IET Communications

Research Article

IET Journals
The Institution of Engineering and Technology

Physical layer security using massive multiple-input and multiple-output: passive and active eavesdroppers

ISSN 1751-8628
Received on 5th March 2015
Revised on 5th August 2015
Accepted on 24th September 2015
doi: 10.1049/iet-com.2015.0216
www.ietdl.org

Azzam Al-nahari ✉

Department of Electrical Engineering, Ibb University, Ibb, Yemen
✉ *E-mail: azzamyn@gmail.com*

Abstract: Physical layer security is considered as a promising technique that exploits the channel properties in order to send confidential messages to the legitimate receiver even in the presence of a powerful eavesdropper and the absence of its channel information. In this study, the authors consider the effect of massive multiple-input and multiple-output (MMIMO) system operating in TDD mode in improving the physical layer security in the presence of multi-antennas eavesdropper. The channel state information (CSI) of the eavesdropper is assumed not known at the transmitter side, and also imperfect CSI of the legitimate receiver is assumed. The first important finding is that MMIMO is a valuable technique to combat passive eavesdropping, where it is shown that the achievable secrecy rate increases logarithmically with the number of transmit antennas. However, the eavesdropper can be active and attack the training phase of the legitimate transmitter. As a consequence, this dramatically reduces the achievable secrecy rate. The second contribution of this study is a simple protocol that can effectively detect this attack so that a countermeasure can be taken. Closed-form expressions for the detection and false-alarm probabilities are derived. Moreover, the authors analyse the intercept probability and show that asymptotically exponential diversity is achieved.

1 Introduction

The broadcast nature of wireless communications presents two main challenges; namely, fading due to multipath propagation, and the possibility of overhearing the transmitted information by unintended receivers, known as eavesdroppers. The traditional techniques for information security are based on cryptography technology. The physical layer security is an emerging technique that exploits the channel variations to confidentially communicate with the legitimate destination while the eavesdropper cannot interpret the source information, without any assumptions for the eavesdropper nodes (computational power, available information) and without relying on the conventional higher layer encryption [1, 2]. Depending on the working mode as a receiver or a transmitter, the eavesdropper can be classified, respectively, as (i) passive eavesdropper that tries only to interpret the information intended to another user in the system [1], or (ii) an active (malicious) eavesdropper that has the ability to destroy the information received at the legitimate transmitter (e.g. the base station in the training phase) and/or the intended user [3, 4].

Massive multiple-input-multiple-output (MMIMO) technique has recently emerged as a candidate for next generation wireless systems and is today a hot topic in this field [5, 6]. An important aspect of MMIMO that has yet only received limited attention in existing literature is its role in physical layer security [7–9]. In [7], a MMIMO technique is used to encrypt a secret key between the transmitter and the legitimate receiver. In [8], different linear precoding techniques were considered for secure communication but both the number of antennas and the number of users grow to infinity with fixed ratio which is somewhat different from the concept of MMIMO where the number of base station antennas grows to infinity with small number of users. In [9], a regularised channel inversion precoding for secure transmission in the cellular systems is proposed and analysed. A large system analysis was also presented with the same assumptions as in [8], and the optimal value of the base station deployment density that maximises the secrecy rate was derived.

In this paper, we will consider the MMIMO for physical layer security in the presence of multi-antenna eavesdropper that try to intercept the information intended for a legitimate receiver. We consider two cases of the eavesdropper: passive eavesdropper that overhear the transmitted signal but does not send any signal, and active eavesdropper that attack the training phase of the legitimate user. In both cases, the channel state information of the eavesdropper is assumed unknown at the transmitter side. We make the important observation that MMIMO is grossly more robust against passive eavesdropping than normal (small) MIMO is. This observation is a game changer for the eavesdropper as it must change from a passive listening-only mode, into an active mode in order to be able to attack the security of the MMIMO system. The eavesdropper must attack the training phase of the MMIMO system. In this case (active eavesdropping), we propose a simple detection scheme to determine whether the eavesdropper is present or not and study its performance by analysing the detection and false-alarm probabilities. Moreover, we analyse the intercept probability of this system with passive eavesdropper and derive a closed-form expression of the intercept probability, from which it can be seen that a diversity order equal to the number of transmit antennas is achieved. With asymptotically unlimited number of transmitted antennas, it is shown that exponential secrecy diversity is achieved.

It should be noted that this attack has been studied in [4] and goes under the name 'pilot attack'. However, the proposed technique in this paper has two main differences compared with this system mode. First, in the case of passive eavesdropper, it has been shown in [4] that in order to prevent the eavesdropper from intercepting the information, a randomised precoding technique that was proposed in [10] is used, which is more appropriate with the BPSK modulation. In this paper, this advantage is obtained by exploiting the property of channel hardening when using MMIMO system with simple matched filter precoding, without the need of using the randomised precoding and regardless of the modulation type. About zero rate is achieved at the eavesdropper side due to the channel hardening properties of MMIMO system. Second, there are no countermeasures taken in [4], but we will propose a simple protocol to determine whether an active eavesdropper is present or not using also the channel properties of MMIMO. Moreover, multi-antennas eavesdropper is considered. Moreover, it

should be noted that the phenomenon of pilot contamination discussed in [5, 11], where the pilot signal suffers from interference arising from the users in the neighbouring cells is somewhat similar to the pilot attack. The principal difference is that in the later case the attack is intentional malicious attack in order to get as much information as possible as we will see later, whereas pilot contamination is due to the frequency reuse.

The rest of this paper is organised as follows. In Section 2, the system and channel models are introduced. In Section 3, we present the performance analysis of the secrecy rate with passive and active eavesdroppers. The proposed detection scheme is presented and analysed in Section 4. In Section 5, the intercept probability and secrecy diversity order are presented. Section 6 presents the numerical and simulation results. Finally, Section 7 gives the concluding remarks.

Notation: $(.)^{\mathrm{T}}$ and $(.)^{\mathrm{H}}$denote transpose and Hermitian transpose operations, respectively. Moreover, $[x]^{+} = \max(0, x)$, $E[.]$ denotes expectation, and tr(.) denotes trace of the matrix.

2 System and channel models

We consider the transmission between a legitimate transmitter, Alice, equipped with an array of M-antennas, single-antenna intended user, Bob, in the presence of an eavesdropper, Eve with N antennas, as shown in Fig. 1. The wireless channels between the three terminals experience small-scale as well as large-scale fading. The transmitter Alice here may represent the base station, but instead we used the conventional security notations for the purpose of simplicity of presentation. We model the transmission channel between Alice and Bob as $\sqrt{\beta_{\mathrm{AB}}}\boldsymbol{h}_{\mathrm{AB}}$, where β_{AB} is a scalar random variable which models the large-scale fading between Alice and Bob, and $\boldsymbol{h}_{\mathrm{AB}}$ is an $1 \times M$ vector comprising independent and identically distributed (i.i.d) circularly symmetric complex Gaussian random variables, each one with unit variance and zero mean. Similarly, the channel between Alice and the Eve is given by $\sqrt{\beta_{\mathrm{AE}}}\boldsymbol{H}_{\mathrm{AE}}$, where $\boldsymbol{H}_{\mathrm{AE}}$ is an $N \times M$ matrix, where each element has the same distribution as the elements of $\boldsymbol{h}_{\mathrm{AB}}$. The ith row of $\boldsymbol{H}_{\mathrm{AE}}$ is denoted as $\boldsymbol{h}_{\mathrm{AE}_i}$, which represents the channel vector between Alice and the ith antenna at Eve. Many techniques can be used at Eve to decode the received signal such as maximum ratio combining, antenna selection (AS), minimum mean square error, and so on. In this paper, we consider AS, where Eve select the antenna that gives the maximum signal-to-noise ratio (SNR) at his receiver side.

A fully reciprocal TDD system is assumed. As a result, both uplink and downlink channels are perfectly reciprocal. In this case, $\boldsymbol{h}_{\mathrm{AB}} = \boldsymbol{h}_{\mathrm{BA}}^{\mathrm{T}}$. To do beamforming in the downlink (and more generally, user separation via precoding if there is more than one user present in the system), Bob transmits a pilot symbol x_{p} to Alice so that the downlink channel can be estimated at Alice. Furthermore, we assume that Eve operates in half-duplex mode.

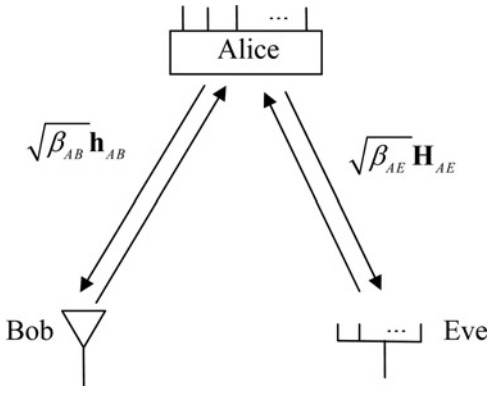

Fig. 1 *System model*

2.1 Training phase

In this phase, Alice estimates the channel to Bob. Since we assume TDD system, the channel can be obtained by sending training pilots from Bob to Alice, and this estimated channel is used in the precoding for data transmission to Bob. In this and the following subsection, we assume that Eve is passive. In other words, Eve is operating in the receive mode only and does not transmit any signal in the training phase. The received signal at Alice is given by

$$\boldsymbol{y}_{\mathrm{Ap}} = \sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}x_{\mathrm{p}} + \boldsymbol{n}_{\mathrm{p}} \tag{1}$$

where P_{B} is the transmitted power per symbol at Bob, and x_{p} is the pilot signal. $\boldsymbol{n}_{\mathrm{p}}$ denotes the additive white Gaussian noise vector of elements of zero mean and variance $N_{0,\mathrm{A}}$. For simplicity, and without loss of generality, we shall assume that $E[|x_{\mathrm{p}}|^2] = 1$. If we assume least square channel estimation, then the estimated channel at Alice is given by

$$\begin{aligned}\hat{\boldsymbol{h}} &= \left(\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}} + \boldsymbol{n}_{\mathrm{p}}\right)^{\mathrm{T}} \\ &= \sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{AB}} + \boldsymbol{n}\end{aligned} \tag{2}$$

Alice now constructs an $M \times 1$ precoding vector $\boldsymbol{w}$ as a scaled version of matched filter as

$$\begin{aligned}\boldsymbol{w} &= \frac{1}{\sqrt{\gamma}}\hat{\boldsymbol{h}}^{\mathrm{H}} \\ &= \frac{1}{\sqrt{\gamma}}\left(\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}} + \boldsymbol{n}^{\mathrm{H}}\right)\end{aligned} \tag{3}$$

where γ is a factor that normalises the average transmitted energy at Alice. With an average energy constraint, there are two main choices for γ [12]; we will consider the following normalisation factor:

$$\gamma = \mathrm{tr}(\hat{\boldsymbol{h}}\hat{\boldsymbol{h}}^{\mathrm{H}}) = ||\hat{\boldsymbol{h}}||^2 \tag{4}$$

2.2 Data transmission phase

In this phase, Alice uses the precoding vector in (3) to do a beamforming for the data transmission to Bob. For each symbol transmission, the received signal at Bob is given as

$$\begin{aligned}y_{\mathrm{B}} &= \sqrt{P_{\mathrm{A}}\beta_{\mathrm{AB}}}\boldsymbol{h}_{\mathrm{AB}}\boldsymbol{w}x_d + n_{\mathrm{B}} \\ &= \sqrt{\frac{P_{\mathrm{A}}\beta_{\mathrm{AB}}}{\gamma}}\boldsymbol{h}_{\mathrm{AB}}\hat{\boldsymbol{h}}^{\mathrm{H}}x_d + n_{\mathrm{B}} \\ &= \sqrt{\frac{P_{\mathrm{A}}P_{\mathrm{B}}\beta_{\mathrm{AB}}\beta_{\mathrm{BA}}}{\gamma}}\boldsymbol{h}_{\mathrm{AB}}\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}}x_d + \sqrt{\frac{P_{\mathrm{A}}\beta_{\mathrm{AB}}}{\gamma}}\boldsymbol{h}_{\mathrm{AB}}\boldsymbol{n}^{\mathrm{H}}x_d + n_{\mathrm{B}}\end{aligned} \tag{5}$$

where x_d is a single transmitted symbol to Bob, and n_{B} is the zero-mean complex Gaussian noise at Bob with unit variance. Similarly, the received signal of the selected antenna at Eve is given as

$$\begin{aligned}y_{\mathrm{E}} &= \sqrt{P_{\mathrm{A}}\beta_{\mathrm{AB}}}\boldsymbol{h}_{\mathrm{AE}_s}\boldsymbol{w}x_d + n_{\mathrm{E}} \\ &= \sqrt{\frac{P_{\mathrm{A}}\beta_{\mathrm{AB}}}{\gamma}}\boldsymbol{h}_{\mathrm{AE}_s}\hat{\boldsymbol{h}}^{\mathrm{H}}x_d + n_{\mathrm{E}} \\ &= \sqrt{\frac{P_{\mathrm{A}}P_{\mathrm{B}}\beta_{\mathrm{AB}}\beta_{\mathrm{BA}}}{\gamma}}\boldsymbol{h}_{\mathrm{AE}_s}\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}}x_d + \sqrt{\frac{P_{\mathrm{A}}\beta_{\mathrm{AB}}}{\gamma}}\boldsymbol{h}_{\mathrm{AE}_s}\boldsymbol{n}^{\mathrm{H}}x_d + n_{\mathrm{E}},\end{aligned} \tag{6}$$

where $\boldsymbol{h}_{\mathrm{AE}_s}$ is the channel vector between the transmitter and the

selected antenna at Eve; this antenna is selected such that $|\boldsymbol{h}_{\mathrm{AE}_s}\boldsymbol{w}|^2 = \max_{i\in\{1,2,\ldots,N\}} |\boldsymbol{h}_{\mathrm{AE}_i}\boldsymbol{w}|^2$.

2.3 Active eavesdropping

In the following, we assume that Eve attacks the training phase and send the same pilot sequence as Bob. This is justified by the assumption that the training sequence is fixed and used repeatedly over time, so that it can be obtained easily if there is a sophisticated eavesdropper [4]. According to this possible scenario, and during the training phase, both Bob and Eve transmit the pilot signal. Now, the received signal at Alice in this phase is given by

$$\boldsymbol{y}_{\mathrm{Ap}} = \sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}x_{\mathrm{p}} + \sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{E}_s\mathrm{A}}x_{\mathrm{p}} + \boldsymbol{n}_{\mathrm{p}} \tag{7}$$

where P_{E} is the transmitted power per symbol at Eve. If we assume least square channel estimation, then the estimated channel at Alice is given by

$$\hat{\boldsymbol{h}} = \sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{AB}} + \sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{AE}_s} + \boldsymbol{n} \tag{8}$$

As before, Alice constructs an $M\times 1$ precoding vector $\boldsymbol{w}$ as a scaled version of matched filter as follows

$$\boldsymbol{w} = \frac{1}{\sqrt{\gamma}}\left(\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}} + \sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{AE}_s}^{\mathrm{H}} + \boldsymbol{n}^{\mathrm{H}}\right) \tag{9}$$

Following similar steps to get (5) and (6), it can be shown that the received signals at Bob and Eve are given as

$$y_{\mathrm{B}} = \sqrt{\frac{P_{\mathrm{A}}P_{\mathrm{B}}\beta_{\mathrm{AB}}\beta_{\mathrm{BA}}}{\gamma}}\boldsymbol{h}_{\mathrm{AB}}\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}}x_d + \sqrt{\frac{P_{\mathrm{A}}P_{\mathrm{E}}\beta_{\mathrm{AB}}\beta_{\mathrm{EA}}}{\gamma}}\boldsymbol{h}_{\mathrm{AB}}\boldsymbol{h}_{\mathrm{AE}_s}^{\mathrm{H}}x_d + \sqrt{\frac{P_{\mathrm{A}}\beta_{\mathrm{AB}}}{\gamma}}\boldsymbol{h}_{\mathrm{AB}}\boldsymbol{n}^{\mathrm{H}}x_d + n_{\mathrm{B}} \tag{10}$$

$$y_{\mathrm{E}} = \sqrt{\frac{P_{\mathrm{A}}P_{\mathrm{B}}\beta_{\mathrm{AB}}\beta_{\mathrm{BA}}}{\gamma}}\boldsymbol{h}_{\mathrm{AE}_s}\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}}x_d + \sqrt{\frac{P_{\mathrm{A}}P_{\mathrm{E}}\beta_{\mathrm{AB}}\beta_{\mathrm{EA}}}{\gamma}}\boldsymbol{h}_{\mathrm{AE}_s}\boldsymbol{h}_{\mathrm{AE}_s}^{\mathrm{H}}x_d + \sqrt{\frac{P_{\mathrm{A}}\beta_{\mathrm{AB}}}{\gamma}}\boldsymbol{h}_{\mathrm{AE}_s}\boldsymbol{n}^{\mathrm{H}}x_d + n_{\mathrm{E}} \tag{11}$$

It should be noted that when Eve is working in the active mode, he needs only one antenna as Bob to send the pilot attack. In the receiver side at Eve, the same antenna is selected as it will give the maximum SNR. This means that Eve need only one antenna when working as an active eavesdropper using AS technique.

3 Achievable secrecy rate analysis

In this section, we derive the achievable secrecy rate for the system model presented earlier and investigate the effect of MMIMO on the secrecy rate in the absence and presence of the pilot attack.

3.1 Secrecy rate analysis – passive eavesdropper

The received signal (5) at Bob is decoded using pilots transmitted at the beginning of each packet in the data transmission phase. Under this assumption, the instantaneous SNR at Bob is given as

$$\mathrm{SNR}_{\mathrm{B}} = P_{\mathrm{A}}\beta_{\mathrm{AB}}\left|\boldsymbol{h}_{\mathrm{AB}}\frac{\hat{\boldsymbol{h}}}{||\hat{\boldsymbol{h}}||}\right|^2 \tag{12}$$

where $\hat{\boldsymbol{h}}$ is given in (2). Similarly, the SNR at Eve, operating in the receive mode, is given by

$$\mathrm{SNR}_{\mathrm{E}} = P_{\mathrm{A}}\beta_{\mathrm{AE}}\left|\boldsymbol{h}_{\mathrm{AE}_s}\frac{\hat{\boldsymbol{h}}}{||\hat{\boldsymbol{h}}||}\right|^2 \tag{13}$$

The achievable secrecy rate between Alice and Bob is given by [13]

$$\begin{aligned} R_{\mathrm{S}} &= \left[R_{\mathrm{AB}} - R_{\mathrm{AE}}\right]^+ \\ &= \left[\log_2\left(1+\mathrm{SNR}_{\mathrm{B}}\right) - \log_2\left(1+\mathrm{SNR}_{\mathrm{E}}\right)\right]^+ \end{aligned} \tag{14}$$

where R_{AB} and R_{AE} are the achievable rate for Alice–Bob and Alice–Eve links, respectively. Now, we want to investigate the achievable secrecy rate when the transmitter at Alice is equipped with unlimited number of antenna, that is, when $M\to\infty$. According to the theory of large numbers, it can be shown that [14]

$$\lim_{M\to\infty}\frac{\boldsymbol{h}_{\mathrm{AE}}\boldsymbol{h}_{\mathrm{AE}}^{\mathrm{H}}}{M} = \lim_{M\to\infty}\frac{\boldsymbol{h}_{\mathrm{AB}}\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}}}{M} = 1 \tag{15}$$

$$\lim_{M\to\infty}\frac{\boldsymbol{h}_{\mathrm{AB}}\boldsymbol{h}_{\mathrm{AE}}^{\mathrm{H}}}{M} = \lim_{M\to\infty}\frac{\boldsymbol{h}_{\mathrm{AE}}\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}}}{M} = \lim_{M\to\infty}\frac{\boldsymbol{h}_{\mathrm{AB}}\boldsymbol{n}^{\mathrm{H}}}{M} = \lim_{M\to\infty}\frac{\boldsymbol{h}_{\mathrm{AE}}\boldsymbol{n}^{\mathrm{H}}}{M} = 0 \tag{16}$$

Taking into account (15) and (16), the received signals in (5) and (6) are converged as

$$\lim_{M\to\infty}\frac{y_{\mathrm{B}}}{M} \to \frac{\sqrt{P_{\mathrm{A}}P_{\mathrm{B}}\beta_{\mathrm{AB}}\beta_{\mathrm{BA}}}}{\sqrt{M\left(P_{\mathrm{B}}\beta_{\mathrm{BA}}+1\right)}} \tag{17}$$

$$\lim_{M\to\infty}\frac{y_{\mathrm{E}}}{M} \to 0 \tag{18}$$

Therefore, from the last two equations, the SNRs at Bob and Eve given in (12) and (13) are asymptotically, with unlimited number of antennas, given as

$$\mathrm{SNR}_{\mathrm{B}}^{o} = \lim_{M\to\infty}\mathrm{SNR}_{\mathrm{B}} = \frac{MP_{\mathrm{A}}P_{\mathrm{B}}\beta_{\mathrm{AB}}\beta_{\mathrm{BA}}}{\left(P_{\mathrm{B}}\beta_{\mathrm{BA}}+1\right)} \tag{19}$$

$$\mathrm{SNR}_{\mathrm{E}}^{o} = \lim_{M\to\infty}\mathrm{SNR}_{\mathrm{E}} = \mathcal{O}(1) \tag{20}$$

where $\mathcal{O}(1)$ denotes any random variable s with the property $\lim_{M\to\infty}(s/M^{\theta}) = 0, \quad \theta > 0$. This identity is a simple consequence of the strong law of large numbers. Note that the SNR at Bob depends on M, but this is not the case for the SNR at Eve, which scales as the order $\mathcal{O}(1)$ which can be neglected. As a result, the achievable secrecy rate $R_{\mathrm{S}} \simeq R_{\mathrm{AB}}$. Hence, the achievable secrecy rate can be enhanced by increasing the number of antennas at Alice. This is an important observation as MMIMO performs like a beamforming only in the direction of the legitimate receiver Bob, and nothing outside that. As mentioned above, SNR_B^o increases linearly with M in (19). This is due to the fact that the power gain is harvested as an increase in the SNR in the receiver rather than a power saving in the transmitter. The power efficiency of the MMIMO systems can alternatively be exploited as power saving by normalising the power transmitted at Alice, P_{A}, by M so that the rate R_{AB} will not depend on M, and for sufficiently large number of antennas, the SNR saturates with fixed value.

3.2 Secrecy rate analysis – active eavesdropper

In this case, following similar assumptions as in previous subsection, the SNRs at Bob and Eve are given as

$$\mathrm{SNR}_{\mathrm{B}} = P_{\mathrm{A}}\beta_{\mathrm{AB}}\left|\boldsymbol{h}_{\mathrm{AB}}\frac{\hat{\boldsymbol{h}}}{||\hat{\boldsymbol{h}}||}\right|^2, \tag{21}$$

$$\mathrm{SNR}_{\mathrm{E}} = P_{\mathrm{A}}\beta_{\mathrm{AE}}\left|\boldsymbol{h}_{\mathrm{AE}_s}\frac{\hat{\boldsymbol{h}}}{||\hat{\boldsymbol{h}}||}\right|^2, \tag{22}$$

respectively, where $\hat{\boldsymbol{h}}$ is given in (8). Using unlimited number of antennas at Alice side, and taking into account (15) and (16), the received signals in (10) and (11) are converged as

$$\lim_{M\to\infty}\frac{y_{\mathrm{B}}}{M} \to \frac{\sqrt{P_{\mathrm{A}}P_{B}\beta_{\mathrm{AB}}\beta_{\mathrm{BA}}}}{\sqrt{M\left(P_{\mathrm{B}}\beta_{\mathrm{BA}}+P_{\mathrm{B}}\beta_{\mathrm{BA}}+1\right)}} \tag{23}$$

$$\lim_{M\to\infty}\frac{y_{\mathrm{B}}}{M} \to \frac{\sqrt{P_{\mathrm{A}}P_{\mathrm{E}}\beta_{\mathrm{AB}}\beta_{\mathrm{EA}}}}{\sqrt{M\left(P_{\mathrm{B}}\beta_{\mathrm{BA}}+P_{\mathrm{B}}\beta_{\mathrm{BA}}+1\right)}} \tag{24}$$

Therefore, the asymptotic SNRs at Bob and Eve, are given as

$$\mathrm{SNR}_{\mathrm{B}}^{o} = \lim_{M\to\infty}\mathrm{SNR}_{\mathrm{B}} = \frac{M\,P_{\mathrm{A}}P_{\mathrm{B}}\beta_{\mathrm{AB}}\beta_{\mathrm{BA}}}{\left(P_{\mathrm{B}}\beta_{\mathrm{BA}}+P_{\mathrm{E}}\beta_{\mathrm{EA}}+1\right)}, \tag{25}$$

$$\mathrm{SNR}_{\mathrm{E}}^{o} = \lim_{M\to\infty}\mathrm{SNR}_{\mathrm{E}} = \frac{M\,P_{\mathrm{A}}P_{\mathrm{E}}\beta_{\mathrm{AB}}\beta_{\mathrm{EA}}}{\left(P_{\mathrm{B}}\beta_{\mathrm{BA}}+P_{\mathrm{E}}\beta_{\mathrm{EA}}+1\right)}, \tag{26}$$

respectively. Note that both $\mathrm{SNR}_{\mathrm{B}}^{o}$ and $\mathrm{SNR}_{\mathrm{E}}^{o}$ depend on M. As a result, the achievable secrecy rate $R_{\mathrm{S}} \simeq 0$ if Bob and Eve have the same transmitted power and they are at symmetric location relative to Alice, that is, $\beta_{\mathrm{AB}} = \beta_{\mathrm{AE}}$. This detrimental effect happens when Eve can attack the training phase. Therefore, detecting this attack is essential and this will be discussed in the following section. Moreover, let $\lambda_{\mathrm{me}} = \beta_{\mathrm{AB}}/\beta_{\mathrm{AE}}$ denotes the ratio of the average channel gain of the Alice–Bob to Alice–Eve links. Therefore, λ_{me} is referred to as mean-to-eavesdropper ratio (MER) in this paper, and is used as a dominant factor in determining the intercept probability and diversity order in context of physical layer security [15, 16]. When the value of λ_{me} is less than one, this means that Eve is closer to Alice than Bob.

4 Simple detection scheme for active eavesdropper

In the previous section, we have shown that the passive eavesdropper is not dangerous and about zero rate can be achieved at the eavesdropper side using MMIMO technique. However, as the eavesdropper does pilot attack and being active, about zero secrecy rate is achieved. Therefore, detecting the presence of the eavesdropper is necessary in order to stop overhearing the transmitted information. In this section, we propose a simple detection scheme for the active eavesdropper so that the system can take a countermeasure such as halting the transmission or changing the pilot sequence. Moreover, we evaluate the effectiveness of the proposed scheme for detecting the presence of the active eavesdropper; we derive exact expressions for the detection probability and the probability of false alarm.

4.1 Simple detection protocol

Suppose that Alice uses the following measured scalar (see (27) at the bottom of the page). With unlimited number of antennas, α is converged as follows

$$\alpha^{o} = \lim_{M\to\infty}\alpha \simeq M\left(P_{\mathrm{B}}\beta_{\mathrm{BA}}+P_{\mathrm{E}}\beta_{\mathrm{EA}}+1\right) \tag{28}$$

Now, let us define the following parameter

$$\beta = M\left(P_{\mathrm{B}}\beta_{\mathrm{BA}}+\phi+1\right) \tag{29}$$

where ϕ is a parameter that accounts for the error arising in the convergence given in (15) and (16) due to a practical considerations of using large but limited number of antennas. It can also be considered as a system parameter that accounts for the tradeoff between detection and false-alarm probabilities required by the system. Note that if $\phi = 0$, then $\beta = \alpha^{o}$, at $P_{\mathrm{E}} = 0$ (no pilot attack); normally, ϕ has small values due to the practical considerations of MMIMO systems. This indicates that if $\alpha > \beta$, this implies the presence of pilot attack at the training phase. Note that α has the same value as the normalisation factor γ defined in (4). Therefore, Alice does not need to do any extra measurements. Moreover, in normal transmission from Alice to Bob, without pilot attack, Bob already needs to estimate the downlink channel for the demodulation purpose. Hence, eavesdropping detection can be done at Bob with some similar processing. This also reflects the simplicity of the proposed protocol. Finally, it should be mentioned here that the scalar β, defined in (29), is assumed to be known at Alice. M and ϕ are system parameters. The large-scale fading parameter β_{BA} is assumed to be known. In fact, this is a long-term parameter and can be estimated at Alice.

4.2 Detection and false-alarm probabilities

As mentioned in the previous subsection, the decision for the detection of the eavesdropper can be defined by the event ($\alpha > \beta$), when $P_{\mathrm{E}} \neq 0$. The detection probability is defined as the probability of the event ($\alpha > \beta$) when the eavesdropper is active as also introduced in [17]. Hence, the detection probability can be given as

$$\Pr(D) = \Pr\left(\alpha > \beta | P_{\mathrm{E}} \neq 0\right) \tag{30}$$

Defining $k_1 = \sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}$, $k_2 = \sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}$, $\hat{\boldsymbol{h}}$ is written as

$$\begin{aligned}\hat{\boldsymbol{h}} &= k_1\boldsymbol{h}_{\mathrm{AB}} + k_2\boldsymbol{h}_{\mathrm{AE}} + \boldsymbol{n}\\ &= [h_1 h_2,\ \ldots,\ h_M]\end{aligned} \tag{31}$$

where h_i, $i = 1, 2, \ldots, M$ are i.i.d complex Gaussian random variables each with zero mean and variance $\sigma^2 = k_1^2 + k_2^2 + 1$. Therefore, the random variable α can be given as

$$\alpha = \hat{\boldsymbol{h}}\hat{\boldsymbol{h}}^{\mathrm{H}} = |h_1|^2 + |h_2|^2 + \ldots + |h_M|^2 \tag{32}$$

where $|h_i|^2$, $i = 1, 2, \ldots, M$ are exponential random variables each of mean $\mu = k_1^2 + k_2^2 + 1$. Hence, α is gamma distributed, with the following cumulative distribution function (CDF)

$$F_{\alpha}(x) = \frac{\gamma(k, \lambda x)}{\Gamma(k)} \tag{33}$$

where $\gamma(k, \lambda x) = \int_0^x \lambda^k u^{k-1} e^{-\lambda u}\mathrm{d}u$ is the lower incomplete gamma function, $\Gamma(k)$ is the gamma function, $k = M$, and $\lambda = 1/\mu = 1/\left(k_1^2 + k_2^2 + 1\right)$. Now the detection probability is

$$\alpha = \hat{\boldsymbol{h}}\hat{\boldsymbol{h}}^{\mathrm{H}} = \left(\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{AB}} + \sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{AE}} + \boldsymbol{n}\right)\left(\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}} + \sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{AE}}^{\mathrm{H}} + \boldsymbol{n}^{\mathrm{H}}\right) \tag{27}$$

given by

$$\begin{aligned}\Pr(D) &= \Pr\left(\alpha > \beta | P_{\mathrm{E}} \neq 0\right) \\ &= 1 - \Pr\left(\alpha < \beta | P_{\mathrm{E}} \neq 0\right) \\ &= 1 - \frac{\gamma(k, \lambda\beta)}{\Gamma(k)}\bigg|_{P_{\mathrm{E}} \neq 0}\end{aligned} \tag{34}$$

Similarly, the false-alarm probability is defined as the probability of the event $\alpha > \beta$ when actually there is no pilot attack, and is given by

$$\begin{aligned}\Pr(\mathrm{FA}) &= 1 - \Pr\left(\alpha < \beta | P_{\mathrm{E}} = 0\right) \\ &= 1 - \frac{\gamma(k, \lambda\beta)}{\Gamma(k)}\bigg|_{P_{\mathrm{E}} = 0}\end{aligned} \tag{35}$$

Following a simple algorithm, ϕ can be easily obtained from (35) for a required target false-alarm probability. According to this value of ϕ, the detection probability for a given Eav's power can be calculated from (34). In this way, an appropriate tradeoff between the detection and false-alarm probabilities can be obtained by appropriate choice of ϕ.

5 Intercept probability and secrecy diversity order analysis

In this section, we derive a closed-form expression for the intercept probability and investigate the secrecy diversity order achieved by the system model described above. The intercept probability is commonly used as another performance metric in analysing physical layer security [15, 18]. It is defined as the probability that the secrecy rate is less than zero. In other words, the intercept event occurs when the wiretap link is better than that the main link. For simplicity of analysis, we will consider perfect channel estimation at the transmitter side and derive closed-form expression for the intercept probability, from which we derive the secrecy diversity order. Then, we derive an asymptotic intercept probability when $M \to \infty$. Let us first introduce the definition of the diversity order. The traditional diversity order is given as [19]

$$d = \frac{\ln P_{\mathrm{e}}(\mathrm{SNR})}{\ln(\mathrm{SNR})} \tag{36}$$

where P_{e} denotes the bit error rate. However, in the context of physical layer surety, this definition is not suitable as the intercept probability, as will be seen in this section, does not depend on the SNR; this is due to the fact that the transmitted power affects both the legitimate receiver and the eavesdropper. Therefore, a more suitable definition of the secrecy diversity order is given as [15]

$$\bar{d} = \frac{\ln P_{\mathrm{int}}(\lambda_{\mathrm{me}})}{\ln(\lambda_{\mathrm{me}})} \tag{37}$$

where P_{int} is the intercept probability.

5.1 Intercept probability analysis

According to the above analysis, the intercept probability is given as

$$\begin{aligned}P_{\mathrm{int}} &= \Pr\left\{R_{\mathrm{AB}} - R_{\mathrm{AE}} < 0\right\} \\ &= \Pr\left\{P_{\mathrm{A}}\beta_{\mathrm{AB}}\left|\boldsymbol{h}_{\mathrm{AB}}\frac{\boldsymbol{h}_{\mathrm{AB}}{}^{\mathrm{H}}}{||\boldsymbol{h}_{\mathrm{AB}}||}\right|^2 < P_{\mathrm{A}}\beta_{\mathrm{AE}}\left|\boldsymbol{h}_{\mathrm{AE}_s}\frac{\boldsymbol{h}_{\mathrm{AB}}{}^{\mathrm{H}}}{||\boldsymbol{h}_{\mathrm{AB}}||}\right|^2\right\} \\ &= 1 - \Pr\left\{\left|\boldsymbol{h}_{\mathrm{AE}_s}\frac{\boldsymbol{h}_{\mathrm{AB}}{}^{\mathrm{H}}}{||\boldsymbol{h}_{\mathrm{AB}}||}\right|^2 < \lambda_{\mathrm{me}}\left|\boldsymbol{h}_{\mathrm{AB}}\frac{\boldsymbol{h}_{\mathrm{AB}}{}^{\mathrm{H}}}{||\boldsymbol{h}_{\mathrm{AB}}||}\right|^2\right\}\end{aligned} \tag{38}$$

Define $X = |\boldsymbol{h}_{\mathrm{AE}_s}(\boldsymbol{h}_{\mathrm{AB}}{}^{\mathrm{H}}/\|\boldsymbol{h}_{\mathrm{AB}}\|)|^2 = \max_{i\in\{1,2,\ldots,N\}}|\boldsymbol{h}_{\mathrm{AE}_i}(\boldsymbol{h}_{\mathrm{AB}}{}^{\mathrm{H}}/\|\boldsymbol{h}_{\mathrm{AB}}\|)|^2$. Note that $|\boldsymbol{h}_{\mathrm{AE}_i}(\boldsymbol{h}_{\mathrm{AB}}{}^{\mathrm{H}}/||\boldsymbol{h}_{\mathrm{AB}}||)|^2$ is chi-square random variable with two degrees of freedom which is equivalent to exponential distributed random variable of unit mean. Therefore, according to the theory of order statistics, the CDF of X is given as $F_X(x) = (1 - \mathrm{e}^{-x})^N$. On the other hand, $Y = |\boldsymbol{h}_{\mathrm{AB}}(\boldsymbol{h}_{\mathrm{AB}}{}^{\mathrm{H}}/||\boldsymbol{h}_{\mathrm{AB}}||)|^2$ is a chi-square random variable with $2M$ degrees of freedoms. The PDF of Y is given as

$$f_Y(y) = \frac{y^{M-1}\mathrm{e}^{-y}}{\Gamma(M)} \tag{39}$$

Therefore, the intercept probability is given as

$$\begin{aligned}P_{\mathrm{int}} &= 1 - \int_0^\infty F_X(\lambda_{\mathrm{me}}y)f_Y(y)\mathrm{d}y \\ &= 1 - \int_0^\infty \left(1 - \exp(-\lambda_{\mathrm{me}}y)\right)^N \exp(-y)\frac{y^{M-1}}{\Gamma(M)}\mathrm{d}y\end{aligned} \tag{40}$$

Using the binomial expansion theorem, it can be shown that

$$\left(1 - \exp(-\lambda_{\mathrm{me}}y)\right)^N = 1 + \sum_{k=1}^{N}(-1)^{N-k}\binom{N}{k}\exp(-k\lambda_{\mathrm{me}}y) \tag{41}$$

Substituting (41) into (40) and changing the orders of integration and summation, the intercept probability is given as

$$\begin{aligned}P_{\mathrm{int}} &= -\sum_{k=1}^{N}\frac{(-1)^{N-k}}{\Gamma(M)}\binom{N}{k}\int_0^\infty y^{M-1}\exp(-y(1 + k\lambda_{\mathrm{me}})\mathrm{d}y \\ &= -\sum_{k=1}^{N}(-1)^{N-k}\binom{N}{k}(1 + k\lambda_{\mathrm{me}})^{-M}\end{aligned} \tag{42}$$

Note that for sufficiently large λ_{me}, such that $k\lambda_{\mathrm{me}} \gg 1$, $(1 + k\lambda_{\mathrm{me}}) \simeq k\lambda_{\mathrm{me}}$, and the intercept probability is given as

$$P_{\mathrm{int}} \simeq -\sum_{k=1}^{N}(-1)^{N-k}\binom{N}{k}(k)^{-M}.\left(\frac{1}{\lambda_{\mathrm{me}}}\right)^M \tag{43}$$

Substituting (43) into (37), we get the secrecy diversity order as

$$\bar{d} = M \tag{44}$$

Therefore, a secrecy diversity order of M is achieved.

5.2 Asymptotic intercept probability ($M \to \infty$)

In this subsection, we exploit the channel hardening property of MMIMO to derive the asymptotic intercept probability and secrecy diversity order when $M \to \infty$. We have seen that the SNR at Bob diverges to a constant value $\mathrm{SNR}_{\mathrm{B}}^{o}$ as given in (19). Defining $R_{\mathrm{AB}}^{o} \triangleq \log_2(1 + \mathrm{SNR}_{\mathrm{B}}^{o})$, the asymptotic intercept probability is calculated as

$$\begin{aligned}P_{\mathrm{int}}^{M\to\infty} &= \Pr\left\{R_{\mathrm{AB}}^{o} - R_{\mathrm{AE}} < 0\right\} \\ &= 1 - \Pr\left\{P_{\mathrm{A}}\beta_{\mathrm{AB}}\left|\boldsymbol{h}_{\mathrm{AE}_s}\frac{\boldsymbol{h}_{\mathrm{AB}}{}^{\mathrm{H}}}{||\boldsymbol{h}_{\mathrm{AB}}||}\right|^2 < \mathrm{SNR}_{\mathrm{B}}^{0}\right\} \\ &= 1 - \Pr\left\{X < \lambda_{\mathrm{em}}\frac{MP_{\mathrm{B}}\beta_{\mathrm{AB}}}{1 + P_{\mathrm{B}}\beta_{\mathrm{AB}}}\right\} \\ &= 1 - \left[1 - \exp\left(-\lambda_{\mathrm{em}}\frac{MP_{\mathrm{B}}\beta_{\mathrm{AB}}}{1 + P_{\mathrm{B}}\beta_{\mathrm{AB}}}\right)\right]^N\end{aligned} \tag{45}$$

It can be observed from (45) that the intercept probability is an increasing function of N and decreasing function of M. As

IET Commun., 2016, Vol. 10, Iss. 1, pp. 50–56

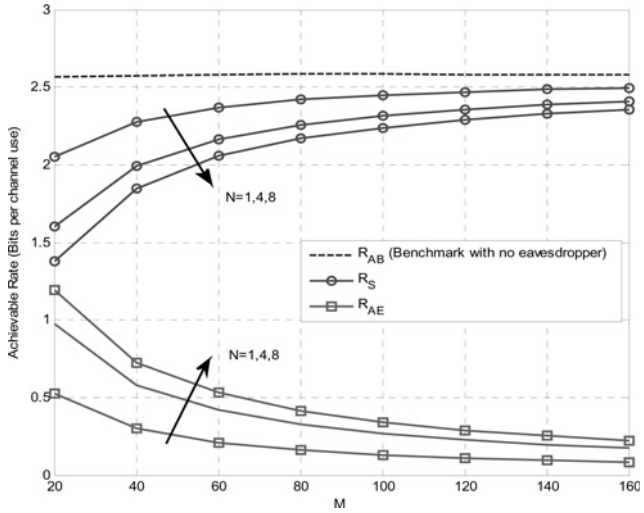

Fig. 2 *Achievable secrecy rate against the number of antennas M, with passive eavesdropper, $P_A = 10$ dB, $P_B = 0$ dB, and $\beta_{AB} = \beta_{AE} = 1$*

$M \to \infty$, $P_{\text{int}}^{M\to\infty} \to 0$ even if the number of antennas at Eve is large. Therefore, the problem that the eavesdropper has more antennas than the intended user Bob can be solved with MMIMO system. Moreover, as $\lambda_{\text{me}} \to 0$, $\exp(-\lambda_{\text{me}}(MP_{\text{B}}\beta_{\text{AB}}/1 + P_{\text{B}}\beta_{\text{AB}})) \to 0$ and $[1 - \exp(-\lambda_{\text{me}}(MP_{\text{B}}\beta_{\text{AB}}/1 + P_{\text{B}}\beta_{\text{AB}}))]^N \simeq 1 - \exp(-\lambda_{\text{me}}(MP_{\text{B}}\ \beta_{\text{AB}}/1 + P_{\text{B}}\beta_{\text{AB}}))$. Hence, the asymptotic intercept probability is approximated as

$$P_{\text{int}}^{M\to\infty} \simeq \exp\left(-\lambda_{\text{me}} \frac{MP_{\text{B}}\beta_{\text{AB}}}{1 + P_{\text{B}}\beta_{\text{AB}}}\right) \tag{46}$$

so that exponential diversity can be achieved. Substituting (46) into (37), it can easily be shown that infinite secrecy diversity order is obtained with unlimited number of antenna at the transmitter. This confirms the fact that MMIMO system can effectively neglect the small-scale fading due to channel hardening properties [5, 6].

6 Simulation results

To illustrate our results, we have done some simulations considering the system model described above. In all simulations we set $N_{0,\text{A}} = 1$. First we show the effect of increasing the number of antennas at Alice on the achievable secrecy rate with passive eavesdropper, and with different number of antennas at Eve as indicated in Fig. 2. In this case, the transmitted power at Alice P_{A} is normalised by M in order to best illustrate the effect of MMIMO on the secrecy rate. As can be seen, the achievable secrecy rate approaches R_{AB} with increasing M. This is because of the property of channel hardening of MMIMO, which decreases the achievable rate in the Alice–Eve link with increasing M. Note also that the rate R_{AE} is increasing function of N, and hence, the secrecy rate R_{S} is decreasing function of N. However, as M increases, the effect of increasing N diminishes, which confirm the analytical results in Section 3.

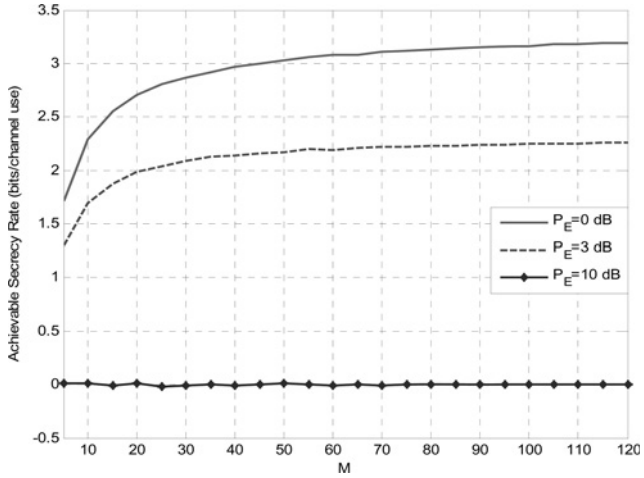

Fig. 3 *Achievable secrecy rate against M, with active eavesdropper for different values of Eve's power, $\beta_{AB} = \beta_{AE} = 1$, $P_A = 10$ dB, and $P_B = 10$ dB*

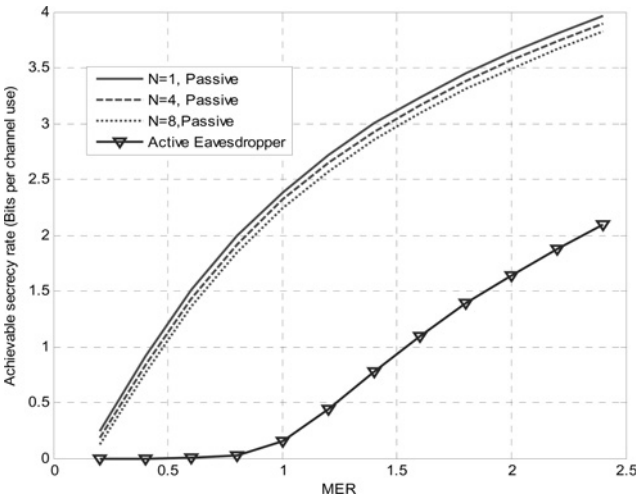

Fig. 4 *Achievable secrecy rate against MER for different number of Eve's antennas N, $P_A = 10$ dB, $P_B = 0$ dB, and $M = 100$*

Next, we consider the case of active eavesdropper. Fig. 3 shows the achievable secrecy rate versus M for different values of P_{E}. As shown in the figure, the achievable secrecy rate depends on the transmitted power at Eve in the training phase. The secrecy rate decreases with increasing P_{E}, and when $P_{\text{E}} = P_{\text{B}}$, zero secrecy rate is achieved; this illustrates the detrimental effect of active eavesdropping. However, as will be seen shortly, as P_{E} increases, our ability to detect the existence of Eve also increases through the proposed detection scheme. It is also interesting to note that the achievable secrecy rate is large for small values of Eve's power. This means that we can slightly reduce the target secrecy rate in order to avoid the missed detection at small values of Eve's power. Moreover, it can be seen from Fig. 3 that increasing M

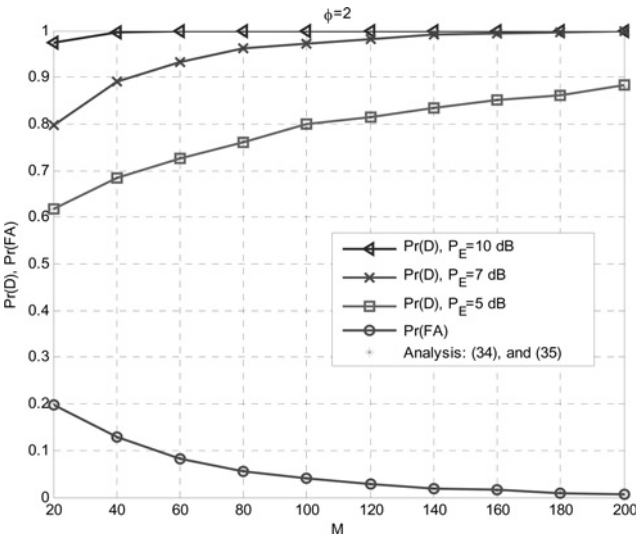

Fig. 5 *Effect of increasing the number of antennas on the detection probability and probability of false alarm with different values of Eve's power, $P_A = 10$ dB, $P_B = 10$ dB, and $\lambda_{me} = 1$*

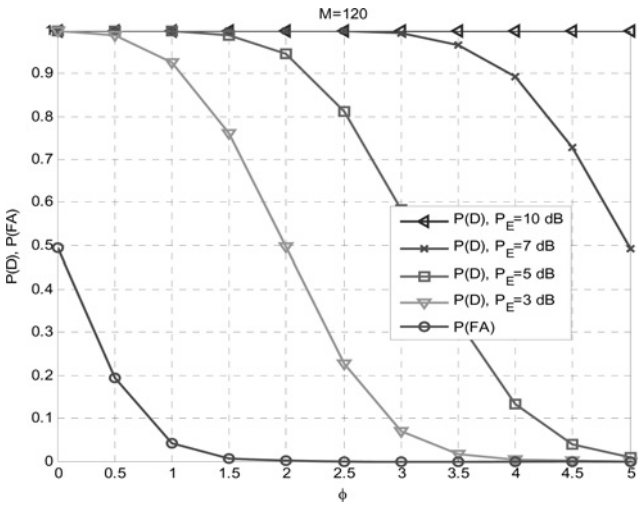

Fig. 6 *Detection and false-alarm probabilities against ϕ with different values of Eve's power, $P_A = 10$ dB, $P_B = 10$ dB, and $\lambda_{me} = 1$*

increases the achievable secrecy rate, especially at low values of Eve's power, before it saturates.

To illustrate the effect of the location of Eve relative to Bob on the achievable secrecy rate, we plot the secrecy rate versus the MER, λ_{me}, as shown in Fig. 4, with $M = 100$. Two important conclusions are drawn from the figure. First, with sufficiently large number of antennas at Alice, the effect of increasing the number of antennas at passive Eve on the secrecy rate is small specially at low values of λ_{me}. This reflects the ability of MMIMO system to solve the problem that Eve has large number of antennas. Second, when $\lambda_{\text{me}} \leq 1$, about zero secrecy rate is obtained, which reflect the detrimental effect of the eavesdropper being active. Therefore, detecting the presence of any active eavesdropper is very important to secure the communication network.

Fig. 5 shows the detection and false-alarm probabilities against M. The values of α are obtained by averaging the received energy over three consecutive frames. It can be seen that, with MIMIMO, the detection and false-alarm probabilities approach their optimum values. However, for small values of the eavesdropper power, we need to increase M to get higher detection probability. Also note that the numerical results match well with the simulation results. In Fig. 6, we investigate the variation of both detection and false-alarm probabilities againstϕ. It is clearly seen that there is a tradeoff between both probabilities. The choice of the parameterϕ

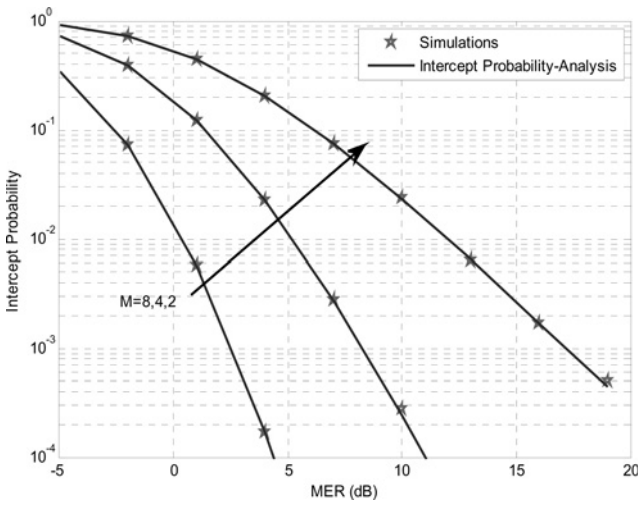

Fig. 7 *Intercept probability against MER of the passive eavesdropper with different numbers of transmit antennas, M, $P_A = 10$ dB, $P_B = 0$ dB, and $N = 4$*

plays an important role in determining this tradeoff. There is also decrement in the detection probability with small values of Eve's power. This can be compensated by increasing M.

Finally, Fig. 7 shows the intercept probability versus MER at different number of transmit antennas M. It can be noted that as M increases from 2 to 8, the intercept probability significantly reduces. The slope of the curves at high values of MER increases. This reflects the secrecy diversity order achieved, which is equal to the number of transmit antennas. Note also that the analytical results match well with the simulation results.

7 Conclusions

This paper has dealt with the use of MMIMO in order to enhance the physical layer security. It has been shown that without pilot attack the eavesdropper can get approximately no information as MMIMO acts as a beamformer only toward the legitimate receiver. In the case of pilot attack, we have proposed a simple protocol between Alice and Bob that can detect the presence of Eve. Analytical and simulation results showed the effectiveness of the proposed scheme in detecting the active eavesdropping in MMIMO systems. Moreover, we have shown that increasing the number of antennas of the eavesdropper has small effect on the achievable secrecy rate with MMIMO systems. Moreover, we derived a closed-form expression for the intercept probability, and it has been shown that asymptotically with unlimited number of transmit antennas an exponential secrecy diversity is achieved.

8 References

1 Wyner, A.D.: 'The wire-tap channel', *Bell Syst. Tech. J.*, 1975, **54**, pp. 1355–1387
2 Mukherjee, A., Fakoorian, A., Huang, J., *et al.*: 'Principles of physical-layer security in multiuser wireless networks: a survey', *IEEE Commun. Surv. Tutor.*, 2014, **16**, (3), pp. 1550–1573
3 Mukherjee, A., Swindlehurst, A.L.: 'A full-duplex active eavesdropper in MIMO wiretap channels: construction and countermeasures'. Proc. 45th Asilomar Conf. on Signals, Systems and Computers (ASILOMAR), 2011, pp. 265–269
4 Zhou, X., Maham, B., Hjørungnes, A.: 'Pilot contamination for active eavesdropping', *IEEE Trans. Wirel. Commun.*, 2012, **11**, (3), pp. 903–907
5 Marzetta, T.: 'Noncooperative cellular wireless with unlimited numbers of base station antennas', *IEEE Trans. Wirel. Commun.*, 2010, **9**, pp. 3590–3600
6 Rusek, F., Persson, D., Lau, B.K., *et al.*: 'Scaling up MIMO: opportunities and challenges with very large arrays', *IEEE Signal Process. Mag.*, 2013, **30**, (1), pp. 40–60
7 Dean, T., Goldsmith, A.: 'Physical cryptography through massive MIMO'. Proc. of IEEE Information Theory Workshop (ITW), Sevilla, September 2013, pp. 1–5
8 Geraci, G., Al-nahari, A., Yuan, J., *et al.*: 'Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation', *IEEE Commun. Lett.*, 2013, **17**, (6), pp. 1164–1167
9 Geraci, G., Dhillon, H.S., Andrews, J.G., *et al.*: 'Physical layer security in downlink multi-antenna cellular networks', *IEEE Trans. Commun.*, 2014, **62**, (6), pp. 2006–2021
10 Li, X., Chen, M., Ratazzi, E.P.: 'Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy'. Proc. of IEEE SPAWC, 2005, pp. 811–815
11 Juse, J., Ashikhmin, A., Marzetta, T., *et al.*: 'Pilot contamination and precoding in multi-cell TDD systems', *IEEE Trans. Wirel. Commun.*, 2011, **10**, (8), pp. 2640–32651
12 Peel, C., Hochwald, B., Swindlehurst, A.L.: 'A vector-perturbation technique for near-capacity multiantenna multiuser communication – part I: channel inversion and regularization', *IEEE Trans. Commun.*, 2005, **53**, (1), pp. 195–202
13 Barros, J., Rodrigues, M.R.D.: 'Secrecy capacity of wireless channels'. Proc. of IEEE Int. Symp. on Information Theory, Seattle, USA, July 2006, pp. 356–360
14 Cramer, H.: 'Random variables and probability distributions' (Cambridge University Press, Cambridge, UK, 1970)
15 Zou, Y., Li, X., Liang, Y.: 'Secrecy outage and diversity analysis of cognitive radio systems', *IEEE J. Sel. Areas Commun.*, 2014, **32**, (11), pp. 2222–2236
16 Zhu, J., Zou, Y., Wang, G., *et al.*: 'On secrecy performance of antenna selection aided MIMO systems against eavesdropping', *IEEE Trans. Veh. Technol.*, 2015, (9), arxiv.org/abs/1501.06407
17 Digham, F., Alouini, M., Simon, M.: 'On the energy detection of unknown signals over fading channels'. IEEE Int. Conf. on Communications, ICC'03, May 2003, pp. 3575–3579
18 Zou, Y., Wang, X., Shen, W.: 'Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack'. Proc. of IEEE Int. Conf. on Communications (ICC 2013), June 2013, pp. 1–5
19 Zheng, L., Tse, D.: 'Diversity and multiplexing: a fundamental tradeoff in multiple antenna channels', *IEEE Trans. Inf. Theory*, 2003, **49**, (5), pp. 1073–1096