ISBN 978-981-14-1455-8
Proceedings of 2019 the 9th International Workshop on Computer Science and Engineering
WCSE_2019_SPRING
Yangon, Myanmar, February 27-March 1, 2019, pp. 118-125
doi:10.18178/wcse.2019.03.021

Towards the Secrecy Outage Probability of Transmit-Receive Diversity Systems in the Presence of Multiantenna Eavesdroppers

Piriya Wangnilrat+ and Kiattisak Maichalernnukul

College of Digital Innovation and Information Technology, Rangsit University, Thailand

Abstract. We analyze the information-theoretic security of transmit-receive diversity systems in the presence of multiantenna eavesdroppers. Specifically, exact and asymptotic closed-form expressions are derived for the secrecy outage probability of such systems in a Rayleigh fading environment. Based on the latter expression, the corresponding secrecy diversity order and secrecy array gain are determined. Numerical results are presented to verify the analytical results and to investigate the impact of various system parameters, including the antenna configuration and the number of eavesdroppers.

Keywords: multiple-input multiple-output, transmit-receive diversity, secrecy outage probability.

1. Introduction

Since the 1990s, the use of multiple antennas in wireless communication systems has attracted great attention in both industry and academia [1], [2]. The multiple antennas in multiple-input multiple-output (MIMO) systems can be exploited in various ways to obtain diversity, array gains, or even multiplexing. For instance, diversity can be realized by employing space-time codes without transmit channel knowledge [3], [4], or alternatively by transmit beamforming and receive combining when the channel state information is available at the transmitter [5], [6]. Compared to space-time coding, transmit beamforming and receive combining achieve an array gain. In the sequel, a MIMO system with transmit beamforming and receive combining is referred to as "transmit-receive diversity system" [6].

More recently, a large amount of effort has been devoted to exploring the information-theoretic security issues in MIMO wireless communications [7]–[10]. The key performance measures of transmit-receive diversity systems, e.g., their error probability, outage and ergodic capacity, have been extensively studied in the literature [5], [6], [11], [12]. Nevertheless, little is known about the secrecy performance of these systems in the presence of multiantenna eavesdroppers.[1] In this paper, we derive exact and asymptotic expressions for the secrecy outage probability in such MIMO wiretap channels with Rayleigh fading, and quantify the achievable secrecy diversity order and secrecy array gain.

We adopt the following notation. $\frac{\mathrm{d}}{\mathrm{d}x}(\cdot)$ and $\mathrm{E}[\cdot]$ denote the first derivative operator with respect to variable x and the expectation operator, respectively. $\binom{\cdot}{\cdot}$ denotes the multinomial coefficient. $\Upsilon(\cdot,\ \cdot)$ and $\log(\cdot)$ denote the lower incomplete gamma function defined in [15, Equation (8.350.1)] and the natural logarithm, respectively. We write a function $g(x)$ of x as $o(x)$ if $\lim_{x\to 0}\frac{g(x)}{x} = 0$. $\|\cdot\|$ denotes the Euclidean norm of a vector. $[\cdot]_{ij}$, $(\cdot)^{\dagger}$, and $\det(\cdot)$ denote the (i,j)-th element, conjugate transpose, and determinant of a matrix, respectively. $\mathbf{I}_N$ is the identity matrix of size $N \times N$. $\mathcal{CN}(\mathbf{0},\mathbf{K})$ denotes a zero-mean circularly-

+ Corresponding author. Tel.: +66897607058.
E-mail address: piriya.w57@rsu.ac.th.

[1] To the best of our knowledge, the related secrecy analysis appears only in [13], [14] where a single-eavesdropper scenario is considered.

symmetric complex Gaussian distribution with covariance $\mathbf{K}$, $\mathcal{L}_{\max}\{\cdot\}$ denotes the largest eigenvalue of a square matrix, and $P\{\cdot\}$ denotes the corresponding eigenvector.

2. System Model

A transmit-receive diversity system which consists of a transmitter with M_{t} antennas, a legitimate receiver with M_{r} antennas, and N passive eavesdroppers, each of which has M_{e} antennas is considered. After matched filtering and sampling at the symbol interval, the received signal vectors at the receiver and i-th eavesdropper ($i = 1, 2, \ldots, N$) are given by

$$\mathbf{y}_{\mathrm{r}} = \mathbf{H}_{\mathrm{r}}\mathbf{w}_{\mathrm{t}}s + \mathbf{n}_{\mathrm{r}}$$

and

$$\mathbf{y}_{\mathrm{e},i} = \mathbf{H}_{\mathrm{e},i}\mathbf{w}_{\mathrm{t}}s + \mathbf{n}_{\mathrm{e},i}$$

respectively, where s is the transmitted symbol with $\mathrm{E}[|s|^2] \le P$, $\mathbf{w}_{\mathrm{t}}$ is the $M_{\mathrm{t}} \times 1$ transmit beamforming vector, $\mathbf{H}_{\mathrm{r}}$ and $\mathbf{H}_{\mathrm{e},i}$ are respectively the $M_{\mathrm{r}} \times M_{\mathrm{t}}$ and $M_{\mathrm{e}} \times M_{\mathrm{t}}$ complex channel matrices, and $\mathbf{n}_{\mathrm{r}} \sim \mathcal{CN}(\mathbf{0}, \sigma_{\mathrm{r}}^2\mathbf{I}_{M_{\mathrm{r}}})$ and $\mathbf{n}_{\mathrm{e},i} \sim \mathcal{CN}(\mathbf{0}, \sigma_{\mathrm{e}}^2\mathbf{I}_{M_{\mathrm{e}}})$ are the noise vectors. In our work, we focus on an ensemble corresponding to Rayleigh fading in which $\mathbf{H}_{\mathrm{r}}$ and $\mathbf{H}_{\mathrm{e},i}$ are independent, and each has independent identically-distributed $\mathcal{CN}(0,1)$ entries. Moreover, we assume that all terminals know $\mathbf{H}_{\mathrm{r}}$, but $\mathbf{H}_{\mathrm{e},i}$ is available only at the i-th eavesdropper.

In order for the legitimate receiver to estimate the transmitted symbol s, the receive combining vector $\mathbf{z}_{\mathrm{r}}$ is applied to the received signal vector $\mathbf{y}_{\mathrm{r}}$. The estimate of the symbol is given by

$$\mathbf{z}_{\mathrm{r}}^{\dagger}\mathbf{y}_{\mathrm{r}} = \mathbf{z}_{\mathrm{r}}^{\dagger}\mathbf{H}_{\mathrm{r}}\mathbf{w}_{\mathrm{t}}s + \mathbf{z}_{\mathrm{r}}^{\dagger}\mathbf{n}_{\mathrm{r}}\ .$$

To maximize the SNR of this estimate, the transmit beamforming and receive combining vectors are chosen as [5], [6]

$$\mathbf{w}_{\mathrm{t}} = \frac{\mathbf{H}_{\mathrm{r}}^{\dagger}\mathbf{z}_{\mathrm{r}}}{\left\|\mathbf{H}_{\mathrm{r}}^{\dagger}\mathbf{z}_{\mathrm{r}}\right\|}$$

and

$$\mathbf{z}_{\mathrm{r}} = P\{\mathbf{H}_{\mathrm{r}}\mathbf{H}_{\mathrm{r}}^{\dagger}\}$$

respectively. The resulting SNR is

$$\gamma_{\mathrm{r}} = \bar{\gamma}_{\mathrm{r}}\mathcal{L}_{\max}\{\mathbf{H}_{\mathrm{r}}\mathbf{H}_{\mathrm{r}}^{\dagger}\} \tag{1}$$

where $\bar{\gamma}_{\mathrm{r}} = \frac{P}{\sigma_{\mathrm{r}}^2}$ is the average SNR at the receiver for the case of $M_{\mathrm{t}} = M_{\mathrm{r}} = 1$. Similarly, the estimate of the symbol s at the i-th eavesdropper ($i = 1, 2, \ldots, N$) is given by

$$\mathbf{z}_{\mathrm{e},i}^{\dagger}\mathbf{y}_{\mathrm{e},i} = \mathbf{z}_{\mathrm{e},i}^{\dagger}\mathbf{H}_{\mathrm{e},i}\mathbf{w}_{\mathrm{t}}s + \mathbf{z}_{\mathrm{e},i}^{\dagger}\mathbf{n}_{\mathrm{e},i}$$

where the receive combining vector

$$\mathbf{z}_{\mathrm{e},i} = \frac{\mathbf{H}_{\mathrm{e},i}\mathbf{w}_{\mathrm{t}}}{\left\|\mathbf{H}_{\mathrm{e},i}\mathbf{w}_{\mathrm{t}}\right\|}$$

is optimal in yielding the maximum SNR, i.e.,

$$\gamma_{\mathrm{e},i} = \bar{\gamma}_{\mathrm{e}}\left\|\mathbf{H}_{\mathrm{e},i}\mathbf{w}_{\mathrm{t}}\right\|^2 \tag{2}$$

where $\bar{\gamma}_{\mathrm{e}} = \frac{P}{\sigma_{\mathrm{e}}^2}$ is the average SNR at each eavesdropper for the case of $M_{\mathrm{t}} = M_{\mathrm{e}} = 1$.

Let $\lambda = \mathcal{L}_{\max}\{\mathbf{H}_{\mathrm{r}}\mathbf{H}_{\mathrm{r}}^{\dagger}\}$, $L = \min(M_{\mathrm{t}}, M_{\mathrm{r}})$, and $K = \max(M_{\mathrm{t}}, M_{\mathrm{r}})$. The cumulative distribution function (CDF) of λ is given by [6]

$$F_{\lambda}(x) = \frac{\det(\mathbf{S}(x))}{\left[\prod_{p=1}^{L}(K-p)!\,(L-p)!\right]} \tag{3}$$

where $\mathbf{S}(x)$ is the $L \times L$ Hankel matrix with

$$[\mathbf{S}(x)]_{ij} = \Upsilon(K - L + i + j - 1, x)\,.$$

By careful inspection of the entries of $\mathbf{S}(x)$, this CDF can be rewritten as

$$F_{\lambda}(x) = \sum_{m=1}^{L} \sum_{n=K-L}^{(K+L-2m)m} \frac{a_{m,n}}{n!} \Upsilon(n+1, mx) \tag{4}$$

where $a_{m,n} = \frac{c_{m,n} n!}{m^{n+1}[\prod_{p=1}^{L}(K-p)!(L-p)!]}$ and $c_{m,n}$ is the coefficient calculated from employing curve fitting on the plot of $\frac{\mathrm{d}}{\mathrm{d}x}\det(\mathbf{S}(x))$ [6]. Using (4) and [16, Example 5-1], the CDF of γ_{r} is given by

$$F_{\gamma_{\mathrm{r}}}(x) = \sum_{m=1}^{L} \sum_{n=K-L}^{(K+L-2m)m} \frac{a_{m,n}}{n!} \Upsilon\left(n+1, \frac{mx}{\bar{\gamma}_{\mathrm{r}}}\right). \tag{5}$$

Let $\beta_i = \left\|\mathbf{H}_{\mathrm{e},i}\mathbf{w}_{\mathrm{t}}\right\|^2$ where $i = 1, 2, \dots, N$. Using the result of [17, Section 7.1], it can be shown that $\mathbf{H}_{\mathrm{e},i}\mathbf{w}_{\mathrm{t}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{M_{\mathrm{e}}})$. Since the squared norm of a vector of M_{e} complex Gaussians has a chi-squared probability density function (PDF) with $2M_{\mathrm{e}}$ degrees of freedom [18, Chapter 1], we have

$$f_{\beta_i}(x) = \frac{x^{M_{\mathrm{e}}-1} e^{-x}}{(M_{\mathrm{e}} - 1)!}\,. \tag{6}$$

Using (6) and [16, Equation (5-6)], the PDF and CDF of $\gamma_{\mathrm{e},i}$ are given by

$$f_{\gamma_{\mathrm{e},i}}(x) = \frac{x^{M_{\mathrm{e}}-1} e^{-\frac{x}{\bar{\gamma}_{\mathrm{e}}}}}{(M_{\mathrm{e}} - 1)!\, \bar{\gamma}_{\mathrm{e}}^{M_{\mathrm{e}}}} \tag{7}$$

and

$$F_{\gamma_{\mathrm{e},i}}(x) = \frac{\Upsilon\left(M_{\mathrm{e}}, \frac{x}{\bar{\gamma}_{\mathrm{e}}}\right)}{(M_{\mathrm{e}} - 1)!} \tag{8}$$

respectively. Letting $\gamma_{\mathrm{e,max}} = \max(\gamma_{\mathrm{e},1}, \gamma_{\mathrm{e},2}, \dots, \gamma_{\mathrm{e},N})$ and using (7), (8) and [19, Equation (2.1.6)], we get

$$f_{\gamma_{\mathrm{e,max}}}(x) = \frac{N x^{M_{\mathrm{e}}-1} e^{-\frac{x}{\bar{\gamma}_{\mathrm{e}}}} \left[\Upsilon\left(M_{\mathrm{e}}, \frac{x}{\bar{\gamma}_{\mathrm{e}}}\right)\right]^{N-1}}{[(M_{\mathrm{e}} - 1)!]^N \bar{\gamma}_{\mathrm{e}}^{M_{\mathrm{e}}}}\,. \tag{9}$$

Hence, the instantaneous secrecy capacity of the considered system is given by [20, Lemma 1]

$$C_{\mathrm{s}} = \begin{cases} \log(1 + \gamma_{\mathrm{r}}) - \log(1 + \gamma_{\mathrm{e,max}}), & \text{if } \gamma_{\mathrm{r}} > \gamma_{\mathrm{e,max}} \\ 0, & \text{if } \gamma_{\mathrm{r}} \le \gamma_{\mathrm{e,max}}\,. \end{cases}$$

3. Exact Secrecy Outage Probability

The secrecy outage probability is defined as the probability that the instantaneous secrecy capacity is less than a target secrecy rate $R > 0$ [20]. Mathematically, this performance metric is given by

$$\begin{aligned} P_{\mathrm{out}}(R) &= \Pr\{C_{\mathrm{s}} < R\} \\ &= \Pr\{\gamma_{\mathrm{r}} < e^R \gamma_{\mathrm{e,max}} + e^R - 1\} \\ &= \int_0^{\infty} f_{\gamma_{\mathrm{e,max}}}(v) F_{\gamma_{\mathrm{r}}}(e^R v + e^R - 1)\, \mathrm{d}v\,. \end{aligned} \tag{10}$$

From (5), (9), and (10), we can derive the exact secrecy outage probability as follows:

$$P_{\mathrm{out}}(R) = \frac{N}{[(M_{\mathrm{e}} - 1)!]^N \bar{\gamma}_{\mathrm{e}}^{M_{\mathrm{e}}}} \sum_{m=1}^{L} \sum_{n=K-L}^{(K+L-2m)m} \frac{a_{m,n}}{n!}$$

$$\times \int_0^{\infty} v^{M_e-1} e^{-\frac{v}{\bar{\gamma}_e}} \Upsilon\left(n+1, \frac{m(e^R v + e^R - 1)}{\bar{\gamma}_r}\right)\left[\Upsilon\left(M_e, \frac{v}{\bar{\gamma}_e}\right)\right]^{N-1} \mathrm{d}v$$

$$= \frac{N}{[(M_e-1)!]^N \bar{\gamma}_e^{M_e}} \sum_{m=1}^{L} \sum_{n=K-L}^{(K+L-2m)m} a_{m,n} \left[\int_0^{\infty} v^{M_e-1} e^{-\frac{v}{\bar{\gamma}_e}} \left[\Upsilon\left(M_e, \frac{v}{\bar{\gamma}_e}\right)\right]^{N-1} \mathrm{d}v\right.$$

$$\left. - e^{-\frac{m(e^R-1)}{\bar{\gamma}_r}} \sum_{k=0}^{n} \left(\frac{m}{\bar{\gamma}_r}\right)^k \sum_{l=0}^{k} \frac{e^{lR}(e^R-1)^{k-l}}{l!\,(k-l)!} \int_0^{\infty} v^{l+M_e-1} e^{-\left(\frac{me^R}{\bar{\gamma}_r}+\frac{1}{\bar{\gamma}_e}\right)v} \left[\Upsilon\left(M_e, \frac{v}{\bar{\gamma}_e}\right)\right]^{N-1} \mathrm{d}v\right]$$

$$= 1 - \frac{N}{[(M_e-1)!]^N \bar{\gamma}_e^{M_e}} \sum_{m=1}^{L} \sum_{n=K-L}^{(K+L-2m)m} a_{m,n} e^{-\frac{m(e^R-1)}{\bar{\gamma}_r}} \sum_{k=0}^{n} \left(\frac{m}{\bar{\gamma}_r}\right)^k \sum_{l=0}^{k} \frac{e^{lR}(e^R-1)^{k-l}}{l!\,(k-l)!}$$

$$\times \int_0^{\infty} v^{l+M_e-1} e^{-\left(\frac{me^R}{\bar{\gamma}_r}+\frac{1}{\bar{\gamma}_e}\right)v} \left[\Upsilon\left(M_e, \frac{v}{\bar{\gamma}_e}\right)\right]^{N-1} \mathrm{d}v$$

$$= 1 - \frac{N}{(M_e-1)!\,\bar{\gamma}_e^{M_e}} \sum_{m=1}^{L} \sum_{n=K-L}^{(K+L-2m)m} a_{m,n} e^{-\frac{m(e^R-1)}{\bar{\gamma}_r}} \sum_{k=0}^{n} \left(\frac{m}{\bar{\gamma}_r}\right)^k \sum_{l=0}^{k} \frac{e^{lR}(e^R-1)^{k-l}}{l!\,(k-l)!} \sum_{r=0}^{N-1} \binom{N-1}{r} (-1)^r$$

$$\times \sum_{j_1+j_2+\ldots+j_{M_e}=r} \binom{r}{j_1, j_2, \ldots, j_{M_e}} \frac{\left(l+\sum_{q=1}^{M_e}(q-1)j_q + M_e - 1\right)!}{\prod_{q=1}^{M_e}[(q-1)!]^{j_q}\, \bar{\gamma}_e^{\sum_{q=1}^{M_e}(q-1)j_q}} \left(\frac{me^R}{\bar{\gamma}_r} + \frac{r+1}{\bar{\gamma}_e}\right)^{-l-\sum_{q=1}^{M_e}(q-1)j_q - M_e} \quad (11)$$

where the second equality is obtained by using [15, Equation (8.352.1)] and [21, Section 24.1.2], the third equality is obtained by using [11, Equation (11)] and [15, Equation (8.356.4)], and the last equality is obtained by using [15, Equations (3.351.3) and (8.352.1)] and [21, Section 24.1.2]. In the case of $N = 1$, the secrecy outage probability expression in (11) reduces to

$$P_{\mathrm{out}}(R) = 1 - \frac{1}{(M_e-1)!\,\bar{\gamma}_e^{M_e}} \sum_{m=1}^{L} \sum_{n=K-L}^{(K+L-2m)m} a_{m,n} e^{-\frac{m(e^R-1)}{\bar{\gamma}_r}} \sum_{k=0}^{n} \left(\frac{m}{\bar{\gamma}_r}\right)^k \times \sum_{l=0}^{k} \frac{(l+M_e-1)!\, e^{lR}(e^R-1)^{k-l}}{l!\,(k-l)!} \left(\frac{me^R}{\bar{\gamma}_r} + \frac{1}{\bar{\gamma}_e}\right)^{-l-M_e}. \quad (12)$$

4. Asymptotic Secrecy Outage Probability

We proceed to derive the asymptotic secrecy outage probability of the aforementioned system as $\bar{\gamma}_r \to \infty$. This expression enables one to analyze the secrecy performance in the high SNR regime through two performance indicators: secrecy diversity order and secrecy array gain [10].

First, we look for a first-order expansion of (3), which will be immediate from a first-order expansion of $\det(\mathbf{S}(x))$. Following the approach outlined in [12, Appendix B.7], it is straightforward to show that the first-order Taylor expansion of $\det(\mathbf{S}(x))$ around $x = 0$ is

$$\det(\mathbf{S}(x)) = \left[\prod_{p=1}^{L} \frac{(K-p)!\,[(L-p)!]^2}{(K+L-p)!}\right] x^{KL} + o(x^{KL}). \quad (13)$$

Substituting (13) into (3) yields

$$F_{\lambda}(x) = \left[\prod_{p=1}^{L} \frac{(L-p)!}{(K+L-p)!}\right] x^{KL} + o(x^{KL}). \quad (14)$$

Using (14) and [16, Example 5-1], the first-order expansion of the CDF of γ_r is given by

$$F_{\gamma_{\rm r}}(x) = \left[\prod_{p=1}^{L}\frac{(L-p)!}{(K+L-p)!}\right]\frac{x^{KL}}{\bar{\gamma}_{\rm r}{}^{KL}} + o\left(\frac{x^{KL}}{\bar{\gamma}_{\rm r}{}^{KL}}\right). \tag{15}$$

Using (9), (10), and (15), and following the same procedure as in (11), an asymptotic expression for $P_{\rm out}(R)$ with $\bar{\gamma}_{\rm r} \to \infty$ is obtained as

$$P_{\rm out}^{\infty}(R) = (G_{\rm a}\bar{\gamma}_{\rm r})^{-G_{\rm d}} + o\left(\bar{\gamma}_{\rm r}{}^{-G_{\rm d}}\right) \tag{16}$$

where the secrecy diversity gain is

$$G_{\rm d} = KL \tag{17}$$

and the secrecy array gain is

$$G_{\rm a} = \left[\left[\prod_{p=1}^{L}\frac{(L-p)!}{(K+L-p)!}\right]\frac{N}{(M_{\rm e}-1)!}\sum_{n=0}^{KL}\binom{KL}{n}e^{nR}(e^{R}-1)^{KL-n}\bar{\gamma}_{\rm e}{}^{n}\sum_{r=0}^{N-1}\binom{N-1}{r}(-1)^{r}\right.$$
$$\left.\times\sum_{j_1+j_2+\ldots+j_{M_{\rm e}}=r}\binom{r}{j_1,j_2,\ldots,j_{M_{\rm e}}}\frac{\left(n+\sum_{q=1}^{M_{\rm e}}(q-1)j_q+M_{\rm e}-1\right)!}{\prod_{q=1}^{M_{\rm e}}[(q-1)!]^{j_q}\,(r+1)^{n+\sum_{q=1}^{M_{\rm e}}(q-1)j_q+M_{\rm e}}}\right]^{-\frac{1}{KL}}. \tag{18}$$

Recall that $L = \min(M_{\rm t}, M_{\rm r})$ and $K = \max(M_{\rm t}, M_{\rm r})$. It is clear from (17) that the secrecy diversity order is dependent on $M_{\rm t}$ and $M_{\rm r}$ and independent of $M_{\rm e}$ and N. It can also be seen from (18) that the eavesdropper channels have an adverse impact on the secrecy array gain. Accordingly, increasing the number of eavesdroppers or the number of antennas at each eavesdropper lessens the secrecy array gain, thereby rising the secrecy outage probability.

5. Numerical Results and Concluding Remarks

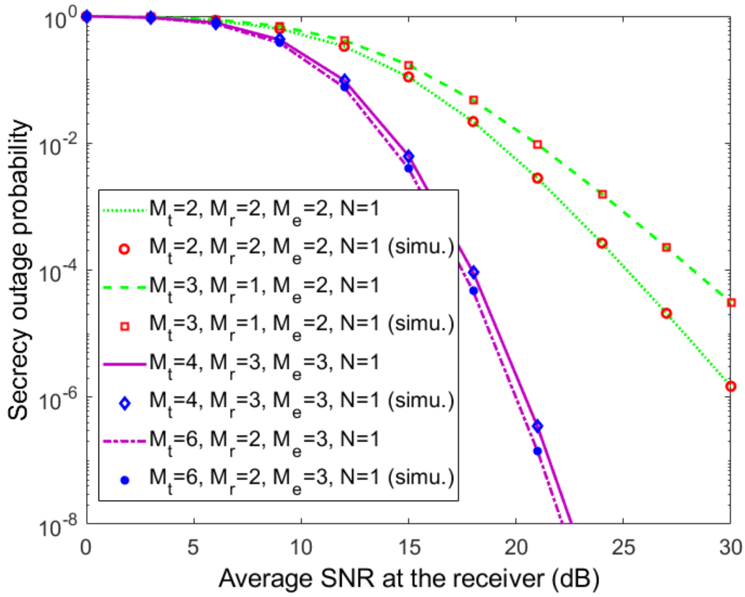

Fig. 1: Secrecy outage probability versus $\bar{\gamma}_{\rm r}$ for $N = 1$.

In this section, we validate the preceding theoretical analysis and investigate the effect of the various system parameters. Recall that $\bar{\gamma}_{\rm r}$ and $\bar{\gamma}_{\rm e}$ are the average SNRs at the legitimate receiver and passive eavesdroppers, respectively. We set $\bar{\gamma}_{\rm e} = 10$ dB and $R = \log(2)$ nats/s/Hz (i.e., 1 bit/s/Hz). Figs. 1 and 2 show the theoretical secrecy outage probability of transmit-receive diversity systems against $\bar{\gamma}_{\rm r}$ for $N = 1$ and $N = 4$ (computed with (12) and (11)), respectively. For comparison, the simulated secrecy outage curves are also plotted and labeled with "(simu.)". From both figures, we can see that the theoretical results

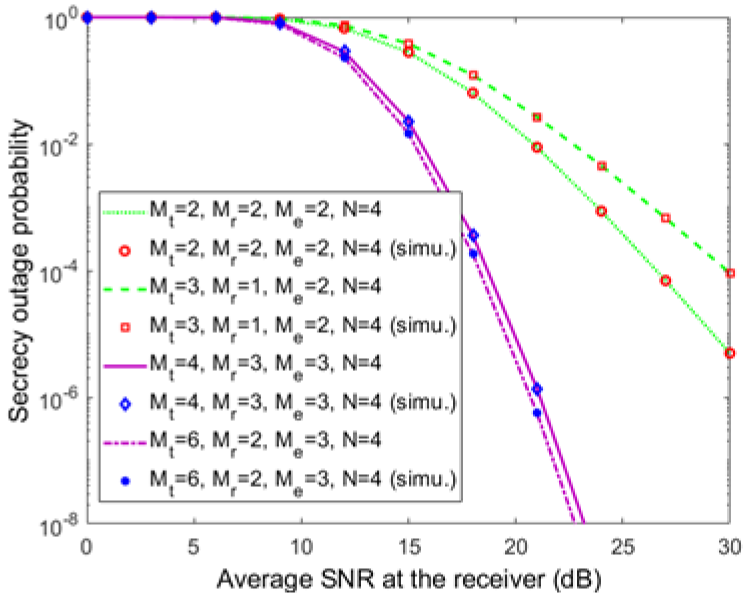

Fig. 2: Secrecy outage probability versus $\bar{\gamma}_{\mathrm{r}}$ for $N = 4$.

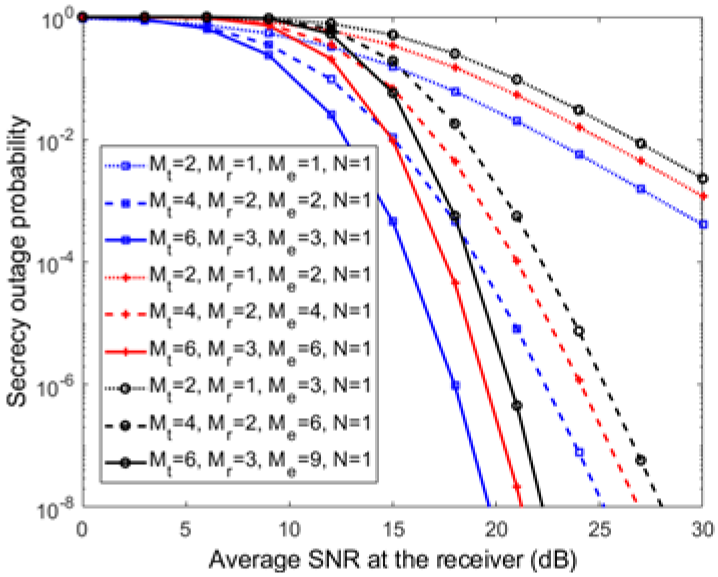

Fig. 3: Secrecy outage probability for different combinations of M_{t}, M_{r}, and M_{e}.

perfectly match their simulation counterparts. For a given $\bar{\gamma}_{\mathrm{r}}$, when $M_{\mathrm{t}} + M_{\mathrm{r}} = 4$ and $M_{\mathrm{e}} = 2$, the secrecy outage probability with $M_{\mathrm{t}} = 2$ and $M_{\mathrm{r}} = 2$ is lower than that with $M_{\mathrm{t}} = 3$ and $M_{\mathrm{r}} = 1$. This is consistent with the fact that for a fixed total number of antennas at the transmitter and legitimate receiver $(M_{\mathrm{t}} + M_{\mathrm{r}})$, a more-balanced antenna configuration provides a larger diversity gain [6], [11]. Specifically, from (17), we have $G_{\mathrm{d}} = 4$ for $M_{\mathrm{t}} = 2$ and $M_{\mathrm{r}} = 2$, and $G_{\mathrm{d}} = 3$ for $M_{\mathrm{t}} = 3$ and $M_{\mathrm{r}} = 1$. However, when $M_{\mathrm{t}} M_{\mathrm{r}} = 12$ and $M_{\mathrm{e}} = 3$, the secrecy outage probability with $M_{\mathrm{t}} = 4$ and $M_{\mathrm{r}} = 3$ is higher than that with $M_{\mathrm{t}} = 6$ and $M_{\mathrm{r}} = 2$. The reason is that for the same product of M_{t} and M_{r}, an increase in $M_{\mathrm{t}} + M_{\mathrm{r}}$ yields a performance enhancement [6].

Fig. 3 depicts the theoretical secrecy outage probability for different combinations of M_{t}, M_{r}, and M_{e}. We can see that for a given $\bar{\gamma}_{\mathrm{r}}$, the secrecy outage probability with $(M_{\mathrm{t}}, M_{\mathrm{r}}, M_{\mathrm{e}}) = (2, 1, 1)$ is higher than that with $(M_{\mathrm{t}}, M_{\mathrm{r}}, M_{\mathrm{e}}) = (4, 2, 2)$. Meanwhile, the secrecy outage probability with $(M_{\mathrm{t}}, M_{\mathrm{r}}, M_{\mathrm{e}}) = (4, 2, 2)$ is higher than that with $(M_{\mathrm{t}}, M_{\mathrm{r}}, M_{\mathrm{e}}) = (6, 3, 3)$. Similar performance trends can be observed when $(M_{\mathrm{t}}, M_{\mathrm{r}}, M_{\mathrm{e}})$ goes from $(2, 1, 2)$ to $(6, 3, 6)$ or from $(2, 1, 3)$ to $(6, 3, 9)$. These results reveal that increasing M_{t} and M_{r} proportionally to M_{e} is advantageous.

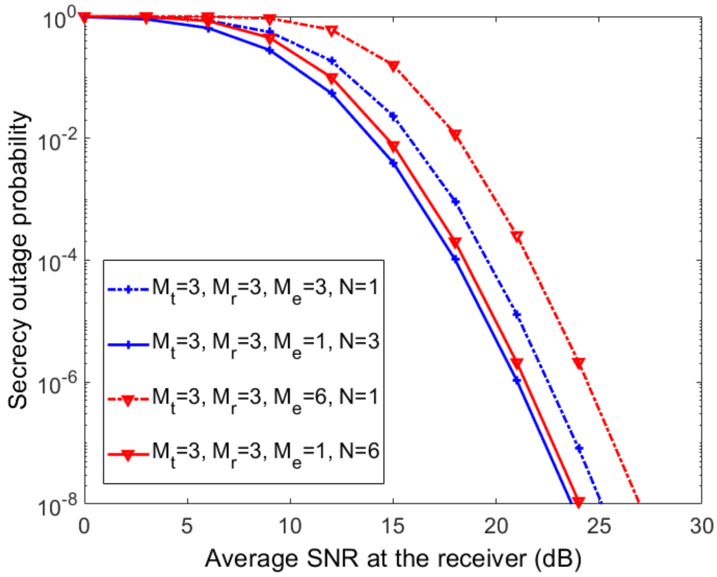

Fig. 4: Tradeoff between M_e and N.

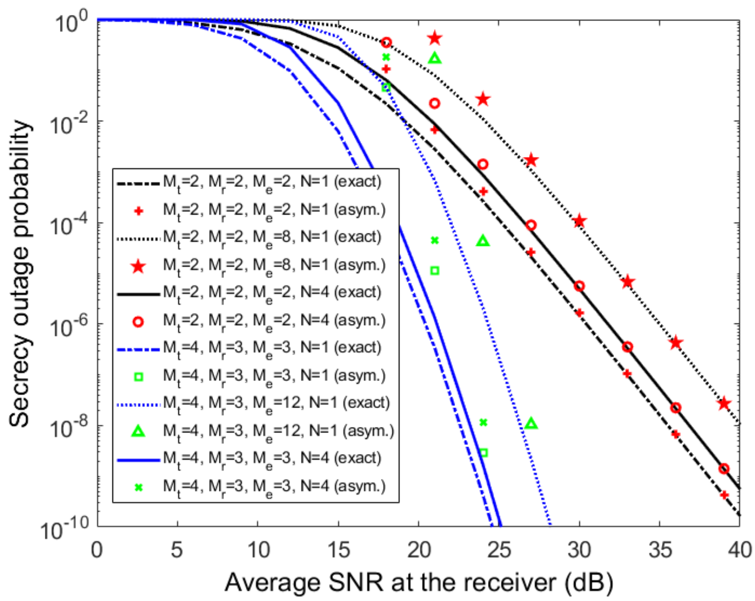

Fig. 5: Comparison of exact and asymptotic secrecy outage probability.

More insight into the effect of the number of eavesdroppers and that of the number of eavesdropping antennas is gained by varying the two numbers while keeping their product fixed, e.g., by varying N and M_e while $NM_e = 3, 6$ as illustrated in Fig. 4. Obviously, increasing the number of eavesdropping antennas causes more severe performance degradation than increasing the number of eavesdroppers.

Fig. 5 verifies the asymptotic secrecy outage probability derived in (16)-(18) at a fixed $\bar{\gamma}_e$ (i.e., $\bar{\gamma}_e = 10$ dB). The exact and asymptotic secrecy outage curves are labeled with "(exact)" and "(asym.)", respectively. As $\bar{\gamma}_r$ grows, the asymptotic curves approach the exact ones for different values of M_t, M_r, M_e, and N. It can also be observed that the secrecy diversity gain is KL, as predicted by (17), and the secrecy array gain diminishes with increasing M_e and N, as predicted by (18).

6. References

[1] A. Paulraj, R. Nabar, and D. Gore. *Introduction to Space-Time Wireless Communications*. Cambridge, UK: Cambridge University Press, 2003.

[2] J. Mietzner, R. Schober, L. Lampe, W. H. Gerstacker, and P. A. Hoeher. Multiple-antenna techniques for wireless communications - A comprehensive literature survey. *IEEE Commun. Surv. Tutor.* 2009, **11** (2): 87–105.

[3] S. M. Alamouti. A simple transmit diversity technique for wireless communications. *IEEE J. Sel. Areas Commun.* 1998, **16** (8): 1451–1458.

[4] V. Tarokh, N. Seshadri, and A. R. Calderbank. Space-time codes for high data rate wireless communication: Performance criterion and code construction. *IEEE Trans. Inf. Theory*. 1998, **44** (2): 744–765.

[5] T. K. Y. Lo. Maximum ratio transmission. *IEEE Trans. Commun.* 1999, **47** (10): 1458–1461.

[6] P. A. Dighe, R. K. Mallik, and S. S. Jamuar. Analysis of transmit-receive diversity in Rayleigh fading. *IEEE Trans. Commun.* 2003, **51** (4): 694–703.

[7] R. Bustin, R. Liu, H. V. Poor, and S. Shamai. An MMSE Approach to the Secrecy Capacity of the MIMO Gaussian Wiretap Channel, In: *Proc. of 2009 IEEE International Symposium on Information Theory*. 2009, pp. 2602–2606.

[8] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel. *IEEE Trans. Inf. Theory*. 2010, **56** (11): 5515–5532.

[9] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theory*. 2011, **57** (8): 4961–4972.

[10] 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.* 2013, **61** (1): 144–154.

[11] A. Maaref and S. Aissa. Closed-form expressions for the outage and ergodic Shannon capacity of MIMO MRC systems. *IEEE Trans. Commun.* 2005, **53** (7): 1092–1095.

[12] M. R. McKay. *Random Matrix Theory Analysis of Multiple Antenna Communication Systems*. University of Sydney, Australia, 2006.

[13] K. Maichalernnukul. Secrecy Capacity Analysis of Transmit-Receive Diversity Systems. In: *Proc. of 2018 IEEE Statistical Signal Processing Workshop (SSP)*. 2018, pp. 159–163.

[14] M. L. Ammari and P. Fortier. Physical layer security of multiple-input–multiple-output systems with transmit beamforming in Rayleigh fading. *IET Commun.* 2015, **9** (8): 1096–1103.

[15] I. S. Gradshteyn, I. M. Ryzhik, and A. Jeffrey. *Table of Integrals, Series, and Products*. 7th ed. New York: Academic Press, 2007.

[16] A. Papoulis and S. U. Pillai. *Probability, Random Variables, and Stochastic Processes*. 4th ed. New York: McGraw-Hill, 2002.

[17] C. H. Gierull. Statistical analysis of the eigenvector projection method for adaptive spatial filtering of interference. *IEE Proc. - Radar Sonar Navig.* 1997, **144** (2): 57–63.

[18] M. K. Simon. *Probability Distributions Involving Gaussian Random Variables: A Handbook for Engineers and Scientists.* New York: Springer, 2006.

[19] H. A. David and H. N. Nagaraja. *Order Statistics.* 3rd ed. New Jersey: John Wiley & Sons, 2003.

[20] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic security. *IEEE Trans. Inf. Theory*. 2008, **54** (6): 2515–2534.

[21] M. Abramowitz and I. A. Stegun. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover Press, 1970.