# Physical Layer Authentication over an OFDM Fading Wiretap Channel

Paolo Baracca
Department of Information Engineering
University of Padua
baraccap@dei.unipd.it

Nicola Laurenti
Department of Information Engineering
University of Padua
nil@dei.unipd.it

Stefano Tomasin
Department of Information Engineering
University of Padua
tomasin@dei.unipd.it

## ABSTRACT

Precise channel estimation at the physical layer allows to authenticate the source of a message in a wireless environment without the need of a pre-shared secret key based on the rapid spatial decorrelation of the channel. We consider the authentication scheme proposed by Xiao *et al.* and modify to suit a wiretap environment with orthogonal frequency division multiplexing (OFDM) modulation and fading channels. By formulating a nearly optimal attack strategy, and allowing some correlation among the channels, we evaluate the robustness of the scheme against challenging conditions and discuss the choice of system parameters.

## Categories and Subject Descriptors

C.2.0 [**Computer-communication networks**]: General—*Security and protection*; C.2.1 [**Computer-communication networks**]: Network architecture and design—*Wireless communication*

## General Terms

Security

## Keywords

OFDM, physical layer authentication, wiretap channel, channel estimation

## 1. INTRODUCTION

The problem of message authentication is certainly, together with that of message confidentiality, one of the most common tasks in information security. The traditional cryptographic solution is to employ hash and sign protocols so that forging and illegitimate modification of the message can be detected.

It is perhaps surprising that while physical layer secrecy, based on information-theoretic grounds, enjoys a rich literature and many promising solutions, corresponding results for the authentication problem are still lacking. The seminal paper by Maurer [1] can be considered the authentication counterpart of Shannon's fundamental secrecy paper, since it performs an information theoretic analysis of authentication with a secret key and noiseless transmission, in the framework of hypothesis testing. His work is extended in [2] to introduce legitimate distortions of the message and joint typicality decoding, while [3] takes into account a noisy channel, deriving useful bounds on the probability of a successful attack for arbitrarily low false alarm rate.

The current attempts at using physical layer characteristics as authentication keys for the message source follow different approaches. One possibility assumes the existence of a pre-shared secret key that is hidden in the modulation, and detected by the receiver [4, 5]. In keyless transmitter-based (aka wireless fingerprinting) methods, device-specific non-ideal transmission parameters that can be extracted from the received signal are identified as characteristics of the claimed source, and are compared to those from previous authenticated transmissions.

On the other hand, channel-based schemes compare the estimated channel response from the current message to previous transmissions by the claiming source (thus actually authenticating the position of the transmitter rather than its identity). It is clear that in order to be able to distinguish channels from two different positions, some source of diversity must be exploited, either spatial using the set of power levels measured at many distinct and cooperating receivers [6, 7, 8] or in the frequency domain with the use of wideband transmission and channel estimation [9, 10, 11, 12]. However in the above cited works, the attacker is assumed to only use higher layer identity forging (e.g. spoofing of MAC address) and does not try to cheat the physical layer authentication methods into assuming a false channel response.

Channel diversity in the frequency domain is efficiently exploited with OFDM, which has become the most widely used modulation scheme in wired and wireless communication systems in the last few years. It avoids intersymbol interference using a guard interval (GI) and mitigates frequency selectivity of multipath channels with a simple one-tap equalizer per-subcarrier. Indeed, almost all the recent standards developed for wireless scenarios such as digital video broadcasting (DVB), long term evolution (LTE) by 3GPP and wireless LAN (802.11) adopt OFDM in order to meet high bit-rate requirements.


SECURENETS 2011, May 16, Paris, France

DOI 10.4108/icst.valuetools.2011.245789

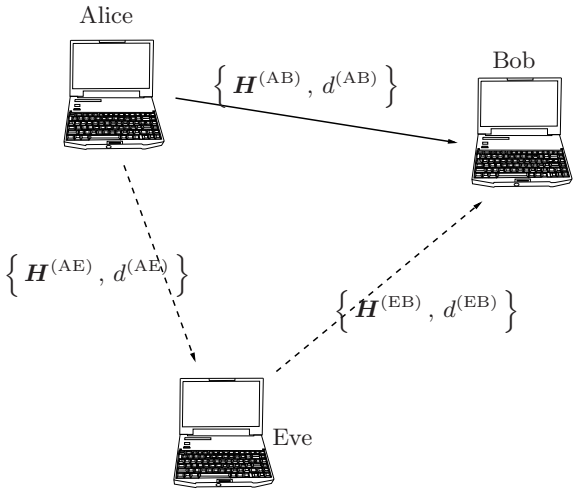


**Figure 1: The authentication channel model.**

In this work, we consider the scheme proposed in [9, 10] and we discuss the choice of channel estimation techniques and parameters, and evaluate its robustness to clever attack strategies in a wiretap OFDM environment with Rayleigh fading channels.

The rest of the paper is organized as follows. In Section 2 we present the system model, with the statistical description of the channels involved. In Section 3 we derive an effective authentication technique within the hypothesis testing framework, based on the generalized likelihood ratio test (GLRT). Then in Section 4 we formulate effective strategies for the attacker, based on sequential guessing. In Section 5 we numerically evaluate the performance of the scheme in terms of the probability of missed detection (which represents a successful attack) and eventually draw conclusions in Section 6.

*Notation*: We use $(\cdot)^T$ to denote transpose and $(\cdot)^*$ conjugate transpose. $\mathbf{0}_{N\times M}$ denotes the matrix of size $N\times M$ with all zero entries, $\boldsymbol{I}_N$ the identity matrix of size $N$, $\det(\boldsymbol{X})$ the determinant of matrix $\boldsymbol{X}$ and $[\boldsymbol{X}]_{n,m}$ the entry on row $n$ and column $m$ of $\boldsymbol{X}$. Expectation and probability are denoted by $\mathrm{E}[\cdot]$ and $\mathrm{P}[\cdot]$, respectively.

## 2. SYSTEM MODEL

Using the traditional terminology employed by the security community, we consider three different agents: Alice, Bob and Eve. In particular, Alice is the legitimate transmitter who starts the communication, Bob is the legitimate receiver for whom the transmission is intended and Eve is the adversary who transmits toward Bob with the aim of impersonating Alice. Physical-layer authentication develops techniques to provide authentication between Alice and Bob allowing Bob to accept legitimate messages coming from Alice and to refuse illegitimate messages coming from Eve. As shown in Fig. 1 we assume that the three agents are randomly positioned in space and they are connected to each other through wireless channels. Transmissions toward Bob employ OFDM, and each OFDM block includes $N$ pilot tones for channel estimation purposes. In detail, we assume that a known symbol $D_n(i)$ with unit amplitude is transmitted on the $n$-th subcarrier of $i$-th OFDM symbol, as is customary in many standard. The corresponding sample received by Bob can be written as

$$R_n(i) = H_n D_n(i) + W_n(i)\,, \quad n = 0, 1, \ldots, N-1\,, \qquad (1)$$

where $W_n \sim \mathcal{CN}(0, \sigma^2)$ is the noise term and $H_n$ is the channel frequency response (CFR) in correspondence of the pilot tones from either Alice or Eve to Bob.

We assume that all channels are frequency-selective and that the $N$ samples of the frequency response corresponding to the pilot tones are zero-mean complex circularly symmetric Gaussian variables. For the sake of tractability, we also assume that the pilot frequencies are sufficiently spaced apart so that the samples can be modeled as independent and identically distributed, i.e.

$$\boldsymbol{H} = [H_0, H_1, \ldots, H_{N-1}] \sim \mathcal{CN}(\mathbf{0}_{N\times 1}, \boldsymbol{I}_N)\,. \qquad (2)$$

Let $\boldsymbol{H}^{(\mathrm{AB})}$, $\boldsymbol{H}^{(\mathrm{AE})}$ and $\boldsymbol{H}^{(\mathrm{EB})}$ be the frequency response of the channel at pilot tones between Alice and Bob, between Eve and Alice and between Eve and Bob, respectively. We assume time division duplexing, so the Alice-Bob channel is the same as the Bob-Alice channel. We consider the Jakes' model [13, §2] to establish the spatial correlation among the considered channels. The correlation between two channels linking some node Z to two distinct nodes X and Y is modeled as

$$\rho^{(\mathrm{XY})} = J_0\left(2\pi \frac{d^{(\mathrm{XY})}}{\lambda_c}\right)\,, \qquad (3)$$

where $J_0(\cdot)$ is the Bessel function of the first kind, $\lambda_c$ is the carrier wavelength and $d^{(\mathrm{XY})}$ is the distance between the nodes X and Y. From (3), in the case that the distance is high with respect to $\lambda_c$, the related CFRs become almost independent. Thus we have

$$\mathrm{E}\left[\boldsymbol{H}^{(\mathrm{AB})}\boldsymbol{H}^{(\mathrm{AE})*}\right] = \rho^{(\mathrm{EB})}\boldsymbol{I}_N\,, \qquad (4a)$$

$$\mathrm{E}\left[\boldsymbol{H}^{(\mathrm{AB})}\boldsymbol{H}^{(\mathrm{EB})*}\right] = \rho^{(\mathrm{AE})}\boldsymbol{I}_N\,, \qquad (4b)$$

$$\mathrm{E}\left[\boldsymbol{H}^{(\mathrm{AE})}\boldsymbol{H}^{(\mathrm{EB})*}\right] = \rho^{(\mathrm{AB})}\boldsymbol{I}_N\,. \qquad (4c)$$

We can alternatively represent $\boldsymbol{H}^{(\mathrm{AE})}$ and $\boldsymbol{H}^{(\mathrm{EB})}$ in terms of $\boldsymbol{H}^{(\mathrm{AB})}$ using an auto-regressive model of order 1, i.e.

$$\boldsymbol{H}^{(\mathrm{AE})} = \rho^{(\mathrm{EB})}\boldsymbol{H}^{(\mathrm{AB})} + \sqrt{1-\rho^{(\mathrm{EB})2}}\,\boldsymbol{\epsilon}^{(\mathrm{AE})}\,, \qquad (5a)$$

$$\boldsymbol{H}^{(\mathrm{EB})} = \rho^{(\mathrm{AE})}\boldsymbol{H}^{(\mathrm{AB})} + \sqrt{1-\rho^{(\mathrm{AE})2}}\,\boldsymbol{\epsilon}^{(\mathrm{EB})}\,, \qquad (5b)$$

where $\boldsymbol{\epsilon}^{(\mathrm{AE})}, \boldsymbol{\epsilon}^{(\mathrm{EB})} \sim \mathcal{CN}(\mathbf{0}_{N\times 1}, \boldsymbol{I}_N)$ are both complex Gaussian noise vectors independent of $\boldsymbol{H}^{(\mathrm{AB})}$.

## 3. AUTHENTICATION BASED ON CHANNEL ESTIMATION

Authentication between Alice and Bob exploits the rapid spatial decorrelation of the channel in wireless systems. The authentication procedure comprises two phases:

- **Phase 1:** Alice sends a known message to Bob. We assume that there is some way (external to the authentication procedure) to ensure that Alice (and not Eve)

is transmitting to Bob in this phase. This initial transmission enables Bob to obtain a reference estimate of the channel $\hat{\boldsymbol{H}}^{(\mathrm{AB})}$ with respect to Alice.

- **Phase 2:** In this phase Bob is receiving data packets and aims at authenticating the source. Phase two may be repeated many times, i.e. many packets can be sent to Bob. Authentication is performed by comparing the estimate of the channel performed on the message $\hat{\boldsymbol{H}}$ with the reference estimate of phase 1.

We assume block-fading channels, i.e. all the channels connecting the three agents are time-invariant during both phases.

*First Phase.* In the first phase, Alice probes the channel transmitting $M$ OFDM symbols and allowing Bob to store a reliable but noisy estimate of $\boldsymbol{H}^{(\mathrm{AB})}$, i.e.

$$\hat{\boldsymbol{H}}^{(\mathrm{AB})} = \boldsymbol{H}^{(\mathrm{AB})} + \boldsymbol{W}^{(\mathrm{B})}\,, \tag{6}$$

where $\boldsymbol{W}^{(\mathrm{B})}$ is a complex Gaussian noise vector. As in our model we consider a time-invariant channel, $\hat{H}_n^{(\mathrm{AB})}$ can be obtained averaging the channel estimates computed for all the $M$ OFDM symbols, i.e.

$$\hat{H}_n^{(\mathrm{AB})} = \frac{1}{M}\sum_{i=0}^{M-1}\frac{R_n(i)}{D_n(i)}\,, \tag{7}$$

and

$$W_n^{(\mathrm{B})} \sim \mathcal{CN}\left(0, \frac{\sigma^2}{M}\right)\,. \tag{8}$$

*Second Phase.* In the second phase Bob receives a message which comprises $P$ OFDM symbols and uses an hypothesis test [14] to decide if the transmission is performed by Alice or Eve. In particular, let $\hat{\boldsymbol{H}}$ be the estimate of the channel obtained by Bob on the pilots of the message according to (7), where now the average is done over $P$ OFDM blocks. Under the hypothesis $\mathcal{H}_0$ the transmitter is Alice and Bob accepts the message if a chosen test statistic $\Psi$ is below a given threshold $\theta$. On the other hand, under the hypothesis $\mathcal{H}_1$ the transmitter is Eve and Bob refuses the message if $\Psi$ is over the threshold $\theta$:

$$\mathcal{H}_0: \quad \hat{\boldsymbol{H}} = \boldsymbol{H}^{(\mathrm{AB})} + \boldsymbol{W}'\,, \tag{9a}$$

$$\mathcal{H}_1: \quad \hat{\boldsymbol{H}} = \boldsymbol{G} + \boldsymbol{W}'\,, \tag{9b}$$

where $\boldsymbol{W}' \sim \mathcal{CN}(\boldsymbol{0}_{N\times 1}, \sigma^2/P\boldsymbol{I}_N)$ and $\boldsymbol{G}$ is the equivalent channel between Eve and Bob.

Considering that Eve knows the pilot symbols, she can modify the symbols transmitted on the pilot tones with the aim of replicating channel $\hat{\boldsymbol{H}}^{(\mathrm{AB})}$. By substituting $D_n(i)$ with

$$\tilde{D}_n(i) = \frac{D_n(i)}{\hat{H}_n^{(\mathrm{EB})}}G_n\,, \quad n = 0, 1, \ldots, N-1\,, \tag{10}$$

Eve can pretend[1] that her channel to Bob has an arbitrary CFR $\boldsymbol{G}$. Therefore, we introduce a more general attack model than [9] since there Eve was only using her true channel $\boldsymbol{H}^{(\mathrm{EB})}$. We also assume that Eve can estimate $\boldsymbol{H}^{(\mathrm{AE})}$ and $\boldsymbol{H}^{(\mathrm{EB})}$ and exploit spatial correlation between channels. Moreover, as another generalization with respect to [9], we allow $M \neq P$ because the channel estimation for $\hat{\boldsymbol{H}}^{(\mathrm{AB})}$ and $\hat{\boldsymbol{H}}$ could be performed on a different number of OFDM symbols leading to different covariance matrix on channel estimates.

[1] We neglect possible limitations to (10) due to Eve's power constraints.

## 3.1 Generalized Likelihood Ratio Test

The optimum test strategy is the likelihood ratio test, where

$$\tilde{\Psi} = \frac{f\left(\hat{\boldsymbol{H}}|\mathcal{H}_1\right)}{f\left(\hat{\boldsymbol{H}}|\mathcal{H}_0\right)}\,. \tag{11}$$

Using (6) and (9a), Bob completely knows the probability density function (PDF) of $\hat{\boldsymbol{H}}$ under hypothesis $\mathcal{H}_0$, which can be expressed as

$$f\left(\hat{\boldsymbol{H}}|\mathcal{H}_0\right) = \frac{1}{\pi^N\nu^N}\exp\left\{-\frac{1}{\nu}\sum_{n=0}^{N-1}\left|\hat{H}_n - \hat{H}_n^{(\mathrm{AB})}\right|^2\right\}\,, \tag{12}$$

where

$$\nu = \frac{\sigma^2}{M} + \frac{\sigma^2}{P}\,. \tag{13}$$

On the other hand, we have

$$f\left(\hat{\boldsymbol{H}}|\mathcal{H}_1\right) = \frac{M^N}{\pi^N\sigma^{2N}}\exp\left\{-\frac{M}{\sigma^2}\sum_{n=0}^{N-1}\left|\hat{H}_n - G_n\right|^2\right\}\,. \tag{14}$$

However, this would require the knowledge of $\boldsymbol{G}$ by Bob, which is unrealistic. Therefore we resort to the GLRT [14] in which the unknown vector $\boldsymbol{G}$ is substituted by its maximum likelihood estimation. Note that differently to us, [10] assumes that the probability density function (PDF) of $\hat{\boldsymbol{H}}$ under hypothesis $\mathcal{H}_1$ is completely known by Bob by modeling $\boldsymbol{G}$ as a complex Gaussian vector with known mean and covariance matrix. From (9b) the maximum likelihood estimation of $\boldsymbol{G}$ is $\hat{\boldsymbol{H}}$ and the test statistic can be modified into

$$\tilde{\Psi} = \frac{f\left(\hat{\boldsymbol{H}}|\mathcal{H}_1, \boldsymbol{G}=\hat{\boldsymbol{H}}\right)}{f\left(\hat{\boldsymbol{H}}|\mathcal{H}_0\right)} = \frac{M^N/(\pi^N\sigma^{2N})}{f\left(\hat{\boldsymbol{H}}|\mathcal{H}_0\right)}\,. \tag{15}$$

By taking the logarithm of $\tilde{\Psi}$ and after a normalization, we can write a new test statistic, which results in the scaled mean square error between $\hat{\boldsymbol{H}}^{(\mathrm{AB})}$ and $\hat{\boldsymbol{H}}$, i.e.

$$\Psi = \frac{2}{\nu}\sum_{n=0}^{N-1}\left|\hat{H}_n - \hat{H}_n^{(\mathrm{AB})}\right|^2\,. \tag{16}$$

Under the hypothesis $\mathcal{H}_0$, $\Psi$ results in a central chi-square random variable with $2N$ degrees of freedom, i.e.

$$\begin{aligned}\Psi^{(\mathcal{H}_0)} &= \frac{2}{\nu}\sum_{n=0}^{N-1}\left|W_n' - W_n^{(\mathrm{B})}\right|^2 \\ &\sim \chi^2_{2N,0}\,.\end{aligned} \tag{17}$$

Under the hypothesis $\mathcal{H}_1$, $\Psi$ is a noncentral chi-square random variable with $2N$ degrees of freedom i.e.

$$\begin{aligned}\Psi^{(\mathcal{H}_1)} &= \frac{2}{\nu}\sum_{n=0}^{N-1}\left|G_n + W'_n - \left(H_n^{(\mathrm{AB})} + W_n^{(\mathrm{B})}\right)\right|^2 \\ &\sim \chi^2_{2N,\mu}\,,\end{aligned} \tag{18}$$

with noncentrality parameter

$$\mu = \frac{2}{\nu}\sum_{n=0}^{N-1}\left|G_n - H_n^{(\mathrm{AB})}\right|^2 . \tag{19}$$

## 3.2 False Alarm and Missed Detection Probability

Two types of error can be done in a hypothesis testing problem: a *false alarm* when $\Psi^{(\mathcal{H}_0)} > \theta$, i.e. when Bob refuses a message coming from Alice, and a *missed detection* when $\Psi^{(\mathcal{H}_1)} < \theta$, i.e. when Bob accepts a message coming from Eve. For a given threshold $\theta$, the probability of false alarm $P_{\mathrm{FA}}$ and missed detection $P_{\mathrm{MD}}$ events are

$$P_{\mathrm{FA}} = \mathrm{P}\left[\Psi^{(\mathcal{H}_0)} > \theta\right] = 1 - F_{\chi^2_{2N,0}}(\theta)\,, \tag{20a}$$

$$P_{\mathrm{MD}} = \mathrm{P}\left[\Psi^{(\mathcal{H}_1)} < \theta\right] = F_{\chi^2_{2N,\mu}}(\theta)\,, \tag{20b}$$

where $F_{\chi^2_{N,\mu}}(\cdot)$ denotes the cumulative distribution function (CDF) of a chi-square random variable with $N$ degrees of freedom and noncentrality parameter $\mu$. For a target $P_{\mathrm{FA}}$, the given threshold is set from (20a) to

$$\theta = F^{-1}_{\chi^2_{2N,0}}(1 - P_{\mathrm{FA}})\,, \tag{21a}$$

and the missed detection probability can be computed as

$$P_{\mathrm{MD}} = F_{\chi^2_{2N,\mu}}\left(F^{-1}_{\chi^2_{2N,0}}(1 - P_{\mathrm{FA}})\right)\,, \tag{21b}$$

which depends on the equivalent channel $\boldsymbol{G}$ through $\mu$.

## 3.3 Information Theoretic Bound

We consider the information-theoretic bound obtained in [3] on Eve's success for authentication over a wiretap channel. In our scenario Alice and Bob guarantee authentication employing two correlated but not identical sequences: the channel $\boldsymbol{H}^{(\mathrm{AB})}$ and its noisy version $\hat{\boldsymbol{H}}^{(\mathrm{AB})}$ estimated by Bob. Theorem 3 in [3] shows that for an arbitrary small $P_{\mathrm{FA}}$ and when the number of OFDM symbols $P$ employed in the transmission of the message goes to infinity, there exists an $N_0 > 0$, such that $\forall N > N_0$, the optimal authentication scheme provides

$$P_{\mathrm{MD}} \simeq 2^{-I(\boldsymbol{H}^{(\mathrm{AB})};\hat{\boldsymbol{H}}^{(\mathrm{AB})})}\,, \tag{22}$$

where $I(x;y)$ is the mutual information between $x$ and $y$. Note that when $P$ goes to infinity, the channel estimation on the message could be refined resulting in a signal-to-noise ratio (SNR) of the message going to infinity. From the model in (2) and (6), we can write the mutual information in (22) as [15, §9]

$$I(\boldsymbol{H}^{(\mathrm{AB})};\hat{\boldsymbol{H}}^{(\mathrm{AB})}) = N\log_2\left(1 + M/\sigma^2\right)\,. \tag{23}$$

Expression in (22) can now be written as

$$P_{\mathrm{MD}} \simeq \left(1 + \frac{M}{\sigma^2}\right)^{-N}\,. \tag{24}$$

# 4. AN EFFECTIVE ATTACK STRATEGY

In this section we consider the strategy adopted by Eve in order to break the authentication system of Bob. As Eve observes the transmission from Alice to Bob, we assume that she estimates channel $\boldsymbol{H}^{(\mathrm{AE})}$. Moreover, in all communications in which Bob transmits toward Alice (for example sending an acknowledgment of reception) such as LTE or 802.11, we also assume that Eve can estimate channel $\boldsymbol{H}^{(\mathrm{EB})}$. We denote the channel estimates performed by Eve as

$$\hat{\boldsymbol{H}}^{(\mathrm{AE})} = \boldsymbol{H}^{(\mathrm{AE})} + \boldsymbol{W}^{(\mathrm{AE})}\,, \tag{25a}$$

$$\hat{\boldsymbol{H}}^{(\mathrm{EB})} = \boldsymbol{H}^{(\mathrm{EB})} + \boldsymbol{W}^{(\mathrm{EB})}\,, \tag{25b}$$

where $\boldsymbol{W}^{(\mathrm{AE})} \sim \mathcal{CN}(\boldsymbol{0}_{N\times 1}, \sigma^2_{\mathrm{AE}}\boldsymbol{I}_N)$ and $\boldsymbol{W}^{(\mathrm{EB})} \sim \mathcal{CN}(\boldsymbol{0}_{N\times 1}, \sigma^2_{\mathrm{EB}}\boldsymbol{I}_N)$.

In the following we focus on the derivation of $G_n$ in order to maximize the probability of breaking the authentication system.

## 4.1 Single Attack Strategy

When a single attack (SA) is considered, Eve computes $G_n$ in order to maximize the probability of breaking the authentication system, using as equivalent channel the ML estimation of $\hat{H}_n^{(\mathrm{AB})}$, i.e.

$$\begin{aligned}G_n^{(\mathrm{SA})} = \arg\max_{x\in\mathbb{C}} \mathrm{P}\Big[\hat{H}_n^{(\mathrm{AB})} = x \,\Big|\, \\ \hat{H}_n^{(\mathrm{AE})}, \hat{H}_n^{(\mathrm{EB})}\Big]\,.\end{aligned} \tag{26}$$

As derived in Appendix A, we have

$$\begin{aligned}G_n^{(\mathrm{SA})} = &\left[\left(1+\sigma^2_{\mathrm{AE}}\right)\left(1+\sigma^2_{\mathrm{EB}}\right) - \rho^{(\mathrm{AB})2}\right]^{-1} \\ &\left[\hat{H}_n^{(\mathrm{AE})}\left(\rho^{(\mathrm{EB})}\left(1+\sigma^2_{\mathrm{EB}}\right) - \rho^{(\mathrm{AB})}\rho^{(\mathrm{AE})}\right) + \right. \\ &\left.\hat{H}_n^{(\mathrm{EB})}\left(\rho^{(\mathrm{AE})}\left(1+\sigma^2_{\mathrm{AE}}\right) - \rho^{(\mathrm{AB})}\rho^{(\mathrm{EB})}\right)\right]\,.\end{aligned} \tag{27}$$

*Long Distance Solution.* A further simplification of (27) can be obtained through following assumptions on the distances among the three agents:

$$d^{(\mathrm{AB})} \gg \lambda_c\,, \tag{28a}$$

$$\max\{d^{(\mathrm{AE})}, d^{(\mathrm{EB})}\} \gg \lambda_c\,, \tag{28b}$$

$$\max\{d^{(\mathrm{AE})}, d^{(\mathrm{EB})}\} \gg \min\{d^{(\mathrm{AE})}, d^{(\mathrm{EB})}\}\,. \tag{28c}$$

In fact, (28a) is a realistic hypothesis which is always satisfied for a wireless communication, whereas with (28b) and (28c) we assume that only one channel between $\boldsymbol{H}^{(\mathrm{AE})}$ and $\boldsymbol{H}^{(\mathrm{EB})}$ provides useful information to Eve, meaning that Eve performs an attack better than a simple guessing of $\hat{\boldsymbol{H}}^{(\mathrm{AB})}$ only if she is sufficiently near to Alice or Bob. Assuming that Eve is able to perfectly estimate $\boldsymbol{H}^{(\mathrm{AE})}$ and $\boldsymbol{H}^{(\mathrm{EB})}$, i.e. $\sigma^2_{\mathrm{AE}} = \sigma^2_{\mathrm{EB}} = 0$, using (28), we obtain

$$G_n^{(\mathrm{SA})} = \begin{cases}\rho^{(\mathrm{EB})}\hat{H}_n^{(\mathrm{AE})}, & d^{(\mathrm{EB})} < d^{(\mathrm{AE})} \\ \rho^{(\mathrm{AE})}\hat{H}_n^{(\mathrm{EB})}, & d^{(\mathrm{AE})} < d^{(\mathrm{EB})}\end{cases}\,. \tag{29}$$

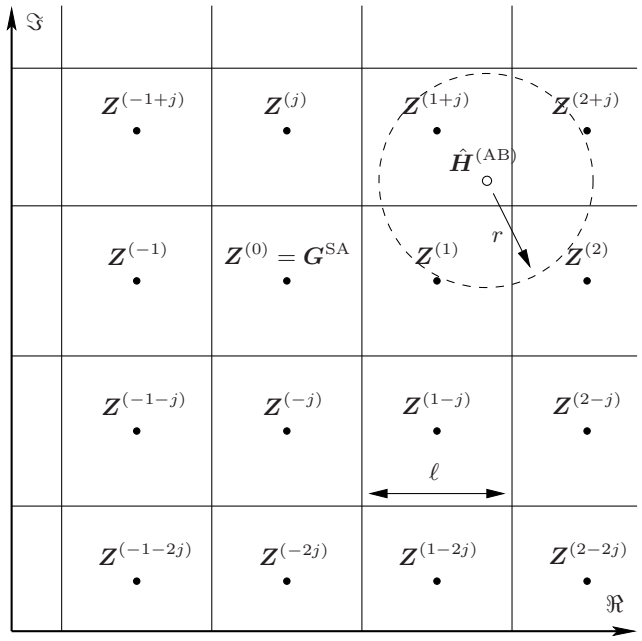


**Figure 2: Illustration of multiple attacks strategy for $N = 1$.**

In this asymptotic case, we can also compute a closed form expression of the MD probability. Let us define

$$\rho = \min\left\{\rho^{(\mathrm{AE})}, \rho^{(\mathrm{EB})}\right\}, \tag{30}$$

and

$$\lambda = \frac{\nu}{2(1-\rho^2)}. \tag{31}$$

As derived in Appendix B, the average MD probability can be written as

$$\begin{aligned}\mathrm{E}\left[P_{\mathrm{MD}}\right] = &\left(\frac{\lambda}{\lambda+\frac{1}{2}}\right)^N \sum_{j=0}^{+\infty} \binom{N+j-1}{N-1} \frac{1}{(2\lambda+1)^j} \\ &\left(1 - e^{-\frac{\theta}{2}} \sum_{k=0}^{N+j-1} \frac{(\theta/2)^k}{k!}\right).\end{aligned} \tag{32}$$

## 4.2 Multiple Attack Strategy

We now assume that Eve performs multiple attacks (MAs) by transmitting a sequence of messages in order to break the authentication system. In particular, we define with $\boldsymbol{G}^{(\mathrm{MA})}(\tau)$ and $\hat{\boldsymbol{H}}(\tau)$ the equivalent channel from Eve to Bob and the channel estimated by Bob (9b) at time $\tau = 1, 2, \ldots$, respectively.

We aim at finding the sequence of tested values $\boldsymbol{G}^{(\mathrm{MA})}(\tau)$ that minimizes the average time required to break the authentication procedure. Note that this is a particular instance of the sequential guessing problem [16, 17] with some degree of distortion allowed [18] and trial errors [19]. However, the solution to this problem would require the optimization over the continuous $N$-dimensional complex set $\mathbb{C}^N$ and is exceedingly complex. Instead we focus here on a suboptimal approach, where the sequence $\boldsymbol{G}^{(\mathrm{MA})}(\tau)$ is taken from a pre-determined discrete set of vectors uniformly distributed in the $N$-dimensional complex space as in Fig. 2. The set of points is

$$\boldsymbol{Z}^{(\boldsymbol{i})} = [Z_0^{(\boldsymbol{i})}, Z_1^{(\boldsymbol{i})}, \ldots, Z_{N-1}^{(\boldsymbol{i})}], \tag{33}$$

with $\boldsymbol{i}$ a $N$-dimensional complex vector with entry $n = 0, 1, \ldots, N-1$,

$$i_n = \Re\{i_n\} + j\Im\{i_n\}, \quad \Re\{i_n\}, \Im\{i_n\} \in \mathbb{Z}^N. \tag{34}$$

Since we want the multiple attacks strategy to be optimal also in the case of single attack, one of the points $\boldsymbol{Z}^{(\boldsymbol{i})}$ must be the attack derived in the previous section. Without loss of generality we impose $\boldsymbol{Z}^{(\boldsymbol{0}_{N\times 1})} = \boldsymbol{G}^{(\mathrm{SA})}$. Then the other points are uniformly distributed in the space with distance $\ell$ along each dimension, i.e.

$$\Re\{Z_n^{(\boldsymbol{i})}\} = \ell\Re\{i_n\} + \Re\{G_n^{(\mathrm{SA})}\}, \tag{35a}$$

$$\Im\{Z_n^{(\boldsymbol{i})}\} = \ell\Im\{i_n\} + \Im\{G_n^{(\mathrm{SA})}\}. \tag{35b}$$

We observe that Bob accepts a message if its related channel $\hat{\boldsymbol{H}}(\tau)$ is inside a sphere $\mathcal{S}(\hat{\boldsymbol{H}}^{(\mathrm{AB})}) \subseteq \mathbb{C}^N$ centered around $\hat{\boldsymbol{H}}^{(\mathrm{AB})}$ and having radius

$$r = \sqrt{\frac{\theta}{2}\nu}. \tag{36}$$

Let $\boldsymbol{n}(\tau)$ be the index of the selected point at time $\tau$, i.e. the multiple attacks strategy is $\boldsymbol{G}^{(\mathrm{MA})}(\tau) = \boldsymbol{Z}^{(\boldsymbol{n}(\tau))}$. At time $\tau$, the target channel is selected in order to maximize the probability of Eve's success given that the previous $\tau - 1$ attempts failed. Then we have

$$\begin{aligned}\boldsymbol{n}(\tau) = \arg\max_{\boldsymbol{i}} \mathrm{P}\Bigg[&\hat{\boldsymbol{H}}(\tau) \in \mathcal{S}(\hat{\boldsymbol{H}}^{(\mathrm{AB})}) \,| \\ &| \bigcap_{\tau'=1}^{\tau-1} \left\{\boldsymbol{G}^{(\mathrm{MA})}(\tau') = \boldsymbol{Z}^{(\boldsymbol{n}(\tau'))}, \hat{\boldsymbol{H}}(\tau') \notin \mathcal{S}(\hat{\boldsymbol{H}}^{(\mathrm{AB})})\right\}, \\ &\boldsymbol{G}^{(\mathrm{MA})}(\tau) = \boldsymbol{Z}^{(\boldsymbol{i})}\Bigg].\end{aligned} \tag{37}$$

Unfortunately the probability in (37) cannot be easily computed. Therefore we introduce an approximation in the model. For each $\boldsymbol{Z}^{(\boldsymbol{i})}$ consider the hypercube

$$\begin{aligned}\mathcal{R}^{(\boldsymbol{i})} = \Bigg\{&[a_0, a_1, \ldots, a_{N-1}] \in \mathbb{C}^N : \\ &\Re\{a_n\} \in \left[\Re\{Z_n^{(\boldsymbol{i})}\} - \frac{\ell}{2}, \Re\{Z_n^{(\boldsymbol{i})}\} + \frac{\ell}{2}\right], \\ &\Im\{a_n\} \in \left[\Im\{Z_n^{(\boldsymbol{i})}\} - \frac{\ell}{2}, \Im\{Z_n^{(\boldsymbol{i})}\} + \frac{\ell}{2}\right], \\ &n = 0, 1, \ldots, N-1\Bigg\}.\end{aligned} \tag{38}$$

It is easy to see that the $\mathcal{R}^{(\boldsymbol{i})}$ make up a tiling of $\mathbb{C}^N$. Then we replace the sphere $\mathcal{S}(\hat{\boldsymbol{H}})$ with the hypercube containing $\hat{\boldsymbol{H}}$ and in particular we confuse the following events

$$\left\{\hat{\boldsymbol{H}}^{(\mathrm{AB})} \in \mathcal{S}(\hat{\boldsymbol{H}}(\tau)) \,|\, \hat{\boldsymbol{H}}(\tau) \in \mathcal{R}^{(j)}\right\} \approx \left\{\hat{\boldsymbol{H}}^{(\mathrm{AB})} \in \mathcal{R}^{(j)}\right\}, \tag{39a}$$

$$\left\{\cdot \,|\, \hat{\boldsymbol{H}}(\tau) \in \mathcal{R}^{(\boldsymbol{j})}, \hat{\boldsymbol{H}}^{(\mathrm{AB})} \notin \mathcal{S}(\hat{\boldsymbol{H}}(\tau))\right\} \approx \approx \left\{\cdot \,|\, \hat{\boldsymbol{H}}^{(\mathrm{AB})} \notin \mathcal{R}^{(\boldsymbol{j})}\right\}. \tag{39b}$$

In this case, let us indicate the probability that the reference channel belongs to hypercube of index $\boldsymbol{i}$ as

$$p(\boldsymbol{i}) = \mathrm{P}\left[\hat{\boldsymbol{H}}^{(\mathrm{AB})} \in \mathcal{R}^{(\boldsymbol{i})}\right], \tag{40}$$

and the probability that $\hat{\boldsymbol{H}}(\tau)$ is in the hypercube of index $\boldsymbol{i}$, given that $\boldsymbol{G}^{(\mathrm{MA})}(\tau) = \boldsymbol{Z}^{(\boldsymbol{j})}$ as

$$q(\boldsymbol{i}|\boldsymbol{j}) = \mathrm{P}\left[\hat{\boldsymbol{H}}(\tau) \in \mathcal{R}^{(\boldsymbol{i})} | \boldsymbol{G}^{(\mathrm{MA})}(\tau) = \boldsymbol{Z}^{(\boldsymbol{j})}\right]. \tag{41}$$

As derived in Appendix C, we have

$$\boldsymbol{n}(\tau) = \arg\max_{\boldsymbol{i}} \sum_{\boldsymbol{j}(1)} \sum_{\boldsymbol{j}(2)} \cdots \sum_{\boldsymbol{j}(\tau)\neq\boldsymbol{j}(1),\boldsymbol{j}(2),\ldots,\boldsymbol{j}(\tau-1)} q\left(\boldsymbol{j}(\tau)|\boldsymbol{i}\right) \prod_{\tau'=1}^{\tau-1} q\left(\boldsymbol{j}(\tau')|\boldsymbol{n}(\tau')\right) \frac{p(\boldsymbol{j}(\tau))}{1 - \sum_{\tau'=1}^{\tau-1} p(\boldsymbol{j}(\tau'))}. \tag{42}$$

*On the choice of $\ell$.* For the choice of $\ell$ we observe that the most critical case is when $P \to \infty$, since if Eve wants to make sure that at least one point $\boldsymbol{Z}^{(\boldsymbol{i})}$ is within the sphere – and hence to break the authentication system – the largest value of $\ell$ is such that the hypercubes are inscribed into $\mathcal{S}(\hat{\boldsymbol{H}}^{(\mathrm{AB})})$. Therefore we have

$$\ell \leq \sqrt{\frac{\theta}{N}\nu}. \tag{43}$$

Note that when $\ell$ satisfies (43) with equality, approximation (39) is good for low values of $N$ because the volume of $\mathcal{S}(\hat{\boldsymbol{H}})$ is quite close to the volume of $\mathcal{R}^{(\boldsymbol{i})}$.

## 5. NUMERICAL RESULTS

We define $d$ as the minimum between Alice to Bob and Eve to Bob distances. First of all, we consider that Eve performs a single attack by using the strategy (29).

In Fig. 3 we verify the correctness of the analysis in Appendix B by plotting the expected value of $P_{\mathrm{MD}}$ with respect to channel distribution by using (32) and through Monte Carlo simulations for different values of the system parameters. As we can see, the analytical function perfectly fits the numerical results.

In Fig.s 4 and 5 we compare the performance of the considered authentication scheme with respect to the information-theoretic bound computed in Section 3.3. In particular, we plot the $P_{\mathrm{MD}}$ in terms of the number of pilot tones $N$ for $M/\sigma^2 = 15$ and 20 dB, respectively, and considering $P \to \infty$, $d/\lambda_c = 20$ and different values of $P_{\mathrm{FA}}$. Note that for a particular setting of a realistic scenario, higher values of $N$ can be obtained only by increasing the signal bandwidth employed by Alice to transmit toward Bob. As expected, the $P_{\mathrm{MD}}$ is a decreasing function of both $N$ and $P_{\mathrm{FA}}$. Note that while the expression in (24) is true for an arbitrary small $P_{\mathrm{FA}}$, the performance of the considered authentication scheme is evaluated only for small but fixed $P_{\mathrm{FA}}$. However, we observe that (24) provides a better $P_{\mathrm{MD}}$ than that obtained with the considered method even with higher values of $P_{\mathrm{FA}}$. Moreover, the slope of (24) in terms of $N$ is higher with respect to that of the considered scheme.

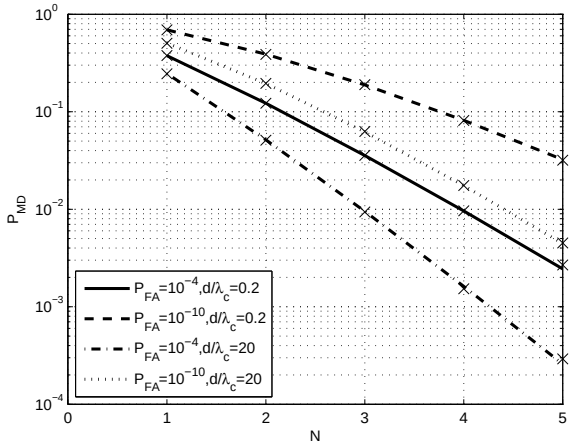


**Figure 3: Probability of missed detection $P_{\mathrm{MD}}$ versus $N$ computed using (32) and Monte Carlo simulations (crosses). Here $M/\sigma^2 = 15$ dB and $P \to \infty$.**

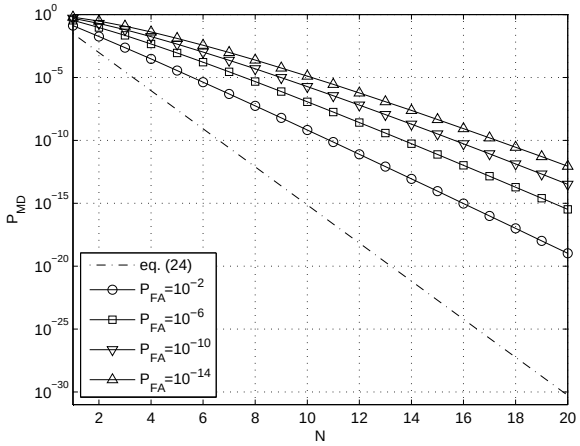


**Figure 4: Probability of missed detection $P_{\mathrm{MD}}$ versus $N$. Here $M/\sigma^2 = 15$ dB, $P \to \infty$ and $d/\lambda_c = 20$.**

In Fig. 6 we evaluate the performance of the considered method in terms of the Eve's knowledge of the channel which is strictly related to the distance $d$. We assume $P/\sigma^2 = 25$ dB and $P_{\mathrm{FA}} = 10^{-4}$. As the wireless channel quickly decorrelates in space, we observe that Eve can increase the $P_{\mathrm{MD}}$ only if she is very close to Bob with $d < \lambda_c$. However, if we consider for example an 802.11 scenario with $f_c = 2.4$ GHz, previous condition imposes Eve to be at a distance $d < 12.5$ cm from Bob, which is a bit unrealistic. This observation proves the merits of the considered physical-layer authentication scheme.

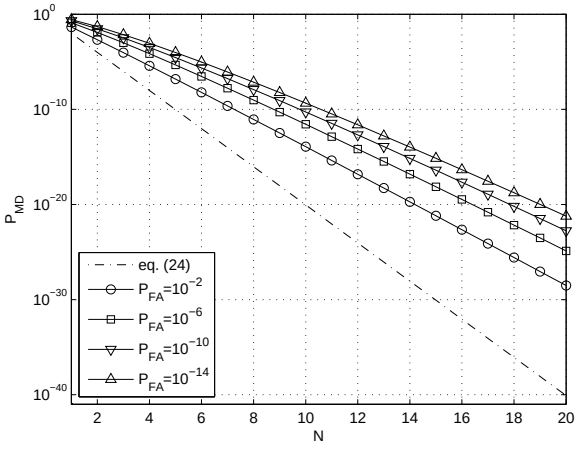


**Figure 5: Probability of missed detection $P_{\rm MD}$ versus $N$. Here $M/\sigma^2 = 20$ dB, $P \to \infty$ and $d/\lambda_c = 20$.**

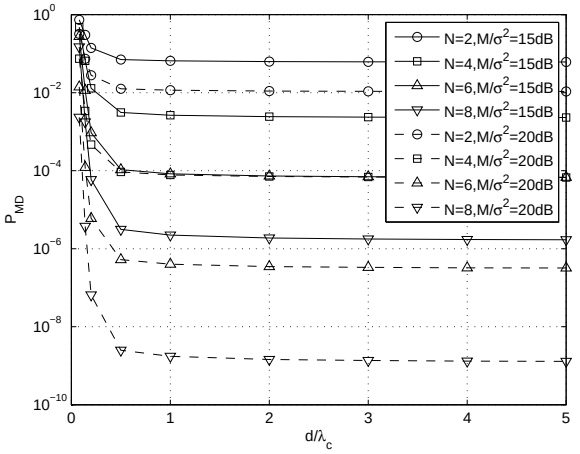


**Figure 6: Probability of missed detection $P_{\rm MD}$ versus $d/\lambda_c$. Here $P/\sigma^2 = 25$ dB and $P_{\rm FA} = 10^{-4}$.**

In Fig. 7 we impose $P/\sigma^2 = 25$ dB and $P_{\rm FA} = 10^{-4}$ and we provide the performance in terms of $M/\sigma^2$. As expected, $P_{\rm MD}$ is a decreasing function of $M/\sigma^2$ and better results are obtained for higher values of $N$ and higher values of $d$. Note that there is a saturation of $P_{\rm MD}$ when $M > P$. Indeed, even if Bob has a better knowledge of channel $\boldsymbol{H}^{(\rm AB)}$, the performance of the system is degraded by the noise on the current received message.

In Fig.s 8 and 9 we assume that Eve tries to cheat Bob by sending a sequence of messages with strategy (42). In particular we plot the probability $P_{\rm MD}(\tau)$ that the first missed detection event happens in the first $\tau$ Eve's attempts. By assuming $P \to \infty$, $d/\lambda_c = 20$ and $N = 1$ in Fig. 8 and $N = 2$ in Fig. 9, we observe that $P_{\rm MD}(\tau)$ is an increasing function of $\tau$. However, while with $N = 1$ $P_{\rm MD}(\tau)$ is very high after few attempts, much better performance is obtained with $N = 2$, in particular for higher values of $M/\sigma^2$.

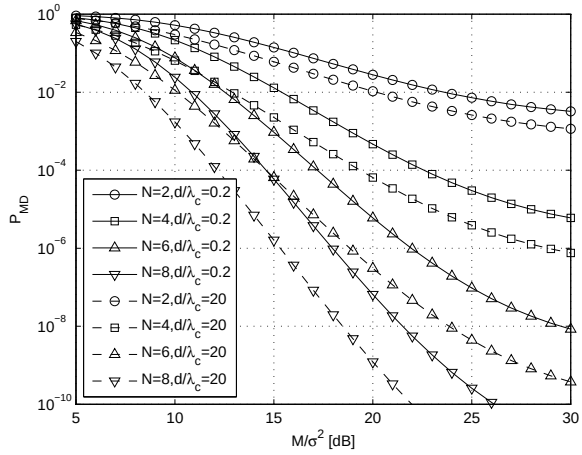


**Figure 7: Probability of missed detection $P_{\rm MD}$ versus $M/\sigma^2$. Here $P/\sigma^2 = 25$ dB and $P_{\rm FA} = 10^{-4}$.**

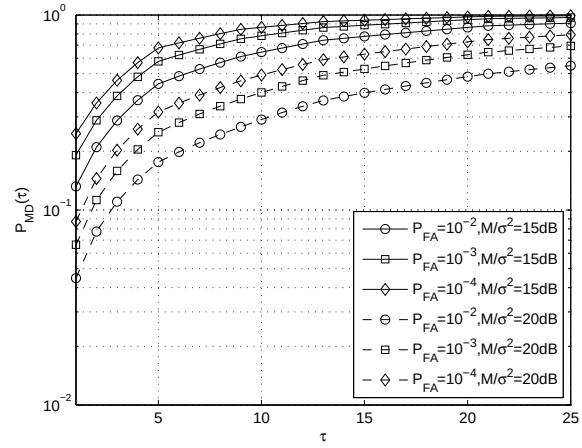


**Figure 8: $P_{\rm MD}(\tau)$ versus $\tau$. Here $N = 1$, $P \to \infty$ and $d/\lambda_c = 20$.**

# 6. CONCLUSIONS

In this paper we have considered the physical-layer technique developed in [9, 10] to provide authentication between Alice and Bob assuming a more general model for the attack employed by Eve. In particular, we provide the optimal Eve's strategy in the case of single attack and we perform an analytical computation of $\mathrm{E}[P_{\rm MD}]$ with respect to channel distribution. Moreover, we formulate a suboptimal multiple attacks strategy for Eve consisting in a sequence of messages and CFR guesses aiming to break authentication. Numerical results confirm the merits of the considered method as it provides good performance against both attack strategies when $N$ is sufficiently high and when Eve is far away from Alice and Bob because of the rapid spatial decorrelation of the channel in wireless systems.

# 7. REFERENCES

[1] U.M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, Jul. 2000,

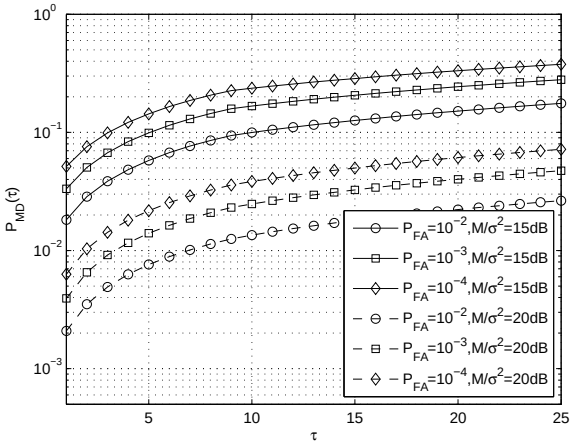


**Figure 9:** $P_{\mathrm{MD}}(\tau)$ **versus** $\tau$**. Here** $N = 2$**,** $P \to \infty$ **and** $d/\lambda_c = 20$**.**


pp. 1350-1356.

[2] E. Martinian, G.W. Wornell, and B. Chen, "Authentication with distortion criteria," *IEEE Trans. Inf. Theory*, vol. 51, 2005, pp. 2523-2542.

[3] L. Lai, H. El Gamal and H.V. Poor, "Authentication over noisy channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906-916, Feb. 2009.

[4] P.L. Yu, J.S. Baras, and B.M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics and Security*, vol. 3, 2008, pp. 38-51.

[5] P.L. Yu, J.S. Baras, and B.M. Sadler, "Power allocation tradeoffs in multicarrier authentication systems," *IEEE Sarnoff Symposium*, pp. 1-5, Princeton (NJ), Mar. 2009.

[6] D.B. Faria and D.R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," *ACM WiSe*, pp. 43-52, Los Angeles (CA), Sep. 2006.

[7] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," *International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Buffalo (NY), Jun. 2006.

[8] Y. Chen, W. Trappe, and R.P. Martin, "Detecting and localizing wireless spoofing attacks," *IEEE SECON*, pp. 193-202, San Diego (CA), Jun. 2007.

[9] L. Xiao, L.J. Greenstein, N.B. Mandayam and W. Trappe, "Fingerprints in the ether: using the physical layer for wireless authentication," *International Conference on Communications (ICC)*, Glasgow (UK), Jun. 2007.

[10] L. Xiao, L.J. Greenstein, N.B. Mandayam and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," *International Conference on Communications (ICC)*, Beijing (China), May 2008.

[11] L. Xiao, L.J. Greenstein, L. Fellow, N.B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, 2009, pp. 5948-5956.

[12] L. Xiao, A. Reznik, W. Trappe, C. Ye, Y. Shah, and L.J. Greenstein, "PHY-authentication protocol for spoofing detection in wireless networks," *IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1-6, Miami (FL), Dec. 2010.

[13] D. Tse and P. Viswanath, *Fundamentals of wireless communications.* Cambridge University Press, 2005.

[14] S. Kay, *Fundamentals of statistical signal processing: detection theory.* Prentice Hall, 1993.

[15] T.M. Cover and J.A. Thomas, *Elements of information theory.* Wiley, 2006.

[16] J.L. Massey, "Guessing and entropy," *IEEE International Symposium on Information Theory (ISIT)*, p. 204, Trondheim (Norway), Jun. 1994.

[17] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Trans. Inf. Theory*, vol. 42, n. 1, pp. 99–105, Jan. 1996.

[18] E. Arikan and N. Merhav, "Guessing subject to distortion," *IEEE Trans. Inf. Theory*, vol. 44, n. 3, pp. 1041–1056, May 1998.

[19] E. Arikan and S. Boztas, "Guessing with lies,' *IEEE International Symposium on Information Theory (ISIT)*, p. 208, Lausanne (Switzerland), Jul. 2002.

[20] S. Kay, *Fundamentals of statistical signal processing: estimation theory.* Prentice Hall, 1993.

[21] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables.* Dover Publications, 1965.


# APPENDIX

## A. OPTIMAL STRATEGY FOR A SINGLE ATTACK

We define for $n = 0, 1, \ldots, N-1$,

$$\hat{\boldsymbol{A}}_n = \left[\hat{H}_n^{(\mathrm{AB})}\,,\, \hat{H}_n^{(\mathrm{AE})}\,,\, \hat{H}_n^{(\mathrm{EB})}\right]^T\,, \tag{44}$$

where $\boldsymbol{A}_n \sim \mathcal{CN}(\boldsymbol{0}_{3\times 1}, \boldsymbol{R}_n)$, with

$$\boldsymbol{R}_n = \begin{bmatrix} 1+\frac{\sigma^2}{M} & \rho^{(\mathrm{EB})} & \rho^{(\mathrm{AE})} \\ \rho^{(\mathrm{EB})} & 1+\sigma^2_{\mathrm{AE}} & \rho^{(\mathrm{AB})} \\ \rho^{(\mathrm{AE})} & \rho^{(\mathrm{AB})} & 1+\sigma^2_{\mathrm{EB}} \end{bmatrix}\,. \tag{45}$$

From (26) we have

$$\begin{aligned} G_n^{(\mathrm{SA})} &= \arg \max_{\hat{H}_n^{(\mathrm{AB})}\in\mathbb{C}} \mathrm{P}\left[\boldsymbol{A}_n = \hat{\boldsymbol{A}}_n\right] \\ &= \arg \max_{\hat{H}_n^{(\mathrm{AB})}\in\mathbb{C}} \frac{1}{(\pi)^3 \det(\boldsymbol{R}_n)} \exp\left\{-\hat{\boldsymbol{A}}_n^* \boldsymbol{R}_n^{-1} \hat{\boldsymbol{A}}_n\right\} \\ &= \arg \min_{\hat{H}_n^{(\mathrm{AB})}\in\mathbb{C}} \hat{\boldsymbol{A}}_n^* \boldsymbol{R}_n^{-1} \hat{\boldsymbol{A}}_n\,. \end{aligned} \tag{46}$$

Note that for the considered channel model, the ML estimator in (46) becomes the linear minimum mean-square-error (MMSE) estimator [20], which is optimal for the test statistic employed by Bob (16). The objective function in (46)

can be expressed in terms of the variable $\hat{H}_n^{(\mathrm{AB})}$ as

$$\begin{aligned}\hat{\boldsymbol{A}}_n^* \boldsymbol{R}_n^{-1} \hat{\boldsymbol{A}}_n = |\hat{H}_n^{(\mathrm{AB})}|^2 \left[\boldsymbol{R}_n^{-1}\right]_{0,0} + \\ 2\Re\left\{\hat{H}_n^{(\mathrm{AB})*}\left(\left[\boldsymbol{R}_n^{-1}\right]_{0,1}\hat{H}_n^{(\mathrm{AE})} + \left[\boldsymbol{R}_n^{-1}\right]_{0,2}\hat{H}_n^{(\mathrm{EB})}\right)\right\} + \\ + \left[\boldsymbol{R}_n^{-1}\right]_{1,1}|\hat{H}_n^{(\mathrm{AE})}|^2 + \left[\boldsymbol{R}_n^{-1}\right]_{2,2}|\hat{H}_n^{(\mathrm{EB})}|^2 + \\ 2\Re\left\{\left[\boldsymbol{R}_n^{-1}\right]_{1,2}\hat{H}_n^{(\mathrm{AE})*}\hat{H}_n^{(\mathrm{EB})}\right\}.\end{aligned} \tag{47}$$

By setting the gradient of (47) with respect to $\hat{H}_n^{(\mathrm{AB})}$ to zero, we obtain

$$G_n^{(\mathrm{SA})} = -\frac{\left[\boldsymbol{R}_n^{-1}\right]_{0,1}\hat{H}_n^{(\mathrm{AE})} + \left[\boldsymbol{R}_n^{-1}\right]_{0,2}\hat{H}_n^{(\mathrm{EB})}}{\left[\boldsymbol{R}_n^{-1}\right]_{0,0}}. \tag{48}$$

Let

$$\delta = \frac{1}{\det(\boldsymbol{R}_n)}, \tag{49}$$

$$\omega^{(\mathrm{AE})} = 1 + \sigma_{\mathrm{AE}}^2, \quad \omega^{(\mathrm{EB})} = 1 + \sigma_{\mathrm{EB}}^2, \tag{50}$$

we can write

$$\left[\boldsymbol{R}_n^{-1}\right]_{0,0} = \delta\left(\omega^{(\mathrm{AE})}\omega^{(\mathrm{EB})} - \rho^{(\mathrm{AB})2}\right),$$

$$\left[\boldsymbol{R}_n^{-1}\right]_{0,1} = \delta\left(\rho^{(\mathrm{AB})}\rho^{(\mathrm{AE})} - \rho^{(\mathrm{EB})}\omega^{(\mathrm{EB})}\right),$$

$$\left[\boldsymbol{R}_n^{-1}\right]_{0,2} = \delta\left(\rho^{(\mathrm{AB})}\rho^{(\mathrm{EB})} - \rho^{(\mathrm{AE})}\omega^{(\mathrm{AE})}\right).$$

Then from (48) we obtain (27).

## B. ANALYTICAL COMPUTATION OF (32)

In this section we perform an analytical computation of $\mathrm{E}[P_{\mathrm{MD}}]$ for a given $P_{\mathrm{FA}}$ considering the channel model presented in Section 2 and the optimal Eve's strategy discussed in Section 4. Using (4) and (29) we can write the channel used by Eve to cheat Bob in terms of $\boldsymbol{H}^{(\mathrm{AB})}$ for $n = 0, 1, \ldots, N-1$, as

$$G_n^{(\mathrm{SA})} = \rho^2 H_n^{(\mathrm{AB})} + \rho\sqrt{1-\rho^2}\epsilon_n, \tag{51}$$

where $\epsilon_n \sim \mathcal{CN}(0,1)$. Note that

$$G_n^{(\mathrm{SA})} \sim \mathcal{CN}\left(0, \rho^2\right), \tag{52a}$$

$$\mathrm{E}\left[G_n^{(\mathrm{SA})} H_n^{(\mathrm{AB})*}\right] = \rho^2. \tag{52b}$$

For each channel realization and for a given $P_{\mathrm{FA}}$, the threshold $\theta$ is set by (21a) and the $P_{\mathrm{MD}}$ can be computed using (20b). However, if we consider the average $\mathrm{E}[P_{\mathrm{MD}}]$ with respect to $\boldsymbol{H}^{(\mathrm{AB})}$, we have to compute the distribution of the noncentrality parameter $\mu$ of $\Psi^{(\mathcal{H}_1)}$.

Using (51) in (19) and after some calculations, $\mu$ turns out to be an Erlang random variable with shape parameter $N$ and rate parameter $\lambda$. Indeed, we have

$$\begin{aligned}\mu &= \frac{2}{\nu}\sum_{n=0}^{N-1}\left|H_n^{(\mathrm{AB})} - G_n^{(\mathrm{SA})}\right|^2 \\ &= \sum_{n=0}^{N-1}\left[\left(\sqrt{\frac{2}{\nu}}\Re\left\{H_n^{(\mathrm{AB})}(1-\rho^2) - \right.\right.\right. \\ &\quad \left.\left.\left.\rho\sqrt{1-\rho^2}\epsilon_n\right\}\right)^2 + \right. \\ &\quad \left. + \left(\sqrt{\frac{2}{\nu}}\Im\left\{H_n^{(\mathrm{AB})}(1-\rho^2) - \rho\sqrt{(1-\rho^2)}\epsilon_n\right\}\right)^2\right] \\ &= \sum_{n=0}^{2N-1} A_n^2, \text{ where } A_n \sim \mathcal{N}\left(0, \frac{1}{2\lambda}\right) \\ &= \sum_{n=0}^{N-1} B_n, \text{ where } B_n \sim \mathrm{Exp}(\lambda) \\ &\sim \mathrm{Erlang}(\lambda).\end{aligned} \tag{53}$$

The PDF of $\mu$ and the CDF of $\Psi^{(\mathcal{H}_1)}$ can be expressed as [20]

$$f_\mu(x) = \frac{\lambda^N x^{N-1} e^{-\lambda x}}{(N-1)!}, \tag{54a}$$

$$F_{\Psi^{(\mathcal{H}_1)}}(x) = e^{-\frac{\mu}{2}}\sum_{j=0}^{+\infty}\frac{(\mu/2)^j}{j!}\left(1 - e^{-\frac{x}{2}}\sum_{k=0}^{N+j-1}\frac{(x/2)^k}{k!}\right), \tag{54b}$$

for $x \geq 0$. The expected value of $P_{\mathrm{MD}}$ with respect to $\boldsymbol{H}^{(\mathrm{AB})}$ can be computed as [21]

$$\begin{aligned}\mathrm{E}[P_{\mathrm{MD}}] &= \int_0^{+\infty} F_{\chi^2_{2N,x}}(\theta) f_\mu(x) dx \\ &= \int_0^{+\infty} e^{-\frac{x}{2}}\sum_{j=0}^{+\infty}\frac{(x/2)^j}{j!}\left(1 - \right. \\ &\quad \left. e^{-\frac{\theta}{2}}\sum_{k=0}^{N+j-1}\frac{(\theta/2)^k}{k!}\right)\frac{\lambda^N x^{N-1} e^{-\lambda x}}{(N-1)!}dx.\end{aligned} \tag{55}$$

Thus obtaining (32).

## C. MULTIPLE ATTACKS STRATEGY

From (5) and (6) we can write $\hat{\boldsymbol{H}}^{(\mathrm{AB})}$ in terms of the Eve's knowledge of the channel as

$$\hat{\boldsymbol{H}}^{(\mathrm{AB})} = \boldsymbol{G}^{(\mathrm{SA})} + \sqrt{(1-\rho^2) + \sigma^2/M}\,\boldsymbol{\epsilon}, \tag{56}$$

where $\boldsymbol{\epsilon} \sim \mathcal{CN}(\boldsymbol{0}_{N\times 1}, \boldsymbol{I}_N)$. From (56), we conclude that the appropriate model of $\hat{\boldsymbol{H}}^{(\mathrm{AB})}$ for Eve is

$$\hat{\boldsymbol{H}}^{(\mathrm{AB})} \sim \mathcal{CN}(\boldsymbol{G}^{(\mathrm{SA})}, ((1-\rho^2) + \sigma^2/M)\boldsymbol{I}_N). \tag{57}$$

$$\boldsymbol{n}(\tau) = \arg\max_{\boldsymbol{i}} \sum_{\boldsymbol{j}(1)} \sum_{\boldsymbol{j}(2)} \cdots \sum_{\boldsymbol{j}(\tau)} \mathrm{P}\Bigg[\hat{\boldsymbol{H}}^{(\mathrm{AB})} \in \mathcal{S}(\hat{\boldsymbol{H}}(\tau)) \,|\, \bigcap_{\tau'=1}^{\tau-1} \Big\{\boldsymbol{G}(\tau') = \boldsymbol{Z}^{(\boldsymbol{n}(\tau'))}, \\ , \hat{\boldsymbol{H}}(\tau') \in \mathcal{R}^{(\boldsymbol{j}(\tau'))}, \hat{\boldsymbol{H}}^{(\mathrm{AB})} \notin \mathcal{S}(\hat{\boldsymbol{H}}(\tau'))\Big\}, \boldsymbol{G}(\tau) = \boldsymbol{Z}^{(\boldsymbol{i})}, \hat{\boldsymbol{H}}(\tau) \in \mathcal{R}^{(\boldsymbol{j}(\tau))}\Bigg] \cdot \\ \mathrm{P}\Bigg[\bigcap_{\tau'=1}^{\tau} \Big\{\hat{\boldsymbol{H}}(\tau') \in \mathcal{R}^{(\boldsymbol{j}(\tau'))}\Big\} | \bigcap_{\tau'=1}^{\tau-1} \Big\{\boldsymbol{G}(\tau') = \boldsymbol{Z}^{(\boldsymbol{n}(\tau'))}, \hat{\boldsymbol{H}}^{(\mathrm{AB})} \notin \mathcal{S}(\hat{\boldsymbol{H}}(\tau'))\Big\}, \boldsymbol{G}(\tau) = \boldsymbol{Z}^{(\boldsymbol{i})}\Bigg] \tag{60}$$

$$\mathrm{P}\Bigg[\bigcap_{\tau'=1}^{\tau} \Big\{\hat{\boldsymbol{H}}(\tau') \in \mathcal{R}^{(\boldsymbol{j}(\tau'))}\Big\} | \bigcap_{\tau'=1}^{\tau-1} \Big\{\boldsymbol{G}(\tau') = \boldsymbol{Z}^{(\boldsymbol{n}(\tau'))}, \hat{\boldsymbol{H}}^{(\mathrm{AB})} \notin \mathcal{S}(\hat{\boldsymbol{H}}(\tau'))\Big\}, \boldsymbol{G}(\tau) = \boldsymbol{Z}^{(\boldsymbol{i})}\Bigg] = \\ = \mathrm{P}\left[\hat{\boldsymbol{H}}(\tau) \in \mathcal{R}^{(\boldsymbol{j}(\tau))} | \boldsymbol{G}(\tau) = \boldsymbol{Z}^{(\boldsymbol{i})}\right] \prod_{\tau'=1}^{\tau-1} \mathrm{P}\left[\hat{\boldsymbol{H}}(\tau') \in \mathcal{R}^{(\boldsymbol{j}(\tau'))} | \boldsymbol{G}(\tau') = \boldsymbol{Z}^{(\boldsymbol{n}(\tau'))}\right] \\ = q\left(\boldsymbol{j}(\tau) | \boldsymbol{i}\right) \prod_{\tau'=1}^{\tau-1} q\left(\boldsymbol{j}(\tau') | \boldsymbol{n}(\tau')\right) . \tag{61}$$

From (40) we have

$$p(\boldsymbol{i}) = \prod_{n=0}^{N-1} \left[\mathrm{Q}\left(\frac{\ell\Re\{i_n\} - \ell/2}{\sqrt{((1-\rho^2) + \sigma^2/M)/2}}\right) \right. \\ -\mathrm{Q}\left.\left(\frac{\ell\Re\{i_n\} + \ell/2}{\sqrt{((1-\rho^2) + \sigma^2/M)/2}}\right)\right] \cdot \\ \cdot \left[\mathrm{Q}\left(\frac{\ell\Im\{i_n\} - \ell/2}{\sqrt{((1-\rho^2) + \sigma^2/M)/2}}\right) - \right. \\ \left.\mathrm{Q}\left(\frac{\ell\Im\{i_n\} + \ell/2}{\sqrt{((1-\rho^2) + \sigma^2/M)/2}}\right)\right] , \tag{58}$$

while from (41) we have

$$q(\boldsymbol{i}|\boldsymbol{j}) = \prod_{n=0}^{N-1} \left[\mathrm{Q}\left(\frac{\ell\left(\Re\{i_n\} - \Re\{j_n\}\right) - \ell/2}{\sqrt{\sigma^2/(2P)}}\right) - \right. \\ \left.\mathrm{Q}\left(\frac{\ell\left(\Re\{i_n\} - \Re\{j_n\}\right) + \ell/2}{\sqrt{\sigma^2/(2P)}}\right)\right] \cdot \\ \cdot \left[\mathrm{Q}\left(\frac{\ell\left(\Im\{i_n\} - \Im\{j_n\}\right) - \ell/2}{\sqrt{\sigma^2/(2P)}}\right) - \right. \\ \left.\mathrm{Q}\left(\frac{\ell\left(\Im\{i_n\} - \Im\{j_n\}\right) + \ell/2}{\sqrt{\sigma^2/(2P)}}\right)\right] , \tag{59}$$

where $\mathrm{Q}(x)$ is the tail probability of the standard normal distribution. Now, from (37) we have (60) and the second probability in (60) can be written in terms of $q(\boldsymbol{i}|\boldsymbol{j})$ as reported in (61).

Using (61), the optimal region at time $\tau$ in (37) can be expressed as

$$\boldsymbol{n}(\tau) = \arg\max_{\boldsymbol{i}} \sum_{\boldsymbol{j}(1)} \sum_{\boldsymbol{j}(2)} \cdots \sum_{\boldsymbol{j}(\tau)} q\left(\boldsymbol{j}(\tau)|\boldsymbol{i}\right) \prod_{\tau'=1}^{\tau-1} q\left(\boldsymbol{j}(\tau')|\boldsymbol{n}(\tau')\right) \\ \mathrm{P}\Bigg[\hat{\boldsymbol{H}}^{(\mathrm{AB})} \in \mathcal{S}(\hat{\boldsymbol{H}}(\tau)) \,|\, \bigcap_{\tau'=1}^{\tau-1} \Big\{\boldsymbol{G}(\tau') = \boldsymbol{Z}^{(\boldsymbol{n}(\tau'))}, \\ , \hat{\boldsymbol{H}}(\tau') \in \mathcal{R}^{(\boldsymbol{j}(\tau'))}, \hat{\boldsymbol{H}}^{(\mathrm{AB})} \notin \mathcal{S}(\hat{\boldsymbol{H}}(\tau'))\Big\}, \\ , \boldsymbol{G}(\tau) = \boldsymbol{Z}^{(\boldsymbol{i})}, \hat{\boldsymbol{H}}(\tau) \in \mathcal{R}^{(\boldsymbol{j}(\tau))}\Bigg] . \tag{62}$$

Using (39) in (62) we obtain

$$\boldsymbol{n}(\tau) = \arg\max_{\boldsymbol{i}} \sum_{\boldsymbol{j}(1)} \sum_{\boldsymbol{j}(2)} \cdots \sum_{\boldsymbol{j}(\tau)} q\left(\boldsymbol{j}(\tau)|\boldsymbol{i}\right) \prod_{\tau'=1}^{\tau-1} q\left(\boldsymbol{j}(\tau')|\boldsymbol{n}(\tau')\right) \cdot \\ \cdot \mathrm{P}\Bigg[\hat{\boldsymbol{H}}^{(\mathrm{AB})} \in \mathcal{R}^{(\boldsymbol{j}(\tau))} | \bigcap_{\tau'=1}^{\tau-1} \Big\{\hat{\boldsymbol{H}}^{(\mathrm{AB})} \notin \mathcal{R}^{(\boldsymbol{j}(\tau'))}\Big\}\Bigg] , \tag{63}$$

and then (42).