PeerJ Computer Science

On the secrecy performance of transmit-receive diversity and spatial multiplexing systems

Kiattisak Maichalernnukul

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

ABSTRACT

Emerging from the information-theoretic characterization of secrecy, physical-layer security exploits the physical properties of the wireless channel for security purpose. In recent years, a great deal of attention has been paid to investigating the physical-layer security issues in multiple-input multiple-output (MIMO) wireless communications. This paper analyzes the secrecy performance of transmit-receive diversity system and spatial multiplexing systems with zero-forcing equalization and minimum mean-square-error equalization. Specifically, exact and asymptotic closed-form expressions are derived for the secrecy outage probability of such MIMO systems in a Rayleigh fading environment, and the corresponding secrecy diversity orders and secrecy array gains are determined. Numerical results are presented to corroborate the analytical results and to examine the impact of various system parameters, including the numbers of antennas at the transmitter, the legitimate receiver, and the eavesdropper. These contributions bring about valuable insights into the physical-layer security in MIMO wireless systems.

Subjects Computer Networks and Communications, Security and Privacy

Keywords Physical-layer security, Secrecy outage probability, Transmit-receive diversity, Multiple-Input Multiple-Output, Spatial multiplexing

Submitted 7 December 2018
Accepted 13 March 2019
Published 22 April 2019

Corresponding author
Kiattisak Maichalernnukul,
kiattisak.m@rsu.ac.th

Academic editor
Shlomi Dolev

Additional Information and Declarations can be found on page 18

DOI **10.7717/peerj-cs.186**

Copyright
2019 Maichalernnukul

Distributed under
Creative Commons CC-BY 4.0

OPEN ACCESS

INTRODUCTION

Wireless communication systems are intrinsically prone to eavesdropping because of the open nature of the wireless medium. In this context, physical-layer security arising from the information-theoretic analysis of secrecy has attracted a lot of interest so far. This approach indeed takes advantage of the physical characteristics of the radio channel to support secure communications. Groundbreaking works on physical-layer security (*Wyner, 1975*; *Csiszár & Körner, 1978*; *Leung-Yan-Cheong & Hellman, 1978*; *Bloch et al., 2008*) focused on a basic wiretap channel, where the transmitter, the legitimate receiver, and the eavesdropper possess a single antenna, and established the so-called secrecy capacity. One of their common remarks was that to have a positive secrecy capacity, the channel quality of the transmitter–receiver link has to be better than that of the transmitter-eavesdropper link.

Stimulated by advances in multiple-antenna technology for wireless communications, the physical-layer security issues in multiple-input multiple-output (MIMO) wiretap

channels[1] have been recently explored in the literature (*Goel & Negi, 2008*; *Khisti & Wornell, 2010*; *Oggier & Hassibi, 2011*; *Mukherjee & Swindlehurst, 2011*; *Yang et al., 2013*; *Ferdinand, Da Costa & Latva-aho, 2013*; *Lin, Tsai & Lin, 2014*; *Wang, Wang & Ng, 2015*; *Schaefer & Loyka, 2015*; *Wang et al., 2016b*; *Maichalernnukul, 2018*). A brief overview of these works is provided in the following subsection.

[1] In our context, a MIMO wiretap channel implies that there are multiple antennas at the transmitter, the legitimate receiver, and the eavesdropper. This is generally known as co-located MIMO. For a discussion on its alternative, called distributed or cooperative MIMO, readers are referred to (*Dong et al., 2010*; *He, Man & Wang, 2011*; *Zou, Wang & Shen, 2013*; *Wang et al., 2016a*).

Related works

In *Khisti & Wornell (2010)*, a closed-form expression for the secrecy capacity of the Gaussian MIMO wiretap channel was derived from solving a minimax problem. Meanwhile, the problem of computing the perfect secrecy capacity of such a channel was analytically investigated in *Oggier & Hassibi (2011)*. By relaxing the assumption of perfect channel state information (CSI) used in *Khisti & Wornell (2010)*, *Oggier & Hassibi (2011)*, *Schaefer & Loyka (2015)* studied the secrecy capacity of the compound Gaussian MIMO wiretap channel. In *Mukherjee & Swindlehurst (2011)*, a few beamforming schemes were proposed to improve the secrecy capacity of the Gaussian MIMO wiretap channel in the presence of CSI errors. With the objective of achieving perfect secrecy at the physical layer, MIMO precoding and postcoding designs using the signal-to-noise ratio (SNR) criterion were presented in *Lin, Tsai & Lin (2014)*.

In all aforementioned works, the channel was assumed to be fixed over the whole transmission time. More precisely, the channel gains for the Gaussian MIMO wiretap channel are constant. This is rarely practical for the wireless medium as multipath propagation normally makes transmission conditions vary with time (*Poor & Schaefer, 2017*). Such variation is called fading. In (*Yang et al., 2013*; *Ferdinand, Da Costa & Latva-aho, 2013*; *Maichalernnukul, 2018*), the secrecy capacity of the fading MIMO wiretap channel[2] was characterized. Specifically, *Yang et al. (2013)* focused on the physical-layer security enhancement through transmit antenna selection in a flat-fading MIMO channel, and characterized the corresponding performance in terms of the secrecy outage probability and the probability of non-zero secrecy capacity. In the meantime, *Ferdinand, Da Costa & Latva-aho (2013)* analyzed the secrecy outage probability of orthogonal space–time block code (OSTBC) MIMO systems when the transmitter–receiver and transmitter-eavesdropper links experience different kinds of fading. In contrast to space–time coding (which is based on transmit diversity), transmit beamforming and receive combining (which is based on transmit-receive diversity) achieve additional array gain (*Tse & Viswanath, 2005*). Besides, *Goel & Negi (2008)* showed that multiple transmit antennas can be deployed to generate artificial noise, such that only the transmitter-eavesdropper link is degraded. This idea enables secret communication (*Csiszár & Körner, 1978*) and has been extended to more practical MIMO scenarios, e.g., frequency-division duplex systems (*Wang, Wang & Ng, 2015*) and heterogeneous cellular networks (*Wang et al., 2016b*).

[2] For this kind of channel, the channel gains are allowed to change from channel use to channel use (*Poor & Schaefer, 2017*).

More recently, in *Maichalernnukul (2018)*, the average secrecy capacity of transmit-receive diversity systems in the fading MIMO wiretap channel and its upper bound were derived in closed form. Nevertheless, the corresponding secrecy outage probability has not been investigated yet. There are two reasons why we should study this performance. First,

the closed-form results of *Maichalernnukul (2018)* are complicated, and from these results, it is not clear how the system parameters (e.g., the numbers of antennas at the transmitter, the legitimate receiver, and the eavesdropper) affect the secrecy performance. In fact, quantifying the secrecy outage probability at high SNR in terms of two parameters, namely secrecy diversity order and secrecy array gain, can provide insights into this effect (*Yang et al., 2013*). Second, it was shown in *Bashar, Ding & Li (2011)* that although transmit beamforming in the transmit-receive diversity systems maximizes the achievable capacity of the main channel (i.e., that for the transmitter–receiver link), they still have secrecy outages at an arbitrary target secrecy rate. The first objective of our work is to present the exact and asymptotic (high-SNR) analysis of the secrecy outage probability of these systems.

It is well known that the multiple antennas of MIMO systems can be exploited to obtain spatial multiplexing, i.e., transmission of independent data streams in parallel (*Tse & Viswanath, 2005*). This leads to an increase in the data rate. While several key performance metrics of spatial multiplexing MIMO systems, e.g., error probability, outage and ergodic capacity, have been extensively studied in the literature (*Chen & Wang, 2007*; *Smith, 2007*; *Ordóñez et al., 2007*; *Kumar, Caire & Moustakas, 2009*; *Jiang, Varanasi & Li, 2011*), little is known about the secrecy performance of these systems in the fading MIMO wiretap channel. The second objective of our work is to fill this knowledge gap by providing a relevant secrecy outage probability characterization.

Contributions

The main contributions of this work are summarized as follows:

- We derive exact and asymptotic closed-form expressions for the secrecy outage probability of a transmit-receive diversity system in the fading MIMO wiretap channel. We also do the same for the secrecy outage probability of spatial multiplexing systems with linear equalization, especially zero-forcing (ZF) and minimum mean-square-error (MMSE).[3] It is shown that all exact secrecy outage results simplify to the well-known result (*Bloch et al., 2008*, Equation (9)) for the case where the transmitter, the legitimate receiver, and the eavesdropper have a single antenna.
- We determine the secrecy diversity order and secrecy array gain that the above systems achieve, and discuss the impact of the numbers of antennas at the transmitter, the legitimate receiver, and the eavesdropper, denoted as M_t, M_r, and M_e, respectively, on the system secrecy and complexity. Through numerical results, it is verified that the transmit-receive diversity system attains a secrecy diversity order of M_tM_r, while the spatial multiplexing systems with ZF equalization and MMSE equalization yield the same secrecy diversity order of $M_r - M_t + 1$. All of these secrecy diversity orders turn out to be independent of M_e.

Notation and organization

Throughout this paper, we write a function $g(x)$ of variable x as $o(x)$ if $\lim_{x\to 0}\frac{g(x)}{x} = 0$, and denote $\binom{\cdot}{\cdot}$ as the multinomial coefficient, $\mathbb{E}[\cdot]$ as the expectation operator, $\frac{\mathrm{d}}{\mathrm{d}x}(\cdot)$ as the first derivative operator with respect to variable x, $\|\cdot\|$ as the Euclidean norm of a vector, and $\mathbf{I}_N$ as the identity matrix of size $N \times N$. Moreover, $\det(\cdot)$, $(\cdot)^{\mathrm{T}}$, $(\cdot)^{\dagger}$, $(\cdot)^{-1}$, and $[\cdot]_{ij}$

[3] The rationale for using these "classical" detection techniques for the spatial multiplexing MIMO systems is twofold. First, the ZF and MMSE detectors are the basic building blocks of advanced MIMO communication architectures (e.g., layered space–time architectures (*Foschini, 1996*; *Seethaler, Artés & Hlawatsch, 2004*) and joint transmit-receive equalizers (*Palomar & Lagunas, 2003*; *Jiang, Li & Hager, 2005*)), and have been extensively addressed in the MIMO literature (*Jankiraman, 2004*; *Biglieri et al., 2007*; *Heath Jr & Lozano, 2018*). Second, they have low computational complexity compared to the (optimum) maximum likelihood (ML) detector, and their performance can be very close to the ML performance for a well-conditioned MIMO channel, i.e., its condition number is near to unity (see *Seethaler, Artés & Hlawatsch (2005)* for more details).

denote the determinant, transpose, conjugate transpose, inverse, and (i,j)-th element of a matrix, respectively, and $\Upsilon(\cdot,\cdot)$ and $\Gamma(\cdot,\cdot)$ are the lower and upper incomplete gamma functions defined in (*Gradshteyn & Ryzhik, 2000*, Equation (8.350.1)) and (*Gradshteyn & Ryzhik, 2000*, Equation (8.350.2)), respectively. We also denote $\mathcal{CN}(\mathbf{0},\mathbf{K})$ as a zero-mean circularly-symmetric complex Gaussian distribution with covariance $\mathbf{K}$ (*Gallager, 2008*, Section 7.8.1), and $\mathcal{L}_{\max}\{\cdot\}$ and $\mathcal{P}\{\cdot\}$ as the largest eigenvalue of a square matrix and the associated eigenvector, respectively.

The layout of the paper is as follows. 'System Model' describes the system model of interest. 'Exact Secrecy Outage Probability' and 'Asymptotic Secrecy Outage Probability' present exact and asymptotic analysis of the corresponding secrecy outage probability, respectively. 'Numerical Results' provides the numerical results of theoretical analysis and simulations, followed by the conclusion given in 'Conclusion'.

SYSTEM MODEL

In this section, we consider transmit-receive diversity and spatial multiplexing systems where the transmitter, the legitimate receiver, and the passive eavesdropper are equipped with M_t, M_r, and M_e antennas, respectively. The instantaneous secrecy capacity of these systems is given by (*Bloch et al., 2008*, Lemma 1)

$$C_\mathrm{s} = \begin{cases} \log_2(1+\gamma_\mathrm{r}) - \log_2(1+\gamma_\mathrm{e}), & \text{if } \gamma_\mathrm{r} > \gamma_\mathrm{e} \\ 0, & \text{if } \gamma_\mathrm{r} \leq \gamma_\mathrm{e} \end{cases} \tag{1}$$

where γ_r and γ_e are the instantaneous received SNRs at the receiver and the eavesdropper, respectively.

Transmit-receive diversity system

For the transmit-receive diversity system, the received signal vector at the legitimate receiver, $\mathbf{y}_\mathrm{r} \in \mathbb{C}^{M_\mathrm{r}\times 1}$, and that at the passive eavesdropper, $\mathbf{y}_\mathrm{e} \in \mathbb{C}^{M_\mathrm{e}\times 1}$, depend on the transmitted symbol $s \in \mathbb{C}$ (with $\mathrm{E}[|s|^2] = P$) according to

$$\mathbf{y}_\mathrm{r} = \mathbf{H}_\mathrm{r}\mathbf{w}_\mathrm{t}s + \mathbf{n}_\mathrm{r} \tag{2}$$

and

$$\mathbf{y}_\mathrm{e} = \mathbf{H}_\mathrm{e}\mathbf{w}_\mathrm{t}s + \mathbf{n}_\mathrm{e} \tag{3}$$

respectively, where $\mathbf{w}_\mathrm{t} \in \mathbb{C}^{M_\mathrm{t}\times 1}$ is the transmit weight (beamforming) vector, and $\mathbf{n}_\mathrm{r}$ and $\mathbf{n}_\mathrm{e}$ are independent circularly-symmetric complex-valued Gaussian noises: $\mathbf{n}_\mathrm{r} \sim \mathcal{CN}(\mathbf{0}, \sigma_\mathrm{r}^2\mathbf{I}_{M_\mathrm{r}})$ and $\mathbf{n}_\mathrm{e} \sim \mathcal{CN}(\mathbf{0}, \sigma_\mathrm{e}^2\mathbf{I}_{M_\mathrm{e}})$. We focus on a Rayleigh-fading wiretap channel, meaning that the channel matrices $\mathbf{H}_\mathrm{r}$ and $\mathbf{H}_\mathrm{e}$ have independent identically-distributed $\mathcal{CN}(0,1)$ entries. In addition, we assume that the three terminals know $\mathbf{H}_\mathrm{r}$, but $\mathbf{H}_\mathrm{e}$ is available only at the eavesdropper.[4]

The receiver estimates the symbol s by applying the receive weight (combining) vector $\mathbf{z}_\mathrm{r}$ to the received signal vector $\mathbf{y}_\mathrm{r}$:

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

[4] This assumption holds, for example, if the receiver and eavesdropper are able to perfectly estimate $\mathbf{H}_\mathrm{r}$ and $\mathbf{H}_\mathrm{e}$, respectively, and the receiver sends $\mathbf{H}_\mathrm{r}$ to the transmitter through a noiseless broadcast channel, which can be heard by the eavesdropper (*Goel & Negi, 2008*).

The optimal choices of $\mathbf{w}_t$ and $\mathbf{z}_r$ in the sense of maximizing the SNR of this estimate (i.e., the instantaneous received SNR) are given by *Dighe, Mallik & Jamuar (2003)*

$$\mathbf{w}_t = \frac{\mathbf{H}_r^\dagger \mathbf{z}_r}{\|\mathbf{H}_r^\dagger \mathbf{z}_r\|}$$

and

$$\mathbf{z}_r = \mathcal{P}\{\mathbf{H}_r \mathbf{H}_r^\dagger\}$$

respectively, and the resultant SNR is

$$\gamma_{r,TR} = \bar{\gamma}_r \mathcal{L}_{\max}\{\mathbf{H}_r \mathbf{H}_r^\dagger\} \tag{4}$$

where $\bar{\gamma}_r = \frac{P}{\sigma_r^2}$ is the average SNR at the receiver. The subscript TR refers to the transmit-receive diversity system, and is sometimes used to avoid confusion between this system and the spatial multiplexing system. Let $\lambda = \mathcal{L}_{\max}\{\mathbf{H}_r \mathbf{H}_r^\dagger\}$, $L = \min(M_t, M_r)$, and $K = \max(M_t, M_r)$. The cumulative distribution function (CDF) of λ is given by *Dighe, Mallik & Jamuar (2003)*

$$F_\lambda(x) = \frac{\det(\mathbf{S}(x))}{\left[\prod_{p=1}^{L}(K-p)!(L-p)!\right]} \tag{5}$$

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

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

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

$$F_\lambda(x) = \sum_{m=1}^{L} \sum_{n=|M_t-M_r|}^{(M_t+M_r-2m)m} \frac{a_{m,n}}{n!} \Upsilon(n+1, mx) \tag{6}$$

where $a_{m,n} = \frac{c_{m,n} n!}{m^{n+1}\left[\prod_{p=1}^{L}(K-p)!(L-p)!\right]}$ and $c_{m,n}$ is the coefficient computed by using curve fitting on the plot of $\frac{\mathrm{d}}{\mathrm{d}x}\det(\mathbf{S}(x))$ (*Dighe, Mallik & Jamuar, 2003*). Using Eq. (6) and (*Papoulis & Pillai, 2002*, Example 5-1), the CDF of $\gamma_{r,TR}$ in Eq. (4) is given by

$$F_{\gamma_{r,TR}}(x) = \sum_{m=1}^{L} \sum_{n=|M_t-M_r|}^{(M_t+M_r-2m)m} \frac{a_{m,n}}{n!} \Upsilon\left(n+1, \frac{mx}{\bar{\gamma}_r}\right). \tag{7}$$

Similarly, the eavesdropper can estimate the symbol s as

$$\mathbf{z}_e^\dagger \mathbf{y}_e = \mathbf{z}_e^\dagger \mathbf{H}_e \mathbf{w}_t s + \mathbf{z}_e^\dagger \mathbf{n}_e$$

where the receive weight vector

$$\mathbf{z}_e = \frac{\mathbf{H}_e \mathbf{w}_t}{\|\mathbf{H}_e \mathbf{w}_t\|}$$

is chosen to maximize the SNR of the estimate, yielding

$$\gamma_{e,TR} = \bar{\gamma}_e \|\mathbf{H}_e \mathbf{w}_t\|^2 \tag{8}$$

where $\bar{\gamma}_e = \frac{P}{\sigma_e^2}$ is the average SNR at the eavesdropper. The probability density function (PDF) of $\gamma_{e,TR}$ in Eq. (8) is given by *Maichalernnukul (2018)*

$$f_{\gamma_{e,TR}}(x) = \frac{x^{M_e-1}e^{-\frac{x}{\bar{\gamma}_e}}}{(M_e-1)!\bar{\gamma}_e^{M_e}}. \tag{9}$$

Spatial multiplexing system

Unlike the transmit-receive diversity system, the spatial multiplexing system allows the simultaneous transmission of different symbols, i.e., the ith antenna ($i = 1, 2, \ldots, M_t$) at the transmitter is used to transmit the symbol $s_i \in \mathbb{C}$ (with $\mathbf{E}[|s_i|^2] = P$) . Let $\mathbf{s} = [s_1, s_2, \ldots, s_{M_t}]^T$. The received signal vectors at the legitimate receiver and the passive eavesdropper are given, respectively, by

$$\mathbf{y}_r = \mathbf{H}_r\mathbf{s} + \mathbf{n}_r$$

where $\mathbf{H}_r$ and $\mathbf{n}_r$ are defined in Eq. (2), and

$$\mathbf{y}_e = \mathbf{H}_e\mathbf{s} + \mathbf{n}_e$$

where $\mathbf{H}_e$ and $\mathbf{n}_e$ are defined in Eq. (3). We assume that the receiver and the eavesdropper know $\mathbf{H}_r$ and $\mathbf{H}_e$, respectively, and the numbers of antennas at these two terminals (M_r and M_e) are no less than the number of antennas at the transmitter (M_t). The assumption on M_t, M_r, and M_e is necessary for the theoretical analysis hereafter.

In order for the receiver to estimate $\mathbf{s}$, the ZF or MMSE receive weight (equalizing) matrix is applied to $\mathbf{y}_r$. These matrices are given by *Tse & Viswanath (2005)*

$$\mathbf{W}_{r,ZF} = \left(\mathbf{H}_r^\dagger\mathbf{H}_r\right)^{-1}\mathbf{H}_r^\dagger$$

and

$$\mathbf{W}_{r,MMSE} = \left(\mathbf{H}_r^\dagger\mathbf{H}_r + \frac{1}{\bar{\gamma}_r}\mathbf{I}_{M_t}\right)^{-1}\mathbf{H}_r^\dagger.$$

It is noteworthy that as the average SNR at the receiver grows very large, i.e., $\bar{\gamma}_r \to \infty$, $\mathbf{W}_{r,MMSE}$ approaches $\mathbf{W}_{r,ZF}$. Left multiplying $\mathbf{y}_r$ by $\mathbf{W}_{r,ZF}$ and $\mathbf{W}_{r,MMSE}$, we obtain the ith symbol estimate ($i = 1, 2, \ldots, M_t$), the SNRs of which are, respectively, (*Jiang, Varanasi & Li, 2011*)

$$\gamma_{r,ZF,i} = \frac{\bar{\gamma}_r}{\left[\left(\mathbf{H}_r^\dagger\mathbf{H}_r\right)^{-1}\right]_{ii}} \tag{10}$$

and

$$\gamma_{r,MMSE,i} = \frac{\bar{\gamma}_r}{\left[\left(\mathbf{H}_r^\dagger\mathbf{H}_r + \frac{1}{\bar{\gamma}_r}\mathbf{I}_{M_t}\right)^{-1}\right]_{ii}} - 1. \tag{11}$$

The CDFs of $\gamma_{r,ZF,i}$ and $\gamma_{r,MMSE,i}$ are given, respectively, by *Chen & Wang (2007)*

$$F_{\gamma_{r,ZF}}(x) = 1 - e^{-\frac{x}{\bar{\gamma}_r}}\sum_{m=0}^{M_r-M_t}\frac{x^m}{m!\bar{\gamma}_r^m} \tag{12}$$

and *Smith (2007)*

$$F_{\gamma_{\mathrm{r,MMSE}}}(x) = 1 - \frac{e^{-\frac{x}{\bar{\gamma}_\mathrm{r}}}}{(x+1)^{M_\mathrm{t}-1}} \sum_{m=0}^{M_\mathrm{r}-1} d_m x^m \tag{13}$$

where $d_m = \sum_{n=\max(0,m-M_\mathrm{t}+1)}^{m} \binom{M_\mathrm{t}-1}{m-n} \frac{1}{n!\bar{\gamma}_\mathrm{r}^n}$. The symbol index i is omitted from Eqs. (12) and (13) because all the elements of $\mathbf{H}_\mathrm{r}$ are statistically independent and identically distributed.

Similarly, the eavesdropper performs ZF or MMSE equalization, and the resulting SNRs of the ith symbol estimate (i.e., $\gamma_{\mathrm{e,ZF},i}$ and $\gamma_{\mathrm{e,MMSE},i}$) can be expressed, respectively, as Eqs. (10) and (11) with the subscript r being replaced by the subscript e. Replacing the subscript r with the subscript e in Eqs. (12) and (13), and taking the derivative of these equations with respect to x, we obtain the PDFs for $\gamma_{\mathrm{e,ZF},i}$ and $\gamma_{\mathrm{e,MMSE},i}$, respectively, as

$$f_{\gamma_{\mathrm{e,ZF}}}(x) = \frac{x^{M_\mathrm{e}-M_\mathrm{t}} e^{-\frac{x}{\bar{\gamma}_\mathrm{e}}}}{(M_\mathrm{e}-M_\mathrm{t})!\bar{\gamma}_\mathrm{e}^{M_\mathrm{e}-M_\mathrm{t}+1}} \tag{14}$$

and

$$f_{\gamma_{\mathrm{e,MMSE}}}(x) = \frac{e^{-\frac{x}{\bar{\gamma}_\mathrm{e}}}}{(x+1)^{M_\mathrm{t}}} \sum_{m=0}^{M_\mathrm{e}-1} g_m \left[\frac{x^{m+1}}{\bar{\gamma}_\mathrm{e}} + \left(M_\mathrm{t} + \frac{1}{\bar{\gamma}_\mathrm{e}} - m - 1 \right) x^m - m x^{m-1} \right] \tag{15}$$

where g_m is similar to d_m, except that the subscript r is replaced by the subscript e.

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 $R > 0$ (*Bloch et al., 2008*). From Eq. (1), this performance metric can be expressed as

$$\begin{aligned} P_\mathrm{out}(R) &= \Pr\{C_\mathrm{s} < R\} \\ &= \Pr\left\{\gamma_\mathrm{r} < 2^R\gamma_\mathrm{e} + 2^R - 1\right\} \\ &= \int_0^\infty f_{\gamma_\mathrm{e}}(v) F_{\gamma_\mathrm{r}}\left(2^R v + 2^R - 1\right) \mathrm{d}v. \end{aligned} \tag{16}$$

Transmit-receive diversity system

From Eqs. (7), (9) and (16), we can derive the exact secrecy outage probability for the transmit-receive diversity system as follows:

$$\begin{aligned} P_\mathrm{out,TR}(R) = {} & \frac{1}{(M_\mathrm{e}-1)!\bar{\gamma}_\mathrm{e}^{M_\mathrm{e}}} \sum_{m=1}^{L} \sum_{n=|M_\mathrm{t}-M_\mathrm{r}|}^{(M_\mathrm{t}+M_\mathrm{r}-2m)m} \frac{a_{m,n}}{n!} \int_0^\infty v^{M_\mathrm{e}-1} e^{-\frac{v}{\bar{\gamma}_\mathrm{e}}} \\ & \times \Upsilon\left(n+1, \frac{(2^R v + 2^R - 1)m}{\bar{\gamma}_\mathrm{r}}\right) \mathrm{d}v \\ = {} & \frac{1}{(M_\mathrm{e}-1)!\bar{\gamma}_\mathrm{e}^{M_\mathrm{e}}} \sum_{m=1}^{L} \sum_{n=|M_\mathrm{t}-M_\mathrm{r}|}^{(M_\mathrm{t}+M_\mathrm{r}-2m)m} a_{m,n} \left[\int_0^\infty v^{M_\mathrm{e}-1} e^{-\frac{v}{\bar{\gamma}_\mathrm{e}}} \mathrm{d}v \right. \\ & \left. - e^{-\frac{(2^R-1)m}{\bar{\gamma}_\mathrm{r}}} \sum_{k=0}^{n} \left(\frac{m}{\bar{\gamma}_\mathrm{r}}\right)^k \sum_{l=0}^{k} \frac{2^{lR}(2^R-1)^{k-l}}{l!(k-l)!} \int_0^\infty v^{l+M_\mathrm{e}-1} e^{-\left(\frac{2^R m}{\bar{\gamma}_\mathrm{r}} + \frac{1}{\bar{\gamma}_\mathrm{e}}\right)v} \mathrm{d}v \right] \end{aligned}$$

$$= 1 - \frac{1}{(M_e-1)!\bar{\gamma}_e^{M_e}} \sum_{m=1}^{L} \sum_{n=|M_t-M_r|}^{(M_t+M_r-2m)m} a_{m,n} e^{-\frac{(2^R-1)m}{\bar{\gamma}_r}} \sum_{k=0}^{n} \left(\frac{m}{\bar{\gamma}_r}\right)^k \times \sum_{l=0}^{k} \frac{(l+M_e-1)!2^{lR}(2^R-1)^{k-l}}{l!(k-l)!\left(\frac{2^R m}{\bar{\gamma}_r}+\frac{1}{\bar{\gamma}_e}\right)^{l+M_e}} \quad (17)$$

where the second equality is obtained by using (*Gradshteyn & Ryzhik, 2000*, Equations (1.111) and (8.352.1)), and the last equality is obtained by using (*Gradshteyn & Ryzhik, 2000*, Equation (3.351.3)) and (*Maaref & Aïssa, 2005*, Equation (11)). For the special case of $M_t = M_r = M_e = 1$, the secrecy outage probability expression in Eq. (17) reduces to

$$P_{\text{out,TR}}(R) = 1 - \frac{\bar{\gamma}_r e^{-\frac{2^R-1}{\bar{\gamma}_r}}}{\bar{\gamma}_r + 2^R\bar{\gamma}_e} \quad (18)$$

which agrees exactly with a result given in (*Bloch et al., 2008*, Equation (9)).

Spatial multiplexing system

From Eqs. (12), (14) and (16), we can derive the exact secrecy outage probability for the spatial multiplexing system with ZF equalization as follows:

$$\begin{aligned} P_{\text{out,ZF}}(R) &= \int_0^\infty f_{\gamma_{e,\text{ZF}}}(v)\mathrm{d}v - \frac{e^{-\frac{2^R-1}{\bar{\gamma}_r}}}{(M_e-M_t)!\bar{\gamma}_e^{M_e-M_t+1}} \sum_{m=0}^{M_r-M_t} \frac{1}{m!\bar{\gamma}_r^m} \\ &\quad \times \int_0^\infty (2^R v + 2^R - 1)^m v^{M_e-M_t} e^{-\left(\frac{2^R}{\bar{\gamma}_r}+\frac{1}{\bar{\gamma}_e}\right)v}\mathrm{d}v \\ &= 1 - \frac{e^{-\frac{2^R-1}{\bar{\gamma}_r}}}{(M_e-M_t)!\bar{\gamma}_e^{M_e-M_t+1}} \sum_{m=0}^{M_r-M_t} \frac{1}{\bar{\gamma}_r^m} \sum_{n=0}^{m} \frac{2^{nR}(2^R-1)^{m-n}}{n!(m-n)!} \\ &\quad \times \int_0^\infty v^{n+M_e-M_t} e^{-\left(\frac{2^R}{\bar{\gamma}_r}+\frac{1}{\bar{\gamma}_e}\right)v}\mathrm{d}v \\ &= 1 - \frac{e^{-\frac{2^R-1}{\bar{\gamma}_r}}}{(M_e-M_t)!\left(\frac{2^R\bar{\gamma}_e}{\bar{\gamma}_r}+1\right)^{M_e-M_t+1}} \\ &\quad \times \sum_{m=0}^{M_r-M_t} \frac{1}{\bar{\gamma}_r^m} \sum_{n=0}^{m} \frac{2^{nR}(2^R-1)^{m-n}(n+M_e-M_t)!}{n!(m-n)!\left(\frac{2^R}{\bar{\gamma}_r}+\frac{1}{\bar{\gamma}_e}\right)^n} \end{aligned} \quad (19)$$

where the second equality is obtained by using (*Gradshteyn & Ryzhik, 2000*, Equation (1.111)) and (*Papoulis & Pillai, 2002*, Equation (4-18)), and the last equality is obtained by using (*Gradshteyn & Ryzhik, 2000*, Equation (3.351.3)). For the special case of $M_t = M_r = M_e = 1$, Eq. (19) simplifies to Eq. (18).

Meanwhile, the secrecy outage probability for the spatial multiplexing system with MMSE equalization can be derived from Eqs. (13), (15) and (16) as follows:

$$
\begin{aligned}
P_{\text{out,MMSE}}(R) &= \int_0^{\infty} f_{\gamma_{\text{e,MMSE}}}(v)\,\mathrm{d}v - \frac{e^{-\frac{2^R-1}{\bar{\gamma}_\text{r}}}}{2^{(M_\text{t}-1)R}} \sum_{m=0}^{M_\text{e}-1} g_m \sum_{n=0}^{M_\text{r}-1} d_n \\
&\quad \times \left[\int_0^{\infty} \frac{(2^R v + 2^R - 1)^n e^{-\left(\frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}}\right)v}}{(v+1)^{2M_\text{t}-1}} \right. \\
&\quad \left. \times \left[\frac{v^{m+1}}{\bar{\gamma}_\text{e}} + \left(M_\text{t} + \frac{1}{\bar{\gamma}_\text{e}} - m - 1 \right) v^m - m v^{m-1} \right] \mathrm{d}v \right] \\
&= 1 - \frac{e^{\frac{1}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}}}}{2^{(M_\text{t}-1)R}} \sum_{m=0}^{M_\text{e}-1} g_m \sum_{n=0}^{M_\text{r}-1} d_n \sum_{k=0}^{n} \binom{n}{k} (-1)^k 2^{(n-k)R} \\
&\quad \times \left[\frac{1}{\bar{\gamma}_\text{e}} \sum_{l_1=0}^{m+1} \binom{m+1}{l_1} (-1)^{l_1} \int_1^{\infty} v^{m+n-k-l_1-2M_\text{t}+2} e^{-\left(\frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}}\right)v} \mathrm{d}v \right. \\
&\quad + \left(M_\text{t} + \frac{1}{\bar{\gamma}_\text{e}} - m - 1 \right) \sum_{l_2=0}^{m} \binom{m}{l_2} (-1)^{l_2} \int_1^{\infty} v^{m+n-k-l_2-2M_\text{t}+1} e^{-\left(\frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}}\right)v} \mathrm{d}v \\
&\quad \left. + m \sum_{l_3=0}^{m-1} \binom{m-1}{l_3} (-1)^{l_3} \int_1^{\infty} v^{m+n-k-l_3-2M_\text{t}} e^{-\left(\frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}}\right)v} \mathrm{d}v \right] \\
&= 1 - \frac{e^{\frac{1}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}}}}{2^{(M_\text{t}-1)R}} \sum_{m=0}^{M_\text{e}-1} g_m \sum_{n=0}^{M_\text{r}-1} d_n \sum_{k=0}^{n} \binom{n}{k} (-1)^k 2^{(n-k)R} \\
&\quad \times \left[\frac{1}{\bar{\gamma}_\text{e}} \sum_{l_1=0}^{m+1} \binom{m+1}{l_1} \frac{(-1)^{l_1} \Gamma\left(m+n-k-l_1-2M_\text{t}+3, \frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}} \right)}{\left(\frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}} \right)^{m+n-k-l_1-2M_\text{t}+3}} \right. \\
&\quad + \left(M_\text{t} + \frac{1}{\bar{\gamma}_\text{e}} - m - 1 \right) \sum_{l_2=0}^{m} \binom{m}{l_2} \frac{(-1)^{l_2} \Gamma\left(m+n-k-l_2-2M_\text{t}+2, \frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}} \right)}{\left(\frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}} \right)^{m+n-k-l_2-2M_\text{t}+2}} \\
&\quad \left. + m \sum_{l_3=0}^{m-1} \binom{m-1}{l_3} \frac{(-1)^{l_3} \Gamma\left(m+n-k-l_3-2M_\text{t}+1, \frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}} \right)}{\left(\frac{2^R}{\bar{\gamma}_\text{r}} + \frac{1}{\bar{\gamma}_\text{e}} \right)^{m+n-k-l_3-2M_\text{t}+1}} \right]
\end{aligned} \tag{20}
$$

where the second equality is obtained by changing the limits of integration and using (*Gradshteyn & Ryzhik, 2000*, Equation (1.111)) and (*Papoulis & Pillai, 2002*, Equation (4-18)), and the last equality is obtained by using (*Gradshteyn & Ryzhik, 2000*, Equation (3.381.3)). For the special case of $M_\text{t} = M_\text{r} = M_\text{e} = 1$, Eq. (20) reduces to Eq. (18).

ASYMPTOTIC SECRECY OUTAGE PROBABILITY

In this section, we focus on deriving the asymptotic secrecy outage probability of the aforementioned systems as $\bar{\gamma}_\text{r} \to \infty$. 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 (*Yang et al., 2013*). The secrecy diversity order indicates the slope of the secrecy outage probability versus $\bar{\gamma}_\text{r}$ curve at high SNR in a log–log scale, whereas

the secrecy array gain indicates the shift of the curve with respect to the benchmark secrecy outage curve.

Transmit-receive diversity system

First, we look for a first-order expansion of Eq. (5), which will be immediate from a first-order expansion of $\det(\mathbf{S}(x))$. Following the approach outlined in (*McKay, 2006*, Appendix B.7) and using (*Kalman, 1984*, Equations (1) and (2)), it is straightforward to show that the first-order Taylor expansion of $\det(\mathbf{S}(x))$ around $x=0$ is

$$\det(\mathbf{S}(x)) = \left[\prod_{p=1}^{L} \frac{(K-p)!\,[(L-p)!]^2}{(M_\mathrm{t}+M_\mathrm{r}-p)!}\right] x^{M_\mathrm{t}M_\mathrm{r}} + o\left(x^{M_\mathrm{t}M_\mathrm{r}}\right). \tag{21}$$

Substituting Eq. (21) into Eq. (5) yields

$$F_\lambda(x) = \left[\prod_{p=1}^{L} \frac{(L-p)!}{(M_\mathrm{t}+M_\mathrm{r}-p)!}\right] x^{M_\mathrm{t}M_\mathrm{r}} + o\left(x^{M_\mathrm{t}M_\mathrm{r}}\right). \tag{22}$$

Using Eq. (22) and (*Papoulis & Pillai, 2002*, Example 5-1), the first-order expansion of the CDF of $\gamma_{\mathrm{r,TR}}$ is given by

$$F_{\gamma_{\mathrm{r,TR}}}(x) = \left[\prod_{p=1}^{L} \frac{(L-p)!}{(M_\mathrm{t}+M_\mathrm{r}-p)!}\right] \left(\frac{x}{\bar{\gamma}_\mathrm{r}}\right)^{M_\mathrm{t}M_\mathrm{r}} + o\left(\left(\frac{x}{\bar{\gamma}_\mathrm{r}}\right)^{M_\mathrm{t}M_\mathrm{r}}\right). \tag{23}$$

Using Eqs. (9), (16) and (23), and following the same procedure as used in Eq. (17), an asymptotic expression for $P_{\mathrm{out,TR}}(R)$ with $\bar{\gamma}_\mathrm{r} \to \infty$ is obtained as

$$P^{\infty}_{\mathrm{out,TR}}(R) = (A_\mathrm{TR}\bar{\gamma}_\mathrm{r})^{-D_\mathrm{TR}} + o\left(\bar{\gamma}_\mathrm{r}^{-D_\mathrm{TR}}\right) \tag{24}$$

where the secrecy diversity gain is

$$D_\mathrm{TR} = M_\mathrm{t}M_\mathrm{r} \tag{25}$$

and the secrecy array gain is

$$A_\mathrm{TR} = \left[\frac{1}{(M_\mathrm{e}-1)!}\left[\prod_{p=1}^{L} \frac{(L-p)!}{(M_\mathrm{t}+M_\mathrm{r}-p)!}\right] \sum_{n=0}^{M_\mathrm{t}M_\mathrm{r}} \binom{M_\mathrm{t}M_\mathrm{r}}{n} \times (n+M_\mathrm{e}-1)!\,2^{nR}(2^R-1)^{M_\mathrm{t}M_\mathrm{r}-n}\bar{\gamma}_\mathrm{e}^{n}\right]^{-\frac{1}{M_\mathrm{t}M_\mathrm{r}}}. \tag{26}$$

It is clear from Eq. (25) that the secrecy diversity order is dependent on M_t and M_r, and independent of M_e. It can also be seen from Eq. (26) that the eavesdropper channel has an adverse impact on the secrecy array gain. Accordingly, increasing the number of antennas at the eavesdropper lessens the secrecy array gain, thereby rising the secrecy outage probability.

Spatial multiplexing system

Applying (*Gradshteyn & Ryzhik, 2000*, Equation (1.211.1)) to the exponential function in Eq. (12) and performing some algebraic manipulations, the first-order expansion of the

CDF of $\gamma_{\mathrm{r,ZF},i}$ can be derived as

$$F_{\gamma_{\mathrm{r,ZF}}}(x) = \frac{x^{M_\mathrm{r}-M_\mathrm{t}+1}}{(M_\mathrm{r}-M_\mathrm{t}+1)!\bar{\gamma}_\mathrm{r}^{M_\mathrm{r}-M_\mathrm{t}+1}} + o\left(\left(\frac{x}{\bar{\gamma}_\mathrm{r}}\right)^{M_\mathrm{r}-M_\mathrm{t}+1}\right). \tag{27}$$

Using Eqs. (14), (16) and (27), and following the same procedure as used in Eq. (19), an asymptotic expression for $P_{\mathrm{out,ZF}}(R)$ with $\bar{\gamma}_\mathrm{r} \to \infty$ is obtained as

$$P^{\infty}_{\mathrm{out,ZF}}(R) = (A_{\mathrm{ZF}}\bar{\gamma}_\mathrm{r})^{-D_{\mathrm{ZF}}} + o\left(\bar{\gamma}_\mathrm{r}^{-D_{\mathrm{ZF}}}\right) \tag{28}$$

where

$$D_{\mathrm{ZF}} = M_\mathrm{r} - M_\mathrm{t} + 1 \tag{29}$$

and

$$A_{\mathrm{ZF}} = \left[\frac{\sum_{n=0}^{M_\mathrm{r}-M_\mathrm{t}+1}\binom{M_\mathrm{r}-M_\mathrm{t}+1}{n}2^{nR}(2^R-1)^{M_\mathrm{r}-M_\mathrm{t}+1-n}(n+M_\mathrm{e}-M_\mathrm{t})!\bar{\gamma}_\mathrm{e}^{n}}{(M_\mathrm{r}-M_\mathrm{t}+1)!(M_\mathrm{e}-M_\mathrm{t})!}\right]^{-\frac{1}{M_\mathrm{r}-M_\mathrm{t}+1}}. \tag{30}$$

Adopting the same steps as for deriving the first-order expansion of $F_{\gamma_{\mathrm{r,ZF}}}(x)$, we obtain

$$F_{\gamma_{\mathrm{r,MMSE}}}(x) = \frac{x^{M_\mathrm{r}}}{(M_\mathrm{r}-M_\mathrm{t}+1)!\bar{\gamma}_\mathrm{r}^{M_\mathrm{r}-M_\mathrm{t}+1}(x+1)^{M_\mathrm{t}-1}} + o\left(\left(\frac{x}{\bar{\gamma}_\mathrm{r}}\right)^{M_\mathrm{r}-M_\mathrm{t}+1}\right). \tag{31}$$

Using Eqs. (15), (16) and (31), and following the same procedure as used in Eq. (20), an asymptotic expression for $P_{\mathrm{out,MMSE}}(R)$ with $\bar{\gamma}_\mathrm{r} \to \infty$ is obtained as

$$P^{\infty}_{\mathrm{out,MMSE}}(R) = (A_{\mathrm{MMSE}}\bar{\gamma}_\mathrm{r})^{-D_{\mathrm{MMSE}}} + o\left(\bar{\gamma}_\mathrm{r}^{-D_{\mathrm{MMSE}}}\right) \tag{32}$$

where

$$D_{\mathrm{MMSE}} = M_\mathrm{r} - M_\mathrm{t} + 1 \tag{33}$$

and

$$\begin{aligned} A_{\mathrm{MMSE}} = \Bigg[& \frac{e^{\frac{1}{\bar{\gamma}_\mathrm{e}}}2^{(M_\mathrm{r}-M_\mathrm{t}+1)R}}{(M_\mathrm{r}-M_\mathrm{t}+1)!}\sum_{m=0}^{M_\mathrm{e}-1} g_m \sum_{n=0}^{M_\mathrm{r}}\binom{M_\mathrm{r}}{n}\frac{(-1)^n\bar{\gamma}_\mathrm{e}^{m-n+M_\mathrm{r}-2M_\mathrm{t}+1}}{2^{nR}} \\ & \times\Bigg[\bar{\gamma}_\mathrm{e}\sum_{k_1=0}^{m+1}\binom{m+1}{k_1}\left(-\frac{1}{\bar{\gamma}_\mathrm{e}}\right)^{k_1}\Gamma\left(m-n-k_1+M_\mathrm{r}-2M_\mathrm{t}+3,\frac{1}{\bar{\gamma}_\mathrm{e}}\right) \\ & +\bar{\gamma}_\mathrm{e}\left(M_\mathrm{t}+\frac{1}{\bar{\gamma}_\mathrm{e}}-m-1\right)\sum_{k_2=0}^{m}\binom{m}{k_2}\left(-\frac{1}{\bar{\gamma}_\mathrm{e}}\right)^{k_2}\Gamma\left(m-n-k_2+M_\mathrm{r}-2M_\mathrm{t}+2,\frac{1}{\bar{\gamma}_\mathrm{e}}\right) \\ & -m\sum_{k_3=0}^{m-1}\binom{m-1}{k_3}\left(-\frac{1}{\bar{\gamma}_\mathrm{e}}\right)^{k_3}\Gamma\left(m-n-k_3+M_\mathrm{r}-2M_\mathrm{t}+1,\frac{1}{\bar{\gamma}_\mathrm{e}}\right)\Bigg]\Bigg]^{-\frac{1}{M_\mathrm{r}-M_\mathrm{t}+1}}. \end{aligned} \tag{34}$$

It is obvious from Eqs. (29) and (33) that the secrecy diversity orders of the spatial multiplexing systems with ZF equalization and MMSE equalization are dependent on M_t and M_r, and independent of M_e. It can also be observed from Eqs. (30) and (34) that increasing M_e decreases the corresponding secrecy array gains.

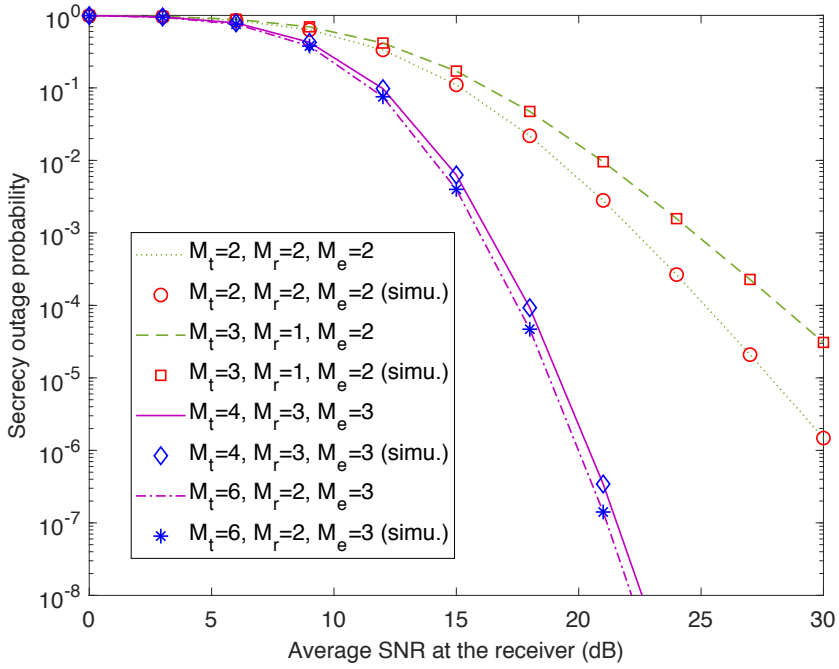

Figure 1 Secrecy outage probability of transmit-receive diversity system ($P_{\text{out,TR}}$) as a function of $\bar{\gamma}_{\text{r}}$. This figure shows the theoretical and simulated secrecy outage curves for the transmit-receive diversity system with different numbers of antennas at the transmitter (M_{t}), the legitimate receiver (M_{r}), and the eavesdropper (M_{e}). The simulation results are labeled with "simu.".

Full-size DOI: 10.7717/peerjcs.186/fig-1

NUMERICAL RESULTS

In this section, we validate the preceding theoretical analysis and investigate the effect of the various system parameters. For these purposes, theoretical and simulation results are obtained by using MATLAB. Specifically, we use the closed-form expressions derived above to generate the theoretical results, and adopt the Monte Carlo method to generate the simulation results. Remember that $\bar{\gamma}_{\text{r}}$ and $\bar{\gamma}_{\text{e}}$ are the average SNRs at the legitimate receiver and the passive eavesdropper, respectively. Unless otherwise indicated, the SNR $\bar{\gamma}_{\text{e}}$ is set to 10 dB, and the target secrecy rate R is set to 1 bit/s/Hz. Figure 1 shows the theoretical secrecy outage probability of the transmit-receive diversity system (computed with Eq. (17)) and its simulation counterpart (labeled with "simu.") against $\bar{\gamma}_{\text{r}}$. As seen in the figure, the theoretical and simulation results match perfectly. For a given $\bar{\gamma}_{\text{r}}$, when $M_{\text{t}}+M_{\text{r}}=4$ and $M_{\text{e}}=2$, the secrecy outage probability with $M_{\text{t}}=2$ and $M_{\text{r}}=2$ is lower than that with $M_{\text{t}}=3$ and $M_{\text{r}}=1$. This is consistent with the fact that for a fixed total number of antennas at the transmitter and legitimate receiver ($M_{\text{t}}+M_{\text{r}}$), a more-balanced antenna configuration provides a larger diversity gain (*Dighe, Mallik & Jamuar, 2003*; *Maaref & Aïssa, 2005*). Specifically, from Eq. (25), we have $D_{\text{TR}}=4$ for $M_{\text{t}}=2$ and $M_{\text{r}}=2$, and $D_{\text{TR}}=3$ for $M_{\text{t}}=3$ and $M_{\text{r}}=1$. However, when $M_{\text{t}}M_{\text{r}}=12$ and $M_{\text{e}}=3$, the secrecy outage probability with $M_{\text{t}}=4$ and $M_{\text{r}}=3$ is higher than that with $M_{\text{t}}=6$ and $M_{\text{r}}=2$.

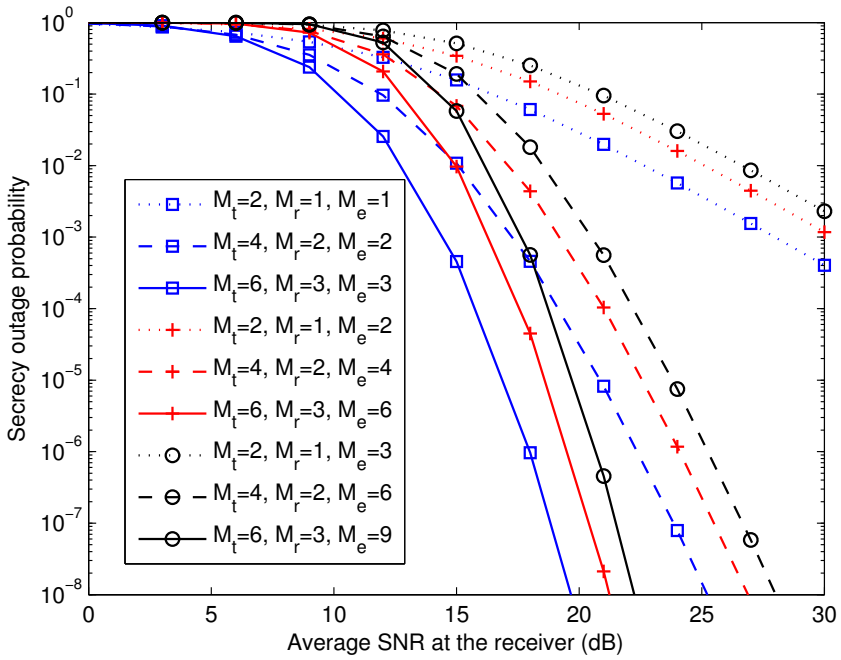

Figure 2 $P_{\text{out,TR}}$ **for different combinations of** M_t, M_r, **and** M_e. This figure shows the theoretical secrecy outage curves for the transmit-receive diversity system, comparing different numbers of antennas at the transmitter (M_t), the legitimate receiver (M_r), and the eavesdropper (M_e).

Full-size DOI: 10.7717/peerjcs.186/fig-2

The reason is that for the same product of M_t and M_r, an increase in $M_t + M_r$ yields a performance enhancement (*Dighe, Mallik & Jamuar, 2003*).

Figure 2 depicts the theoretical secrecy outage probability of the aforementioned system for different combinations of M_t, M_r, and M_e. We observe that when (M_t, M_r) is kept fixed (i.e., at $(2,1)$, $(4,2)$, or $(6,3)$), the larger M_e is, the smaller the array gain (as discussed in Eq. (26)), which worsens the secrecy outage performance. Furthermore, it can be seen that for a given $\bar{\gamma}_r$, the secrecy outage probability with $(M_t, M_r, M_e) = (2,1,1)$ is higher than that with $(M_t, M_r, M_e) = (4,2,2)$. Meanwhile, the secrecy outage probability with $(M_t, M_r, M_e) = (4,2,2)$ is higher than that with $(M_t, M_r, M_e) = (6,3,3)$. The same performance trend occurs when (M_t, M_r, M_e) increases from $(2,1,2)$ to $(6,3,6)$ or from $(2,1,3)$ to $(6,3,9)$. These results reveal that adding M_t and M_r proportionally to M_e is advantageous.

Figure 3 verifies the asymptotic secrecy outage probability of the transmit-receive diversity system derived in Eqs. (24)–(26) 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, and M_e. It can also be observed that the secrecy diversity gain is $M_t M_r$, as predicted by Eq. (25), and the secrecy array gain diminishes with increasing M_e, as predicted by Eq. (26).

Figure 4 compares the theoretical secrecy outage results for the spatial multiplexing systems with ZF equalization (computed with Eq. (19)) and MMSE equalization (computed with Eq. (20)), and their simulation counterparts. The theoretical and simulation results

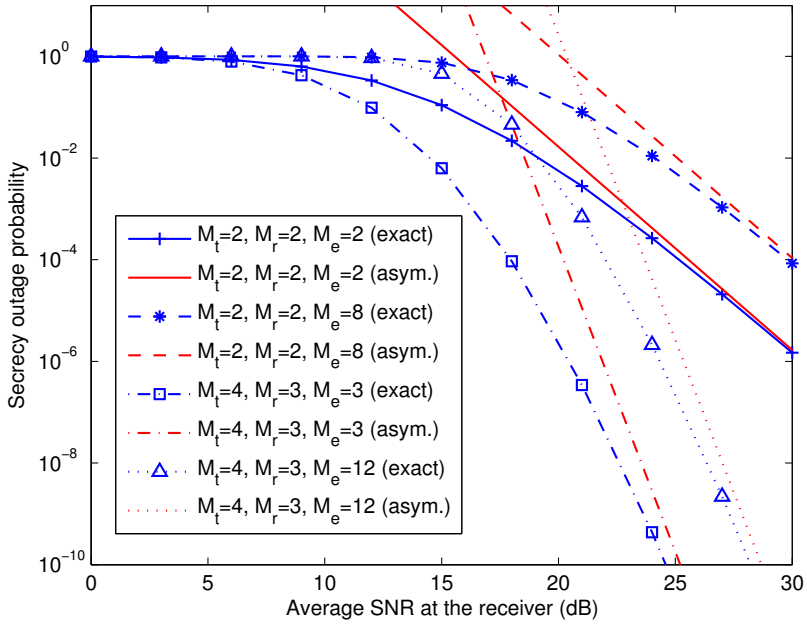

Figure 3 Comparison of exact and asymptotic secrecy outage probability of transmit-receive diversity system. This figure shows the exact and asymptotic secrecy outage curves for the transmit-receive diversity system with different numbers of antennas at the transmitter (M_t), the legitimate receiver (M_r), and the eavesdropper (M_e). The exact and asymptotic results are labeled with "exact" and "asym.", respectively.
Full-size DOI: 10.7717/peerjcs.186/fig-3

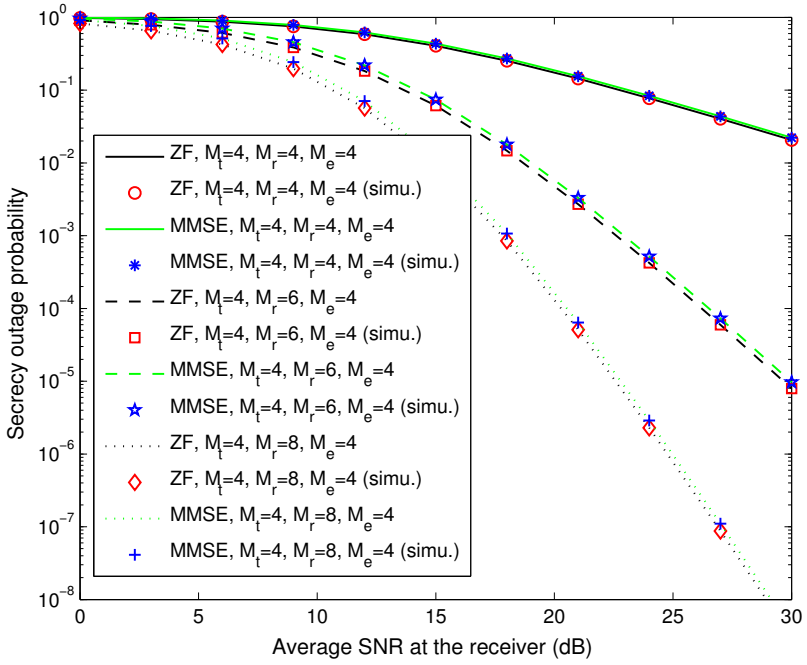

Figure 4 Secrecy outage probability of spatial multiplexing systems with ZF equalization ($P_{out,ZF}$) and MMSE equalization ($P_{out,MMSE}$). This figure shows the theoretical and simulated secrecy outage curves for the ZF equalization-based and MMSE equalization-based spatial multiplexing systems with different numbers of antennas at the legitimate receiver (M_r) and fixed numbers of antennas at the transmitter (M_t) and the eavesdropper (M_e). The simulation results are labeled with "simu.".
Full-size DOI: 10.7717/peerjcs.186/fig-4

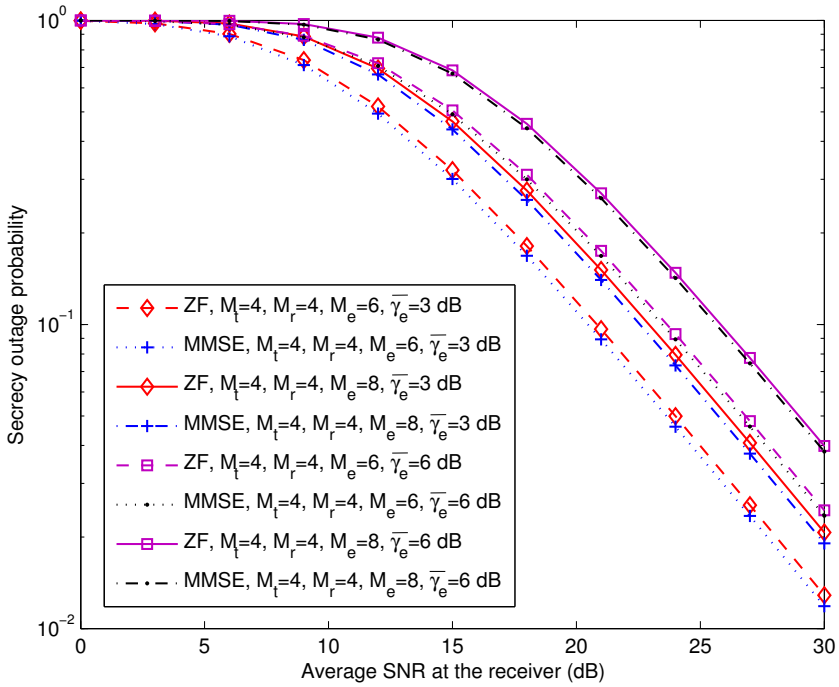

Figure 5 $P_{\text{out,ZF}}$ **versus** $P_{\text{out,MMSE}}$ **for various** M_{e} **at fixed** M_{t} **and** M_{r} **(**$M_{\text{t}} = M_{\text{r}} = 4$**).** This figure shows the theoretical secrecy outage curves for the ZF equalization-based and MMSE equalization-based spatial multiplexing systems with different numbers of antennas and average SNRs at the eavesdropper (M_{e} and $\bar{\gamma}_{\text{e}}$), and fixed numbers of antennas at the transmitter (M_{t}) and the legitimate receiver (M_{r}).
Full-size DOI: 10.7717/peerjcs.186/fig-5

agree well, and both kinds of systems exhibit similar secrecy outage performance. Indeed, the spatial multiplexing system with MMSE equalization achieves lower secrecy outage probability when the number of antennas at the eavesdropper is more than that at the receiver, as illustrated in Fig. 5. In addition, most noteworthy in Eq. (19) is the fact that, when the values of $(M_{\text{r}} - M_{\text{t}})$ and $(M_{\text{e}} - M_{\text{t}})$ are fixed, the secrecy outage probability of the spatial multiplexing system with ZF equalization remains the same regardless of the value of M_{t} that is used. This fact is confirmed by Fig. 6, where we plot the simulated secrecy outage curves in the case of $M_{\text{r}} - M_{\text{t}} = 0, M_{\text{e}} - M_{\text{t}} = 0$ and that of $M_{\text{r}} - M_{\text{t}} = 2, M_{\text{e}} - M_{\text{t}} = 4$.

Figures 7 and 8 verify the asymptotic secrecy outage probability of the spatial multiplexing system with ZF equalization derived in Eqs. (28)–(30) and that of the spatial multiplexing system with MMSE equalization derived in Eqs. (32)–(34), respectively, at a fixed $\bar{\gamma}_{\text{e}}$ (i.e., $\bar{\gamma}_{\text{e}} = 10$ dB). As $\bar{\gamma}_{\text{r}}$ increases, the asymptotic curves tend towards the exact ones for different values of M_{t}, M_{r}, and M_{e}. It can also be noticed that the secrecy diversity gains of the two systems are $M_{\text{r}} - M_{\text{t}} + 1$, as predicted by Eqs. (29) and (33), and the corresponding secrecy array gains lessen with growing M_{e}, as predicted by Eqs. (30) and (34).

Finally, it is interesting to compare the computational complexity of all three systems. To this end, we express such complexity in terms of the number of floating-point operations (flops), and the relevant calculations are summarized as follows:[5] (1) the number of flops

[5] For a detailed analysis of the number of flops required for matrix–vector operations such as associated summations and multiplications, readers are referred to *Hunger (2007)*.

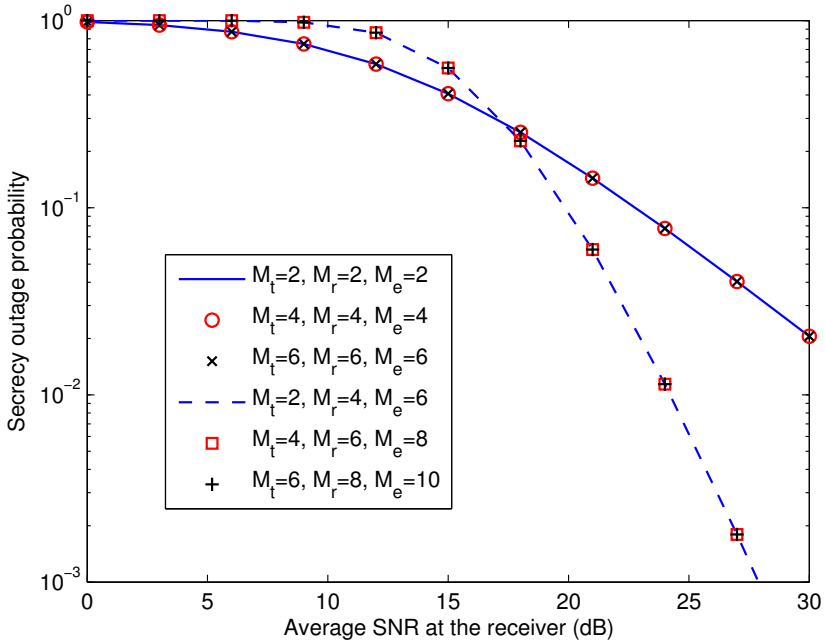

Figure 6 **Examples of $P_{\text{out,ZF}}$ with $M_t = M_r = M_e$ and that with $M_r = M_t + 2$ and $M_e = M_t + 4$.** This figure shows the simulated secrecy outage curves for the ZF equalization-based spatial multiplexing system in the case that the numbers of antennas at the transmitter (M_t), the legitimate receiver (M_r), and the eavesdropper (M_e) are the same, and the case of $M_r = M_t + 2$, $M_e = M_t + 4$.

Full-size DOI: 10.7717/peerjcs.186/fig-6

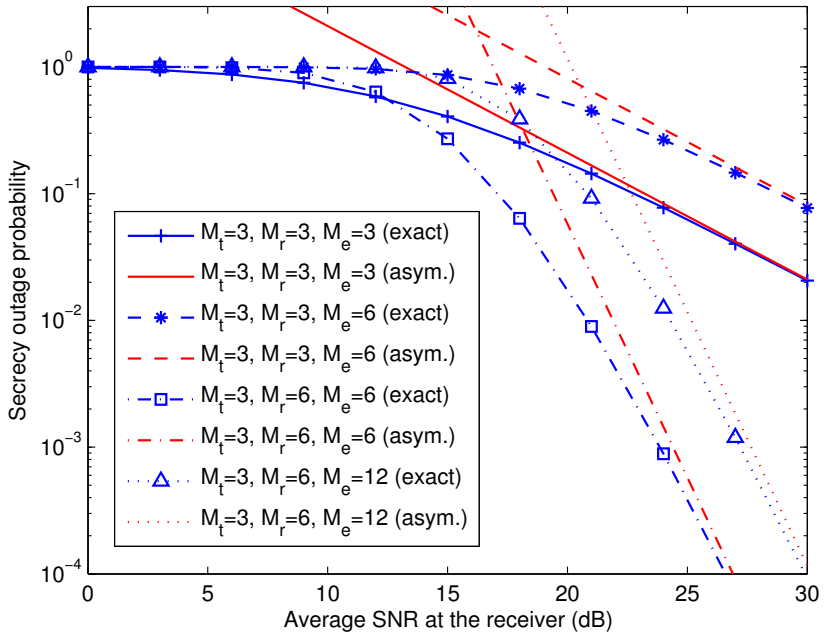

Figure 7 **Comparison of exact and asymptotic secrecy outage probability of spatial multiplexing system with ZF equalization.** This figure shows the exact and asymptotic secrecy outage curves for the ZF equalization-based spatial multiplexing system with different numbers of antennas at the legitimate receiver (M_r) and the eavesdropper (M_e), and a fixed number of antennas at the transmitter (M_t). The exact and asymptotic results are labeled with "exact" and "asym.", respectively.

Full-size DOI: 10.7717/peerjcs.186/fig-7

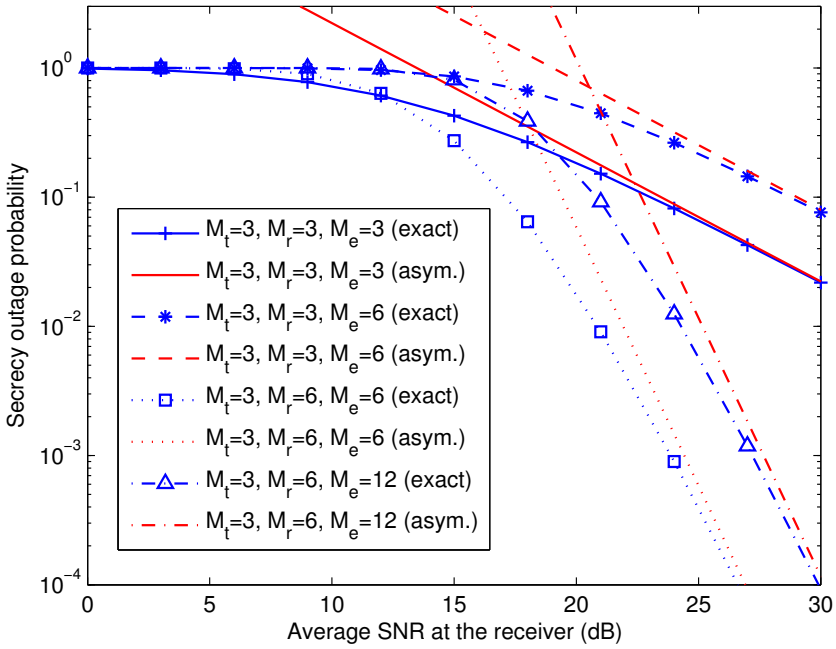

Figure 8 Comparison of exact and asymptotic secrecy outage probability of spatial multiplexing system with MMSE equalization. This figure shows the exact and asymptotic secrecy outage curves for the MMSE equalization-based spatial multiplexing system with different numbers of antennas at the legitimate receiver (M_r) and the eavesdropper (M_e), and a fixed number of antennas at the transmitter (M_t). The exact and asymptotic results are labeled with "exact" and "asym.", respectively.

Full-size DOI: 10.7717/peerjcs.186/fig-8

required to compute $\mathbf{z}_r$ (via power iteration (*Golub & Van Loan, 2013*, Section 7.3)), $\mathbf{w}_t$, and $\mathbf{z}_e$ for the transmit-receive diversity system; (2) the number of flops required to compute $\mathbf{W}_{r,ZF}$ and $\mathbf{W}_{e,ZF}$ for the spatial multiplexing system with ZF equalization; and (3) the number of flops required to compute $\mathbf{W}_{r,MMSE}$ and $\mathbf{W}_{e,MMSE}$ for the spatial multiplexing system with MMSE equalization. The results are given in Table 1, where N is the number of iterations used in the power iteration method.[6] Figure 9 shows the system complexity as a function of M_t for $M_t = M_r = M_e$ and for $M_r = M_e = 2M_t$. From this figure, we see that the computational complexity of the spatial multiplexing system with ZF equalization is comparable to that of the spatial multiplexing system with MMSE equalization, while the transmit-receive diversity system has the highest computational complexity, even with $N = 1$.

[6] In practice, the choice of N depends on the ratio between the magnitude of the second largest eigenvalue of $\mathbf{H}_r\mathbf{H}_r^{\dagger}$ and that of the corresponding largest eigenvalue as it dictates the rate of convergence (see *Golub & Van Loan (2013)*, Section 7.3) for more details).

CONCLUSION

We have presented exact and asymptotic analysis of the secrecy outage probability of the transmit-receive diversity system and spatial multiplexing systems with ZF equalization and MMSE equalization in a Rayleigh-fading MIMO wiretap channel. This asymptotic analysis has shown that the transmit-receive diversity system achieves a secrecy diversity order of M_tM_r, whereas the two spatial multiplexing systems offer the same secrecy diversity order of $M_r - M_t + 1$. Interestingly, all of these secrecy diversity orders do not rely on M_e.

Table 1 System complexity in terms of floating-point operations. This table shows the computational complexity of the transmit-receive diversity system and the spatial multiplexing systems with ZF equalization and MMSE equalization.

System	Number of Flops
Transmit-Receive Diversity	$2M_tM_r^2+2M_tM_r+2M_tM_e+2M_t$ $+(2N-1)M_r^2+2NM_r+2M_e$
Spatial Multiplexing with ZF	$2M_t^2+4M_tM_r+4M_tM_e-M_r-M_e+2$
Spatial Multiplexing with MMSE	$2M_t^2+4M_tM_r+4M_tM_e-M_r-M_e+4$

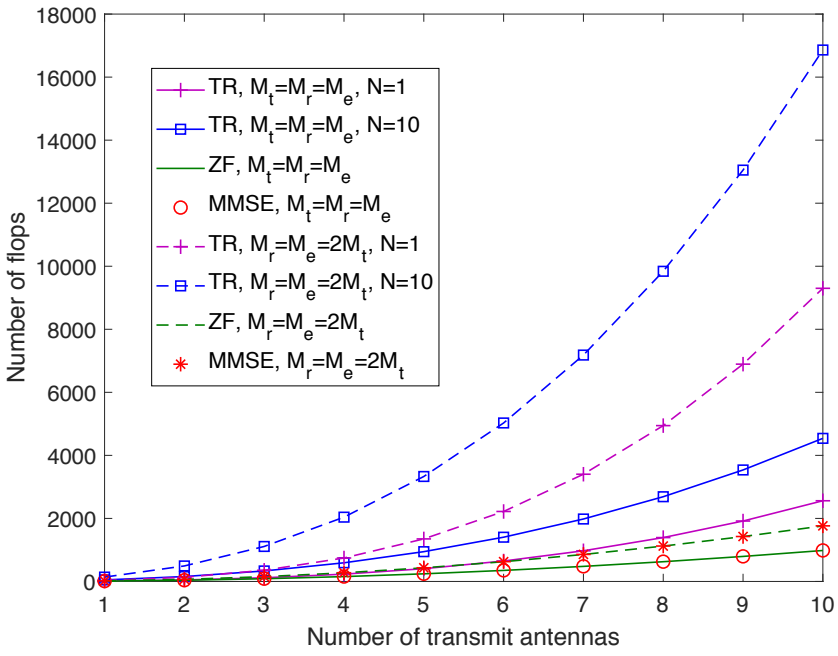

Figure 9 Comparison of system complexity for $M_t = M_r = M_e$ and for $M_r = M_e = 2M_t$. This figure shows the system complexity for the case that the numbers of antennas at the transmitter (M_t), the legitimate receiver (M_r), and the eavesdropper (M_e) are the same, and the case of $M_r = M_e = 2M_t$.
Full-size DOI: 10.7717/peerjcs.186/fig-9

Numerical results based on both theoretical analysis and simulations have demonstrated how M_t, M_r, and M_e affect the secrecy performance of such MIMO systems.

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

The author received no funding for this work.

Competing Interests

The author declares there are no competing interests.

Author Contributions

- Kiattisak Maichalernnukul conceived and designed the experiments, performed the experiments, analyzed the data, contributed reagents/materials/analysis tools, prepared figures and/or tables, performed the computation work, authored or reviewed drafts of the paper, approved the final draft.

Data Availability

The following information was supplied regarding data availability:

Data is available at GitHub: https://github.com/Secrecy1234/peerj.

REFERENCES

Bashar S, Ding Z, Li GY. 2011. On secrecy of codebook-based transmission beamforming under receiver limited feedback. *IEEE Transactions on Wireless Communications* **10(4)**:1212–1223 DOI 10.1109/TWC.2011.020111.100378.

Biglieri E, Calderbank R, Constantinides A, Goldsmith A, Paulraj AJ, Poor HV. 2007. *MIMO wireless communications*. New York: Cambridge University Press.

Bloch M, Barros J, Rodrigues MRD, McLaughlin SW. 2008. Wireless information-theoretic security. *IEEE Transactions on Information Theory* **54(6)**:2515–2534 DOI 10.1109/TIT.2008.921908.

Chen C-J, Wang L-C. 2007. Performance analysis of scheduling in multiuser MIMO systems with zero-forcing receivers. *IEEE Journal on Selected Areas in Communications* **25(7)**:1435–1445 DOI 10.1109/JSAC.2007.070916.

Csiszár I, Körner J. 1978. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory* **24(3)**:339–348 DOI 10.1109/TIT.1978.1055892.

Dighe PA, Mallik RK, Jamuar SS. 2003. Analysis of transmit-receive diversity in Rayleigh fading. *IEEE Transactions on Communications* **51(4)**:694–703 DOI 10.1109/TCOMM.2003.810871.

Dong L, Han Z, Petropulu AP, Poor HV. 2010. Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing* **58(3)**:1875–1888 DOI 10.1109/TSP.2009.2038412.

Ferdinand NS, Da Costa DB, Latva-aho M. 2013. Physical layer security in MIMO OSTBC line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation. *IEEE Wireless Communications Letters* **2(5)**:467–470 DOI 10.1109/WCL.2013.052813.130191.

Foschini GJ. 1996. Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas. *Bell Labs Technical Journal* **1(2)**:41–59 DOI 10.1002/bltj.2015 .

Gallager RG. 2008. *Principles of digital communication*. New York: Cambridge University Press.

Goel S, Negi R. 2008. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications* **7(6)**:2180–2189 DOI 10.1109/TWC.2008.060848.

Golub GH, Van Loan CF. 2013. *Matrix computations*. Baltimore: Johns Hopkins University Press.

Gradshteyn IS, Ryzhik IM. 2000. *Table of integrals, series and products*. New York: Academic Press.

He F, Man H, Wang W. 2011. Maximal ratio diversity combining enhanced security. *IEEE Communications Letters* **15(5)**:509–511 DOI 10.1109/LCOMM.2011.030911.102343.

Heath Jr RW, Lozano A. 2018. *Foundation of MIMO communication*. New York: Cambridge University Press.

Hunger R. 2007. Floating point operations in matrix-vector calculus. Technical report. Department of Electrical and Computer Engineering, Munich: Technical University of Munich.

Jankiraman M. 2004. *Space-time codes and MIMO systems*. Boston: Artech House.

Jiang Y, Li J, Hager WW. 2005. Uniform channel decomposition for MIMO communications. *IEEE Transactions on Signal Processing* **53(11)**:4283–4294 DOI 10.1109/TSP.2005.857052.

Jiang Y, Varanasi MK, Li J. 2011. Performance analysis of ZF and MMSE equalizers for MIMO systems: an in-depth study of the high SNR regime. *IEEE Transactions on Information Theory* **57(4)**:2008–2026 DOI 10.1109/TIT.2011.2112070.

Kalman D. 1984. The maximum and minimum of two numbers using the quadratic formula. *College Mathematics Journal* **15(4)**:329–330 DOI 10.2307/2686400.

Khisti A, Wornell GW. 2010. Secure transmission with multiple antennas–part II: the MIMOME wiretap channel. *IEEE Transactions on Information Theory* **56(11)**:5515–5532 DOI 10.1109/TIT.2010.2068852.

Kumar KR, Caire G, Moustakas AL. 2009. Asymptotic performance of linear receivers in MIMO fading channels. *IEEE Transactions on Information Theory* **55(10)**:4398–4418 DOI 10.1109/TIT.2009.2027493.

Leung-Yan-Cheong SK, Hellman ME. 1978. The Gaussian wire-tap channel. *IEEE Transactions on Information Theory* **24(4)**:451–456 DOI 10.1109/TIT.1978.1055917.

Lin C-H, Tsai S-H, Lin Y-P. 2014. Secure transmission using MIMO precoding. *IEEE Transactions on Information Forensics and Security* **9(5)**:801–813 DOI 10.1109/TIFS.2014.2309211.

Maaref A, Aïssa S. 2005. Closed-form expressions for the outage and ergodic Shannon capacity of MIMO MRC systems. *IEEE Transactions on Communications* **53(7)**:1092–1095 DOI 10.1109/TCOMM.2005.851564.

Maichalernnukul K. 2018. Secrecy capacity analysis of transmit-receive diversity systems. In: *Proceedings of the IEEE statistical signal processing workshop*. IEEE: Freiburg, Piscataway, 159–163 DOI 10.1109/SSP.2018.8450857.

McKay MR. 2006. Random matrix theory analysis of multiple antenna communication systems. PhD dissertation, The University of Sydney, Australia.

Mukherjee A, Swindlehurst AL. 2011. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Transactions on Signal Processing* **59(1)**:351–361 DOI 10.1109/TSP.2010.2078810.

Oggier F, Hassibi B. 2011. The secrecy capacity of the MIMO wiretap channel. *IEEE Transactions on Information Theory* **57(8)**:4961–4972 DOI 10.1109/TIT.2011.2158487.

Ordóñez LG, Palomar DP, Pagès-Zamora A, Fonollosa JR. 2007. High-SNR analytical performance of spatial multiplexing MIMO systems with CSI. *IEEE Transactions on Signal Processing* **55(11)**:5447–5463 DOI 10.1109/TSP.2007.896109.

Palomar DP, Lagunas MA. 2003. Joint transmit-receive space-time equalization in spatially correlated MIMO channels: a beamforming approach. *IEEE Journal on Selected Areas in Communications* **21(5)**:730–743 DOI 10.1109/JSAC.2003.810324.

Papoulis A, Pillai SU. 2002. *Probability, random variables, and stochastic processes*. New York: McGraw-Hill.

Poor HV, Schaefer RF. 2017. Wireless physical layer security. *Proceedings of the National Academy of Sciences of the United States of America* **114(1)**:19–26 DOI 10.1073/pnas.1618130114.

Schaefer RF, Loyka S. 2015. The secrecy capacity of compound Gaussian MIMO wiretap channels. *IEEE Transactions on Information Theory* **61(10)**:5535–5552 DOI 10.1109/TIT.2015.2458856.

Seethaler D, Artés H, Hlawatsch F. 2004. Dynamic nulling-and-cancelling with near-ML performance. In: *Proceedings of the IEEE international conference on acoustics, speech and signal processing*. Montreal, 777–780.

Seethaler D, Artés H, Hlawatsch F. 2005. Detection techniques for MIMO spatial multiplexing systems. *Elektrotechnik und Informationstechnik* **122(3)**:91–96 DOI 10.1007/BF03054042.

Smith PJ. 2007. Exact performance analysis of optimum combining with multiple interferers in flat Rayleigh fading. *IEEE Transactions on Communications* **5(9)**:1674–1677.

Tse D, Viswanath P. 2005. *Fundamentals of wireless communications*. Cambridge: Cambridge University Press.

Wang H-M, Wang C, Ng DWK. 2015. Artificial noise assisted secure transmission under training and feedback. *IEEE Transactions on Signal Processing* **63(23)**:6285–6298 DOI 10.1109/TSP.2015.2465301.

Wang H-M, Wang C, Ng DWK, Lee MH, Xiao J. 2016a. Artificial noise assisted secure transmission for distributed antenna systems. *IEEE Transactions on Signal Processing* **64(15)**:4050–4064 DOI 10.1109/TSP.2016.2558164.

Wang H-M, Zheng T-X, Yuan J, Towsley D, Lee MH. 2016b. Physical layer security in heterogeneous cellular networks. *IEEE Transactions on Communications* **64(3)**:1204–1219 DOI 10.1109/TCOMM.2016.2519402.

Wyner AD. 1975. The wire-tap channel. *The Bell System Technical Journal* **54(8)**:1355–1387 DOI 10.1002/j.1538-7305.1975.tb02040.x.

Yang N, Yeoh PL, Elkashlan M, Schober R, Collings IB. 2013. Transmit antenna selection for security enhancement in MIMO wiretap channels. *IEEE Transactions on Communications* **61(1)**:144–154 DOI 10.1109/TCOMM.2012.12.110670.

Zou Y, Wang X, Shen W. 2013. Physical-layer security with multiuser scheduling in cognitive radio networks. *IEEE Transactions on Communications* **61(12)**:5103–5113 DOI 10.1109/TCOMM.2013.111213.130235.