac{n(2^{R_S}-1)}{N_{\rm B}\overline{\gamma}_{\rm B}}} \times \sum_{u=1}^{\epsilon} \sum_{v=1}^{\varepsilon_u} \frac{\varpi_{u,v}}{\left(\frac{2^{R_S} n \varphi_u \overline{\gamma}_{\rm E}}{N_{\rm B}\overline{\gamma}_{\rm B}} + 1\right)^v}. \quad (27)$$

When $\overline{\gamma}_{\rm B_{FC}} \to \infty$, we derive the asymptotic secrecy outage probability as

$$P_{\rm out}^{\infty}(R_S) = (\Theta_2 \overline{\gamma}_{\rm B})^{-\Delta_2} + o\left(\overline{\gamma}_{\rm B}^{-\Delta_2}\right), \quad (28)$$

where $\Delta_2 = N_{\rm A}$ and Θ_2 is given by

$$\Theta_2 = \frac{N_{\rm B}}{2^{R_S}-1} \left(\sum_{l=0}^{\Delta_2} \delta(\Delta_2) \sum_{u=1}^{\epsilon} \sum_{v=1}^{\varepsilon_u} \frac{\Gamma(l+v)}{\Gamma(v)} \varpi_{u,v} \varphi_u^l \right)^{-\frac{1}{\Delta_2}}. \quad (29)$$

Case 3) $N_{\rm B}$ *and* $N_{\rm E}$ *antennas are fully correlated*. We use (21) and (22) into (9) and obtain the exact secrecy outage probability as

$$P_{\rm out}(R_S) = 1 - \sum_{n=1}^{N_{\rm A}} \binom{N_{\rm A}}{n} \frac{(-1)^{n-1} e^{-\frac{n(2^{R_S}-1)}{N_{\rm B}\overline{\gamma}_{\rm B}}}}{\frac{2^{R_S} n N_{\rm E} \overline{\gamma}_{\rm E}}{N_{\rm B}\overline{\gamma}_{\rm B}} + 1}. \quad (30)$$

We then derive the asymptotic secrecy outage probability for $\overline{\gamma}_{\rm B_{FC}} \to \infty$ as

$$P_{\rm out}^{\infty}(R_S) = (\Theta_3 \overline{\gamma}_{\rm B})^{-\Delta_3} + o\left(\overline{\gamma}_{\rm B}^{-\Delta_3}\right), \quad (31)$$

where $\Delta_3 = N_{\rm A}$ and Θ_3 is given by

$$\Theta_3 = \frac{N_{\rm B}}{2^{R_S}-1} \left(\sum_{l=0}^{\Delta_3} \delta(\Delta_3) \Gamma(l+1) N_{\rm E}^l \right)^{-\frac{1}{\Delta_3}}. \quad (32)$$

Comparing (28) and (31) with (17), we see that for fully correlated $N_{\rm B}$ antennas, the secrecy outage diversity order reduces from $N_{\rm A}N_{\rm B}$ to $N_{\rm A}$. Indeed, Bob cannot exploit any diversity benefits of $N_{\rm B}$ antennas if they experience full correlation. Although not shown, the probability of positive secrecy for *Cases* 1, 2, and 3 can be easily derived by using $\Pr(C_S > 0) = 1 - P_{\rm out}(0)$, where $P_{\rm out}(0)$ is obtained by setting $R_S = 0$ in the expressions for the exact secrecy outage probability in (24), (27), and (30), respectively.

IV. Numerical Results

We present numerical results to examine the impact of antenna correlation on secrecy performance. Throughout this section, $\rho_{\rm B}$ denotes the correlation parameter of the main channel and $\rho_{\rm E}$ denotes the correlation parameter of the eavesdropper's channel. The exact curves in Figs. 1–3 precisely agree with the Monte Carlo simulation results, which validates the correctness of our analysis.

Fig. 1 plots the probability of positive secrecy versus $\overline{\gamma}_{\rm B}$. The exact curves are generated from (15). This figure highlights that correlation is beneficial to the secrecy performance when $\overline{\gamma}_{\rm B}$ is low. Specifically, as $\rho_{\rm B}$ increases, we observe an increase in $\Pr(C_S > 0)$ when $\overline{\gamma}_{\rm B} < -2$ dB. This observation is not surprising since antenna correlation reduces the effective dimensionality at Bob for low $\overline{\gamma}_{\rm B}$, which enables

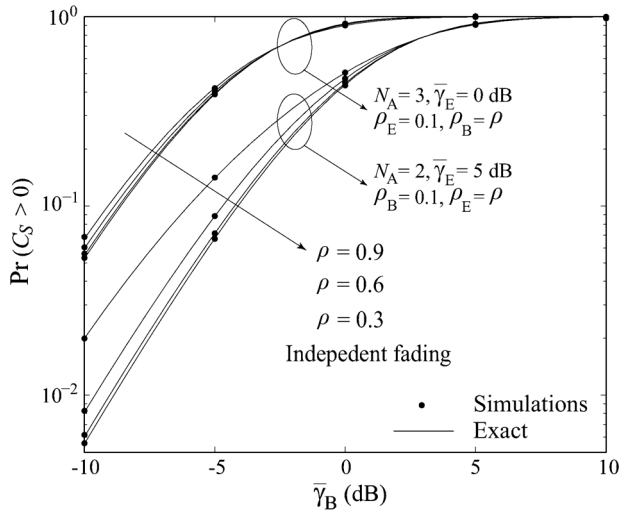

Fig. 1. Probability of positive secrecy for $N_{\rm B} = N_{\rm E} = 2$ with independent fading, uniform correlation with $\rho_{\rm B} = 0.1$ and $\rho_{\rm E} = \rho$ for $N_{\rm A} = 2$ and $\overline{\gamma}_{\rm E} = 5$ dB, and uniform correlation with $\rho_{\rm B} = \rho$ and $\rho_{\rm E} = 0.1$ for $N_{\rm A} = 3$ and $\overline{\gamma}_{\rm E} = 0$ dB.

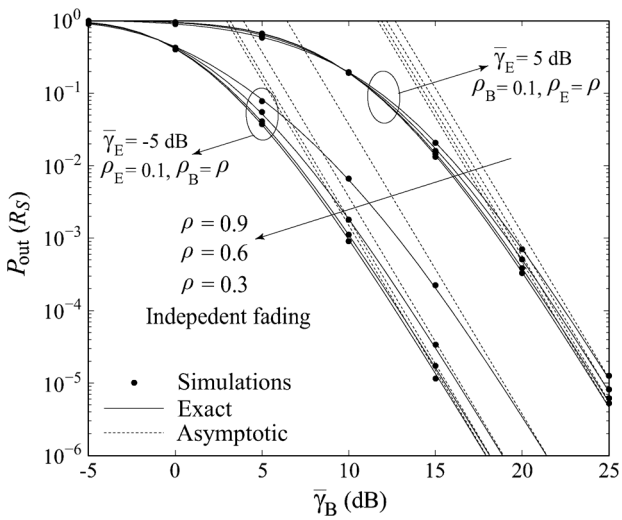

Fig. 2. Secrecy outage probability for $N_{\rm A} = N_{\rm B} = N_{\rm E} = 2$ and $R_S = 1$ with independent fading, exponential correlation with $\rho_{\rm B} = \rho$ and $\rho_{\rm E} = 0.1$ for $\overline{\gamma}_{\rm E} = -5$ dB, and exponential correlation with $\rho_{\rm B} = 0.1$ and $\rho_{\rm E} = \rho$ for $\overline{\gamma}_{\rm E} = 5$ dB.

power focusing. At low SNR, a similar observation for non secrecy MIMO relay systems was found in [17]. Moreover, we observe that $\Pr(C_S > 0)$ increases with increasing $\rho_{\rm E}$ when $\overline{\gamma}_{\rm B} < 3$ dB. In this regime, $\overline{\gamma}_{\rm E}$ is relatively high compared with $\overline{\gamma}_{\rm B}$ and effective dimensionality plays a dominant role at Eve. As such, correlation weakens the eavesdropper's channel quality and thus benefits the secrecy performance. Furthermore, we observe that the performance improvement brought by increasing $\rho_{\rm E}$ is higher than brought by increasing $\rho_{\rm B}$. In addition, we observe a profound improvement in $\Pr(C_S > 0)$ with increasing $N_{\rm A}$, which confirms the benefits of TAS in PHY layer security enhancement.

Fig. 2 plots the secrecy outage probability versus $\overline{\gamma}_{\rm B}$. The exact and asymptotic curves are generated from (13) and (17), respectively. It is evident that the secrecy outage diversity order is not affected by $\rho_{\rm B}$ or $\rho_{\rm E}$, as indicated by the parallel slopes of the asymptotes. This

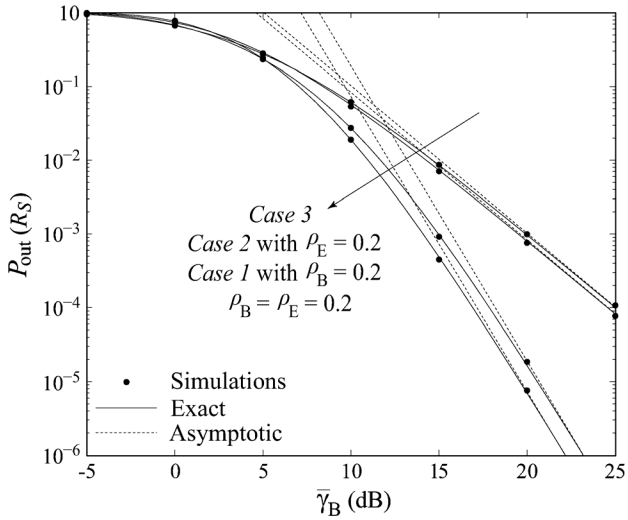

Fig. 3. Secrecy outage probability for $N_{\text{A}} = N_{\text{B}} = N_{\text{E}} = 2$, $\overline{\gamma}_{\text{E}} = 0$ dB, and $R_S = 1$ with exponential correlation with $\rho_{\text{B}} = \rho_{\text{E}} = 0.2$, *Case* 1 with fully correlated N_{E} antennas and $\rho_{\text{B}} = 0.2$, *Case* 2 with fully correlated N_{B} antennas and $\rho_{\text{E}} = 0.2$, and *Case* 3 with fully correlated N_{B} and N_{E} antennas.

figure demonstrates that correlation is detrimental to the secrecy performance when $\overline{\gamma}_{\text{B}}$ is at medium and high levels. In this regime (e.g., $\overline{\gamma}_{\text{B}} > -1$ dB for $\overline{\gamma}_{\text{B}} = -5$ dB and $\overline{\gamma}_{\text{B}} > 9$ dB for $\overline{\gamma}_{\text{B}} = 5$ dB), the secrecy outage probability increases as ρ_{B} or ρ_{E} increases. On one hand, higher ρ_{B} indicates the degraded quality of the main channel, which results in poorer secrecy performance. On the other hand, $\overline{\gamma}_{\text{E}}$ is relatively low compared with $\overline{\gamma}_{\text{B}}$. As such, higher ρ_{E} implies power focusing at Eve, which leads to improved eavesdropper's channel quality and weakening secrecy performance. Moreover, we observe that the performance degradation caused by increasing ρ_{B} is larger than brought by increasing ρ_{E}.

Fig. 3 plots the secrecy outage probability versus $\overline{\gamma}_{\text{B}}$. The exact curves for *Cases* 1, 2, and 3 are generated from (24), (27), and (30), respectively, and the asymptotic curves for *Cases* 1, 2, and 3 are generated from (25), (28), and (31), respectively. We first observe that when N_{B} antennas are fully correlated, e.g., *Cases* 2 and 3, the secrecy outage diversity order reduces from 4 to 2, as predicted by (28) and (31). Second, we observe that when $\overline{\gamma}_{\text{B}}$ is at medium and high levels, the secrecy outage probability achieved by exponential correlation with $\rho_{\text{B}} = \rho_{\text{E}} = 0.2$ is lower than that achieved by *Case* 1. Moreover, the secrecy outage probability achieved by *Case* 2 is lower than that achieved by *Case* 3. As explained previously, higher correlation at Eve degrades the secrecy performance for medium and high $\overline{\gamma}_{\text{B}}$.

V. Conclusions

In this paper, we analyzed the effects of antenna correlation on the secrecy performance of MIMO wiretap channels with transmit antenna selection at the transmitter and maximal-ratio combining at the receiver and the eavesdropper. New closed-form expressions were derived for the probability of positive secrecy, the exact secrecy outage probability, and the asymptotic secrecy outage probability. Some existing results for independent fading are included in our analysis as special cases. We showed that when the average SNR of the main channel is at low level, higher correlation at the eavesdropper offers more beneficial effects on secrecy than higher correlation at the receiver. When the average SNR of the main channel is at medium and high levels, higher correlation at the receiver exerts more detrimental effects on secrecy than higher correlation at the eavesdropper.

References

[1] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[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.*, accepted for publication.

[9] J. P. Kermoal, L. Schumacher, K. I. Pedersen, P. E. Mogensen, and F. Frederiksen, "A stochastic MIMO radio channel model with experimental validation," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 6, pp. 1211–1226, Aug. 2002.

[10] R. K. Mallik, "The uniform correlation matrix and its application to diversity," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1619–1625, May 2007.

[11] G. K. Karagiannidis, D. A. Zogas, and S. A. Kotsopoulos, "On the multivariate Nakagami- m distribution with exponential correlation," *IEEE Trans. Commun.*, vol. 51, no. 8, pp. 1240–1244, Aug. 2003.

[12] N. S. Ferdinand and N. Rajatheva, "Unified performance analysis of two-hop amplify-and-forward relay systems with antenna correlation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3002–3011, Sep. 2011.

[13] X. W. Cui and Z. M. Feng, "Lower capacity bound for MIMO correlated fading channels with keyhole," *IEEE Commun. Lett.*, vol. 8, no. 8, pp. 500–502, Aug. 2004.

[14] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA: Academic, 2007.

[15] M.-S. Alouini, A. Absi, and M. Kaveh, "Sum of Gamma variates and performance of wireless communication systems over Nakagami-fading channels," *IEEE Trans. Veh. Technol.*, vol. 50, no. 6, pp. 1471–1480, Nov. 2001.

[16] E. A. Jorswieck and A. Sezgin, "Impact of spatial correlation on the performance of orthogonal space-time block codes," *IEEE Commun. Lett.*, vol. 8, no. 1, pp. 21–23, Jan. 2004.

[17] R. H. Y. Louie, Y. Li, H. A. Suraweera, and B. Vucetic, "Performance analysis of beamforming in two hop amplify and forward relay networks with antenna correlation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 3131–3142, Jun. 2009.