Physical-Layer Entity Authentication Scheme for Mobile MIMO Systems

Saud Althunibat*, Victor Sucasas†, Georgios Mantas † and Jonathan Rodriguez †
* Al-Hussein Bin Talal University, Ma'an, Jordan
†Instituto de Telecomunicaes, Aveiro, Portugal
E–Mail: saud.althunibat@ahu.edu.jo, vsucasas@av.it.pt, gimantas@av.it.pt, jonathan@av.it.pt

***Abstract*—Exploiting physical layer in achieving different security aspects in wireless communications has been widely encouraged. In this work, we propose an entity authentication scheme for mobile devices with multiple antennas, that is purely based on physical layer parameters. According to the proposed scheme, in order to authenticate a device, a number of predefined authentication signals should be detected at the receive antennas on the authenticator side. The transmitted signals are designed based on the instantaneous channel responses in order to deliver the authentication signals to the receiver. The proposed scheme works efficiently even for mobile users, which is considered a significant improvement over previous related works. Mathematical analysis for the different involved factors along with sufficient simulations show the high performance of the proposed authentication scheme.**

I. Introduction

Entity and message authentication are primary requirements in any personal, commercial or military application that makes use of a secure channel. Communicators need to authenticate each other in order to initiate the communication and authenticate the origin of each received message [1]. Conventionally, entity authentication is performed through the exchange of public-key based certificates, where entities authenticate each other and negotiate a symmetric key used for message authentication. When data transmission commences, the symmetric key is used to generate message authenticated codes (MACs) that are attached to the transmitted messages and that can be verified on reception [2], [3]. Both, entity authentication and message authentication processes can be seen as resource waste processes due to the requirement of exchanging certificates and attaching MACs to messages. An approach for alleviating the overhead cost in conventional authentication is by using physical layer to accomplish authentication between communicators [4], [5]. However, current physical layer authentication schemes, mainly based on channel correlation, require a conventional cryptographic-based authentication every time that the physical layer mechanism fails, which occurs frequently due to the communicators' mobility [6]. Hence, current physical layer authentication mechanisms are an efficient solution in static networks, but not suitable in mobile environments [7].

Exploiting physical layer parameters in order to attain different security aspects has been widely encouraged [8]–[10] as it provides less complexity and lighter cost as compared to the conventional security mechanisms. Different previous works in the literature propose authentication schemes that are based on physical layer approaches. For example, in [11], the time-varying carrier frequency offset of the transmitter is used as an RF signature for authentication purpose. In [12], a hypothesis testing is applied to determine whether the current received message and the previous one are from the same transmitter. Specifically, the channel propagation effects in the current and the previous messages are compared in order to verify if both received messages are sent by the same transmitter or not. It assumes that the transmitter is already authenticated in the beginning, and the proposed scheme serves as a physical-layer verification process that avoids repeating the conventional authentication. However, in case of mobile users, it becomes unrealistic assumption that channel propagation effects remain static over time. The difference between two consecutive noise-mitigated channel impulse response is adopted in [13] as an authentication base. Alternatively, the phase response is used for authentication in multi carrier systems in [14]. A two dimensional quantization algorithm that enhances the physical-layer authentication is proposed in [15] which overcomes the impact of noise and channel estimation errors. In [16], the same authors of [12] have alleviated the negative impact of the mobility on their proposal by considering data are transmitted in burst that contains multiple frames. Thus, at least one probed channel response of the last data burst is used to authenticate the next data burst. A similar approach has been followed in [17] based on a MIMO scenario and different attack strategies. Unlike the above mentioned works, in [18], the power spectral density of the channel realizations has been considered as an authentication base. Specifically, the power spectral density of the current channel realization is compared to the previous ones through a hypotheses test. If they are identical, subsequent messages will be authenticated; otherwise, sender is considered as an attacker. However, there are two main drawbacks in [12], [18]. First, if an attacker can get one transmitted message authenticated, then it will get subsequent messages authenticated as well. Second, all of them suffer from the inefficient performance in highly mobile users due to the time varying channel characteristics. Thus, attackers might be able to successfully authenticate messages. while legal users encounter high authentication fail rate.

Previous works require an entity re-authentication process, through a conventional cryptographic protocol, when the message authentication fails, which increases significantly the overhead. In this paper we solve this issue by proposing a novel physical layer authentication approach to re-authenticate the communicators. Two main assumptions have been considered in the proposed scheme. First, the channel responses of MIMO scheme are assumed available exclusively at the legitimate transmitter and the receiver. This can be performed using channel reciprocity in TDD without a need for a feedback link [12]. Second, an initial authentication phase is performed using conventional authentication protocols. The channel response matrix at the initial authentication phase is stored at both sides as it will be used later in the re-authentication of the same transmitter rather than the conventional authentication. Specifically, at each entity re-authentication phase, the initial channel response together with the current channel response are used to generate a set of *authentication signals*. Then, the transmitter will precode its transmitted signals from all antennas, based on the current channel response, in order to deliver the predefined authentication signals at all receive antennas. If a predefined number of the authentications signals is detected at the receiver, the transmitter is successfully authenticated. After each successful entity re-authentication phase, the stored channel matrix is updated according to a function whose inputs are the previously stored channel and the current channel matrix. Then, subsequent message transmissions can be compared with the updated channel characteristics for message authentication purposes, without requiring a new cryptographic-based authentication process between communicators. As such, a high performance is expected even in the case of the mobile users. A mathematical analysis of the authentication fail rate are presented along with investigation of the impact of different parameters. Moreover, a suitable attack model is considered and its performance is analyzed as well.

The rest of this paper is organized as follows. Section II describes the system model, while Section III presents the proposed authentication scheme. In Section IV, an attack model has been considered and analyzed. Section V explores theoretical and simulation results, and conclusions are drawn in Section VI.

II. System Model

The considered system model consists of two communicators, Alice and Bob, as shown in Fig. 1. Alice acts as a legal transmitter and is equipped by N_t transmit antennas, while Bob acts as receiver and is equipped by N_r receive antennas. The channel matrix between Alice and Bob is denoted by $\mathbf{H}$, where its entries h_{ij} ($1 \leq i \leq N_t$ and $1 \leq j \leq N_r$) represents the channel response between the i^{th} transmit antenna and the j^{th} receive antenna. Without loss of generality, h_{ij} is modeled as a complex Gaussian random variables with zero means and σ^2 variance. The received signal at the j^{th} receive antenna, denoted by y_j, is given as follows

$$y_j = \sum_{i=1}^{N_t} h_{ij} x_i + n_j \tag{1}$$

where x_i is the transmitted signal from the i^{th} antenna, and n_j is an additive white Gaussian noise with zero mean and σ_n^2 variance.

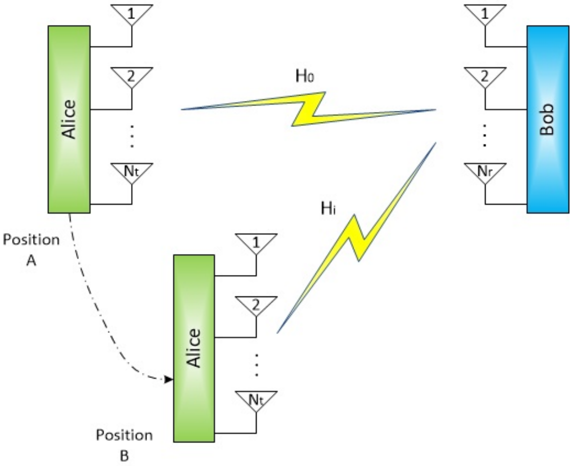

Fig. 1. *The considered system model of Alice and Bob. Alice is assumed a mobile user.*

Alice is assumed a mobile user, while Bob always has a fixed position. The channel response between them is assumed correlated over time. Thus, the channel matrix at a specific time instant $\mathbf{H}_t$ is expressed as follows

$$\mathbf{H}_t = \rho \mathbf{H}_{t-1} + \sqrt{1-\rho^2}\mathbf{H} \tag{2}$$

where $\mathbf{H}_{t-1}$ represents the channel matrix of the previous time instant, $0 \leq \rho \leq 1$ is the time correlation coefficient, and $\mathbf{H}$ is independent of $\mathbf{H}_{t-1}$. The value of ρ depends on the mobility of Alice, where if Alice stays on the same position over the two consecutive time instants, a large value of ρ should be assumed. Otherwise; if Alice moves in another position, the value of ρ is reduced.

Prior data transmission, a channel estimation process is performed by Alice and Bob. The results of this process are available only for the two ends and hidden from any other party. This can be accomplished by avoiding the feedback link between Alice and Bob, where channel response is estimated individually by Alice and Bob by forward and reverse link pilots in TDD systems [12].

At the beginning, an initial authentication phase is accomplished once between Alice and Bob using a pre-shared private key [2]. The estimated channel matrix during the initial phase is stored at both sides, and denoted by $\mathbf{H}_0$.

III. The Proposed Authentication Scheme

As mentioned earlier, conventional authentication protocols generate a heavy overhead, and consequently, consume a significant portion of the available resources. To this end, lightweight authentication schemes are highly required. Previous physical-layer authentication schemes show a good performance of semi-static users. However, in the case of mobile users, their performance is significantly degraded. In the following we present a physical-layer entity re-authentication scheme for mobile MIMO-based users. The proposed scheme follows the same approach of previous works for message authentication, but it introduces a novel physical layer entity re-authentication scheme to re-authenticate the communicators when the message authentication fails due to channel variations. It is worth noting that previous works rely on conventional entity authentication (generally PKI-based authentication) to re-authenticate the communicators. The proposed approach provides an effective manner to perform a non-cryptographic entity authentication.

The proposed scheme includes three phases, namely, the *initialization phase*, the *message authentication phase* and the *entity re-authentication phase.* In the initialization phase, a conventional public key authentication [2] is used to authenticate Alice. The channel responses matrix during the initialization phase, denoted by $\mathbf{H}_0$, is stored at Alice and Bob. During next data transmissions, the message authentication phase is run by Bob. Specifically, Bob always verifies if the transmitter is still Alice or not. For this purpose, Bob uses any of the physical-layer message authentication schemes [12]-[18]. In detail, to verify Alice at time t, Bob compares the difference between $\mathbf{H}_0$ and $\mathbf{H}_t$ to predefined threshold (λ) as follows

$$\mathbf{\Delta_H} = \|\mathbf{H}_0 - \mathbf{H}_t\|^2 \lessgtr \lambda \tag{3}$$

if $\mathbf{\Delta_H} \leq \lambda$, Bob will verify Alice. Otherwise, $\mathbf{\Delta_H} > \lambda$, Bob will realize that either Alice has moved to another position or the transmitter is not Alice. Accordingly, Bob will ask Alice to re-authenticate himself. The entity re-authentication phase is performed as follows

1) Both Alice and Bob will estimate the current channel response $\mathbf{H}_t$.
2) Both Alice and Bob will calculate $\mathbf{Z}_t$ as follows
$$\mathbf{Z}_t = f\big(\mathbf{H}_0, \mathbf{H}_t\big) \tag{4}$$
where $\mathbf{Z}_t$ is an $N_r \times 1$ vector, and $f(\cdot)$ is predefined function between Alice and Bob. The elements of $\mathbf{Z}_t$ are called the authentication signals.
3) Alice will calculate a $N_t \times 1$ transmission vector $\mathbf{X}_t$ as follows
$$\mathbf{Z}_t = \mathbf{H}_t\mathbf{X}_t \tag{5}$$
and the calculated $\mathbf{X}_t$ will be transmitted towards Bob. Notice that the j^{th} element of $\mathbf{Z}_t$, denoted by z_j, is expressed as follows
$$z_j = \sum_{i=1}^{N_t} h_{ij}x_i \tag{6}$$
4) At Bob's side, the received signal at the j^{th} antenna, denoted by y_j, is given as follows
$$y_j = \sum_{i=1}^{N_t} h_{ij}x_i + n_j = z_j + n_j \tag{7}$$
where n_j ($1 \leq j \leq N_r$) is an additive white complex Gaussian noise with zero mean and σ_n^2 variance.
For all receive antennas, Bob will compare the difference between y_j and z_j to the predefined threshold δ as follows
$$\|y_j - z_j\|^2 \lessgtr \delta \tag{8}$$
if it is less than δ, the j^{th} authentication signal is considered correctly received. Otherwise, it will be considered incorrectly received.
5) According to the previous step, if the number of the authentication signals that are correctly received is larger than or equal to the predefined threshold K, Alice will be authenticated. Otherwise, the transmitter will be considered an attacker and will not be authenticated.
6) In the case that Alice is authenticated in step 5, the channel matrix $\mathbf{H}_0$ will be removed and the current channel matrix $\mathbf{H}_t$ will be stored as $\mathbf{H}_0$. Therefore, for any next transmission, message authentication will be performed according to (3).

Notice that applying conventional authentication protocols in all phases is a huge expenditure in users' resources. On the other hand, although physical layer message authentication schemes [12]- [18] are considered lightweight, their efficiency is very low in case of mobile users because they require the entities to re-authenticate through conventional crypto-based protocols, generally based on PKI. However, the proposed scheme works efficiently even for mobile users and it avoids the crypto-based re-authentication phase.

Another issue that worths emphasizing is that the additional computational complexity of the proposed scheme mainly depends on the chosen function $f(\cdot)$ in (5). Thus, simplifying the chosen function leads to a slight increase in the computational complexity as compared to the previous physical-layer techniques.

A. Mathematical Analysis

In this section, the performance of the proposed scheme is investigated in terms of the message authentication-fail rate and the entity re-authentication-fail rate.

From (3), the message authentication-fail probability, denoted by η, can be expressed as follows

$$\eta = \text{Prob.}\{\mathbf{\Delta_H} = \|\mathbf{H}_0 - \mathbf{H}_t\|^2 > \lambda\} \tag{9}$$

based on(2), $\mathbf{\Delta_H}$ has a gamma distribution Gamma$\big(N_r N_t, 2-2\rho\big)$ with the following Cumulative Distribution Function (CDF) :

$$P(x) = \frac{1}{(N_r N_t - 1)!}\gamma(N_r N_t, (2-2\rho)x) \tag{10}$$

where $\gamma(\cdot,\cdot)$ is the incomplete gamma function. Consequently, η is expressed as follows

$$\eta = 1 - \frac{1}{(N_r N_t - 1)!}\gamma(N_r N_t, (2-2\rho)\lambda) \tag{11}$$

Notice that for static users (constant ρ), the threshold λ can be tuned to reduce the message authentication-fail probability. However, as the proper choice of λ depends on ρ, the message authentication-fail rate cannot be guaranteed for mobile users since ρ varies as users move. Thus, the entity re-authentication phase is required for mobile users.

The entity re-authentication-fail probability, denoted by β, can be derived as follows

$$\beta = \sum_{k=0}^{K-1} \binom{N_r}{k} \zeta^k (1-\zeta)^{N_r - k} \tag{12}$$

where ζ is the probability that an authentication signal is correctly received. We consider ζ is identical for all authentication signals. Based on (8), ζ is given as follows

$$\zeta = \text{Prob.}\{\|y_j - z_j\|^2 \leq \delta\} = \text{Prob.}\{\|n_j\|^2 \leq \delta\} \tag{13}$$

Notice that $\|n_j\|^2$ is exponential distributed with a rate $\frac{1}{\sigma_n^2}$ with the following CDF

$$F(x) = 1 - \exp(-\frac{x^2}{\sigma_n^2}) \tag{14}$$

Thus, ζ can be rewritten as follows

$$\zeta = 1 - \exp(-\frac{\delta^2}{\sigma_n^2}) \tag{15}$$

Finally, the probability that the whole authentication process fails and the transmitter is declared as attacker is given as follows

$$\alpha = \eta\beta \tag{16}$$

B. Low SNR Case

Under low SNR conditions, the impact of the added noise is larger. Consequently, the entity re-authentication fail rate of the proposed scheme will be higher. Thus, in this section, we enhance the proposed scheme to alleviate the noise impact. The enhancement implies that re-authentication process can be repeated more than once, say L times. Accordingly, an authentication signal is considered correctly detected if it has been detected at least once among the L times.

Accordingly, the probability that an authentication signal is correctly detected, denoted by $\zeta^{(L)}$, is given as follow

$$\zeta^{(L)} = \text{Prob.}\{\min_{l=1,\ldots,L}(\|y_j^l - z_j^l\|^2) \leq \delta\} \tag{17}$$

which can be simplified as follows

$$\zeta^{(L)} = \text{Prob.}\{\min_{jl=1,\ldots,L}(|n_j^l|^2) \leq \delta\} \tag{18}$$

The value of $\min(|n_j^l|^2)$ is the minimum of L exponential random variables. Hence, using order statistics, it is Cumulative Distribution Function (CDF) is given as follows [19]:

$$P_{1:L}(x) = 1 - \big(1 - F(x)\big)^L = 1 - e^{\frac{-Lx^2}{\sigma_n^2}} \tag{19}$$

where $F(x)$ is the exponential CDF given in (14). (19) can be used to estimate $\zeta^{(L)}$ as follows

$$\zeta^{(L)} = P_{1:L}(\delta) = 1 - e^{\frac{-L\delta^2}{\sigma_n^2}} \tag{20}$$

Therefore, the re-authentication fail rate can be reduced in low SNR conditions to be as follows

$$\beta^{(L)} = 1 - \sum_{k=K}^{N_r} \binom{N_r}{k} \big(1 - e^{\frac{-L\delta^2}{2\sigma_n^2}}\big)^k e^{\frac{-L\delta^2(N_r - k)}{2\sigma_n^2}} \tag{21}$$

Notice that in case that $L = 1$, (20) and (21) are reduced to (15) and (12), respectively.

IV. Attack Model

As the proposed authentication scheme depends mainly on the instantaneous channel characteristics, only attackers that have partial or perfect knowledge about the channel responses can represent a significant threat to the proposed scheme. To this end, we consider an attack model that is perfectly aware of the instantaneous channel responses between himself and Alice and between himself and Bob. However, only an imperfect knowledge is available at the attacker about the channel between Alice and Bob (i.e, $\mathbf{H}$). The main intention of the attack is to impersonate Alice and to get his message authenticated at Bob's receiver. Without loss of generality, the attacker is assumed to have the same number of transmit and receive antennas of Alice and Bob (i.e, N_t and N_r, respectively). Also, seeking for a seamless analysis, we use different notations for the variables related to the attacker as follows. $\mathbf{G}$ denotes the channel matrix between the attacker and Bob, $\mathbf{S}$ denotes the formulated transmission vector from the attacker in the re-authentication process, and $\mathbf{P}$ denotes the authentication signals to be delivered by the attacker to Bob. Fig. 2 describes the considered attack model.

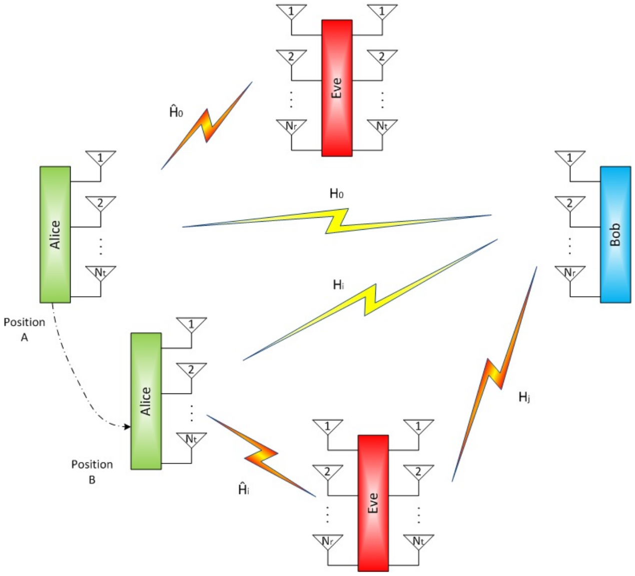

Fig. 2. *The considered system model of Alice and Bob in the presence of an attacker (Eve).*

In the following, three different attack strategies are considered based on the available information about $\mathbf{H}_0$, $\mathbf{H}_t$ and $\mathbf{X}_t$ at the attacker:

A. Attack Strategy A

Strategy A will be followed by an attacker that have only partial information about $\mathbf{H}_0$. Specifically, we assume that the attacker has a corrupted version of $\mathbf{H}_0$, denoted by $\hat{\mathbf{H}}_0$, that is given as follows

$$\hat{\mathbf{H}}_0 = \mathbf{H}_0 + \mathbf{H}_e \tag{22}$$

where $\mathbf{H}_e$ is an estimation error matrix with entries modeled as complex Gaussian random variables with zero mean and ϵ_A variance. Attack strategy A works as follows

1) The attack contacts Bob and both estimate the channel $\mathbf{G}_t$
2) Both will calculate the authentication signals vector using the public function $f(\cdot)$. Specifically, the calculated authentication vector by Bob is given as follows
$$\mathbf{P}_t = f\big(\mathbf{H}_0, \mathbf{G}_t\big) \tag{23}$$
while the attacker will calculate a different authentication vector as follows
$$\hat{\mathbf{P}}_t = f\big(\hat{\mathbf{H}}_0, \mathbf{G}_t\big) \tag{24}$$
3) The attacker calculates its transmission vector $\mathbf{S}_t$ such that $\hat{\mathbf{P}}_t = \mathbf{G}_t\mathbf{S}_t$, and transmits it towards Bob.
4) The received vector at Bob is given as follows
$$\mathbf{Y}_t = \hat{\mathbf{P}}_t + \mathbf{N}_t \tag{25}$$
where each element of $\mathbf{Y}_t$ is compared to the corresponding element in $\mathbf{P}_t$, as given in (8).

B. Attack Strategy B

In this strategy, the attacker has no knowledge about $\mathbf{H}_0$ but it has a partial knowledge about $\mathbf{H}_t$. Specifically, the attacker has a corrupted version of $\mathbf{H}_t$, denoted as $\hat{\mathbf{H}}_t$. Strategy B works as follows

1) The attack contacts Bob and both start a channel estimate process. However, the attacker will modify the pilot signals such that Bob is tricked and the channel response appears as $\hat{\mathbf{H}}_t$ at Bob's receiver.
2) The attacker already overheard the authentication phase between Alice and Bob, and obtained a corrupted version of Alices's transmission vector, denoted by $\hat{\mathbf{X}}_t$
3) Both will calculate the authentication signals vector using the public function $f(\cdot)$. Specifically, the calculated authentication vector by Bob is given as follows
$$\mathbf{P}_t = f\big(\mathbf{H}_0, \hat{\mathbf{H}}_t\big) \tag{26}$$
while the attacker will calculate a different authentication vector as follows
$$\hat{\mathbf{P}}_t = \hat{\mathbf{H}}_t\hat{\mathbf{X}}_t \tag{27}$$
4) The attacker calculates its transmission vector $\mathbf{S}_t$ such that $\hat{\mathbf{P}}_t = \mathbf{G}_t\mathbf{S}_t$, and transmits it towards Bob.

5) The received vector at Bob is given as follows

$$\mathbf{Y}_t = \hat{\mathbf{P}}_t + \mathbf{N}_t \tag{28}$$

where each element of $\mathbf{Y}_t$ is compared to the corresponding element in $\mathbf{P}_t$, as given in (8).

C. Attack Strategy C

This strategy is followed by an attacker in the case that there is no knowledge about either $\mathbf{H}_0$ or $\mathbf{H}_t$. Attack strategy C works as follows

1) The attacker contacts Bob and both estimate the channel $\mathbf{G}_t$.
2) Bob will calculate the authentication signals vector using the public function $f(\cdot)$ as follows

$$\mathbf{P}_t = f\left(\mathbf{H}_0, \mathbf{G}_t\right) \tag{29}$$

3) The attacker already overheard the authentication phase between Alice and Bob, and obtained a corrupted version of Alices's transmission vector, denoted by $\hat{\mathbf{X}}_t$.
4) The attacker transmits $\hat{\mathbf{X}}_t$ towards Bob.
5) The received vector at Bob is given as follows

$$\mathbf{Y}_t = \hat{\mathbf{P}}_t + \mathbf{N}_t \tag{30}$$

where $\hat{\mathbf{P}}_t$ is given as follows

$$\hat{\mathbf{P}}_t = \mathbf{G}_t\hat{\mathbf{X}}_t \tag{31}$$

Each element of $\mathbf{Y}_t$ is compared to the corresponding element in $\mathbf{P}_t$, as given in (8).

V. Performance Evaluation and Simulation Results

In this section, we evaluate the performance of the proposed scheme by investigating all the involved parameters. The performance is measured in terms of the authentication fail rate for Alice and and the considered attack strategies. The curves obtained by Monte Carlo simulations where 10^5 iterations are considered. At each iteration, the one sided noise power σ_n^2 is computed by $\sigma_n^2 = \frac{E[\mathbf{X}^2]}{\text{SNR}}$, where $E[\mathbf{X}^2]$ is the transmitted signal power. Moreover, during the simulations, the function $f(\cdot)$ given in (4) is fixed as follows $f_j(\mathbf{H}_0, \mathbf{H}\ _t) = \text{diag}\{\mathbf{H}_0\mathbf{H}_t^T\}$ where $\text{diag}\{\cdot\}$ represents the diagonal operator, and ^{T} is the transpose operator.

Seeking for a general model of the mobile user, we denote the probability that the transmitter will move at a specific time instant to different location by γ (called mobility probability). In case that the user has moved to another location, the channel correlation coefficient is denoted by ρ_m and is assumed 0.5. On the other hand, if the user has not moved, the channel correlation coefficient is denoted by ρ_s and is assumed 0.9.

In order to highlight the motivation behind our proposal, we investigate the performance of the previous physical-layer schemes ([12]- [16]) in case of mobile users. Specifically, the fail rate of the message authentication given in (4) is plotted versus the mobility probability γ in Fig. 3 at different values of the threshold λ. As shown, the message authentication fail rate increases as the mobility of the transmitter increases. Increasing the value of λ improves the message authentication process. However, for highly mobile users, the message authentication fail rate reaches 1. Notice that increasing λ is not always feasible since it may allow attackers to authenticate illicit messages. Also, we should expect that assuming lower values of ρ_m will definitely lead to a worse performance of the message authentication phase.

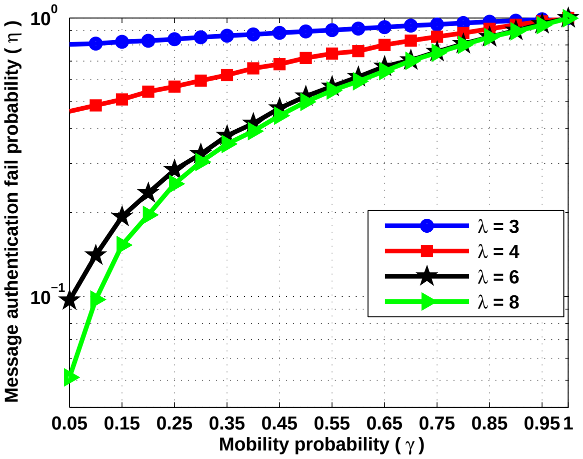

Fig. 3. *The message authentication fail rate versus the mobility probability (γ) for different values of the threshold λ. ($N_t = 4$, $N_r = 4$, $\rho_s = 0.9$, $\rho_m = 0.5$ and SNR $= 10\,dB$).*

Based on the results in Fig. 3, the previous physical-layer message authentication schemes have a poor performance for mobile users. Thus, our proposed scheme is highly motivated. The proposed scheme implies that if the message authentication phase fails, another physical-layer entity re-authentication phase should be performed in order to authenticate the transmitter. Fig. 4 shows the entity re-authentication fail rate (i.e, β given in (12)) and the overall authentication fail rate (i.e, α given in (16)) of the proposed scheme versus the average SNR. Compared to previous works that consider only message authentication schemes, the physical-layer entity re-authentication phase can enhance the overall authentication fail rate since it decreases the need for crypto-based authentication protocols. Clearly, the fail rates decrease as the SNR increases due to the less impact of the noise on the re-authentication phase. Also, notice the huge reduction in the authentication fail rate in the two figures 3 and 4. For example, at $\gamma = 0.2$,

$\lambda = 3$ and SNR=10 dB, the previous works achieves 0.8 (see Fig. 3), while the proposed scheme is able to reduce it to only 0.02 (Fig. 4).

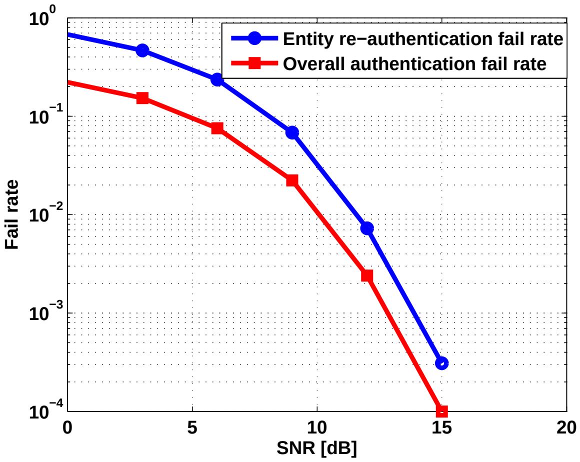

Fig. 4. *The overall authentication fail rate (α) and the entity re-authentication fail rate (β) versus the average SNR. ($N_t = 4$, $N_r = 4$, $\rho_s = 0.9$, $\rho_m = 0.5$, $\gamma = 0.2$, $\lambda = 3$, $K = 1$ and $\delta = 0.5$).*

Several parameters affect the performance of the proposed scheme, such as δ, K and the average SNR. In Fig. 5, the impact of the parameter δ is shown where the authentication fail rate is plotted versus the average SNR at different values of δ. Increasing the threshold δ decreases the authentication fail rate because high values of δ means that a larger noise power can be tolerated at the receiver and more signals are considered correctly authenticated. However, δ should not be very large in order to avoid an incorrect authentication of an attacker.

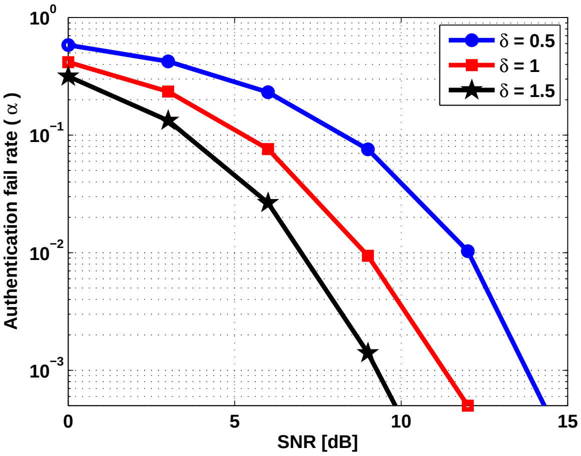

Fig. 5. *The authentication fail rate versus the average SNR for different values of the threshold δ. ($N_t = 4$, $N_r = 4$, $\rho_s = 0.9$, $\rho_m = 0.5$, $\lambda = 3$, $K = 1$ and $\eta = 0.2$).*

The authentication threshold K has a similar effect of δ. In Fig. 6, the authentication fail rate is depicted versus the average SNR at different values of K. At each value of K, at least K receive antennas must correctly identify their corresponding authentication signals in order to authenticate Alice. Thus, high values of K show increase the authentication fail rate as shown in Fig. 6.

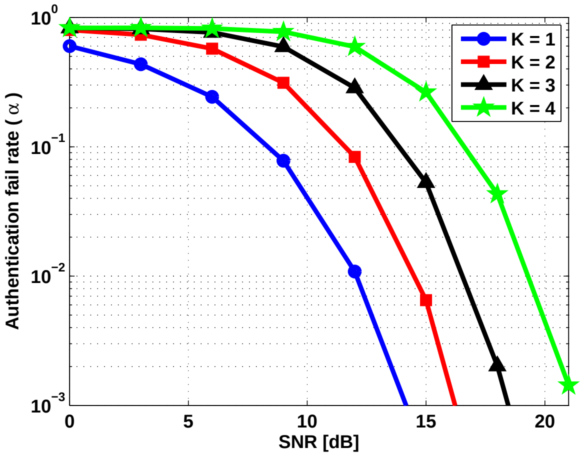

Fig. 6. *The authentication fail rate versus the average SNR for different values of the threshold δ. ($N_t = 4$, $N_r = 4$, $\rho_s = 0.9$, $\rho_m = 0.5$, $\lambda = 3$, $\eta = 0.2$ and $\delta = 0.5$).*

The resilience against attacks is of a paramount importance in order to evaluate any authentication scheme. Thus, aiming at analyzing the resilience against the considered attack strategies in Section IV, we assume that the message authentication fail probability is almost one (i.e, the message authentication phase will always fail). The purpose of this assumption is to better evaluate the proposed re-authentication scheme which is the major contribution of this work. Such an assumption can be realized by setting a low value of λ (see Fig. 3). Also, for a seamless analysis, we consider that the partial information gained by an attacker on either $\mathbf{H}_o$, $\mathbf{H}_t$, $\mathbf{Z}$, or $\mathbf{X}_t$ is modeled by an error matrix with the same dimensions and entries are modeled by complex Gaussian random variables with zero mean and ϵ variance (exactly as formulated in (22)).

Fig. 7 plots the authentication fail rate versus the average SNR for Alice and the three different attack strategies considered in Section IV. For all attack strategies, the error variance is assumed equal to the noise power, i.e, $\epsilon = \sigma_n^2$. For all curves, as SNR increases, the noise power decrease, and hence the authentication fail rate decreases as well. However, the big difference between the legitimate transmitter Alice and the attacker is clear and evident. Comparing the three different attack strategies, it is noted that strategy A has the lowest fail rate, while the others (strategies B and C) encounter a very high authentication fail rate. This is due to the fact that an attacker followed strategy A has partial information about $\mathbf{H}_o$ which is the most effective parameter in the proposed authentication scheme. On other hand, an attacker following strategy B or C does not have any information on $\mathbf{H}_o$, which significantly degrades the performance. Moreover, in strategy B, an attacker relies on partial information about $\mathbf{H}_t$ and $\mathbf{X}_t$, which degrades the performance since two sources of error are present. Regarding strategy C, information about $\mathbf{H}_o$ and $\mathbf{H}_t$ is completely absent, and the strategy is based only in a partial information about $\mathbf{X}_t$.

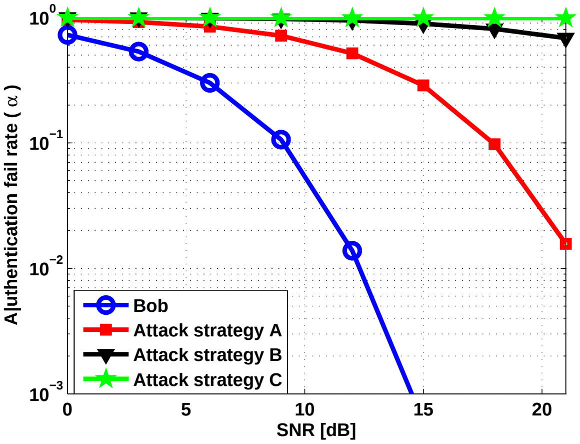

Fig. 7. *The authentication fail rate versus the average SNR for Alice and the different attack strategies considered in Section IV. ($N_t = 4$, $N_r = 4$, $\rho_s = 0.9$, $\rho_m = 0.5$, $\lambda = 2$, $\eta = 0.2$, $K = 1$, $\delta = 0.5$ and $\epsilon = \sigma_n^2$).*

As concluded from Fig. 5, increasing the threshold δ will decrease the authentication fail rate. In Fig. 8, the impact of δ is revisited regarding the attack strategies considered. Increasing δ allows for detecting authentication signal that are highly corrupted, and therefore, the authentication fail rate will decrease as shown in Fig. 8. However, the impact of increasing δ is more effective in Alice performance compared to the attack strategies considered. This is because attackers have only partial knowledge about the authentication signals, which degrade their performance. Also, it is worth noting that Alice can achieve zero authentication fail rate at $\delta > 2$ while attacker still encounters high authentication fail rate.

VI. Conclusions and Future Work

A physical-layer authentication scheme for MIMO-based mobile users has been proposed in this paper. The proposed scheme is based on delivering predefined authentication signals at the receive antennas. The transmitted signals are precoded based on the assumption that channel responses are exclusively available at the transmitter and the receiver. Results have shown a promising performance of the proposed scheme against attackers that have a partial knowledge about channel responses.

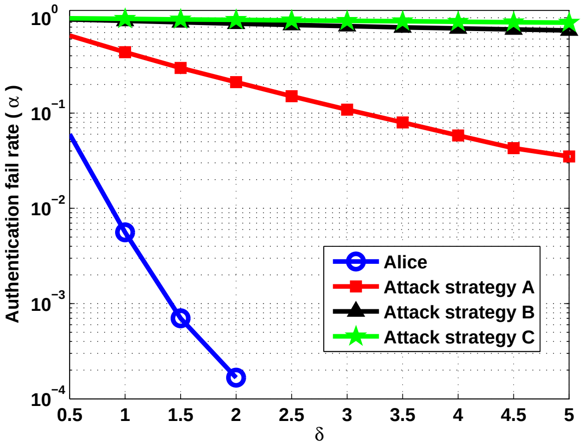

Fig. 8. *The authentication fail rate versus the threshold δ for Alice and the different attack strategies considered in Section IV. ($N_t = 4$, $N_r = 4$, $\rho_s = 0.9$, $\rho_m = 0.5$, $\lambda = 2$, $\eta = 0.2$, $K = 1$, SNR $= 10\,dB$ and $\epsilon = \sigma_n^2$).*

As a future work, the impact of the channel estimation errors on the performance of the proposed scheme can be investigated and analyzed. Also, the computational complexity of the proposed scheme can be reduced in order to improve its applicability in real scenarios.

References

[1] K. Zeng et al., "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, pp. 56-62, Oct. 2010.

[2] A. J. Menezes et al., *Handbook of Applied Cryptography.* CRC Press, 1996.

[3] J. Katz and Y. Lindell, *Introduction to Modern Cryptography.* Chapman & Hall/CRC, 2008.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014.

[5] L.Y. Paul, J.S. Baras, and B.M. Sadler, "Physical-layer authentication." *IEEE Transactions on Information Forensics and Security,* 3.1 (2008): 38-51.

[6] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang and H. H. Chen, "Physical layer security in wireless networks: a tutorial," in *IEEE Wireless Communications,* vol. 18, no. 2, pp. 66-74, April 2011

[7] S. Althunibat et al., "A Physical-Layer Security Scheme by Phase-Based Adaptive Modulation," in *IEEE Transactions on Vehicular Technology,* vol. 66, no. 11, pp. 9931-9942, Nov. 2017.

[8] H. Alves et al., "Performance of Transmit Antenna Selection Physical Layer Security Schemes", *IEEE Signal Process. Lett.,* vol. 19, no. 6, pp. 372-375, June 2012.

[9] H. Hui et al., "Secure Relay and Jammer Selection for Physical Layer Security," *IEEE Signal Process. Lett.,* vol. 22, no. 8, pp. 1147-1151, Aug. 2015.

[10] N. Romero-Zurita et al., "PHY Layer Security Based on Protected Zone and Artificial Noise," *IEEE Signal Process. Lett.,* vol. 20, no. 5, pp. 487-490, May 2013.

[11] W. Hou, X. Wang, J. Y. Chouinard and A. Refaey, "Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets," in *IEEE Transactions on Communications,* vol. 62, no. 5, pp. 1658-1667, May 2014

[12] L. Xiao et al., “Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication,” *IEEE ICC,* Glasgow, 2007, pp. 4646-4651.

[13] F.J. Liu et al., “Robust physical layer authentication using inherent properties of channel impulse response.” *IEEE MILCOM*, 2011.

[14] X. Wu and Z. Yang. “Physical-layer authentication for multi-carrier transmission.” *IEEE Communications Letters,* 19.1 (2015): 74-77.

[15] F.J. Liu et al., “A two dimensional quantization algorithm for CIR-based physical layer authentication.” *IEEE ICC*, 2013.

[16] L. Xiao et al., “A Physical-Layer Technique to Enhance Authentication for Mobile Terminals,” *IEEE ICC,* Beijing, 2008, pp. 1520-1524.

[17] P. Baracca et al., “Physical Layer Authentication over MIMO Fading Wiretap Channels,” in *IEEE Trans. Wireless Commun.,* vol. 11, pp. 2564-2573, July 2012.

[18] J. K. Tugnait, “Wireless User Authentication via Comparison of Power Spectral Densities,” *IEEE J. Sel. Areas Commun.,* vol. 31, no. 9, pp. 1791-1802, Sep. 2013.

[19] N. Balakrishnan, and A.C. Cohen, *Order statistics and inference: estimation methods.* Elsevier, 2014.