On Secrecy of a Multi-Antenna System with Eavesdropper in Close Proximity

Wei Xu, *Senior Member, IEEE*, Zhangjie Peng, and Shi Jin, *Member, IEEE*

***Abstract*—This letter investigates secrecy performance of a wiretap channel where an eavesdropper is located in close proximity to legitimate receiver. In the system, both receivers equip multiple antennas and use maximal ratio combining (MRC) to harvest diversity gains. In order to analyze the impact of eavesdropping in close proximity, we derive closed-form expressions for the system performance in terms of both secrecy capacity and outage probability. Since the derived expressions involve infinite series sums, finite series approximations are then presented with guaranteed truncation error. Moreover, we also characterize the asymptotic behavior of secrecy outage. Some insightful observations are accordingly manifested with numerical verifications.**

***Index Terms*—Multi-antenna system, secrecy performance, outage probability.**

I. Introduction

With the development of decryption capabilities, traditional cryptographical techniques become more vulnerable and the key-based enciphering design faces new challenges [1]. Recently, physical layer secrecy emerges as a promising alternative ensuring secure communications without relying on assumptions of limited decryption power. The philosophy of physical layer security was presented in the landmark literature [2] for a wiretap channel from an information theoretical perspective. Therefore, analysis of the secrecy capacity has been an essential problem in physical layer security systems. In [3], secrecy capacity was characterized under a simple point-to-point system with eavesdropper, where each node is assumed to equip a single antenna. By deploying multiple antennas at transmitter, secrecy capacity was analyzed in [4]. In order to further disturb the eavesdropper using multi-antennas, artificial noise (AN) was introduced in [5] with secrecy enhancement. On the other hand, eavesdroppers can also benefit from multiple antennas, which makes the security issue more challenging [6].

The above studies investigated security system performance under uncorrelated scenarios, while correlation does exist in some scenarios. In [7], [8], the effect of spatial correlation within multi-antenna channels is analyzed in terms of secrecy outage. On the other hand, in some applications, eavesdropper is unknown and it possibly is located in close proximity to legitimate receiver, which may result in a correlation between the two channels from transmitter to legitmate receiver and to eavesdropper [9]. The impact of close eavesdropper on secrecy was asymptotically characterized in [9] for high signal-to-noise ratio (SNR), while an exact expression of secrecy capacity was later derived in [10]. Studies in [11][12] investigated the correlated secrecy system under log-normal fading channels, instead of the previously considered Rayleigh channels. In [13], a secure key generation method was developed for a correlated erasure channel. All studies [9]–[13] considered single-antenna nodes for ease of analytical tractability. In this work, we investigate the secrecy performance when a powerful multi-antenna eavesdropper is located in close proximity to a multi-antenna legitimate receiver. We derive closed-form expressions for the system performance in terms of both secrecy capacity and outage probability. Moreover, we analyze the truncation error of the derived expressions and present asymptotic outage analysis under high SNRs. The results allow us to extract engineering insights on the impacts of channel correlation and antenna setups on secure performance.

Manuscript received February 03, 2015; revised March 05, 2015; accepted March 05, 2015. Date of publication March 11, 2015; date of current version March 18, 2015. This work was supported by the NSFC under Grants 61471114 and 61222102, the 973 Program under 2013CB329204, and by the International Science & Technology Cooperation Program of China under Grant 2014DFT10300. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Chandra Murthy.

W. Xu, Z. Peng, and S. Jin are with the National Mobile Communications Research Lab., Southeast University, Nanjing 210096, China (e-mail: wxu@seu.edu.cn; pengzhangjie@seu.edu.cn; jinshi@seu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LSP.2015.2411612

II. System Model and Preliminaries

We consider a single-input multiple-output system with a multi-antenna eavesdropper (SIMOME), where the transmitter (namely Alice) equips a single antenna and both the legitimate receiver (Bob) and the eavesdropper (Eve), have M antennas on each node. Let $\mathbf{h}_b \in \mathbb{C}^{M\times 1}$ and $\mathbf{h}_e \in \mathbb{C}^{M\times 1}$ be channel vectors from Alice to Bob and to Eve, respectively. The received symbol vectors at Bob and Eve can respectively be expressed as

$$\mathbf{y}_b = \sqrt{P}\mathbf{h}_b s + \mathbf{z}_b, \qquad \mathbf{y}_e = \sqrt{P}\mathbf{h}_e s + \mathbf{z}_e \tag{1}$$

where s is the transmit symbol and P is the transmit power at Alice. Vectors $\mathbf{z}_b$ and $\mathbf{z}_e$ are zero-mean additive white Gaussian noise (AWGN) at Bob and Eve with variances 1 and σ_e^2, respectively. Given perfect channel state information (CSI) at receivers, both Bob and Eve are able to exploit the maximal ratio combining (MRC) for detection, which yields the detected symbols as follows

$$r_b = \sqrt{P}\|\mathbf{h}_b\|^2 s + \mathbf{h}_b^H \mathbf{z}_b, r_e = \sqrt{P}\|\mathbf{h}_e\|^2 s + \mathbf{h}_e^H \mathbf{z}_e \tag{2}$$

where $\|\cdot\|$ is the norm of the input vector. Accordingly, the received SNR at Bob and Eve are respectively calculated as

$$\gamma_b = P\|\mathbf{h}_b\|^2, \qquad \gamma_e = \frac{P}{\sigma_e^2}\|\mathbf{h}_e\|^2. \tag{3}$$

We consider in the following that both $\|\mathbf{h}_b\|^2$ and $\|\mathbf{h}_e\|^2$ are statistically chi-square distributed with different parameters, i.e., $\|\mathbf{h}_b\|^2 \sim c_b\chi^2_{2M}$ and $\|\mathbf{h}_e\|^2 \sim c_e\chi^2_{2M}$, where c_b and c_e are constant values depending on the spatial correlation statistics of $\mathbf{h}_b$ and $\mathbf{h}_e$, respectively. For uncorrelated channels in themselves, it is direct to know that $c_b = c_e = 1$ for standard Rayleigh fading.

While for spatially correlated channel vectors, it has been revealed in [14] that c_b and c_e can be chosen as constants averaging over non-zero eigenvalues of the corresponding spatial correlation matrices. In this way, the chi-square distributions well approximate the statistics of $\|\mathbf{h}_b\|^2$ and $\|\mathbf{h}_e\|^2$ for spatially correlated channels, which facilitates our following analysis. Accordingly, we have

$$\gamma_b = \mu_b q_b \triangleq \psi_b\left(q_b, q_e\right), \qquad \gamma_e = \mu_e q_e \triangleq \psi_e\left(q_b, q_e\right) \tag{4}$$

where $\mu_b = \frac{c_b P}{2}$, $\mu_e = \frac{c_e P}{2\delta_e^2}$, and q_b and q_e are χ^2_{2M}-distributed random variables. Consider channel correlation between $\mathbf{h}_b$ and $\mathbf{h}_e$ because Eve is in close proximity to Bob, which implies that γ_b and γ_e are two correlated random variables following chi-squared distribution. Let $\rho \in [0, 1)$ denote the correlation factor. From [15], the joint probability density function (PDF) of q_b and q_e is given by

$$g\left(q_b, q_e\right) = \sum_{j=0}^{\infty} a_j (q_b q_e)^{N_j} e^{-\frac{q_b+q_e}{2(1-\rho)}} \tag{5}$$

where $a_j = \frac{2^{-2(M+j)}\rho^j(1-\rho)^{-(M+2j)}}{\Gamma(M)\Gamma(N_j+1)\Gamma(j+1)}$ with $N_j = M + j - 1$. By applying the Jacobian transform and from (4), the joint PDF of γ_b and γ_e follows

$$\begin{aligned} f\left(\gamma_b, \gamma_e\right) &= g\left(\psi_b^{-1}\left(\gamma_b, \gamma_e\right), \psi_e^{-1}\left(\gamma_b, \gamma_e\right)\right) \left|\mathcal{J}\left(\gamma_b, \gamma_e\right)\right| \\ &= \sum_{j=0}^{\infty} \frac{a_j}{\mu_b \mu_e} \left(\frac{\gamma_b}{\mu_b}\frac{\gamma_e}{\mu_e}\right)^{N_j} e^{-\frac{\frac{\gamma_b}{\mu_b}+\frac{\gamma_e}{\mu_e}}{2(1-\rho)}} \end{aligned} \tag{6}$$

where $\mathcal{J}(\gamma_b, \gamma_e)$ is the Jacobian matrix, and the last equality holds for that $|\mathcal{J}(\gamma_b, \gamma_e)| = \frac{1}{\mu_b \mu_e}$.

III. Secrecy Performance Analysis

In this section, we will characterize the behavior of secrecy performance with respect to ρ in terms of both secrecy capacity and outage probability with closed-form expressions.

A. Average Secrecy Capacity

Start with the instantaneous secrecy capacity given by

$$C\left(\gamma_b, \gamma_e\right) = \left(\log_2\left(1+\gamma_b\right) - \log_2\left(1+\gamma_e\right)\right)^+ \tag{7}$$

where $(x)^+ = \max\{x, 0\}$. Using (6), the ergodic secrecy capacity can be calculated according to

$$\bar{C} = \int_0^{\infty}\int_0^{\infty} C\left(\gamma_b, \gamma_e\right) f\left(\gamma_b, \gamma_e\right) d\gamma_b d\gamma_e. \tag{8}$$

Lemma 1: For the SIMOME secrecy system with correlated Bob and Eve channels, the ergodic secrecy capacity is characterized by the closed-form expression in (9), shown at the bottom of the page, where $b_j = a_j\Gamma(N_j+1)[2(1-\rho)]^{N_j+1}$ and the function $F(\lambda, k, \mu)$ is defined as (10), shown at the bottom of the page, where $E_m(x) = \int_1^{\infty} e^{-xt}t^{-m}dt$ is the exponential integral function of order m.

Proof: Substitute $f(\gamma_b, \gamma_e)$ in (6) into (8). It yields

$$\begin{aligned} \bar{C} = &\underbrace{\int_0^{\infty} \log_2\left(1+\gamma_b\right)\left[\int_0^{\gamma_b} f\left(\gamma_b, \gamma_e\right) d\gamma_e\right] d\gamma_b}_{\Delta_1} \\ &- \underbrace{\int_0^{\infty} \log_2\left(1+\gamma_e\right)\left[\int_{\gamma_e}^{\infty} f\left(\gamma_b, \gamma_e\right) d\gamma_b\right] d\gamma_e}_{\Delta_2}. \end{aligned} \tag{11}$$

We then calculate Δ_1 and Δ_2 separately. The calculation of Δ_1 follows (12) at the bottom of the next page, where $\gamma(\cdot,\cdot)$ is the incomplete gamma function. Note that equalities (a) and (b) respectively utilize [16, Eq. (3.381.1)] and [16, Eq. (8.352.1)]. Equality (c) holds by using the integral in (10). The calculation of Δ_2 follows similar techniques. By applying some integral manipulations, we have (13), shown at the bottom of the next page. Now the proof completes by plugging (12) and (13) into (11). ■

Remark 1: The derived result retrieves [10], Proposition1] as a special case of *Lemma* 1 with $M = 1$. This is intuitively true because the secrecy system considered in this letter reduces to the scenario in [10] when both Alice and Bob are single-antenna terminals.

The above-derived expression for secrecy capacity involves calculation of infinite series. However, finite series are usually preferred for tractable simplicity. In the following we therefore evaluate the error caused by truncating the infinite series to finite series by summing over the first T terms. Accordingly, the truncation error, denoted by E_{c}, can be defined in (14), shown at the bottom of the next page. The behavior of E_{c} is characterized in the following proposition.

Proposition 1: With T terms used for capacity calculation in (9), the truncation error is strictly upper bounded by

$$E_{\mathrm{c}} < \frac{2M\mu_b}{\ln 2}(1-\rho)^{M+1}\rho^T\Omega_1 \triangleq \overline{E}_{\mathrm{c}} \tag{15}$$

where $\Omega_1 = \sum_{j=1}^{M+1} \frac{(T+M+1)!\rho^j}{(T+j)!(M+1-j)!(1-\rho)^j}$.

Proof: By dropping the last two negative sum terms in the square bracket of (14) and substituting (10) into the first sum term in (14), we can bound the truncation error as follows:

$$\begin{aligned} E_{\mathrm{c}} &< \frac{(1-\rho)^M}{\Gamma(M)\ln 2} e^{\frac{1}{2(1-\rho)\mu_b}} \sum_{j=T+1}^{\infty} \frac{\Gamma\left(N_j+1\right)\rho^j}{\Gamma\left(j+1\right)} \\ &\quad \times \sum_{m=1}^{N_j+1} E_m\left(\frac{1}{2\left(1-\rho\right)\mu_b}\right) \\ &< \frac{2\mu_b(1-\rho)^{M+1}}{\Gamma(M)\ln 2} \underbrace{\sum_{j=T+1}^{\infty} \frac{\Gamma\left(N_j+2\right)}{\Gamma\left(j+1\right)}\rho^j}_{S_0} \end{aligned} \tag{16}$$

$$\bar{C} = \sum_{j=0}^{\infty} \frac{b_j}{\ln 2}\left[\frac{F\left(1, N_j, \frac{1}{2(1-\rho)\mu_b}\right)}{\mu_b^{N_j+1}} - \sum_{k=0}^{N_j} \frac{F\left(1, N_j+k, \frac{1+\frac{\mu_b}{\mu_e}}{2(1-\rho)\mu_b}\right)}{2^k k!\mu_b^{N_j+1}\mu_e^k(1-\rho)^k} - \sum_{k=0}^{N_j} \frac{F\left(1, N_j+k, \frac{1+\frac{\mu_e}{\mu_b}}{2(1-\rho)\mu_e}\right)}{2^k k!\mu_e^{N_j+1}\mu_b^k(1-\rho)^k}\right] \tag{9}$$

$$F\left(\lambda, k, \upsilon\right) = \int_0^{\infty} \ln\left(1+\lambda x\right) e^{-\upsilon x} x^k dx = \frac{\Gamma\left(k+1\right)}{\upsilon^{k+1}e^{-\frac{\upsilon}{\lambda}}} \sum_{m=1}^{k+1} E_m\left(\frac{\upsilon}{\lambda}\right) \tag{10}$$

where the last inequality is obtained according to the fact $E_m(x) < E_1(x) < \frac{e^{-x}}{x}$. We then focus on evaluating S_0 in (16) by transforming the calculation of infinite series. The following calculates S_0 in a recursive manner. Define

$$S_i = \sum_{j=T+i+1}^{\infty} \frac{(M+j-i)!}{j!}\rho^j \tag{17}$$

for any nonnegative integer i which includes S_0 with $i = 0$ as defined in (16). With the definition in (17), by subtracting ρS_i from S_i and after some tedious manipulations, we get

$$(1-\rho)S_i = \frac{(M+T+1)!}{(T+i+1)!}\rho^{T+i+1} + (M-i)S_{i+1}. \tag{18}$$

Moreover from (17) with $i = M$, the definition gives

$$S_M = \sum_{j=T+M+1}^{\infty} \rho^j = \frac{1}{1-\rho}\rho^{T+M+1} \tag{19}$$

where the last equality holds because of the sum formula of an infinite geometric sequence and $0 \le \rho < 1$. Note that S_M in (19) is shown as a simple closed-form expression without sum calculation of any series. Subsequently, by substituting (19) in (18) with $i = M-1$, we can obtain a simplified expression of S_{M-1}, and by analogy obtain S_{M-2} and so forth to S_0. The procedure finally yields

$$S_0 = \sum_{j=1}^{M+1} \frac{M!(T+M+1)!\rho^{T+j}}{(T+j)!(M+1-j)!(1-\rho)^j} \tag{20}$$

which alternatively evaluates S_0 by summing finite terms. Using (20) in (16), we have the desired bound in (15). ∎

Remark 2: From *Proposition* 1, it is observed that the upper bounded truncation error, i.e., $\overline{E}_{\rm c}$, approaches zero when T tends to infinity with $0 \le \rho < 1$. The observation indicates that the sum of infinite series in (9) converges with bounded error.

B. Outage Probability

Outage probability of the secrecy system is defined as [17]

$$P(R) = \Pr\{C(\gamma_b, \gamma_e) < R\} = \Pr\left\{\frac{1+\gamma_b}{1+\gamma_e} < \xi\right\} \tag{21}$$

where $\Pr\{\cdot\}$ denotes the probability of an event, R is the required secrecy rate, and $\xi = 2^R$.

Lemma 2: For the SIMOME system, the outage probability at the desired secrecy rate R is given by (22), shown at the bottom of the page, where $\binom{k}{l} = k!/l!/(k-l)!$ is the binomial coefficient.

$$\begin{aligned}
\Delta_1 &= \sum_{j=0}^{\infty} a_j \int_0^{\infty} \log_2(1+\gamma_b) \frac{\gamma_b^{N_j}}{\mu_b^{N_j+1}} e^{-\frac{\gamma_b}{2(1-\rho)\mu_b}} \left(\int_0^{\gamma_b} \frac{\gamma_e^{N_j}}{\mu_e^{N_j+1}} e^{-\frac{\gamma_e}{2(1-\rho)\mu_e}} d\gamma_e \right) d\gamma_b \\
&\overset{(a)}{=} \sum_{j=0}^{\infty} a_j [2(1-\rho)]^{N_j+1} \int_0^{\infty} \log_2(1+\gamma_b) \frac{\gamma_b^{N_j}}{\mu_b^{N_j+1}} e^{-\frac{\gamma_b}{2(1-\rho)\mu_b}} \gamma\left(N_j+1, \frac{\gamma_b}{2(1-\rho)\mu_e}\right) d\gamma_b \\
&\overset{(b)}{=} \sum_{j=0}^{\infty} \frac{b_j}{\ln 2} \frac{\int_0^{\infty} \ln(1+\gamma_b) \gamma_b^{N_j} e^{-\frac{\gamma_b}{2(1-\rho)\mu_b}} d\gamma_b}{\mu_b^{N_j+1}} - \sum_{j=0}^{\infty} \frac{b_j}{\ln 2} \sum_{k=0}^{N_j} \frac{\int_0^{\infty} \ln(1+\gamma_b) \gamma_b^{N_j+k} e^{-\frac{1+\frac{\mu_b}{\mu_e}}{2(1-\rho)\mu_b}\gamma_b} d\gamma_b}{2^k k! \mu_b^{N_j+1} \mu_e^k (1-\rho)^k} \\
&\overset{(c)}{=} \sum_{j=0}^{\infty} \frac{b_j}{\ln 2} \left[\frac{1}{\mu_b^{N_j+1}} F\left(1, N_j, \frac{1}{2(1-\rho)\mu_b}\right) - \sum_{k=0}^{N_j} \frac{1}{2^k k! \mu_b^{N_j+1} \mu_e^k (1-\rho)^k} F\left(1, N_j+k, \frac{1+\frac{\mu_b}{\mu_e}}{2(1-\rho)\mu_b}\right) \right]
\end{aligned} \tag{12}$$

$$\Delta_2 = \sum_{j=0}^{\infty} \frac{b_j}{\ln 2} \sum_{k=0}^{N_j} \frac{F\left(1, N_j+k, \frac{1+\frac{\mu_e}{\mu_b}}{2(1-\rho)\mu_e}\right)}{2^k k! \mu_e^{N_j+1} \mu_b^k (1-\rho)^k}. \tag{13}$$

$$E_{\rm c} = \sum_{j=T+1}^{\infty} \frac{b_j}{\ln 2} \left[\frac{F\left(1, N_j, \frac{1}{2(1-\rho)\mu_b}\right)}{\mu_b^{N_j+1}} - \sum_{k=0}^{N_j} \frac{F\left(1, N_j+k, \frac{1+\frac{\mu_b}{\mu_e}}{2(1-\rho)\mu_b}\right)}{2^k k! \mu_b^{N_j+1} \mu_e^k (1-\rho)^k} - \sum_{k=0}^{N_j} \frac{F\left(1, N_j+k, \frac{1+\frac{\mu_e}{\mu_b}}{2(1-\rho)\mu_e}\right)}{2^k k! \mu_e^{N_j+1} \mu_b^k (1-\rho)^k} \right] \tag{14}$$

$$P(R) = 1 - \sum_{j=0}^{\infty} b_j e^{-\frac{2^R-1}{2(1-\rho)\mu_b}} \sum_{k=0}^{N_j} \left[\frac{2^R-1}{2(1-\rho)\mu_b}\right]^k \frac{1}{k!} \times \sum_{l=0}^{k} \binom{k}{l} (N_j+l)! \left(\frac{\mu_e 2^R}{2^R-1}\right)^l \left[\frac{2(1-\rho)\mu_b}{\mu_b+\mu_e 2^R}\right]^{N_j+l+1} \tag{22}$$

$$\begin{aligned}
\Pr\left\{\frac{1+\gamma_b}{1+\gamma_e} < \xi\right\} &= 1 - \sum_{j=0}^{\infty} a_j \int_0^{\infty} \frac{\gamma_e^{N_j}}{\mu_e^{N_j+1}} e^{-\frac{\gamma_e}{2(1-\rho)\mu_e}} \left(\int_{\xi(1+\gamma_e)-1}^{\infty} \frac{\gamma_b^{N_j}}{\mu_b^{N_j+1}} e^{-\frac{\gamma_b}{2(1-\rho)\mu_b}} d\gamma_b \right) d\gamma_e \\
&\overset{(a)}{=} 1 - \sum_{j=0}^{\infty} a_j [2(1-\rho)]^{N_j+1} \int_0^{\infty} \frac{\gamma_e^{N_j}}{\mu_e^{N_j+1}} e^{-\frac{\gamma_e}{2(1-\rho)\mu_e}} \Gamma\left(N_j+1, \frac{\xi(1+\gamma_e)-1}{2(1-\rho)\mu_b}\right) d\gamma_e \\
&\overset{(b)}{=} 1 - \sum_{j=0}^{\infty} b_j e^{-\frac{\xi-1}{2(1-\rho)\mu_b}} \sum_{k=0}^{N_j} \left[\frac{\xi-1}{2(1-\rho)\mu_b}\right]^k \frac{1}{k!} \sum_{l=0}^{k} \binom{k}{l} \left(\frac{\xi}{\xi-1}\right)^l \int_0^{\infty} \frac{\gamma_e^{N_j+l}}{\mu_e^{N_j+1}} e^{-\frac{\mu_b+\mu_e\xi}{2(1-\rho)\mu_b\mu_e}\gamma_e} d\gamma_e
\end{aligned} \tag{23}$$

Proof: Substituting (6) in (21), we have (23), shown at the bottom of the previous page. We use [16, Eq. (3.381.3)] to obtain (a), and equality (b) follows by first decomposing the incomplete gamma function $\Gamma(\cdot,\cdot)$ using [16, Eq. (8.352.2)] and then applying the binomial expansion theorem. Further integrate (23) with [16, Eq. (3.381.4)]. It gives (22) with $\xi = 2^R$. ∎

In the following proposition, we characterize the behavior of the truncation error for the outage result in (22). Similar observations can be concluded as that for *Proposition* 1.

Proposition 2: With T terms used for outage calculation, the truncation error $E_{\rm p}$ is strictly upper bounded by

$$E_{\rm p} < (1-\rho)^M \rho^T \Omega_2 \triangleq \overline{E}_{\rm p} \tag{24}$$

where $\Omega_2 = \sum_{j=1}^{M} \frac{(T+M)!}{(T+j)!(M-j)!} \frac{\rho^j}{(1-\rho)^j}$.

Proof: The proof first uses the inequality $\Gamma(n+1,x) < n!$ and then follows a similar philosophy as the proof in *Proposition* 1. Details are omitted for brevity. ∎

Note that this proposition on outage approximation with a finite series sum is useful for asymptotic analysis in the next subsection.

C. Large SNR Behavior

Considering Eve is located very closely to Bob, we assume $\mu_b = \mu_e \triangleq \mu$ in (22) and focus on the asymptotic behavior of secrecy outage under large SNR. Given an increasing SNR μ, it is reasonable to observe the outage $P(R)$ with a correspondingly growing $R = \alpha \log \mu$[18]. Moreover, since *Proposition* 2 validates the effectiveness of approximating (22) with a finite series sum, we can keep only the most dominant term while ignoring higher-order terms for $\mu \to \infty$. After some basic manipulations, we obtain

$$\lim_{\mu\to\infty} P(\alpha \log \mu) = 1 - \beta(1-\rho)^M \mu^{-\alpha M} \tag{25}$$

where $\beta = \sum_{k=0}^{M-1} \frac{\Gamma(M+k)}{\Gamma(M)\Gamma(k+1)}$.

Remark 3: From the asymptotic outage in (25), it reveals that the probability of reliable secure communication, defined by $1 - P(R)$ as in [18], decreases as expected for an increasing channel correlation between Bob and Eve. More specifically, the reliable secrecy probability is affected linearly with respect to the correlation by a multiplier factor of $(1-\rho)^M$. Moreover, regarding the affect of antenna number, it is interesting to find that the asymptotic outage probability grows with an increasing M. It implies that deployment of more antennas plays a more positive effect to Eve although both Bob and Eve can benefit from multi-antenna diversity gains. In order to maintain a security level against eavesdropping, Bob is expected to equip more antennas than Eve.

Different from conventional communication systems, the outage probability in (25) of the wiretap channel degrades if the desired secrecy rate $R = \alpha \log \mu$ increases with system SNR at a fixed α. In order to guarantee non-degraded outage with increasing SNR, the system can only achieve a slowly increasing secrecy rate by decreasing α with respect to μ. A proper choice of α can be easily obtained according to (25) by keeping the value of $\mu^{-\alpha M}$ invariant.

IV. Numerical Verifications

This section provides some numerical results to validate our derived expressions via Monte-Carlo simulations. Both Bob and Eve have the same SNR value, i.e., $\mu_b = \mu_e = \mu$. Fig. 1 shows that our derived theoretical expressions with respect to both capacity and outage perfectly match the numerical results. Note that T terms are considered for calculating the theoretical expressions and the value of T is obtained according to the obtained *Propositions* with bounded truncation errors $\overline{E}_{\rm c} = 10^{-3}$ and $\overline{E}_{\rm p} = 10^{-3}$. For the special case of $\rho = 0$, it is obvious that $T = 0$. While for other cases like $\rho = 0.2$, (15) yields the smallest value of $T = 9$ to ensure the required truncation error. From the comparison result, it shows that the correlation ρ, as expected, imposes a negative impact to the secrecy performance. Moreover, our asymptotic analysis is validated in Fig. 2. The asymptotic outage in (25) accurately presents the high SNR outage under different tested cases. By properly choosing α according to (25), the system is able to achieve a non-degraded outage performance with both growing SNR and outage rate R.

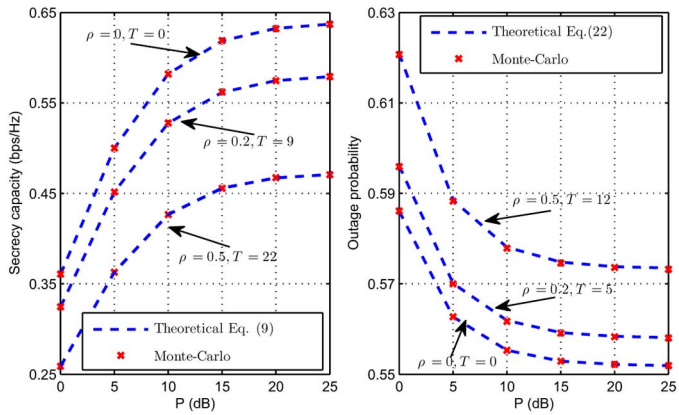

Fig. 1. Secrecy performance verifications under $M = 2$ and $R = 0.2$.

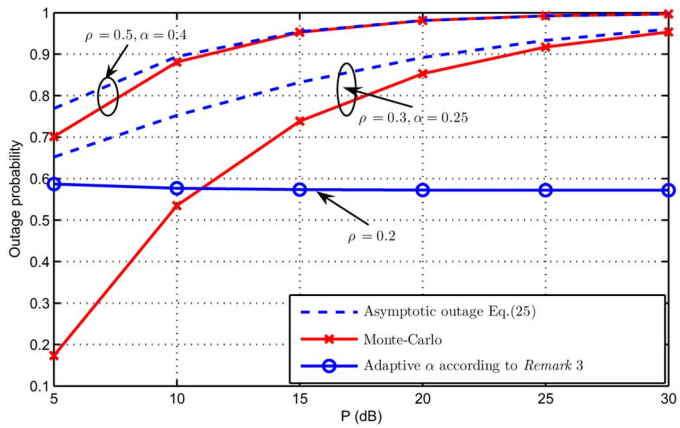

Fig. 2. Asymptotic large SNR outage under $M = 2$.

V. Conclusions

This letter investigates the secure performance for an SIMOME system where the legitimate and eavesdropping nodes are in close proximity. We derive the expressions for both secrecy capacity and outage probability, as well as characterizing truncation errors for evaluating the derived expressions. Impacts of the correlation and antenna number on the outage performance are revealed via asymptotic analysis.

REFERENCES

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.

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

[3] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[4] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[6] K. Cumanan and Z. Ding *et al.*, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

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

[8] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing Security in Correlated Channel With Maximal Ratio Combining Diversity," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6745–6751, Dec. 2012.

[9] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 4005–4019, Apr. 2011.

[10] X. Sun, J. Wang, W. Xu, and C. Zhao, "Performance of secure communications over correlated fading channels," *IEEE Signal Process. Lett.*, vol. 19, no. 8, pp. 479–482, Aug. 2012.

[11] M. Z. I. Sarkar and T. Ratnarajah, "Secrecy capacity over correlated log-normal fading channel," in *in Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 883–887.

[12] X. Liu, "Outage probability of secrecy capacity over correlated log-normal fading channels," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 289–292, Feb. 2013.

[13] Y. S. Khiabani and S. Wei, "ARQ-based symmetric-key generation over correlated erasure channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 7, pp. 1152–1161, Jul. 2013.

[14] K.-H. Yuan and P. M. Bentler, "Two simple approximations to the distributions of quadratic forms," *Brit. J. Math. Statist. Psychol.*, vol. 63, no. 2, pp. 273–291, 2010.

[15] R. F. Gunst and J. T. Webster, "Density functions of the bivariate chi-square distribution," *J. Statist. Comput. Simul.*, pp. 275–288, 1973.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.

[17] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

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