Enhancing the Secrecy Performance in MIMO Wiretap Channels: A Novel Transmit Antenna Selection Scheme

Nuwan S. Ferdinand[†], Daniel Benevides da Costa[‡], and Matti Latva-aho[†]
[†]Centre for Wireless Communications, University of Oulu, Finland
[‡]Wireless Telecom Research Group (GTEL), Federal University of Ceará (UFC), Ceará, Brazil
Emails: {nuferdin,matla}@ee.oulu.fi, danielbcosta@ieee.org

***Abstract*—In this paper, a novel transmit antenna selection scheme for multiple input multiple output (MIMO) wiretap channels is proposed. This new scheme achieves higher secrecy performance by exploiting eavesdropper's channel state information. The key idea behind our proposal is to perform the antenna selection aiming to maximize the overall secrecy rate instead of maximizing the instantaneous signal-to-noise ratio of the main channel. In our analysis, we assume that the legitimate receiver and the eavesdropper employ a maximal-ratio combining technique to combine the received signals from the transmitter. Considering Nakagami-m fading channels, a closed-form expression for the secrecy outage probability is derived, which can be used as a quality of service metric. Further, an asymptotic analysis is carried out and the diversity/array gains are obtained. The ergodic secrecy rate is also investigated for the case of multiple input single output wiretap channels. Representative numerical examples are plotted and validated through Monte Carlo simulations. Insightful discussions are drawn from the proposed analysis.**

I. Introduction

In wireless communications systems, the security has been traditionally addressed via cryptographic approaches implemented at higher layers of the protocol stack [1], [2]. However, with the advent of infrastructure-less networks, the secret key management may be vulnerable to attacks of malicious users [3]. Owing to this fact, recent advances in the research have proposed to implement the security at the physical layer (PHY) [4]–[9]. The key idea behind this strategy is to exploit the spatial-temporal characteristics of the wireless channel to guarantee secure data transmission. A seminal work was proposed by Winer [4], where the wiretap channel was introduced. Since then, PHY security has received a considerable attention from the wireless community as a way to ensure perfect secrecy along the communication process (see, for example, the most recent papers [5]–[13] and references therein). Relevant works are discussed next.

In [10], assuming that the transmitter (Tx) and the eavesdropper are equipped with multiple antennas, while the legitimate receiver (Rx) is a single-antenna device, a transmit antenna selection (TAS) scheme was proposed to improve the secrecy performance. The antenna selection criterium was based on the channel quality between the Tx and Rx, in which the antenna that maximizes the main channel gain is selected. This work was generalized in [11], where a comprehensive performance study of TAS schemes in multiple-input multiple-output (MIMO) wiretap channels was provided. More specifically, the authors in [11] assumed a Nakagami-m wiretap channel with all nodes being equipped with multiple antennas. The Rx and the eavesdropper employed either a maximal-ratio combining (MRC) or a selection combining (SC) scheme to combine the received signals. Closed-form expressions for the secrecy outage probability were derived, from which the respective diversity/array gains were obtained. It was shown that the diversity order depends solely on the number of antennas at the Tx, the number of antennas at the Rx, and the Nakagami-m fading parameter of the main channel. In [12], the impact of antenna correlation at the Rx and eavesdropper on the secrecy performance of MIMO wiretap channels was examined. Finally, in [13] the effects of outdated channel state information (CSI) on the secrecy outage performance of multiple-input single-output (MISO) Nakagami-m wiretap channels with TAS were investigated.

In this paper, differently from all previous works, we propose a novel TAS scheme for MIMO wiretap channels. The key idea behind our proposal is to exploit eavesdropper's channel state information (CSI) and perform the antenna selection aiming to maximize the overall secrecy rate instead of maximizing the instantaneous signal-to-noise ratio (SNR) of the main channel. To this end, the Tx (called Alice) is assumed to know both the main channel and the eavesdropper's channel, as adopted in several works (i.e., [5]–[7] and references therein). As will be seen, compared to traditional TAS scheme [10], [11], the proposed scheme achieves higher secrecy performance. In our analysis, for illustration purposes, we assume that the Rx (called Bob) and the eavesdropper (called Eve) employ a MRC technique to combine the received signals. In order to analyze the secrecy performance, a closed-form expression for the secrecy outage probability is derived, which can be efficiently used as a quality of service (QoS) metric. Moreover, an asymptotic analysis is carried out and the respective diversity/array gains are obtained. The ergodic secrecy rate is also investigated for the case of MISO wiretap channels. Our analysis allows for non-identical Nakagami-m fading parameters and distinct average SNRs between the main channel and the eavesdropper's channel.

Mathematical Notations and Functions: Vectors are denoted by bold lower case letters, conjugate transpose is denoted by $(\cdot)^\dagger$, $\|\cdot\|$ indicates the Frobenius norm, $\Pr(\cdot)$ symbolizes probability, $f_X(\cdot)$ and $F_X(\cdot)$ stand for, respectively, the probability density function (PDF) and the cumulative distribution

978-1-4577-1348-4/13/$31.00 ©2013 IEEE

function (CDF) of a random variable X, and $\mathbb{E}(\cdot)$ denotes the expectation operator. Furthermore, $\Gamma(\cdot)$ represents the Gamma function [14, Eq. (8.310.1)] and $\mathbf{U}(.,.;.)$ denotes the Tricomi's (confluent hypergeometric) function [14, Eq. (9.211.4)].

II. System Model

Consider a MIMO wiretap channel in which a Tx Alice is equipped with N_{A} multiple antennas, whereas a legitimate Rx Bob and an eavesdropper Eve are equipped with N_{B} and N_{E} antennas, respectively. We consider an active eavesdropper scenario where Alice is assumed to know both Bob's and eavesdropper's CSI [5]–[7]. Both main channel and eavesdropper's channel experience slow fading with same fading block length, which is long enough to allow capacity-achieving codes within each block. Alice uses the CSI from Bob and Eve to select an antenna s that maximizes the secrecy rate[1]. Afterwards, Alice transmits a signal x to Bob using the selected antenna such that the received signal at Bob and Eve can be written, respectively, as

$$\mathbf{y}_{\mathrm{B}} = \sqrt{P}\mathbf{h}_{\mathrm{AB},s}x + \mathbf{n}_{\mathrm{B}}, \tag{1}$$

and

$$\mathbf{y}_{\mathrm{E}} = \sqrt{P}\mathbf{h}_{\mathrm{AE},s}x + \mathbf{n}_{\mathrm{E}}, \tag{2}$$

where $\mathbf{h}_{\mathrm{AB},s}$ and $\mathbf{h}_{\mathrm{AE},s}$ are, respectively, the $N_{\mathrm{B}}\times 1$ and $N_{\mathrm{E}}\times 1$ channel vectors at Bob and Eve from the selected antenna s at Alice, P denotes the transmit power at Alice, $\mathbf{n}_{\mathrm{B}}$ and $\mathbf{n}_{\mathrm{E}}$ are the additive white Gaussian noise vectors at Bob and Eve, respectively, with each element having variance n_B and n_E.

Assuming a MRC scheme, Bob multiplies the received signal by a weight vector $\mathbf{w}_{\mathrm{B}} = \frac{\mathbf{h}_{\mathrm{AB},s}^{\dagger}}{\|\mathbf{h}_{\mathrm{AB},s}\|}$ and the resulting signal y_{B} can be written as

$$y_{\mathrm{B}} = \sqrt{P}\|\mathbf{h}_{\mathrm{AB},s}\|x + \mathbf{w}_{\mathrm{B}}\mathbf{n}_{\mathrm{B}}. \tag{3}$$

Thus, the received SNR at Bob can be expressed as $\gamma_{B,s} = \bar{\gamma}_B\|\mathbf{h}_{\mathrm{AB},s}\|^2$, with $\bar{\gamma}_B = P/n_B$. Similarly, the received signal at Eve can be written as

$$y_{\mathrm{E}} = \sqrt{P}\|\mathbf{h}_{\mathrm{AE},s}\|x + \mathbf{w}_{\mathrm{E}}\mathbf{n}_{\mathrm{E}}, \tag{4}$$

where the received SNR at Eve can be expressed as $\gamma_{E,s} = \bar{\gamma}_E\|\mathbf{h}_{\mathrm{AE},s}\|^2$, with $\bar{\gamma}_E = P/n_E$.

III. The Proposed Transmit Antenna Selection Scheme

Let $R_{E,s} = \log_2(1+\gamma_{B,s})$ and $R_{E,s} = \log_2(1+\gamma_{E,s})$ be the achievable rates at Bob and Eve, respectively. The network secrecy rate $R_{S,s}$ can be expressed as

$$R_{S,s} = \begin{cases} R_{B,s} - R_{E,s}, & \gamma_{B,s} > \gamma_{E,s}, \\ 0, & \gamma_{B,s} \leq \gamma_{E,s}. \end{cases} \tag{5}$$

Relying on the maximization of the secrecy rate given in (5), we propose a new strategy to perform the antenna selection at Alice. More specifically, Alice will select the antenna s that maximizes the secrecy rate, i.e.,

$$s = \arg\max_{k} R_{S,k}. \tag{6}$$

[1]Assume for now that the antenna selection at Alice was performed. This selection process will be explained in the next section.

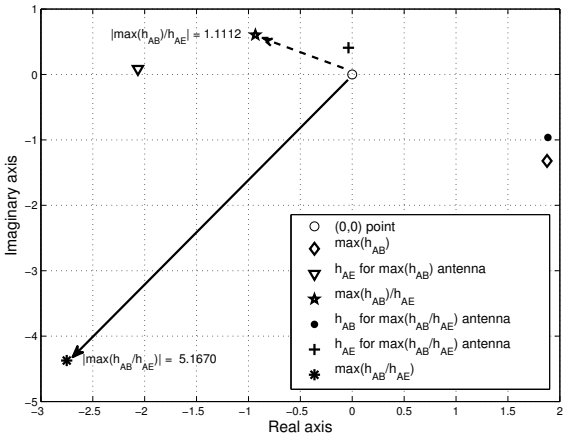

Fig. 1. Cartesian diagram of randomly generated channel vectors. We consider $N_{\mathrm{A}} = 20$, $N_{\mathrm{B}} = N_{\mathrm{E}} = 1$ and generate two complex Gaussian $N_{\mathrm{A}} \times 1$ random vectors, $\mathbf{h}_{\mathrm{AB}}$ and $\mathbf{h}_{\mathrm{AE}}$, to obtain the plot.

Then, by substituting (5) into (6) and after some mathematical simplifications, the antenna selection rule at Alice can be written as

$$s = \arg\max_{k}\left(\frac{1+\gamma_{B,k}}{1+\gamma_{E,k}}\right), \tag{7}$$

where $\gamma_{B,k}$ and $\gamma_{E,k}$ symbolize the instantaneous SNR at Bob and Eve, respectively, from the k^{th} transmit antenna of Alice.

In order to get some insights of the proposed TAS scheme, Fig. 1 shows the cartesian diagram of randomly generated channel vectors to illustrate the advantage of knowing both Bob's and Eve's CSI over the traditional TAS scheme using only Bob's CSI [10], [11]. Note that although the selected antenna using only Bob's CSI (represented by diamond) has higher gain than the proposed scheme (indicated by the black circle), the former scheme also has higher gain for Eve's direction (represented by inverted triangle) than our scheme (indicated by the cross). Therefore, computing these two information jointly and taking the ratio of the channel gains, it can be seen that $\max(\mathbf{h}_{AB}/\mathbf{h}_{AE})$ (which is the essence of the proposed TAS scheme) has a higher gain than $\max(\mathbf{h}_{AB})/\mathbf{h}_{AE}$ (the base of TAS schemes which uses only Bob's CSI). This results in a higher secrecy rate for the proposed TAS scheme.

IV. Secrecy Performance

Assuming that all the links undergo Nakagami-m fading, the PDFs of $\gamma_{B,k}$ and $\gamma_{E,k}$ are given by [15]

$$f_{\gamma_{B,k}}(z) = \frac{m_{\mathrm{B}}^{m_{\mathrm{B}}N_{\mathrm{B}}} z^{m_{\mathrm{B}}N_{\mathrm{B}}-1}}{\bar{\gamma}_B^{m_{\mathrm{B}}N_{\mathrm{B}}}\Gamma(N_{\mathrm{B}}m_{\mathrm{B}})} e^{-\frac{m_{\mathrm{B}}z}{\bar{\gamma}_B}}, \tag{8}$$

$$f_{\gamma_{E,k}}(z) = \frac{m_{\mathrm{E}}^{m_{\mathrm{E}}N_{\mathrm{E}}} z^{m_{\mathrm{E}}N_{\mathrm{E}}-1}}{\bar{\gamma}_E^{m_{\mathrm{E}}N_{\mathrm{E}}}\Gamma(N_{\mathrm{E}}m_{\mathrm{E}})} e^{-\frac{m_{\mathrm{E}}z}{\bar{\gamma}_E}}, \tag{9}$$

where m_{B} and m_{E} denote the Nakagami-m fading parameters of the main channel and eavesdropper channel, respectively.

A. Secrecy Outage Probability

We assumed Alice has both Bob's and Eve's CSI, hence, Alice can adjust her rate such that there will not be an outage. However, to analyze the system performance as QoS perspective, it is important to know what is the average rate that Alice can transmit without an outage and how much diversity/ array gains can be obtained. Hence, here we derive the exact closed form expression for outage probability, which is defined as the probability that $R_{S,s}$ drops below a predefined secrecy rate threshold R and it can be mathematically formulated as

$$P_s(R) = \Pr\left(R_{S,s} < R | \gamma_{B,s} > \gamma_{E,s}\right) + \Pr\left(\gamma_{B,s} < \gamma_{E,s}\right). \quad (10)$$

By substituting $R_{S,s}$ into (10) and after some algebraic manipulations, we obtain

$$P_s(R) = \Pr\left(\frac{\gamma_{B,s}+1}{\gamma_{E,s}+1} < 2^R \middle| \frac{\gamma_{B,s}+1}{\gamma_{E,s}+1} > 1\right) + \Pr\left(\frac{\gamma_{B,s}+1}{\gamma_{E,s}+1} < 1\right). \quad (11)$$

Now, using the concepts of probability theory, it follows that

$$P_s(R) = F_{\gamma_s}\left(2^R\right), \quad (12)$$

where

$$\gamma_s = \frac{\gamma_{B,s}+1}{\gamma_{E,s}+1} = \max_k \gamma_k = \max_k \left(\frac{\gamma_{B,k}+1}{\gamma_{E,k}+1}\right). \quad (13)$$

Hence, the secrecy outage probability can be rewritten as

$$P_s(R) = F_{\gamma_s}\left(2^R\right) = \left[F_{\gamma_k}\left(2^R\right)\right]^{N_\mathrm{A}}, \quad (14)$$

in which

$$F_{\gamma_k}(z) = \int_1^\infty F_{\gamma_{B,k}+1}(zx) f_{\gamma_{E,k}+1}(x) dx. \quad (15)$$

Thus, from (8) and (9), and relying on the statistical standard procedure of transformation of variates, (15) can be attained, yielding

$$P_s(R) = \left[1 - \left(\frac{m_\mathrm{E}}{\bar{\gamma}_E}\right)^{m_\mathrm{E}N_\mathrm{E}} \sum_{i=0}^{m_\mathrm{B}N_\mathrm{B}-1} \frac{1}{i!}\left(\frac{m_\mathrm{B}}{\bar{\gamma}_B}\right)^i \sum_{k=0}^{i}\binom{i}{k} \times \frac{\Gamma(m_\mathrm{E}N_\mathrm{E}+k) 2^{Rk}(2^R-1)^{i-k} e^{-\frac{m_\mathrm{B}(2^R-1)}{\bar{\gamma}_B}}}{\Gamma(m_\mathrm{E}N_\mathrm{E})\left(\frac{m_\mathrm{B}2^R}{\bar{\gamma}_B}+\frac{m_\mathrm{E}}{\bar{\gamma}_E}\right)^{m_\mathrm{E}N_\mathrm{E}+k}}\right]^{N_\mathrm{A}}. \quad (16)$$

By setting $m_\mathrm{B} = m_\mathrm{E} = 1$ in (16), the secrecy outage probability for Rayleigh fading can be derived as

$$P_s(R) = \left[1 - \left(\frac{1}{\bar{\gamma}_E}\right)^{N_\mathrm{E}} \sum_{i=0}^{N_\mathrm{B}-1} \frac{1}{i!}\left(\frac{1}{\bar{\gamma}_B}\right)^i \sum_{k=0}^{i}\binom{i}{k} \times \frac{\Gamma(N_\mathrm{E}+k) 2^{Rk}(2^R-1)^{i-k} e^{-\frac{(2^R-1)}{\bar{\gamma}_B}}}{\Gamma(N_\mathrm{E})\left(\frac{2^R}{\bar{\gamma}_B}+\frac{1}{\bar{\gamma}_E}\right)^{N_\mathrm{E}+k}}\right]^{N_\mathrm{A}}. \quad (17)$$

Now, considering the case where both Bob and Eve are single-antenna devices (MISO scenario) and undergo Rayleigh fading, the secrecy outage probability for this scenario can be obtained by setting $N_\mathrm{B} = N_\mathrm{E} = 1$ in (17), i.e.,

$$P_s(R) = \left[1 - \frac{1}{\bar{\gamma}_E} e^{-\frac{(2^R-1)}{\bar{\gamma}_B}} \left(\frac{2^R}{\bar{\gamma}_B} + \frac{1}{\bar{\gamma}_E}\right)^{-1}\right]^{N_\mathrm{A}}. \quad (18)$$

B. Ergodic secrecy rate for MISO Scenario

Knowing that an exact analysis of the ergodic secrecy rate is mathematically intractable for the more general case, next we derive an approximate expression for this metric assuming Rayleigh fading and $N_\mathrm{B} = N_\mathrm{E} = 1$ (MISO scenario).

Firstly, by using the binomial theorem to expand (18) and after some algebraic manipulations, the CDF of γ_s, given in (13), can be derived as

$$F_{\gamma_s}(z) = 1 - \sum_{p=1}^{N_\mathrm{A}} \binom{N_\mathrm{A}}{p} (-1)^{p-1} e^{\frac{p}{\bar{\gamma}_B}} \left(\frac{\bar{\gamma}_B}{\bar{\gamma}_E}\right)^p e^{-\frac{pz}{\bar{\gamma}_B}} \times \left(z + \frac{\bar{\gamma}_B}{\bar{\gamma}_E}\right)^{-p}. \quad (19)$$

Defining the ergodic secrecy rate as

$$R_{s,\mathrm{erg}} = \mathbb{E}\left(\log_2 \gamma_s\right), \quad (20)$$

note that the evaluation of the above expectation is mathematically intractable due to the $\log_2$ function. In order to provide an efficient way to examine the ergodic secrecy rate, we propose a tight approximation for this metric which relies on the Taylor's series of the function $\log_2(\gamma_s)$. In this case, a second-order approximation for $R_{s,\mathrm{erg}}$ can be attained as

$$R_{s,\mathrm{erg}} \approx \log_2(e)\left[\ln(\mathbb{E}(\gamma_s)) - \frac{\mathbb{E}(\gamma_s^2) - \mathbb{E}(\gamma_s)^2}{2\mathbb{E}(\gamma_s)^2}\right]. \quad (21)$$

By its turn, the generalized moments of γ_s can be derived as

$$\mathbb{E}(\gamma_s^h) = h! \sum_{p=1}^{N_\mathrm{A}} \binom{N_\mathrm{A}}{p} (-1)^{p-1} e^{\frac{p}{\bar{\gamma}_B}} \left(\frac{\bar{\gamma}_B}{\bar{\gamma}_E}\right)^h \times \mathbf{U}\left(h, h+1-p, \frac{p}{\bar{\gamma}_E}\right). \quad (22)$$

Finally, from (22), the first and second moments of γ_s can be easily obtained such that the ergodic secrecy rate can be evaluated.

V. Secrecy Asymptotic Analysis

In this part, the secrecy performance is analyzed at high SNR regions. Our results are compared with the traditional TAS scheme given in [11] and we quantify the performance gain difference that exists in these two TAS schemes. Here, we consider that the Bob's average SNR is significantly higher than the Eve's average SNR, i.e., $\bar{\gamma}_B >> \bar{\gamma}_E$.

In order to characterize the secrecy performance at high SNR, we first derive the CDF of $\gamma_{B,k}$ when $\bar{\gamma}_B \to \infty$. In this case, it can be obtained by expanding the exponential function using Taylor series and taking the first non-zero order term,

which simplifies to

$$\lim_{\bar{\gamma}_B \to \infty} F_{\gamma_{B,k}}(z) = \frac{m_{\mathrm{B}}^{m_{\mathrm{B}}N_{\mathrm{B}}}}{(m_{\mathrm{B}}N_{\mathrm{B}})!}\left(\frac{z}{\bar{\gamma}_B}\right)^{m_{\mathrm{B}}N_{\mathrm{B}}} + o\left[\left(\frac{z}{\bar{\gamma}_B}\right)^{m_{\mathrm{B}}N_{\mathrm{B}}+1}\right]. \quad (23)$$

Thus, by substituting (23) and (9) into (15), we obtain

$$P_s^{\infty}(R) = (\mathbf{A}\bar{\gamma}_B)^{-\mathbf{D}} + o\left(\bar{\gamma}_B^{-\mathbf{D}+1}\right), \quad (24)$$

where $\mathbf{D} = m_{\mathrm{B}}N_{\mathrm{B}}N_{\mathrm{A}}$ is the diversity gain and $\mathbf{A}$ represents the array gain of the considered system. In particular, the array gain can be expressed as

$$\mathbf{A} = \left(\frac{m_{\mathrm{B}}^{m_{\mathrm{B}}N_{\mathrm{B}}}}{(m_{\mathrm{B}}N_{\mathrm{B}})!}\sum_{s=0}^{m_{\mathrm{B}}N_{\mathrm{B}}}\binom{m_{\mathrm{B}}N_{\mathrm{B}}}{s}\frac{(2^R-1)^{m_{\mathrm{B}}N_{\mathrm{B}}-s}2^{sR}}{\Gamma(m_{\mathrm{E}}N_{\mathrm{E}})} \times\Gamma(m_{\mathrm{E}}N_{\mathrm{E}}+s)\left(\frac{m_{\mathrm{E}}}{\bar{\gamma}_E}\right)^{-s}\right)^{-\frac{1}{m_{\mathrm{B}}N_{\mathrm{B}}}}. \quad (25)$$

Note that, for Rayleigh fading, the diversity gain reduces to $\mathbf{D} = N_{\mathrm{B}}N_{\mathrm{A}}$ and the array gain can be simplified as

$$\mathbf{A} = \left(\frac{1}{N_{\mathrm{B}}!}\sum_{s=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{s}\frac{(2^R-1)^{N_{\mathrm{B}}-s}2^{sR}}{\Gamma(N_{\mathrm{E}})} \times\Gamma(N_{\mathrm{E}}+s)\left(\frac{1}{\bar{\gamma}_E}\right)^{-s}\right)^{-\frac{1}{N_{\mathrm{B}}}}. \quad (26)$$

Finally, by setting $N_{\mathrm{B}} = N_{\mathrm{E}} = 1$ in (26), it can be seen that the diversity gain equals to $\mathbf{D}_{\mathrm{MISO}} = N_{\mathrm{A}}$ and the array gain is given by

$$\mathbf{A}_{\mathrm{MISO}} = \left(\left(2^R-1\right) + 2^R\bar{\gamma}_E\right)^{-1}. \quad (27)$$

From the above analysis, firstly note that the diversity order for Nakagami-m fading remains the same (i.e., $m_{\mathrm{B}}N_{\mathrm{B}}N_{\mathrm{A}}$) as [11]. However, as will be verified from the plots, the secrecy performance is considerably improved due to the array gains when compare to [11].

It is further interesting to compare analytically the proposed scheme with the traditional TAS scheme presented in [10], [11]. Although considering the ratio for the more general scenario is possible, herein we consider a MISO scheme for comparison purposes since our intention is to compare the antenna selection schemes at Alice. By setting $N_{\mathrm{B}} = N_{\mathrm{E}} = 1$ and $m_{\mathrm{B}} = m_{\mathrm{E}} = 1$ in [11, Eq. (27)], the MISO array gain of $\mathbf{\Psi}_{\mathrm{MISO}}$, proposed in [10], [11] is attained. Thus, by taking the ratio between $\mathbf{A}_{\mathrm{MISO}}$ and $\mathbf{\Psi}_{\mathrm{MISO}}$, and after some simplifications, we arrive at

$$\frac{\mathbf{A}_{\mathrm{MISO}}}{\mathbf{\Psi}_{\mathrm{MISO}}} = \left(\frac{\sum_{p=0}^{N_{\mathrm{A}}}\binom{N_{\mathrm{A}}}{p}\frac{2^{Rp}\bar{\gamma}_E^p}{(2^R-1)^p}\Gamma(p+1)}{\sum_{p=0}^{N_{\mathrm{A}}}\binom{N_{\mathrm{A}}}{p}\frac{2^{Rp}\bar{\gamma}_E^p}{(2^R-1)^p}}\right)^{\frac{1}{N_{\mathrm{A}}}}. \quad (28)$$

It can be proved from (28) that $\mathbf{A}_{\mathrm{MISO}} > \mathbf{\Psi}_{\mathrm{MISO}}$. Let $G = 10\log\left(\frac{\mathbf{A}_{\mathrm{MISO}}}{\mathbf{\Psi}_{\mathrm{MISO}}}\right)$dB be the secrecy performance gain. Note that G is dependent on N_{A}, R and $\bar{\gamma}_E$. Moreover, it is more sensitive to N_{A} than R or $\bar{\gamma}_E$ and it increases with N_{A}.

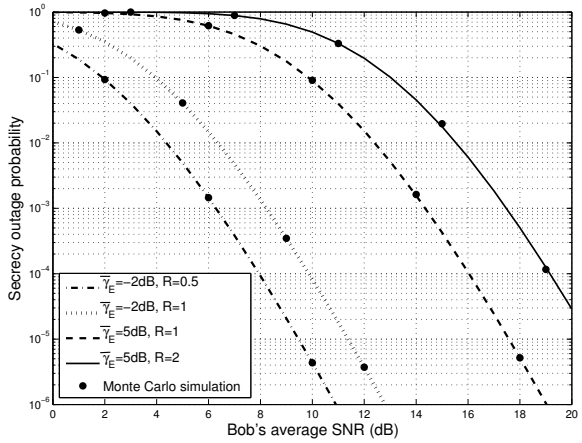

Fig. 2. Secrecy outage probability versus Bob's average SNR for different Eve's average SNR ($N_{\mathrm{A}} = N_{\mathrm{B}} = N_{\mathrm{E}} = 2$ and $m_{\mathrm{B}} = m_{\mathrm{E}} = 2$).

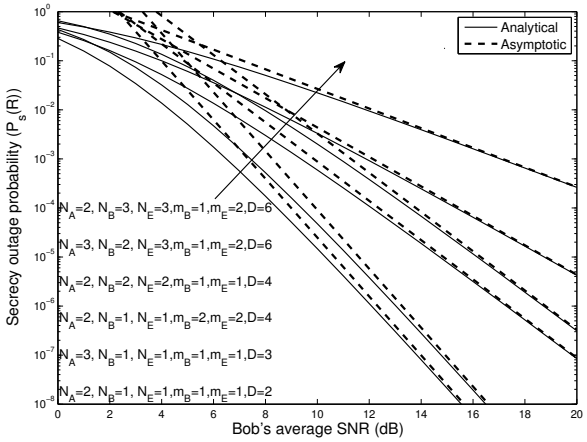

Fig. 3. Secrecy outage probability versus Bob's average SNR ($R = 1$, $\bar{\gamma}_E = -5$dB).

VI. Numerical Results and Discussions

In this Section, representative numerical results are presented in order to illustrate the usefulness of the proposed TAS scheme and get several insights of paramount importance for the system design of MIMO wiretap channels.

Fig. 2 shows the secrecy outage probability versus the Bob's average SNR ($\bar{\gamma}_B$) for different Eve's average SNR ($\bar{\gamma}_E$) and by setting $N_{\mathrm{A}} = N_{\mathrm{B}} = N_{\mathrm{E}} = 2$ and $m_{\mathrm{B}} = m_{\mathrm{E}} = 2$. Two different Eve's average SNR ($\bar{\gamma}_E = -2$dB, 5dB) curves are plotted and one can notice from the two middle curves that the secrecy performance increases when the $\bar{\gamma}_E$ decreases. Furthermore, curves are plotted for different secrecy threshold (R) and it is observed that increasing the threshold also increases the secrecy outage. In addition, Monte Carlo results are included to corroborate the proposed analysis. We have omitted the simulation results in most of the next figures in order to reduce the ambiguity of following the legends.

The secrecy outage probability as a function of the Bob's average SNR is depicted in Fig. 3. We set $R = 1$ and

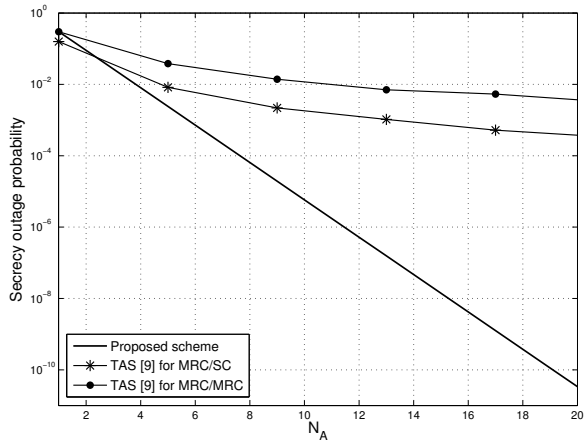

Fig. 4. Secrecy outage probability versus Alice's number of antennas ($N_{\rm B} = N_{\rm E} = 2$, $m_{\rm B} = m_{\rm E} = 2$, $R = 1$, $\bar{\gamma}_E = 5$dB, and $\bar{\gamma}_B = 10$dB).

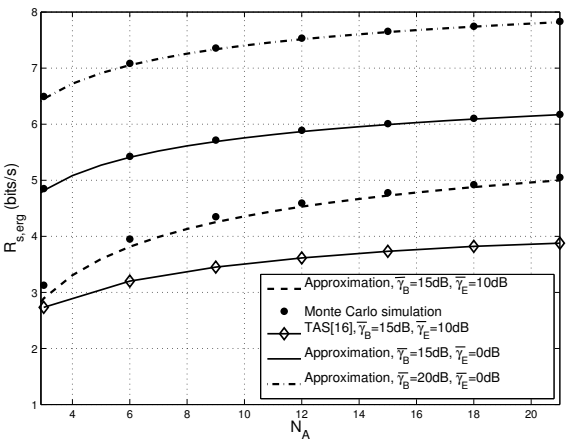

Fig. 5. Ergodic secrecy rate versus number of antennas at Alice.

$\bar{\gamma}_E = -5$dB. When following the legends, it should be noted that different parameters for the analytical curves are ordered as the direction of arrows, e.g., the n^{th} set of parameters are for the n^{th} analytical curve in the direction of the arrow. Secrecy asymptotic curves are plotted and show to be very tight at high SNR regions, validating our analysis. In addition, the diversity gain of $m_{\rm B}N_{\rm B}N_{\rm A}$ can be verified. As expected, there is an improvement on secrecy performance with the increase of $N_{\rm A}, N_{\rm B}, m_{\rm B}$ and $\bar{\gamma}_B$. On the other hand, the secrecy performance decreases with the increase of $N_{\rm E}$ and $m_{\rm E}$. From the two leftmost curves, note that the $\{N_{\rm A} = 2, N_{\rm B} = 3\}$ case outperforms the $\{N_{\rm A} = 3, N_{\rm B} = 2\}$ case, although, both schemes have the same diversity order. This behavior is due to the fact that Bob is using MRC in both cases, and increasing $N_{\rm B}$ also increases the MRC gain. Note that the MRC gain is higher than the antenna selection gain obtained by having higher $N_{\rm A}$ at Alice. Furthermore, it can be noticed from Fig. 3 that due to the MRC gain, the $\{N_{\rm B} = 2, N_{\rm E} = 2, m_{\rm B} = 1, m_{\rm E} = 1\}$ case outperforms the $\{N_{\rm B} = 1, N_{\rm E} = 1, m_{\rm B} = 2, m_{\rm E} = 2\}$ one, although it has the same diversity order (i.e., 4).

Fig. 4 plots the secrecy outage probability versus the number of antennas at Alice by setting $N_{\rm B} = N_{\rm E} = 2$, $m_{\rm B} = m_{\rm E} = 2$, $R = 1$, $\bar{\gamma}_E = 5$dB, and $\bar{\gamma}_B = 10$dB. For comparison purposes, we have simulated the TAS scheme presented in [11] for MRC/MRC and MRC/SC systems. Note that the TAS scheme [11] lags behind in the performance and improvement of secrecy outage is only marginal with the increase of $N_{\rm A}$. This clearly indicates how much performance improvement can be obtained from our proposed TAS scheme.

Finally, Fig. 5 shows the ergodic secrecy rate versus the number of antennas at Alice. Monte Carlo simulations are performed and the derived approximate expressions are compatible with the simulation results. As expected, it is observed from the two top-most curves that the increase of $\bar{\gamma}_B$ increases the ergodic secrecy rate. Similarly, the increase of ergodic secrecy rate is observed with the decrease of $\bar{\gamma}_E$ in the two middle curves. For illustration purposes, we provide a comparison of the proposed method with the TAS scheme presented in [11], as can be observed in the two lowest curves. Note that, for $N_{\rm A} = 20$, the proposed scheme outperforms [11] around 1bit/s.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Technol. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, "Identity-based key management in mobile ad hoc networks: techniques and applications," *IEEE Wireless Commun.*, vol. 15, pp. 46–52, Oct. 2008.

[3] B. Schneier, "Cryptographic design vulnerabilities," *IEEE Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

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

[5] A. Khisti and G. Wornell, "Secure transmission with multiple antennas - part II: The MIMOME wire-tap channel," *IEEE Trans. Inf. Theory,* vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

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

[7] Sabrina G. , C. Scheunert and E. A. Jorswieck, "Secrecy Outage in MISO Systems With Partial Channel Information," *IEEE Trans. on Info. Forensic and Security*, vol. 7, no. 2, 704-716, Apr. 2012

[8] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory,* vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[9] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," *ISIT 2006*, pp. 356–360, Jul. 2006.

[10] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372-375, June 2012.

[11] N. Yang, P. Yeoh, M. Elkashlan, R. Schober and I. Collings,"Transmit antenna selection for security Enhancement in MIMO wiretap channels", *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144-154, Jan. 2013.

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

[13] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection", *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864-867, May. 2013.

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

[15] M. K. Simon and M.-S. Alouini, *Digital Communications over Fading Channels: A Unified Approach to Performance Analysis*, 1st ed., New York: John Wiley and Sons, 2000.