Using the Physical Layer for Wireless Authentication in Time-Variant Channels

Liang Xiao, *Student Member, IEEE,* Larry J. Greenstein, *Life Fellow, IEEE,*
Narayan B. Mandayam, *Senior Member, IEEE* and Wade Trappe, *Member, IEEE,*

***Abstract*—The wireless medium contains domain-specific information that can be used to complement and enhance traditional security mechanisms. In this paper we propose ways to exploit the spatial variability of the radio channel response in a rich scattering environment, as is typical of indoor environments. Specifically, we describe a physical-layer authentication algorithm that utilizes channel probing and hypothesis testing to determine whether current and prior communication attempts are made by the same transmit terminal. In this way, legitimate users can be reliably authenticated and false users can be reliably detected. We analyze the ability of a receiver to discriminate between transmitters (users) according to their channel frequency responses. This work is based on a generalized channel response with both spatial and temporal variability, and considers correlations among the time, frequency and spatial domains. Simulation results, using the ray-tracing tool WiSE to generate the time-averaged response, verify the efficacy of the approach under realistic channel conditions, as well as its capability to work under unknown channel variations.**

***Index Terms*—Wireless authentication, PHY-layer, time-variant channel, cross-layer design, hypothesis testing.**

I. Introduction

As wireless devices become increasingly pervasive and essential, they are becoming both a target for attack and the very weapon with which such an attack can be carried out. Traditional high-level computer and network security techniques can, and must, play an important role in combating such attacks, but the wireless environment presents both the means and the opportunity for new forms of intrusion. The devices that comprise a wireless network are low-cost commodity items that are easily available to potential intruders and also easily modifiable for such intrusion. In particular, wireless networks are open to intrusion from the outside without the need for a physical connection and, as a result, techniques that would provide a high level of security in a wired network have proven inadequate in a wireless network, as many motivated groups of students have readily demonstrated [1]–[3].

Although conventional cryptographic security mechanisms are essential to securing wireless networks, these techniques do not directly leverage the unique properties of the wireless domain to address security threats. The physical properties of the wireless medium are a powerful source of domain-specific information that can be used to complement and enhance traditional security mechanisms. In this paper, we propose a cross-layer approach to augment the security of wireless networks for indoor wireless environments. In particular, we believe that the nature of the wireless medium can be turned to the advantage of the network engineer when trying to secure wireless communications. The enabling factor in our approach is that, in the rich multipath environment typical of wireless scenarios, the response of the medium along any transmit-receive path is *frequency-selective* (or in the time domain, *dispersive*) in a way that is *location-specific*. This means:

1) The channel can be specified by a number of complex samples either in the frequency domain (a set of complex gains at a set of frequencies) or the time domain (a set of impulse response samples at a set of time delays).
2) Such sets of numbers decorrelate from one transmit-receive path to another if the paths are separated by the order of an RF wavelength or more.

While using the physical layer to enhance security might seem to be a radical paradigm shift for wireless systems, we note that this is not the first time that multipath and advanced physical layer methods have proven advantageous. Specifically, we are encouraged in our belief by two notable parallel paradigm shifts in wireless systems: (1) code division multiple access (CDMA) systems [4], where the use of Rake processing transforms multipath into a diversity-enhancing benefit; and (2) multiple-input multiple-output (MIMO) antenna techniques [5], which transform scatter-induced Rayleigh fading into a capacity-enhancing benefit.

Note that there have been recent efforts in studying the information and secrecy capacity [6]–[8], that can be achieved by using the radio channel information. In contrast, this paper studies the feasibility of using such radio channel information. It does so by explicitly devising hypothesis testing procedures to estimate and track the radio channel for authentication purposes.

We begin (Section II) by reviewing some related work. Then (Section III), we provide an overview of our proposed PHY-layer authentication service. We next present a general time-variant channel model (Section IV) that we will use as the basis for our discussions in this paper. In Section V, we describe a hypothesis testing framework for physical layer authentication. In Section VI, we present an overview of our simulation approach. We present our simulation results in Section VII, and wrap up the paper in Section VIII with concluding remarks.

The authors are with WINLAB, the Department of Electrical and Computer Engineering, Rutgers University, North Brunswick, NJ, 08902 USA e-mail: {lxiao, ljg,narayan,trappe}@winlab.rutgers.edu

This research is supported, in part, through a grant CNS-0626439 from the National Science Foundation.

Manuscript received February 2007; revised August 2007.

II. Related Work

In commodity networks, such as 802.11 networks, it is easy for a device to alter its MAC address and claim to be another device by simply issuing an `ifconfig` command. This weakness is a serious threat, and there are numerous attacks, ranging from session hijacking [9] to attacks on access control lists [2], which are facilitated by the fact that an adversarial device may masquerade as another device. In response, researchers have proposed using physical layer information to enhance wireless security. For example, spectral analysis has been used to identify the type of wireless network interface card (NIC), and thus to discriminate among users with different NICs [10]. A similar method, radio frequency fingerprinting, discriminates wireless devices according to the transient behavior of their transmitted signals [11]. For more general networks, the clock skew characteristic of devices has been viewed as a remote fingerprint of devices over the Internet [12]. In addition, the inherent variability in the construction of various digital devices has been used to detect intrusion [13].

More recently, the wireless channel has been explored as a new form of fingerprint for wireless security. The reciprocity and rich multipath of the ultrawideband channel has been used as a means to establish encryption keys [6]. In [14], a practical scheme to discriminate between transmitters was proposed and identifies mobile devices by tracking measurements of signal strength from multiple access points. A similar approach was considered for sensor networks in [15]. Concurrent to these efforts, the present authors have built a significance test that exploits the spatial variability of propagation to enhance the authentication in the stationary, time-invariant channel [16]. In this paper, we have significantly expanded the method to cover a more generalized channel, where there are time variations due to changes in the environment. As in [16], however, the ends of the link remain stationary, as might be the case for a population of users sitting in a room or airport terminal. We will see that, in some cases, the time variations *improve* the authentication.

III. Problem Overview

Authentication is traditionally associated with the assurance that a communication comes from a specific entity [17]. In the context of physical layer authentication, however, we are not interested in identity, *per se*, but rather are interested in recognizing a particular transmitting device. The ability to distinguish between different transmitters would not replace traditional identity-based authentication, but would be particularly valuable as a wireless system enhancement. Such an approach would be beneficial for scenarios where managing cryptographic key material is difficult, and further would reduce the load placed on higher-layer authentication buffers.

Here, we borrow from the conventional terminology of the security community by introducing three different parties: Alice, Bob and Eve. For our purposes, these three entities may be thought of as wireless transmitters/receivers that are potentially located in spatially separated positions, as depicted in Fig. 1. Our two "legal" protagonists are the usual Alice and Bob, and for the sake of discussion throughout this paper, Alice will serve as the transmitter that initiates communication, while Bob will serve as the intended receiver. Their nefarious adversary, Eve, will serve as an active adversary that injects undesirable communications into the medium in the hopes of spoofing Alice.

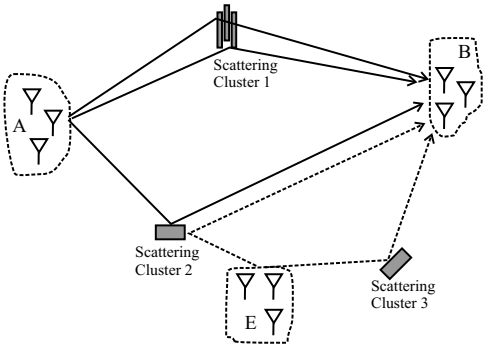

Fig. 1. The adversarial multipath environment involving multiple scattering surfaces. The transmission from Alice (A) to Bob (B) experiences different multipath effects than the transmission by the adversary, Eve (E).

Our security objective, broadly speaking, is to provide authentication between Alice and Bob, despite the presence of Eve. Since Eve is within range of Alice and Bob, and capable of injecting her own signals into the environment to impersonate Alice, Bob must have the ability to differentiate between legitimate signals from Alice and illegitimate signals from Eve.

Consider a simple transmitter identification protocol in which Bob seeks to verify that Alice is the transmitter. Suppose that Alice transmits probes into the channel at a rate sufficient to assure temporal coherence between channel estimates and that, prior to Eve's arrival, Bob has estimated the Alice-Bob channel. Eve wishes to convince Bob that she is Alice. Bob will require that each information-carrying transmission be accompanied by an authenticator signal. The channel response to a transmitted signal between Alice and Bob is a result of the multipath environment. Bob may use the received version of the authenticator signal to estimate the channel response and compare this with a previous record for the Alice-Bob channel. If the two channel estimates are "close" to each other, then Bob will conclude that the source of the message is the same as the source of the previously sent message. If the channel estimates are not similar, then Bob should conclude that the source is likely not Alice.

There are several important issues related to such a procedure that should be addressed before it can be a viable authentication mechanism. First is the specification of the authenticator signal that is used to probe the channel. There are many standardized techniques to probe the channel, ranging from pulse-style probing (including PN sequences) to multitonal probing [18], and we may use these techniques to estimate the channel response. Regardless of what probing method is employed, the channel response can be characterized in the frequency domain, and throughout this paper we will represent our channels in that domain.

A second issue is that in a richly scattered multipath

environment (typical of indoor wireless environments), it is difficult for an adversary to create or precisely model a waveform that is transmitted and received by entities that are more than a wavelength away from the adversary. This assertion is supported by the well-known Jakes uniform scattering model [19], which states that the received signal rapidly decorrelates over a distance of roughly half a wavelength, and that spatial separation of one to two wavelengths is sufficient for assuming independent fading paths. The implication of such a scattering model in a transmitter identification application remains to be tested, and a key objective of this study is to examine the utility of a typical indoor multipath environment for discriminating between Alice-Bob and Eve-Bob channels.

Finally, it should also be noted that the channel response may change with time due to changes in the environment (people moving, doors opening or closing) and in practice it will be necessary to guarantee the continuity of the authentication procedure by probing the channel at time intervals less than the channel's "coherence time". This paper examines the ability to authenticate transmitters in such a time-variant environment, and serves to illustrate the potential for new forms of physical layer security.

IV. Channel Model

A. Basic Form

We assume that Bob first measures and stores the frequency response of the channel connecting Alice with him. Due to his receiver thermal noise, Bob stores a noisy version of the channel response, $H_A(f)$. After awhile, he has to decide whether a transmitting terminal is still Alice, based on a noisy measured version, $H_t(f)$, of that terminal's channel response to Bob. By sampling $H_A(f)$ and $H_t(f)$ at $f \in (f_o - W/2, f_o + W/2]$, Bob obtains two frequency response vectors, $\mathbf{H}_A$ and $\mathbf{H}_t$, of length M, where W is the measurement bandwidth; f_o is the center frequency of the measurement; and the vector elements are frequency response samples at M uniformly spaced frequencies over the measurement bandwidth.

We consider a generalized time-variant channel response, where each frequency response sample is made up of three parts: the fixed part that is the average channel response over time and contains the spatial variability information, the variable part with zero mean, and the receiver noise. Thus the m-th element of $\mathbf{H}_A$ at time kT from some arbitrary time origin can be written as

$$H_{A,m}[k] = \overline{H}_{A,m} + \epsilon_{A,m}[k] + N_{A,m}[k], \quad 1 \le m \le M, \tag{1}$$

where we use the notation that $X_m[k]$ is the sample from $X(t;f)$ at the m-th tone at a sampling time of kT. More specifically, $X_m[k] = X(kT; f_o - W/2 + m\Delta f)$, $m = 1, \cdots, M$, where $\Delta f = W/M$; M is the sample size in the frequency domain; and T is the sampling interval. The term $\overline{H}_{A,m}$ is the average value of the m-th tone over time, $\epsilon_{A,m}[k]$ is the zero-mean variable part at time kT, and $N_{A,m}[k]$ represents thermal noise sample at the m-th tone at time kT. The noises are modelled by $CN(0, \sigma_N^2)$, i.e., zero-mean complex Gaussian samples with variance σ_N^2. Without loss of realism, we can assume that they are independent across time, tone (frequency) and terminal (space), and that $\epsilon_{A,m}[k]$ is independent of $N_{A,m}[k]$.

B. Delay Profile and Doppler Spectrum (Temporal Fading) of the Variable Part

We model the variable part of the channel response as *wide-sense stationary uncorrelated scattering* (WSSUS), and can thus use a multipath tapped delay line to model its impulse response, $h(t,\tau)$ [20]:

$$h(t,\tau) = \sum_{l=0}^{\infty} A_l(t)\delta(t - l\Delta\tau), \tag{2}$$

where t is the observation time, and $l\Delta\tau$ and $A_l(t)$ are, respectively, the delay and complex amplitude of the l-th multipath component, with $E[A_l(t)] = 0$ over time. We set $\Delta\tau = 1/W$, since the receiver cannot resolve two components with time difference smaller than the inverse of the bandwidth.

The frequency response of the variable part is the Fourier transform of $h(t;\tau)$ in terms of τ,

$$\begin{aligned} \epsilon_{A,m}[k] &= \mathcal{F}\{h(t;\tau)\}|_{t=kT, f=f_o-W/2+m\Delta f} \\ &= \sum_{l=0}^{\infty} A_l[k] e^{-j2\pi(f_o - W/2 + m\Delta f)l\Delta}, \end{aligned} \tag{3}$$

where $A_l[k] = A_l(kT)$ is the amplitude sample of the multipath component at time kT.

For illustrative purposes, we use the one-sided exponential distribution to model the power delay spectrum of $A_l[k]$[1], i.e.,

$$P_\tau[l] = \text{Var}[A_l[k]] = \sigma_T^2(1 - e^{-\gamma\Delta\tau})e^{-\gamma\Delta\tau l}, \tag{4}$$

where $\gamma = 2\pi B_c$ is the inverse of the average delay spread, B_c is the coherence bandwidth of the variable part, and σ_T^2 is the average power of $A_l[k]$ over all taps.

Also for illustrative purposes, we use an autoregressive model of order 1 (AR-1) to characterize the temporal process of $A_l[k]$, i.e.,

$$A_l[k] = aA_l[k-1] + \sqrt{(1-a^2)P_\tau[l]}u_l[k], \tag{5}$$

where the AR coefficient a denotes the similarity of two A_l values spaced by T and the random component $u_l[k] \sim CN(0,1)$ is independent of $A_l[k-1]$.

C. Spatial Correlations

As pointed out in Section I, in a typically rich scattering environment, the radio channel response decorrelates quite rapidly in space. Later, we will cite the use of the ray-tracing software WiSE to emulate the spatial correlation characteristics of the *fixed* part of the channel response ($\overline{H}$). As to the *variable* part, however, we consider the two extreme cases:

[1]The literature abounds with empirical data [21] and theoretical examples [22] in which the exponential delay profile appears. We invoke it here for the sake of concreteness, which will allow us to compute numerical results, but we also recognize it to be a realistic condition.

1) *Spatially independent and identically distributed* ϵ. The frequency response sample of the channel between Eve and Bob can be written as

$$H_{E,m}[k] = \overline{H}_{E,m} + \epsilon_{E,m}[k] + N_{E,m}[k], \tag{6}$$

where $1 \le m \le M$, $\overline{H}_{E,m} = E[H_{E,m}[k]]$ is the time average; thermal noise $N_{E,m}[k] \sim CN(0, \sigma_N^2)$; and $\epsilon_{E,m}[k]$ and $\epsilon_{A,m}[k]$ are independent identically distributed (i.i.d.).
2) *Complete spatially correlated variation* ($\epsilon_{E,m}[k] = \epsilon_{A,m}[k]$). Here, we have

$$H_{E,m}[k] = \overline{H}_{E,m} + \epsilon_{A,m}[k] + N_{E,m}[k], \quad 1 \le m \le M. \tag{7}$$

D. Important Relationships

Two important relationships we will use in the hypothesis testing later are as follows (proofs are provided in the Appendix):

Relationship 1:

$$\mathbf{H}_A[k] - \mathbf{H}_A[k-1] \sim CN(\underline{0}, \mathbf{R}), \tag{8}$$

where

$$\begin{aligned} \mathbf{R} &= \text{Cov}[\mathbf{H}_A[k] - \mathbf{H}_A[k-1]] \\ &= [r(m-n)]_{mn}, \quad 1 \le m, n \le M, \end{aligned} \tag{9}$$

$r(0) = 2(1-a)\sigma_T^2 + 2\sigma_N^2$, and

$$r(m) = \frac{2\sigma_T^2(1-a)(1-e^{-2\pi B_c/W})}{1-e^{-2\pi B_c/W - j2\pi m/M}}, \; 1-M \le m \le M-1. \tag{10}$$

Relationship 2: For the case with spatially independent time variation,

$$\mathbf{H}_E[k] - \mathbf{H}_A[k-1] \sim CN((\overline{\mathbf{H}}_E - \overline{\mathbf{H}}_A), \mathbf{G}), \tag{11}$$

where

$$\begin{aligned} \mathbf{G} &= \text{Cov}[\mathbf{H}_E[k] - \mathbf{H}_A[k-1]] \\ &= \begin{bmatrix} 2\sigma_T^2 + 2\sigma_N^2 & \frac{r(-1)}{1-a} & \cdots & \frac{r(1-M)}{1-a} \\ \frac{r(1)}{1-a} & 2\sigma_T^2 + 2\sigma_N^2 & \cdots & \frac{r(2-M)}{1-a} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{r(M-1)}{1-a} & \frac{r(M-2)}{1-a} & \cdots & 2\sigma_T^2 + 2\sigma_N^2 \end{bmatrix}. \end{aligned} \tag{12}$$

V. Hypothesis Testing

Here, we present formulas for hypothesis testing that will be reduced later to numerical results.

A. General Case

As in [16], Bob uses a simple hypothesis test to decide if the transmitting terminal is Alice or a would-be intruder, Eve. The null hypothesis, $\mathcal{H}_0$, is that the terminal is not an intruder, i.e. the claimant is Alice; and Bob accepts this hypothesis if the test statistic he computes, Z, is below some threshold, $\mathcal{T}$. Otherwise, he accepts the alternative hypothesis, $\mathcal{H}_1$, that the claimant terminal is someone else. Thus,

$$\mathcal{H}_0: \quad \mathbf{H}_t[k] = \mathbf{H}_A[k] \tag{13}$$

$$\mathcal{H}_1: \quad \mathbf{H}_t[k] \ne \mathbf{H}_A[k], \tag{14}$$

First, we assume spatially independent time variations and assume Bob knows the key channel variation parameters a, B_c and σ_T. (We will discuss other cases in the later parts of this section.) We choose the test statistic in this default setting as

$$Z = \mathbf{z}^H\mathbf{z} = 2(\mathbf{H}_t[k] - \mathbf{H}_A[k-1])^H\mathbf{R}^{-1}(\mathbf{H}_t[k] - \mathbf{H}_A[k-1]), \tag{15}$$

where $\mathbf{z} = \sqrt{2}(\mathbf{R}_d^H)^{-1}(\mathbf{H}_t[k] - \mathbf{H}_A[k-1])$, $\mathbf{R}$ and $\mathbf{R}_d$ are the covariance matrix of $\mathbf{H}_A[k] - \mathbf{H}_A[k-1]$, (9), and its Cholesky factorization (i.e., $\mathbf{R}$=$\mathbf{R}_d^H\ \mathbf{R}_d$).

It can be shown that, when the transmitting terminal is Alice, each element of $\mathbf{z}$ is i.i.d., following a normal distribution, $\mathbf{z} = \sqrt{2}(\mathbf{R}_d^H)^{-1}(\mathbf{H}_A[k] - \mathbf{H}_A[k-1])$, where the elements are i.i.d., and $z_i \sim CN(0, 2)$, $1 \le i \le M$. Thus the test statistic Z is a chi-square random variable with $2M$ degrees of freedom [23], i.e., $Z = \mathbf{z}^H\mathbf{z} \sim \chi_{2M}^2$.

We define the rejection region for $\mathcal{H}_0$ as $Z > \mathcal{T}$. Thus, the "false alarm rate" (or Type I error) is $\alpha = \text{P}_r\{Z > \mathcal{T}|\mathcal{H}_0\} = 1 - \text{F}_{\chi_{2M}^2}(\mathcal{T})$; and the "miss rate" (or Type II error) is given by (16), where $\text{F}_X(\cdot)$ is the CDF of the random variable X and $\text{F}_X^{-1}(\cdot)$ is the inverse function of $\text{F}_X(\cdot)$. For a specified α, the threshold of the test is $\mathcal{T} = \text{F}_{\chi_{2M}^2}^{-1}(1-\alpha)$, and the miss rate can be obtained by numerical methods.

B. Asymptotic Results for Low Correlation Bandwidth

When the variation is independent over tones (i.e., $B_c/W \ll 1$), the covariance matrices of Eq. (9) and (12) become

$$\begin{aligned} \mathbf{R} &= \text{Cov}[\mathbf{H}_A[k] - \mathbf{H}_A[k-1]] = (2(1-a)\sigma_T^2 + 2\sigma_N^2)\mathbf{I} \\ \mathbf{G} &= \text{Cov}[\mathbf{H}_E[k] - \mathbf{H}_A[k-1]] = (2\sigma_T^2 + 2\sigma_N^2)\mathbf{I}, \end{aligned} \tag{17}$$

where $\mathbf{I}$ is the identity matrix. Thus the test statistic Eq. (15) becomes

$$Z = \frac{|\mathbf{H}_t[k] - \mathbf{H}_A[k-1]|^2}{(1-a)\sigma_T^2 + \sigma_N^2} = Z_2/\rho, \tag{18}$$

where

$$\rho = \frac{(1-a)\sigma_T^2 + \sigma_N^2}{\sigma_T^2 + \sigma_N^2}. \tag{19}$$

It is easy to see that, under $\mathcal{H}_1$, the test statistic is a non-central chi-square distribution with order $2M$, i.e., $Z_2 \sim \chi_{2M,\mu}^2$ with non-central parameter

$$\mu = \frac{\sum_{m=1}^{M} |\overline{H}_{E,m} - \overline{H}_{A,m}|^2}{\sigma_T^2 + \sigma_N^2} \tag{20}$$

Thus, the miss rate for specified α, (16), can be written as

$$\beta = \text{P}_r\{Z < \mathcal{T}|\mathcal{H}_1\} = \text{F}_{\chi_{2M,\mu}^2}(\rho\text{F}_{\chi_{2M}^2}^{-1}(1-\alpha)). \tag{21}$$

$$\beta = \mathrm{P}_r\{Z < \mathcal{T}|\mathcal{H}_1\} = \mathrm{P}_r\{2(\mathbf{H}_E[k] - \mathbf{H}_A[k-1])^H \mathbf{R}^{-1}(\mathbf{H}_{E,t}[k] - \mathbf{H}_A[k-1]) < \mathrm{F}^{-1}_{\chi^2_{2M}}(1-\alpha)\}, \quad (16)$$

C. Asymptotic Results for High Correlation Bandwidth

When the variation is totally correlated over tones (i.e., $B_c/W \gg 1$), the covariance matrices of (9) and (12) degrade to

$$\mathbf{R} = 2\sigma_N^2\mathbf{I} + 2(1-a)\sigma_T^2\mathbf{1} \quad (22)$$

$$\mathbf{G} = 2\sigma_N^2\mathbf{I} + 2\sigma_T^2\mathbf{1}, \quad (23)$$

where $\mathbf{1}$ is a $M \times M$ matrix with each element equals to 1. Again, we can use Eq. (16) to numerically calculate the miss rate β for specified false alarm rate α.

D. Unknown Parameters

When Bob does not know the parameters a, B_c and σ_T, it is reasonable for him to use as the test statistic

$$Z = \frac{1}{\sigma_N^2}|\mathbf{H}_t[k] - \mathbf{H}_A[k-1]|^2. \quad (24)$$

In this case, we can obtain numerical results for the false alarm rate and miss rate for specified threshold $\mathcal{T}$, plotting β vs. α with $\mathcal{T}$ as an implicit parameter.

E. Full Spatial Correlation

Now we consider the other extreme case of spatial correlation, namely, $\epsilon_{E,m}[k] = \epsilon_{A,m}[k]$ (full spatial correlation). The spatial correlation has no impact under the hypothesis $\mathcal{H}_0$. However, under the hypothesis $\mathcal{H}_1$, the correlation matrix of the difference between two measurements becomes $\mathbf{R}$, and $\mathbf{H}_E[k] - \mathbf{H}_A[k-1] \sim CN((\overline{\mathbf{H}}_E - \overline{\mathbf{H}}_A), \mathbf{R})$. Thus, the test statistic under $\mathcal{H}_1$ is non-central chi-square distributed, $Z = |\sqrt{2}(\mathbf{R}_d^H)^{-1}(\mathbf{H}_E[k] - \mathbf{H}_A[k-1])|^2 \sim \chi^2_{2M,\mu}$, with non-central parameter $\mu = |\sqrt{2}(\mathbf{R}_d^H)^{-1}(\overline{\mathbf{H}}_E - \overline{\mathbf{H}}_A)|^2$. Therefore, the miss rate for the fully spatially correlated temporal variation can be written as

$$\beta = \mathrm{F}_{\chi^2_{2M,\mu}}(\mathrm{F}^{-1}_{\chi^2_{2M}}(1-\alpha)). \quad (25)$$

F. Discussion: Impact of Time Variations

As a benchmark, from (21) we have the miss rate for the time-invariant channel as [16],

$$\beta = \mathrm{F}_{\chi^2_{2M,\mu}}(\mathrm{F}^{-1}_{\chi^2_{2M}}(1-\alpha)), \quad (26)$$

where $\mu = \sum_{m=1}^{M} |\overline{H}_{E,m} - \overline{H}_{A,m}|^2/\sigma_N^2$.

In the presence of time variation, however, the miss rate may become smaller. The asymptotic miss rate for the time-variant channel at high bandwidth, (21), increases with ρ, (19), and decreases with μ, (20). As the time variation σ_T^2 rises from 0 to ∞, ρ decreases from 1 to $1-a$ and μ falls from $\sum_{m=1}^{M} |\overline{H}_{E,m} - \overline{H}_{A,m}|^2/\sigma_N^2$ to 0, which may results in a smaller miss rate.

Actually, the temporal-variation has a two-fold impact: 1) It adds uncertainty to the channel from Alice, and thus Bob has to increase the test threshold to accept Alice (negative impact on the performance); 2) the variation is usually strongly correlated in time while very weakly correlated in space, and thus $\epsilon_A[k] - \epsilon_A[k-1] < \epsilon_E[k] - \epsilon_A[k-1]$ (positive impact on performance).

When σ_T is negligible, the channel can be viewed approximately as a time-invariant one, wherein the miss rate is given by (26). As σ_T rises, the miss rate falls since the positive impact dominates. If the variation continues to rise and becomes very large, the miss rate begins to rise, as the need to raise the threshold helps Eve and counteracts the positive impact. When σ_T becomes so large that both the fixed part of the channel response and the thermal noise are relatively negligible (i.e., $\sigma_T^2 \gg \sigma_N^2$, $\sigma_T^2 \gg \sum_{m=1}^{M} |\overline{H}_{E,m} - \overline{H}_{A,m}|^2$), then using (21) we can rewrite the miss rate as

$$\beta \approx \mathrm{F}_{\chi^2_{2M}}((1-a)\mathrm{F}^{-1}_{\chi^2_{2M}}(1-\alpha)), \quad (27)$$

which is a function of the time-correlation of the temporal variation parameter (a), frequency sample size (M), and the false alarm rate (α). If the variation is strongly correlated in time ($a \approx 1$), the miss rate can be less than that for the noise-dominated case, (26), where the thermal noise is usually not negligible due to the limited transmit power. An illustration of this trend will be given later.

Finally, we consider the impact of the spatial correlation of time variations. The miss rate with total spatial correlation, (25), decreases with μ in a manner that is proportional to the inverse of $\mathbf{R}$, (9), and thus rises with σ_T. Since a strong spatial correlation of the time variation damages the spatial variability character of the channel, which is the basis of our scheme, it will degrade the system performance.

VI. Simulation Methodology

A. Simulating the Transfer Functions

In order to test the proposed scheme, it is necessary to model not only "typical" channel responses, but the spatial variability of these responses. Only in this way can we discern the success in detecting would-be intruders like Eve. To that end, we make use of the WiSE Tool, a ray-tracing software package developed by Bell Laboratories [24]. One input to WiSE is the 3-dimensional plan of a specific building, including walls, floors, ceilings and their material properties. With this information, WiSE can predict the rays at any receiver from any transmitter, including their amplitudes, phases and delays. From this, it is straightforward to construct the transmit-receive frequency response over any specified frequency interval (bandwidth).

We have done this for one particular office building (the Alcatel-Lucent Crawford Hill Laboratory in Holmdel, NJ), for which a top view of the first floor is shown in Fig. 2. This floor of this building is 120 meters long, 14 meters wide and 4 meters high. For our numerical experiment, we placed Bob in the hallway (the filled-in circle) at a height of 3 m. For

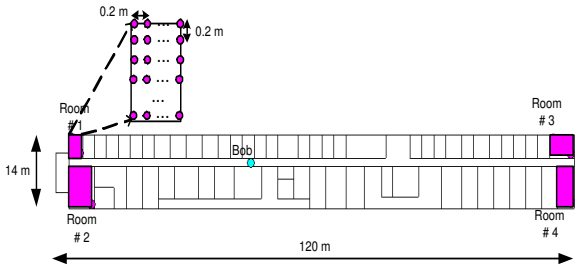

Fig. 2. System topology assumed in the simulations. Bob is located at 2-m height near the center of a 120 m × 14 m × 4 m office building. Alice and Eve are located on dense grids at a height of 2 m. The sizes of the grids are $N_s = 150$, 713, 315, and 348, respectively, for Room # 1, 2, 3 and 4.

the positions of Alice and Eve, we considered four rooms at the extremities of the building (shown shaded). For each room, we assumed Alice and Eve both transmitted from a height of 2 m, each of them being anywhere on a uniform horizontal grid of points with 0.2-meter separations. With N_s grid points in a room, there were $N_s(N_s-1)/2$ possible pairs of Alice-Eve positions. For Rooms 1, 2, 3 and 4, the numbers of grid points were $N_s = 150$, 713, 315 and 348, respectively. For each Alice-Eve pair, (1) WiSE was used to generate the Alice-Bob and Eve-Bob average channel responses ($\overline{H}_A(f)$ and $\overline{H}_E(f)$); and (2) the hypothesis test described above was used to compute β for a specified α. The set of all β-values in a room were used to compute a room-specific mean, $\overline{\beta}$, for each of several selected combinations of bandwidth (W), number of frequency-domain samples (M), transmit power (P_T), and channel variation models.

B. Transmit Power, Receiver Noise, and Time Variation Strength

Assume that, in conjunction with WiSE, we obtain the various transfer functions as dimensionless ratios (e.g., received *E*-field/transmitted *E*-field). Then the proper treatment of the noise variance, σ_N^2, in the hypothesis test is to define it as the receiver noise power per tone, P_N, divided by the transmit power per tone, P_T/M, where P_T is the total transmit power. Noting that $P_N = \kappa\mathcal{T} N_F b$, where $\kappa\mathcal{T}$ is the thermal noise density in mW/Hz, N_F is the receiver noise figure, and b is the measurement noise bandwidth per tone in Hz [18], we can write

$$\sigma_N^2 = \frac{\kappa\mathcal{T} N_F b}{P_T/M} = \frac{M}{\Gamma}, \tag{28}$$

where P_T is in mW, and $\Gamma = P_T/P_N$. We will henceforth refer to Γ by its decibel value.

Let b_T^2 denote the ratio between σ_T^2 and the value of $|H|^2$ averaged over the M frequency samples (or "tones") and the N_s receiver locations. We can thus write the standard deviation of the time variation as

$$\sigma_T = b_T \overline{\overline{H}} = b_T \sqrt{\frac{1}{MN_s} \sum_{m=1}^{M} \sum_{l=1}^{N_s} |H_{l,m}|^2}, \tag{29}$$

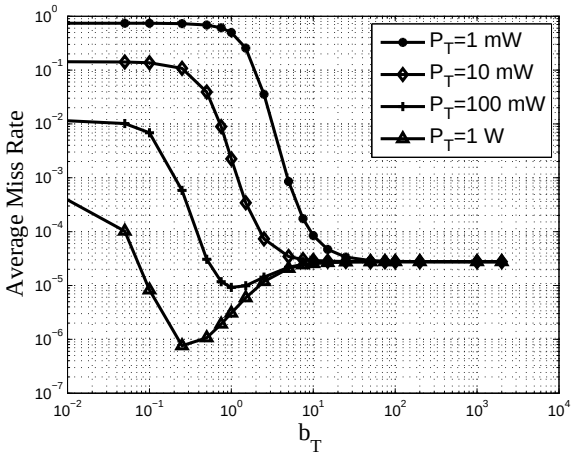

Fig. 3. The average miss rate as function of the relative standard deviation of the time variation, for the channel with spatially independent temporal variation. $M = 10$, $W = 10$ MHz, $a = 0.9$ and $B_c = 0$.

where $\overline{\overline{H}}$ can be regarded as a room parameter, and b_T represents the relative magnitude of the time variation in a given room.

VII. Numerical Results

In our simulations, we set $f_0 = 5$ GHz, $N_F = 10$ (10 dB noise figure), $\kappa\mathcal{T} = 10^{-17.4}$ mW/Hz, $b = 0.25$ MHz, $a = 0.9$, and, unless specified otherwise, $\alpha = 0.01$ [25]. As noted earlier, we place Alice and Eve on dense grids in each of four rooms at the corners of a particular building, with Bob in the hallway, Fig. 2. We obtained a miss rate for each Alice-Eve pair in each room, and then calculated the average mean value for each room in the building. Among them, Room # 4, as the farthest room from Bob, is likely to have the poorest performance in rejecting Eve. In that sense, it lower-bounds the capabilities of our PHY-layer authentication algorithm. For reasons of space, we will only present results for Room # 4, keeping in mind that they are essentially worst-case or close to it.

Figure 3 confirms the efficacy of the algorithm in the presence of channel time variations. We assume realistic system parameter values ($P_T = 1$ mW ~ 1 W, $M = 10$ and $W = 10$ MHz), and find that most average miss rates are smaller than 0.01. The per tone signal-to-noise ratio (SNR) in the channel measurements ranges from -12.8 dB to 14.2 dB, with a media value of 6.4 dB, if using $P_T = 10$ mW, $M = 10$ and $W = 10$ MHz. Also, as pointed out in Section V, our proposed algorithm can exploit the time variations to improve performance. For example, the miss rate falls from around 0.01 to 10^{-5} when b_T rises from 0.01 to 1, with $P_T = 100$ mW. The trend of these curves with time variation confirms the discussion in Section V-F, e.g., the minimum average miss rate is a tradeoff between the positive impact of the time variation and its negative impact resulting from the rise of the threshold. Moreover, the miss rate falls with the transmit power P_T, as expected, since it reduces the measurement noise at the receiver.

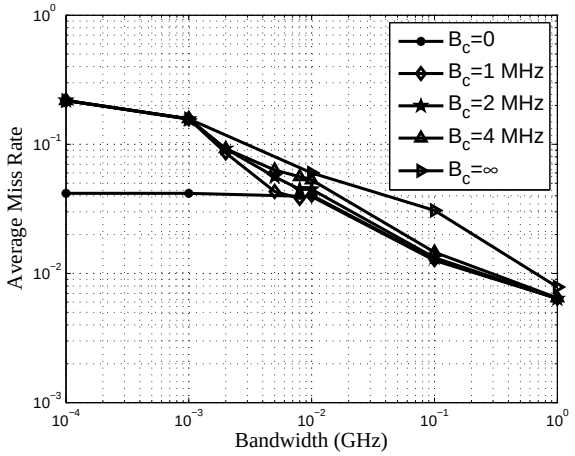

Fig. 4. The average miss rate as a function of the measurement bandwith W, for the channel with spatially independent temporal variation. $M = 5$, $a = 0.9$, $b_T = 0.5$, and $P_T = 10$ mW.

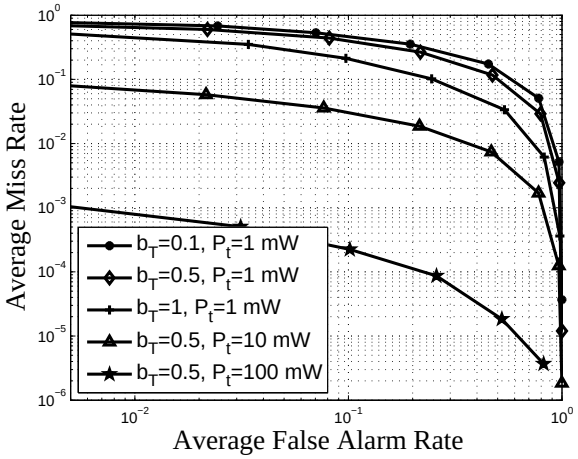

Fig. 6. Average miss rate vs. average false alarm rate when Bob does not know the channel parameters, for the channel with spatially independent temporal variation. $W = 50$ MHz, $M = 10$, $a = 0.9$, and $B_c = 2$ MHz.

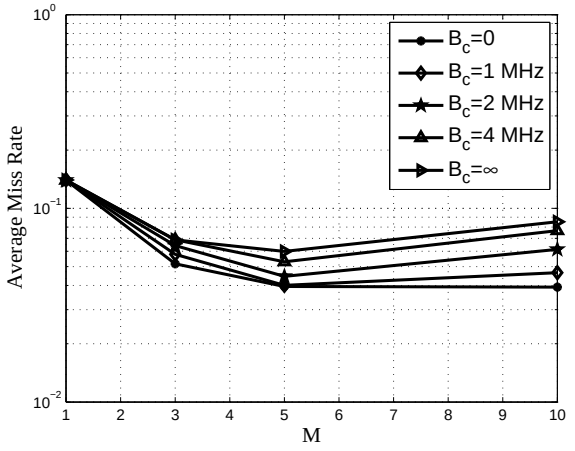

Fig. 5. The average miss rate as a function of the number of frequency samples, for the channel with spatially independent temporal variation. $W = 10$ MHz, $a = 0.9$, $b_T = 0.5$, and $P_T = 10$ mW.

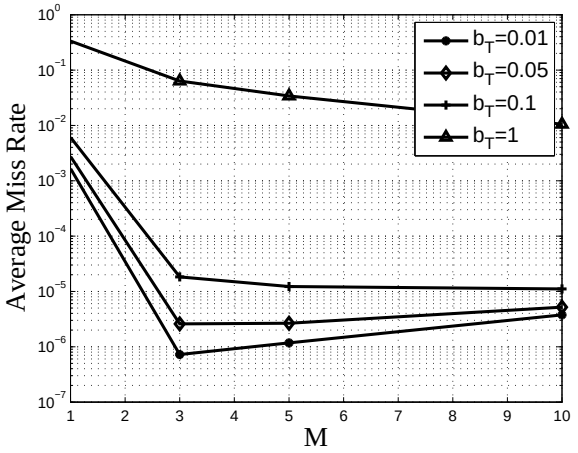

Fig. 7. Average miss rate vs. M, for the channel with totally spatially correlated temporal variation. $W = 100$ MHz, $B_c = 2$ MHz, $P_T = 0.5$ W, and $a = 0.9$.

Figure 4 demonstrates the impact of the bandwidth W and the coherence bandwidth B_c. We note that the results for $B_c = 0$ and $B_c = \infty$ are the lower and upper bounds, respectively, of the miss rates, as well as the asymptotic results for the high- and low-bandwidth regions. It is clear that frequency correlations degrade performance. A related finding is that the miss rate decreases with increasing bandwidth, W, since the frequency response samples are more independent with larger W.

Figure 5 indicates that there is little benefit (or even a deficit) in increasing M beyond ~ 10, unless the frequency correlation is very small (e.g., $B_c = 0$) with high transmit power. Actually, the optimal sample size M in terms of miss rate for specified measurement bandwidth decreases with the coherence bandwidth B_c, because the noise power (28) rises with M and the frequency-response samples are more correlated with larger B_c.

We see in Fig. 6 that the algorithm works even when Bob does not know the key channel parameters, although it requires either more transmit power or greater tolerance for Type II errors. Interestingly, the time-variation may still help here, e.g., the miss rate falls as b_T rises from 0.1 to 1. How to set the test threshold $\mathcal{T}$ in this case is an open topic.

Finally, Fig. 7 shows that the system is very sensitive to the time-variation in an extreme case of full spatial correlation. It requires much more transmit power ($P_T \sim 0.5$W) to reach the same miss rate performance. The reason is quite simple: the mechanism of our scheme is to utilize the spatial variability of the channel responses. The spatial correlation of the time variation decreases the overall spatial variability and thus degrades the performance.

The above assertions apply as well to the other shaded rooms in Fig. 2 and, we can safely assume, to the other rooms in the building.

VIII. Conclusion

We have described and studied a physical layer technique for enhancing authentication in a time-variant wireless environment. Specifically, we assume the user terminals are stationary but changes in the environment produce additive time-varying changes in the channel responses. The technique uses channel frequency response measurements and hypothesis testing to discriminate between a legitimate user (Alice) and a would-be intruder (Eve). With the ability to utilize the temporal-variation, it works even when the receiver does not know the key channel variation parameters, namely, the AR temporal coefficient a, the coherence bandwidth B_c and the standard deviation of the variation σ_T, although these parameters help reduce the miss rate if known.

The algorithm has been verified in a typical in-building environments, where we used the ray-tracing tool WiSE to generate realistic average channel responses and used a multipath tapped delay line channel model for the temporal variation part of the channel response. Simulation results have confirmed the efficacy of the algorithm for realistic values of the measurement bandwidth (e.g., $W \sim 10$ MHz), number of response samples (e.g., $M \leq 10$) and transmit power (e.g., $P_T > 10$ mW). The miss rate is generally smaller than 0.01, for a specified false alarm rate of 0.01, in the presence of moderate channel time variations.

We have found that the channel time variations can improve the performance, e.g., the miss rate falls from around 0.01 to 10^{-5} when the variation index b_T rises from 0.01 to 1, with $P_T = 100$ mW. In addition, the miss rate decreases with the transmit power of the probing signal and the measurement bandwidth, and usually requires frequency samples of fewer than 10. We have also shown that the time correlation of the channel variation is helpful, while coherence in the frequency and spatial domains are harmful.

Research is currently in progress to address the case of user terminal mobility. Effort is also needed, for the stationary case, to explore the parameter space (e.g., the temporal coherence term a); devise means of setting the test threshold $\mathcal{T}$; consider other buildings; and conduct experiments to more accurately characterize the time-variation properties of indoor channels. Moreover, we are working to integrate physical layer authentication into a holistic cross-layer framework for wireless security that will augment traditional "higher-layer" network security mechanisms with physical layer methods.

Appendix A
Proof of Relationship 1

Since $A_l[k] \sim CN(0, P_\tau[l])$, from Eq. (3) and (4), we have

$$E[\epsilon_{A,m}[k]] = \sum_{l=0}^{\infty} E[A_l[k] e^{-j2\pi(f_o - W/2 + m\Delta f) l\Delta}] = 0 \quad (30)$$

and

$$\begin{aligned}\text{Var}[\epsilon_{A,m}[k]] &= \sum_{l=0}^{\infty} \text{Var}[A_l[k] e^{-j2\pi(f_o - W/2 + m\Delta f) l\Delta}] \\ &= \sum_{l=0}^{\infty} \text{Var}[A_l[k]] \\ &= \sum_{l=0}^{\infty} \sigma_T^2 (1 - e^{-\gamma\Delta\tau}) e^{-\gamma\Delta\tau l} = \sigma_T^2 \end{aligned} \quad (31)$$

Here we also utilize the fact that any two different multipath components in a WSSUS channel are uncorrelated, i.e., $\forall l_1 \neq l_2$, $\forall k_1, k_2$,

$$E[A_{l_1}[k_1] A_{l_2}[k_2]] = 0 \quad (32)$$

Considering that $A_l[k-1]$ and $u_l[k]$ are both zero-mean and independent to each other, we see from Eq. (4) and (5) that

$$\begin{aligned} E[A_l[k_1] A_l[k_2]] &= a^{|k_1 - k_2|} \text{Var}[A_l[\min(k_1, k_2)]] \\ &= a^{|k_1 - k_2|} \sigma_T^2 (1 - e^{-\gamma\Delta\tau}) e^{-\gamma\Delta\tau} \end{aligned} \quad (33)$$

Then from (3), (32), and (33), we have

$$\begin{aligned} &E[\epsilon_{A,m}[k_1] \epsilon_{A,n}[k_2]^*] \\ &= \sum_{l_1=0}^{\infty} \sum_{l_2=0}^{\infty} E[A_{l_1}[k_1] A_{l_2}[k_2]] \\ &\quad \cdot e^{-j2\pi[(f_o - W/2 + m\Delta f) l_1 - (f_o - W/2 + n\Delta f) l_2]/W} \\ &= \sum_{l=0}^{\infty} E[A_l[k_1] A_l[k_2]] e^{j2\pi(n-m)\Delta f l/W} \\ &= \sum_{l=0}^{\infty} a^{|k_1 - k_2|} \sigma_T^2 (1 - e^{-\gamma\Delta\tau}) e^{-\gamma\Delta\tau l} e^{j2\pi(n-m)\Delta f l/W} \\ &= \frac{a^{|k_1 - k_2|} \sigma_T^2 (1 - e^{-\gamma\Delta\tau})}{1 - e^{-\gamma\Delta\tau + j2\pi(n-m)\Delta f l \Delta\tau}} \end{aligned} \quad (34)$$

By (1), (31), and (34), we get

$$\begin{aligned} &\text{Var}[H_{A,m}[k] - H_{A,m}[k-1]] \\ &= \text{Var}[\epsilon_{A,m}[k] - \epsilon_{A,m}[k-1] + N_{A,m}[k] - N_{A,m}[k-1]] \\ &= \text{Var}[\epsilon_{A,m}[k]] + \text{Var}[\epsilon_{A,m}[k-1]] \\ &\quad - 2\text{Cov}[\epsilon_{A,m}[k], \epsilon_{A,m}[k-1]] + \text{Var}[N_{A,m}[k]] \\ &\quad + \text{Var}[N_{A,m}[k-1]] \\ &= 2\sigma_T^2 - 2E[\epsilon_{A,m}[k] \epsilon_{A,m}^*[k-1]] + 2\sigma_N^2 \\ &= 2\sigma_T^2 (1 - a) + 2\sigma_N^2 \end{aligned} \quad (35)$$

The thermal noise components are independent of each other and all the other variables, and the fixed part of the channel

can be viewed as constant, so $\forall m \neq n$

$$\begin{aligned} & r(m-n) \\ &= \text{Cov}[H_{A,m}[k] - H_{A,m}[k-1], H_{A,n}[k] - H_{A,n}[k-1]] \\ &= \text{Cov}[\epsilon_{A,m}[k] - \epsilon_{A,m}[k-1], \epsilon_{A,n}[k] - \epsilon_{A,n}[k-1]] \\ &= E[\epsilon_{A,m}[k]\epsilon^*_{A,n}[k]] + E[\epsilon_{A,m}[k-1]\epsilon^*_{A,n}[k-1]] \\ &\quad - E[\epsilon_{A,m}[k]\epsilon^*_{A,n}[k-1]] - E[\epsilon_{A,m}[k-1]\epsilon^*_{A,n}[k]] \\ &= \frac{2\sigma_T^2(1-a)(1-e^{-\gamma\Delta\tau})}{1-e^{-\gamma\Delta\tau+j2\pi(n-m)\Delta\tau\Delta f}} \\ &= \frac{2\sigma_T^2(1-a)(1-e^{-2\pi B_c/W})}{1-e^{-2\pi B_c/W+j2\pi(n-m)/M}} \end{aligned} \quad (36)$$

It can be easily proved that $\mathbf{H}_A[k] - \mathbf{H}_A[k-1]$ has zero mean and is a Gaussian random variable, since it is the linear combination of Gaussian random variables.

APPENDIX B
PROOF OF RELATIONSHIP 2

For the case with spatially independent time variation where $\epsilon_{E,m}[k]$ and $\epsilon_{A,m}[k]$ are independent identically distributed, from (1) and (6) we have

$$\begin{aligned} & \text{Var}[H_{E,m}[k] - H_{A,m}[k-1]] \\ &\quad = \text{Var}[\epsilon_{E,m}[k] - \epsilon_{A,m}[k-1] + N_{E,m}[k] - N_{A,m}[k-1]] \\ &\quad = \text{Var}[\epsilon_{E,m}[k]] + \text{Var}[\epsilon_{A,m}[k-1]] \\ &\qquad + \text{Var}[N_{A,m}[k]] + \text{Var}[N_{E,m}[k]] \\ &\quad = 2\sigma_T^2 + 2\sigma_N^2 \end{aligned} \quad (37)$$

And $\forall m \neq n$,

$$\begin{aligned} & \text{Cov}[H_{E,m}[k] - H_{A,m}[k-1], H_{E,n}[k] - H_{A,n}[k-1]] \\ &\quad = \text{Cov}[\epsilon_{E,m}[k] - \epsilon_{A,m}[k-1], \epsilon_{E,n}[k] - \epsilon_{A,n}[k-1]] \\ &\quad = E[\epsilon_{E,m}[k]\epsilon^*_{E,n}[k]] + E[\epsilon_{A,m}[k-1]\epsilon^*_{A,n}[k-1]] \\ &\quad = \frac{2\sigma_T^2(1-e^{-\gamma\Delta\tau})}{1-e^{-\gamma\Delta\tau+j2\pi(n-m)\Delta\tau\Delta f}} = r(m-n)/(1-a) \end{aligned} \quad (38)$$

From (1) and (6) we also see that $E[\mathbf{H}_E[k] - \mathbf{H}_A[k-1]] = \overline{\mathbf{H}}_E - \overline{\mathbf{H}}_A$. The other part is similar to that of Relationship 1.

REFERENCES

[1] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in Proc. ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), pp. 180–189, Sept. 2002.

[2] A. Mishra, M. Shin, and W. A. Arbaugh, "Your 802.11 network has no clothes," *IEEE Communications Magazine*, vol. 9, pp. 44 – 51, Dec. 2002.

[3] J. Walker, "Unsafe at any key size: an analysis of the WEP encapsulation," IEEE Document 802.11-00/362, 2000.

[4] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*, Redwood City, CA: Addison-Wesley Wireless Communications Series, 1995.

[5] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *IEEE Wireless Personal Communications*, vol. 6, pp. 311–335, March 1998.

[6] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, pp. 364–375, Sept. 2007.

[7] A. E. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, pp. 3235–3249, December 2003.

[8] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. IEEE Military Communications Conference (MILCOM)*, vol. 3, pp. 1501– 1506, Oct. 2005.

[9] A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1x standard," Tech. Rep. CS-TR-4328, University of Maryland, College Park, 2002.

[10] C. Corbett, R. Beyah, and J. Copeland, "A passive approach to wireless NIC identification," in *Proc. IEEE International Conference on Communications*, vol. 5, pp. 2329–2334, June 2006.

[11] J. Hall, M. Barbeau, and E. Kranakis, "Detection of transient in radio frequency fingerprinting using signal phase," in *Wireless and Optical Communications*, ACTA Press, pp. 13-18, July 2003.

[12] T. Kohno, A. Broido, and C. Claffy, "Remote physical device fingerprinting," in *IEEE Transactions on Dependable and Secure Computing*, vol. 2, pp. 93– 108, April–June 2005.

[13] T. Daniels, M. Mina, and S. F. Russell, "Short paper: a signal fingerprinting paradigm for general physical layer and sensor network security and assurance," in *Proc. IEEE/Create Net Secure Commum.*, pp. 219– 221, Sept. 2005.

[14] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proc. ACM Workshop on Wireless Security*, pp. 43 – 52, Los Angeles, California, Sept. 2006.

[15] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proc. International Workshop on Advanced Experimental Activity*, pp. 564 – 570, June, 2006.

[16] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. IEEE International Conference on Communications*, Glasgow, Scotland, June 2007.

[17] W. Trappe and L.C. Washington, *Introduction to Cryptography with Coding Theory*, Upper Saddle River, NJ: Prentice Hall, 2002.

[18] T.S. Rappaport, *Wireless Communications- Principles and Practice*, Englewood Cliffs, NJ: Prentice Hall, 1996.

[19] W.C. Jakes Jr., *Microwave Mobile Communications*, Piscataway, NJ: Wiley-IEEE Press, 1994.

[20] P.A. Bello, "Characterization of randomly time-variant linear channels," *IEEE Trans. Commun. Syst.*, vol. CS-11, pp. 360–393, Dec. 1963.

[21] V. Erceg, D. G. Michelson, S. S. Ghassemzadeh, L. J. Greenstein, A. J. Rustako, P. B. Guerlain, M. K. Dennison, R. S. Roman, D. J. Barnickel, S. C. Wang, and R.R. Miller, "A model for the multipath delay profile of fixed wireless channels," *IEEE J. on Sel. Areas in Commun.*, vol. 17, pp. 399–410, 1999.

[22] P.A. Bello and B.D. Nelin, "The effect of frequency selective fading on the binary error probability of incoherent and differentially coherent matched filter receivers," *IEEE Trans. Commun. Syst.*, vol. CS-11, pp. 170–186, June 1963.

[23] M. Abramowitz and I A. Stegun, *New York: Handbook of Mathematical Functions, With Formulas, Graphs, and Mathematical Tables*, Courier Dover Publications, 1965.

[24] S. J. Fortune, D. H. Gay, B. W. Kernighan, O. Landron, M. H. Wright, and R. A. Valenzuela, "WiSE design of indoor wireless systems: Practical computation and optimization," *IEEE Computational Science and Engineering*, vol. 2, pp. 58-68, Mar. 1995.

[25] A. Tee, "Clarifications on the link budget evaluation," IEEE Document C802.20-05/18, 2005.

Liang Xiao received the B.S. in communication engineering in 2000 from Nanjing University of Posts & Telecommunications, Nanjing, China, and the M.S. in electrical engineering in 2003 from Tsinghua University, Beijing, China. From 2003 and 2004, she was with North Carolina State University, NC. She is currently working toward the Ph.D. degree in WINLAB, Department of Electrical and Computer Engineering, Rutgers University, NJ.

Her research interests include security, radio channel modeling, wireless and mobile communications, wireless networks, and communication theory.

Larry J. Greenstein received the B.S., M.S., and PhD degrees in electrical engineering from Illinois Institute of Technology, Chicago, IL, in 1958, 1961, and 1967, respectively. From 1958 to 1970, he was with IIT Research Institute, Chicago, IL, working on radio frequency interference and anti-clutter airborne radar. He joined Bell Laboratories, in Holmdel, NJ, in 1970. Over a 32-year AT&T career, he conducted research in digital satellites, point-to-point digital radio, optical transmission techniques, and wireless communications. For 21 years during that period (1979-2000), he led a research department renowned for its contributions in these fields. He is now a Research Scientist at Rutgers-WINLAB, North Brunswick, NJ, working in the areas of ultra-wideband (UWB), sensor networks, MIMO-based systems, Broadband Power Line systems and radio channel modeling.

Dr. Greenstein is an AT&T Fellow, recipient of the IEEE Communications Society's Edwin Howard Armstrong Award, and winner of three best paper awards. He is currently a Member-at-Large on the IEEE Communications Society Board of Governors and has been a Guest Editor, Senior Editor and Editorial Board Member for numerous publications.

Narayan B. Mandayam received the B.Tech (Hons.) degree in 1989 from the Indian Institute of Technology, Kharagpur, and the M.S. and Ph.D. degrees in 1991 and 1994 from Rice University, Houston, TX, all in electrical engineering. From 1994 to 1996, he was a Research Associate at the Wireless Information Network Laboratory (WINLAB), Dept. of Electrical & Computer Engineering, Rutgers University. In September 1996, he joined the faculty of the ECE department at Rutgers where he became Associate Professor in 2001 and Professor in 2003. Currently, he also serves as Associate Director at WINLAB. He was a visiting faculty fellow in the Department of Electrical Engineering, Princeton University in Fall 2002 and a visiting faculty at the Indian Institute of Science in Spring 2003.

His research interests are in various aspects of wireless data transmission including system modeling and performance, signal processing and radio resource management with emphasis on techniques for cognitive radio technologies.

Dr. Mandayam is a recipient of the Institute Silver Medal from the Indian Institute of Technology, Kharagpur in 1989 and the National Science Foundation CAREER Award in 1998. He was selected by the National Academy of Engineering in 1999 for the Annual Symposium on Frontiers of Engineering. He is a coauthor with C. Comaniciu and H. V. Poor of the book "Wireless Networks: Multiuser Detection in Cross-Layer Design," Springer, NY. He has served as an Editor for the journals IEEE Communication Letters (1999-2002), IEEE Transactions on Wireless Communications (2002-2004) and as a guest editor of the IEEE JSAC Special Issue on Adaptive, Spectrum Agile and Cognitive Radio Networks. He is currently serving as a guest editor of the IEEE JSAC Special Issue on Game Theory in Communication Systems.

Wade Trappe received his B.A. degree in Mathematics from The University of Texas at Austin in 1994, and the Ph.D. in Applied Mathematics and Scientific Computing from the University of Maryland in 2002. He is currently an associate professor in the Electrical and Computer Engineering Department at Rutgers University, and is Associate Director of the Wireless Information Network Laboratory (WINLAB). His research interests include wireless security, wireless networking, multimedia security, and network security. While at the University of Maryland, Dr. Trappe received the George Harhalakis Outstanding Systems Engineering Graduate Student award. Dr. Trappe is a co-author of the textbook Introduction to Cryptography with Coding Theory, Prentice Hall, 2001. He is the recipient of the 2005 Best Paper Award from the IEEE Signal Processing Society. He is a member of the IEEE Signal Processing and Communications societies, and a member of the ACM.