Channel-Based Spoofing Detection in Frequency-Selective Rayleigh Channels

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

***Abstract*—The radio channel response decorrelates rapidly as the transmitter changes location in an environment with rich scatterers and reflectors. Based on this fact, a channel-based authentication scheme was previously proposed to discriminate between transmitters at different locations, and thus to detect spoofing attacks in wireless networks. In this paper, we study its application in frequency-selective Rayleigh channels, considering channel time variations due to environmental changes and terminal mobility, as well as the channel estimation errors due to the interference from other radios. We propose a generalized likelihood ratio test (GLRT) that is optimal but computationally cumbersome, and a simplified version that requires no *a priori* knowledge of channel parameters and is therefore more practical. We verify the efficacy of the channel-based spoofing detectors via numerical analysis, showing how performance is improved by using multiple antennas, higher transmit power, and wider system bandwidth. We show that, under a wide variety of practical conditions, spoofing can be detected with better than 90% probability while keeping the probability of falsely rejecting valid transmissions below 10%.**

***Index Terms*—Spoofing detection, PHY-layer, frequency-selective Rayleigh channels, cross-layer design, hypothesis testing.**

I. Introduction

BECAUSE of the broadcast nature of wireless medium, wireless networks are especially vulnerable to attacks, such as session hijacking and denial of service, many of which are facilitated by identity-based attacks, and especially by spoofing attacks [1]–[6]. In order to address this problem, several authentication techniques have been proposed, exploiting various types of physical-layer information in wireless networks [4], [7]–[14].

As shown in [15], in a rich-multipath environment typical of indoor scenarios, the response of the medium along any transmit-receive path is *frequency-selective* in a way that is *location-specific*. Thus, the channel response decorrelates from one transmit-receive path to another if the paths are separated by the order of a wavelength or more. In consequence, the channel response is hard to predict and to spoof. We can exploit this property to discriminate between transmitters located in different places. This is the basis of our channel-based spoofing detection, wherein the receiver tracks the channel response for each message and detects spoofing attacks by comparing the channel responses for messages claiming the same user identity. The scheme utilizes the channel estimation mechanism existing in most wireless systems, and therefore introduces no additional system overhead.

To assess the performance of this scheme in practical systems, we address two significant impairments. First, the channel response can vary over time due to terminal mobility and/or environmental changes, e.g., a group of people moving about. Second, the accuracy of channel estimation can be corrupted by factors such as phase drift of the receiver local oscillator, receiver thermal noise, and interference received from other users in the same band.

Our previous work [10]–[13] has partly addressed these impairments and validated the efficacy of the channel-based authentication for various cases, notably, environmental changes [11], and terminal mobility [13]. However, these studies are limited by virtue of using different heuristic test statistics for each scenario. Moreover, previous performance evaluations were based on a specific channel emulation software [16], with results depending closely on a specific network topology and building environment. Here, we present a more unified approach based on a more general characterization of the channel. Specifically, we investigate channel-based spoofing detection using a well-established stochastic channel model, in a generalized scenario that includes Doppler, multiple antennas, and channel estimation errors. We propose a *generalized likelihood ratio test* (GLRT) that is optimal but complicated, and a simplified version that requires no *a priori* knowledge of channel parameters and is therefore more practical. We present and compare their performances via numerical analysis, and we also derive a best-case performance bound for the simpler test. The results presented in this paper will help facilitate the eventual integration of PHY-based security into practical wireless systems.

We begin by briefly reviewing related work in Section II. We describe the problem model in Section III, and we present the underlying stochastic channel model in Section IV. We propose two ways to implement the authentication using hypothesis testing in Section V, and also define our performance metrics. In Section VI, we derive an analytical expression for best-case performance, and then present numerical results for

Manuscript received November 19, 2008; revised July 3, 2009; accepted August 26, 2009. The associate editor coordinating the review of this paper and approving it for publication was G. Durgin.

L. Xiao is now with the Department of Communication Engineering, Xiamen University, Fujian, China, 361005 (e-mail: lxiao@winlab.rutgers.edu).

L. Greenstein, N. Mandayam, and W. Trappe are with WINLAB, the Department of Electrical and Computer Engineering, Rutgers University, North Brunswick, NJ, 08902 USA (e-mail: {ljg, narayan, trappe}@winlab.rutgers.edu).

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

Digital Object Identifier 10.1109/TWC.2009.12.081544

all cases in Section VII. We conclude the paper in Section VIII.

II. Related Work

Several physical-layer authentication techniques have been proposed to enhance security in wireless networks, exploiting the physical-layer information such as the received signal strength (RSS) [4], [7], [8], channel impulse response (CIR) [9], and channel frequency response (CFR) [10]–[13].

Note that CIR and CFR are the time- and frequency- domain expressions of channel response, containing more location-specific information than RSS. Hence the CIR/CFR-based techniques, [9]–[13], can provide higher accuracy than those using RSS, [4], [7], [8].

As a benchmark, we first investigated the channel-based spoofing detection for time-invariant path gains, [10]. Then the impact of channel time variations and terminal mobility were studied in [11] and [13], respectively. We also explored the use of multiple-input multiple-output (MIMO)-techniques with the channel-based detector in [12].

III. Problem Model

As shown in Fig. 1, our analysis is based on an Alice-Bob-Eve model, where Alice and Bob are the legal transmitter and intended receiver, respectively. The spoofing adversary, Eve, injects messages using Alice's identity, e.g., her MAC address, in the hope of spoofing her. The distance from Bob to Alice (Eve) is denoted as d_A (d_E).

Suppose Bob receives two messages at times indexed by k and $k+1$, with the time interval between messages being T. Both messages are labelled with the sender identity of Alice. We assume that Bob knows that Alice indeed sent the first message at k; this can be confirmed using a standard higher-layer protocol (cf., [17]) in parallel, we discuss later. The second message, sent at $k+1$, is either a legal message from Alice or a spoofing one sent by Eve. Bob seeks to use the channel-based spoofing detector to determine whether the second message belongs to Alice.

Without loss of generality, we consider an $N_T \times N_R$ multiple-input multiple-output (MIMO) system [18]: both Alice and Eve use $N_T \geq 1$ transmit antennas, while Bob uses $N_R \geq 1$ receive antennas. The antennas are spaced so that the channel paths of different antenna pairs fade independently. We assume that Alice might move and/or that the propagation environment may change, e.g., due to people moving. Finally, we allow the possibility that channel gain estimation may be corrupted by additive interference, as well as additive noise.

IV. System And Channel Models

A. Channel Samples

The receiver for Bob estimates the channel response based on pilot or preamble symbols in the message, and obtains a channel vector containing M' independent channel samples (in frequency). This can be conveniently implemented in orthogonal frequency division multiplexing (OFDM) systems, where channel responses are measured at M' tones based on pilots equally spaced within the system bandwidth of W. If the minimum frequency separation, W/M', is greater than the channel coherence bandwidth, the M' channel samples are essentially uncorrelated. We assume that is the case here, although the discussion can be easily extended to the case where the channel gains for neighboring pilot tones are correlated.

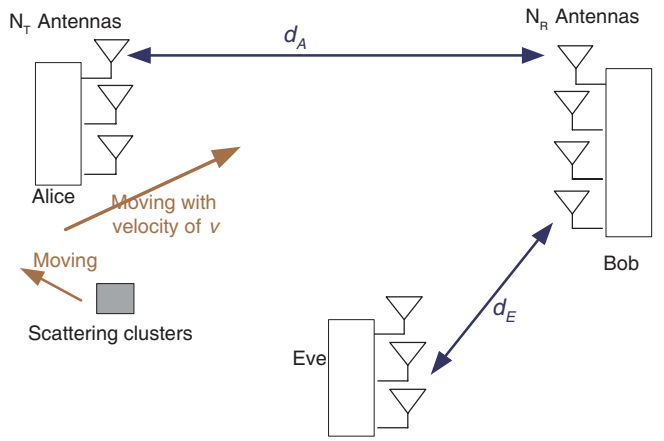


Fig. 1. The adversarial multipath environment involving multiple scattering surfaces. The transmission from Alice with N_T antennas to Bob with N_R antennas, experiences different multipath effects than the transmission by the adversary, Eve. Bob has to discriminate between a legal message from Alice and the spoofing one from Eve. The distance between Alice (Eve) and Bob is denoted as d_A (d_E).

The use of multiple antenna techniques expands the dimension of the channel vector from M' to $M = N_T N_R M'$, and thus improve the channel resolution. Our spoofing detection scheme can benefit from this increase, especially when the overall system bandwidth W is too small to afford a large number of independently faded tones.

B. Channel Estimates

To model the channel estimation at time instant k, we assume an unknown phase measurement error, denoted as $\varphi(k) \in [0, 2\pi)$, due to the drift of the receiver local oscillator. We also assume the receiver thermal noise contributes an additive complex Gaussian error component, $N(k)$, to each channel gain estimate. This error is zero-mean and independent across frequencies and receive antennas, with a common variance σ_N^2.

Another impairment, often omitted in channel estimation models [10]–[13], is interference from other radio users. We can model the interference effect on channel estimation as contributing a random error component, $I(k)$, to the true value of each measured channel gain. As in the noise case, we model these errors as zero-mean, complex Gaussian and independent across frequencies and receive antennas, with a common variance σ_I^2.

The channel estimation vector at time k, $\underline{\hat{H}}(k)$, can thus be given by

$$\underline{\hat{H}}(k) = \underline{H}(k)e^{j\varphi(k)} + \underline{N}(k) + \underline{I}(k), \tag{1}$$

where $\underline{H}(k)$ is the "ideal" channel vector without estimation error; and $\underline{I}(k)$, $\underline{N}(k)$, and $\varphi(k)$, are independent from each other, as well as from their counterparts at time $k+1$. Since

$H(k)$ is estimated by dividing the complex sample of the received pilot tone by $\sqrt{P_T}$, where P_T is the transmitted power per tone, we can write the following for the variances of $\underline{N}$ and $\underline{I}$:

$$\sigma_N^2 = P_N/P_T, \tag{2}$$

and

$$\sigma_I^2 = P_I/P_T, \tag{3}$$

where P_N and P_I are the average receiver noise and interference powers, respectively, for each measured tone. Thus we can write

$$\underline{N} + \underline{I} \sim CN\left(\underline{0}, \left(\sigma_I^2 + \sigma_N^2\right)\mathbf{I}\right), \tag{4}$$

where $\mathbf{I}$ is the $M \times M$ identity matrix.

C. Channel Gains

As noted, we assume the first message at time k is not a spoofing one, i.e., $\underline{H}(k) \equiv \underline{H}_A(k)$, where the subscript 'A' denotes that the transmitter is Alice. The sender of the second message is either Alice or Eve, and thus we have $\underline{H}(k+1) = \underline{H}_A(k+1)$ or $\underline{H}_E(k+1)$, where the subscript 'E' represents Eve.

In our analysis, the three locations (for Bob, Eve, and Alice) are specified, and we assume that $\underline{H}_A(k)$ and $\underline{H}_E(k)$ are independent, frequency-selective Rayleigh channels, i.e.,

$$\underline{H}_i(k) \sim CN\left(\underline{0}, \sigma_i^2\mathbf{I}\right), \quad i = A, E \tag{5}$$

where σ_A^2 and σ_E^2 are the locally averaged power gains along the paths from Alice to Bob and from Eve to Bob, respectively.

Propagation theory shows that, in an environment full of scatterers and reflectors, the channel response decorrelates rapidly as the terminal location changes by the order of a wavelength, which is 6 cm for systems working at 5 GHz [15]. Note that both Alice and Eve can be anywhere in the coverage region of Bob and that in practice, Eve cannot be close to Alice (in units of wavelength). For typical terminal speeds ($\sim$ 1 m/s) and practical time intervals between measurements ($\sim$ 3 ms), we can assume that Eve at time $k+1$ cannot be close to Alice's previous location. We therefore assume that $\underline{H}_A(k)$ and $\underline{H}_E(k+1)$ are independent.

By (1)-(4), we have

$$\begin{aligned}\hat{\underline{H}}_E(k+1) &= \underline{H}_E(k+1)e^{j\varphi(k+1)} + \underline{N}(k+1) + \underline{I}(k+1) \\ &\sim CN\left(\underline{0}, \left(\sigma_E^2 + \sigma_N^2 + \sigma_I^2\right)\mathbf{I}\right).\end{aligned} \tag{6}$$

Similarly,

$$\hat{\underline{H}}_A(k) \sim CN\left(\underline{0}, \left(\sigma_A^2 + \sigma_N^2 + \sigma_I^2\right)\mathbf{I}\right). \tag{7}$$

D. Channel Variations

Assuming a short enough interval between successive transmission T, Alice at time $k+1$ will be close to her previous location, i.e., on the order of a fraction of a wavelength, and thus $\underline{H}_A(k)$ and $\underline{H}_A(k+1)$ are correlated. As an extreme case, we have $\underline{H}_A(k+1) = \underline{H}_A(k)$, e.g., for static channels. In general, however, due to environmental changes and/or terminal mobility, the channel vector can vary with time. For the case of mobility alone, this can be modeled by

$$\underline{H}_A(k+1) = a\underline{H}_A(k) + \underline{\epsilon_1}(k), \tag{8}$$

where a is the correlation coefficient between channel gain samples spaced by T; and $\underline{\epsilon_1}(k)$ is an M-dimensional vector in which each term is an i.i.d. zero-mean complex Gaussian process that is independent of $H(k)$, with each element having a variance

$$\sigma_1^2 = (1-a^2)\sigma_A^2. \tag{9}$$

Assuming that Alice moves with a speed of v, and using the Jakes model [15], we can write

$$E\left[\underline{H}_A(k+1)\underline{H}_A^H(k)\right] = \sigma_A^2 J_0\left(2\pi vT/\lambda\right)\mathbf{I}, \tag{10}$$

where the superscript ^{H} denotes conjugate transpose, λ is the RF wavelength, and $J_0(\cdot)$ is the Bessel function of the first kind and zero-th order. The $J_0(\cdot)$ term is seen to be nothing other than the correlation coefficient a in the above discussion. If Alice moves so slowly that $v \sim 0$ (more specifically, $vT/\lambda \sim 0$), then it is clear that $a \sim 1$.

Finally, we consider the possibility that, even if Alice is stationary, there can be time variations of the path gains due to movement of objects and/or people in the environment. We envision this as a zero-mean gain variation added to an average gain. It is accounted for in (8) by adding a vector $\underline{\epsilon_2}(k)$, which represents the change in the environment-caused variation from time k to time $k+1$. As we will explain in Section IV-E, we model each element of $\underline{\epsilon_2}$ as zero-mean, complex Gaussian and independent across paths and frequencies, with a common variance σ_2^2. With this term included, the additive time variation in (8) can be treated as the sum of *two* random, independent complex Gaussian processes, $\underline{\epsilon_1}$ and $\underline{\epsilon_2}$, due to terminal motion and environment changes [11], respectively, i.e.,

$$\underline{\epsilon_1}(k) = \underline{\epsilon_1} + \underline{\epsilon_2} \sim CN\left(\underline{0}, \left((1-a^2)\sigma_A^2 + \sigma_2^2\right)\mathbf{I}\right). \tag{11}$$

By (1)-(5), (8), and (11), we can write $\hat{\underline{H}}_A(k+1)$, conditioned on the measured $\hat{\underline{H}}(k)$, as

$$\begin{aligned}\hat{\underline{H}}_A(k+1) &= \underline{H}_A(k+1)e^{j\varphi(k+1)} + \underline{N}(k+1) + \underline{I}(k+1) \\ &= \left(a\underline{H}_A(k) + \underline{\epsilon_1}(k)\right)e^{j\varphi(k+1)} + \underline{N}(k+1) + \underline{I}(k+1) \\ &= \left(a\left(\hat{\underline{H}}_A(k) - \underline{N}(k) - \underline{I}(k)\right)e^{-j\varphi(k)} + \underline{\epsilon_1}(k)\right)e^{j\varphi(k+1)} \\ &\quad + \underline{N}(k+1) + \underline{I}(k+1) \\ &\sim CN\left(a\hat{\underline{H}}(k)e^{j\phi_0}, \varrho^2\mathbf{I}\right),\end{aligned} \tag{12}$$

where $\phi_0 = \varphi(k+1) - \varphi(k)$, and

$$\varrho^2 = \left(1+a^2\right)\left(\sigma_N^2 + \sigma_I^2\right) + \left(1-a^2\right)\sigma_A^2 + \sigma_2^2. \tag{13}$$

E. Comments on the Modeling of $\underline{\epsilon_2}$ and $\underline{I}$

In the most general formulation of the problem, the temporal process $\underline{\epsilon_2}(k)$ can be correlated from path to path and/or from frequency to frequency. This process is defined as the change, from time k to time $k+1$, in the gain variation caused by moving scatterers in the environment. We hypothesized a model in [11] for the environment-caused

time variation in a single path gain (the MIMO case was not considered). Specifically, we treated it as a wide-sense stationary uncorrelated scattering (WSSUS) process, with a decaying exponential for the power delay profile and a first-order autoregressive (AR-1) process for the time variation. A limited set of indoor measurements with people moving about was subsequently reported in [19], [20], and it provided support for our hypothesized model. Nevertheless, this topic lacks sufficient empirical data to propose specific correlations in space and frequency. Therefore, to simplify this study that is already rich in parameters, we assume the process $\underline{\epsilon}_2(k)$ to be "white" in both domains. We will also assume mean-square values for it that are quite a bit larger than those we would expect, based on [19], [20], so that we can demonstrate the relatively low impact of this phenomenon.

Similarly, the additive interference, $\underline{I}(t)$, could in reality be correlated across receive antennas (space) and/or frequency. Nevertheless, we treat this process as "white" as well because, of all the many possible assumptions, this is the simplest. As a result of both "whiteness" assumptions, the environment-caused gain variations and the additive interference can both be treated by simply lumping variances, i.e., $\sigma_1^2+\sigma_2^2$ in place of σ_1^2; and $\sigma_N^2+\sigma_I^2$ in place of σ_N^2. This permits us to quantify the impact of $\underline{\epsilon}_2(k)$ and $\underline{I}(k)$ without needlessly complicating our analysis, while leaving room in the formulation for more correlated versions of these processes.

V. Channel-based Authentication Test

Channel-based spoofing detection is based on a hypothesis test. The goal is to determine whether the second message at $k+1$ also belongs to Alice, using two channel vectors, $\underline{\hat{H}}(k)$ and $\underline{\hat{H}}(k+1)$. We build the following hypothesis

$$\mathcal{H}_0:\ \underline{H}(k+1)=\underline{H}_A(k+1), \tag{14}$$

$$\mathcal{H}_1:\ \underline{H}(k+1)=\underline{H}_E(k+1). \tag{15}$$

Under the null hypothesis, $\mathcal{H}_0$, the message at $k+1$ does belong to Alice, i.e., no spoofing attack. Otherwise, under the alternative hypothesis, $\mathcal{H}_1$, there *is* a spoofing attack, i.e., the message belongs to Eve.

A. Generalized Likelihood Ratio Test (GLRT)

A generalized likelihood ratio test for the hypothesis (14) and (15) in the generalized system model is given by

$$L_g=\frac{\left\|\underline{\hat{H}}(k+1)-a\underline{\hat{H}}(k)e^{j\phi}\right\|^2}{\varrho^2}-\frac{\left\|\underline{\hat{H}}(k+1)\right\|^2}{\sigma_E^2+\sigma_N^2+\sigma_I^2}\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\eta', \tag{16}$$

where $||A||$ denotes the Frobenius norm of the matrix A, ϱ^2 is given by (13), and $\phi=Arg(\underline{\hat{H}}(k+1)\underline{\hat{H}}(k)^H)$.

Proof: Since the phase rotation, ϕ, is usually unknown, the generalized likelihood ratio test [21] for the system model can be written as a function of $\underline{\hat{H}}(k+1)$, i.e.,

$$\Lambda_g=\frac{Pr\left(\underline{\hat{H}}(k+1);\mathcal{H}_1\right)}{\max_{\phi_0}Pr\left(\underline{\hat{H}}(k+1);\phi_0,a,\mathcal{H}_0,\underline{\hat{H}}(k)\right)}\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\eta_1. \tag{17}$$

By (6), (12), (14), and (15), we can rewrite (17) as

$$L_g=\frac{\left\|\underline{\hat{H}}(k+1)-a\underline{\hat{H}}(k)e^{j\phi}\right\|^2}{\varrho^2}-\frac{\left\|\underline{\hat{H}}(k+1)\right\|^2}{\sigma_E^2+\sigma_N^2+\sigma_I^2}\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\eta', \tag{18}$$

where

$$\begin{aligned}\phi&=\arg\min_{\phi_0}\left\|\underline{\hat{H}}(k+1)-a\underline{\hat{H}}(k)\exp(j\phi_0)\right\|\\&=Arg\left(\underline{\hat{H}}(k+1)\underline{\hat{H}}(k)^H\right).\end{aligned} \tag{19}$$

■

The phase term $e^{j\phi}$ is introduced to adjust for possible phase drift in the receiver oscillators from one measurement (at k) to another (at $k+1$). If this drift occurs and is not accounted for, Alice can be falsely rejected just because $\left\|\underline{\hat{H}}_A(k+1)-\underline{\hat{H}}_A(k)\right\|^2$ is not zero and might exceed the test threshold. The price paid for making this adjustment, and thus avoiding false rejection of Alice, is that the measurement vector of an intruder (Eve) will also be phase-aligned with the prior measurement, and so the "miss detection probability" (the probability of not detecting spoofing) will also increase. We examine this issue in our numerical results, Section VII.

It is clear that the GLRT requires *a priori* knowledge of the channel parameters such as σ_N, σ_I, σ_E, a, and σ_2. These parameters can in principle be obtained via training at a considerable cost in complexity.

B. A Simpler Test with Unknown Channel Parameters

In practice, wireless systems are not always able to obtain the channel parameters in (16). However, if both the channel time variation and estimation error are so small that $\varrho^2 \ll \sigma_E^2+\sigma_N^2+\sigma_I^2$, then the GLRT (16) can be simplified into a more practical test,

$$L=\left\|\underline{\hat{H}}(k+1)-a\underline{\hat{H}}(k)e^{j\phi}\right\|^2\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\eta, \tag{20}$$

where the test threshold η usually differs from η' in (16). Under the assumption of the Jakes model (i.e., that the arriving multipath at the receiver is uniformly distributed in azimuth), we can identify a as the term $J_0(2\pi vT/\lambda)$ in (10). Even if the terminal speed v is unknown, the receiver (Bob) can implement the simple test by making the approximation $a\sim 1$; this is equivalent to assuming vT/λ to be very small, as it would be in practical scenarios.

The new test L can be viewed as the difference between two channel estimates, utilizing the exponential term to counteract phase measurement rotation. In real system implementation, (20) can be further simplified into

$$L=\left\|\underline{\hat{H}}(k+1)-\frac{\underline{\hat{H}}^H(k)\underline{\hat{H}}(k+1)}{|\underline{\hat{H}}^H(k)\underline{\hat{H}}(k+1)|}\underline{\hat{H}}(k)\right\|^2, \tag{21}$$

indicating small computational overhead. This approach can be viewed as the integration of our previous work in [10], [11] and [13].

C. Test Performance

In order to evaluate the performance of spoofing detection, we define the *false alarm rate* (or Type I error), α, i.e., the probability that the test declares Alice as the intruder Eve by mistake; and the *miss detection rate* (or Type II error), β, i.e., the probability that the test misses the detection of Eve. These metrics are defined, respectively, by

$$\alpha = Pr(L > \eta|\mathcal{H}_0) \quad \text{(false alarm rate)} \tag{22}$$

$$\beta = Pr(L \leq \eta|\mathcal{H}_1) \quad \text{(miss detection rate)} \tag{23}$$

where the probabilities are taken over all channel vectors and measurement errors. We will assume, in our later presentation of results, that a "good" spoofing detector is one for which the false alarm and miss detection probabilities, α and β, are both below 10%. Schemes like those proposed here would almost certainly be paired with standard higher-layer protocols [17] and would have the benefit of reducing higher-layer overhead *plus* reducing miss detection probability [22].

Typically, the threshold η is chosen according to different criteria for performance. As an example, we just consider the Neyman-Pearson test, which minimizes the miss rate subject to a maximum tolerable constraint on the false alarm rate [21]. Before the test, Alice first sends a number of training messages, based on which Bob computes α for several η, via (22). Since α decreases monotonically with η, Bob can conveniently find the test threshold η that reaches the required α.

The performance of the scheme depends on several system parameters in addition to the correlation coefficient a, as given by the $J_0(\cdot)$ term in (10). One is the signal-to-(interference-plus-noise) ratio (SINR) of the channel estimates for Alice, defined by

$$\rho = \frac{\sigma_A^2}{\sigma_I^2 + \sigma_N^2}. \tag{24}$$

Note that ρ increases with transmit power, since the estimation noise and interference variances vary inversely with P_T. Another key parameter is the ratio of the locally averaged path gains for Alice and Eve,

$$\kappa = \sigma_E^2/\sigma_A^2. \tag{25}$$

In general, κ increases as Eve moves closer to Bob (assuming fixed positions for Alice and Bob). Finally, there is the relative change in the locally averaged path gain from Alice to Bob,

$$b = \sigma_2^2/\sigma_A^2. \tag{26}$$

Our numerical results will highlight the influences of these three critical parameters, ρ, κ and b; also, the degrees of freedom, M, and the normalized terminal speed, $\psi = vT/\lambda$.

VI. A Performance Bound For Test L

The analysis of the performance of the test L can be greatly simplified if we assume zero phase drift between measurements and no phase adjustment. In this case, we can replace L in (20) with

$$L' = \left\| \underline{\hat{H}}(k+1) - a\underline{\hat{H}}(k) \right\|^2. \tag{27}$$

Note that L in (20) is, by virtue of minimizing over the phase ϕ, larger than L' in (27). When the transmission at time $k+1$ is due to Alice and not phase-drifted, α will therefore be higher, for a given η, using L'; however, if the transmission is from an intruder (Eve), β will be lower. Overall, the curve of α vs. β will be lower (better) using L', assuming no phase drift and adjustment. We will refer to this case as providing a best-case performance bound and show results for it later.

When the null hypothesis $\mathcal{H}_0$ is true (both channel samples are from Alice), we can approximate $\underline{\hat{H}}_A(k+1) - a\underline{\hat{H}}(k)$ as a vector with M i.i.d. complex Gaussian elements. Each element has zero mean and a variance given by

$$\begin{aligned} &Var\left[\hat{H}_{A,m}(k+1) - a\hat{H}_{A,m}(k)\right] \\ &=(1+a^2)(\sigma_I^2+\sigma_N^2)+\sigma_2^2+(1-a^2)\sigma_A^2. \end{aligned} \tag{28}$$

Thus, L' under $\mathcal{H}_0$ is chi-square distributed with order $2M$ [23]. Given a test threshold η, the false alarm rate can be written as

$$\begin{aligned} \alpha &= 1 - P[L' \leq \eta|\mathcal{H}_0] \\ &= 1 - F_{\chi^2_{2M}}\left(\frac{2\eta}{(1+a^2)(\sigma_I^2+\sigma_N^2)+\sigma_2^2+(1-a^2)\sigma_A^2}\right) \\ &= 1 - F_{\chi^2_{2M}}\left(\frac{2\eta/\sigma_A^2}{(1+a^2)/\rho+1-a^2+b}\right), \end{aligned} \tag{29}$$

where $F_{\chi^2_{2M}}(\cdot)$ is the cumulative distribution function (CDF) of the chi-square distribution of order $2M$. It is clear that α rises as Alice moves faster, and is independent of κ and σ_E.

For a given α, the test threshold can be easily derived using (29):

$$\eta = 0.5\sigma_A^2\left(\frac{1+a^2}{\rho}+1-a^2+b\right)F^{-1}_{\chi^2_{2M}}(1-\alpha), \tag{30}$$

where $F^{-1}(\cdot)$ is the inverse function of $F(\cdot)$. This formula provides a way to set the threshold for the test L.

On the other hand, when $\mathcal{H}_1$ is true ($\underline{\hat{H}}(k)$ is from Eve), the channel vectors, $\underline{\hat{H}}(k+1)$ and $\underline{\hat{H}}(k)$, are independent. By (6) and (7), we have

$$\begin{aligned} &\hat{H}_m(k+1) - a\hat{H}_m(k) \\ &\sim CN\left(0, \left(\left(1+a^2\right)\left(\sigma_I^2+\sigma_N^2\right)+a^2\sigma_A^2+\sigma_E^2\right)\right). \end{aligned} \tag{31}$$

Hence the test statistic L' is also chi-square distributed with order $2M$, and we can simplify the miss rate as

$$\begin{aligned} \beta &= F_{\chi^2_{2M}}\left(\frac{2\eta}{(1+a^2)(\sigma_I^2+\sigma_N^2)+a^2\sigma_A^2+\sigma_E^2}\right) \\ &= F_{\chi^2_{2M}}\left(\frac{2\eta/\sigma_A^2}{(1+a^2)/\rho+a^2+\kappa}\right). \end{aligned} \tag{32}$$

As we see from (29) and (32), the test performance does not depend on the value of σ_A^2, as it is absorbed into the threshold, η. What matters are the estimation SINR, ρ; the Alice-Eve path gain ratio, κ; the relative change in Alice's path gain due to environmental changes, b; and the correlation coefficient, a, which is determined by Alice's speed, v, through the dimensionless parameter $\psi = vT/\lambda$.

VII. Simulation & Numerical Results

We performed Monte Carlo simulations to provide numerical results for the GLRT (L_g) and the more practical test (L), in a wide range of scenarios. We also provide some results for L'. In all cases, the results are given as curves of β vs. α. The value of the test threshold, η (or η'), determines the working point on the β-α curve. In our computations, we make the simplifying assumption (with no loss in generality) that $\sigma_A^2 = 1$.

A. Simulation Method

For each scenario, we first used (6) and (7) to generate two channel vectors, $\underline{\hat{H}}_E(k+1)$ and $\underline{\hat{H}}_A(k)$. Then we obtained $\underline{\hat{H}}_A(k+1)$ via (12) and $\underline{\hat{H}}_A(k)$. Based on these M-element vectors, we calculated the test statistics of L_g via (16) and L via (20), for both $\mathcal{H}_0$ and $\mathcal{H}_1$. We repeated the experiment $N_s = 20,000$ times.

Given test threshold, η, we computed the false alarm rate and miss rate by

$$\alpha = \frac{1}{N_s}\sum_{k=1}^{N_s} I\left(L\left(\underline{\hat{H}}_A(k), \underline{\hat{H}}_A(k+1)\right) > \eta\right), \tag{33}$$

$$\beta = \frac{1}{N_s}\sum_{k=1}^{N_s} I\left(L\left(\underline{\hat{H}}_A(k), \underline{\hat{H}}_E(k+1)\right) \leq \eta\right), \tag{34}$$

where the indicator function $I(A) = 1$ if the statement A is true, and zero otherwise. In this way, we obtained the β-α curve by simply varying η (or η').

B. Path Loss Model

Note that the mean-square values of $\underline{\hat{H}}_E(k+1)$ and $\underline{\hat{H}}_A(k)$, (6) and (7), are denoted by σ_E^2 and σ_A^2. We can model them as the ratio version of the generic dB formula for path loss, [24], i.e.,

$$\sigma_i^2 = \Omega d_i^{-\gamma} S_i, \quad i = A, E, \tag{35}$$

where the path loss exponent γ ranges between 2 and 5 in most wireless environments; Ω denotes a reference path gain value, (e.g., the path gain at $d = 1$ m); and the shadowing S_i is usually modeled as a log-normal random variable.

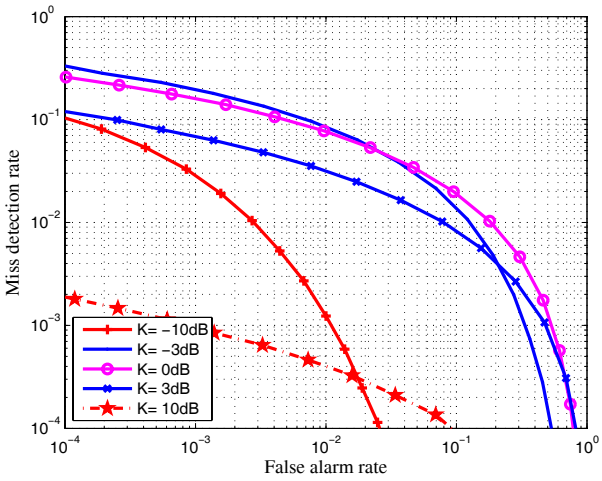
Thus, we can write κ in terms of its dB value,

$$K = 10\gamma \log(d_A/d_E) + (s_E - s_A), \text{ (in dB)}, \tag{36}$$

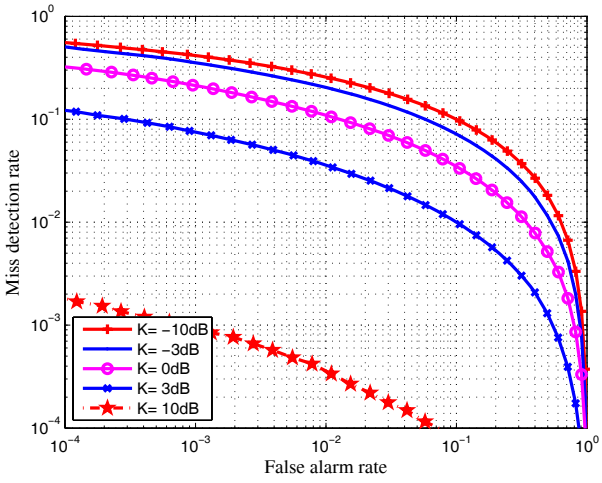
where s_A (or s_E) is the dB value of S_A (or S_E).

For any environment, such as an irregular-shape office building, the probability density function (PDF) of the log-distance ratio can be easily obtained via simulation, where Alice and Eve are assumed to be located with uniform (and independent) randomness anywhere in the coverage area. This PDF can be convolved with the Gaussian PDF of $(s_E - s_A)$ to obtain the PDF of K. At the end of the next sub-section, we will give a specific example wherein (1) shadow fading is assumed to be absent, $s_E - s_A = 0$; and (2) Alice and Eve are distributed at random in a circular area centered on Bob. As proven in the Appendix, the PDF of K in this special case is a double-sided exponential given by

$$f_K(x) = \frac{\ln(10)}{10\gamma} 10^{-|x|/5\gamma}. \tag{37}$$



(a) L_g



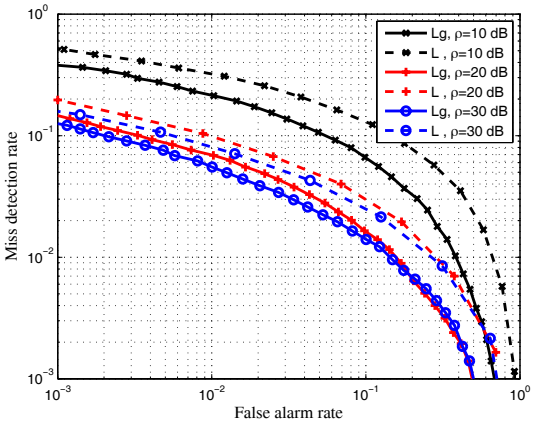
(b) L

Fig. 2. Miss detection rate (β) vs. false alarm rate (α) for two channel-based spoofing detectors: The GLRT, L_g, and a simplified version, L, as a function of $\kappa(= \sigma_E^2/\sigma_A^2)$. In this example, $M = 4$ independent channel samples in each message; the SINR of the channel estimation is $\rho = 20$ dB; the terminal is fixed ($v = 0$), and the channel's relative time variation power is $b = 0.2$.

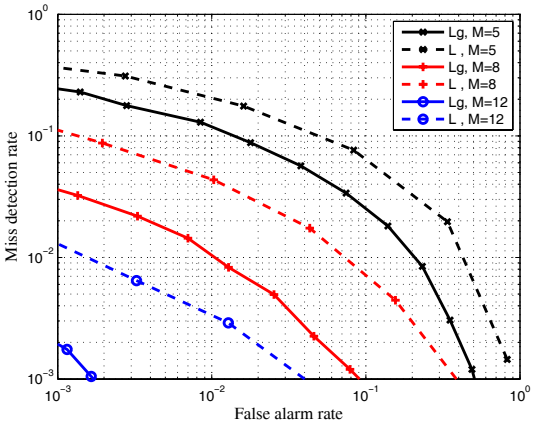
C. Numerical Results

We first present, in Fig. 2, curves of β vs. α for the test statistics L_g and L. The worst case for L_g is when the dB value of κ is 0 dB; in this case, Bob does not have the benefit of different power levels between Alice and Eve, which would aid in detecting spoofing. We see for that case, with $M = 4$ independent channel samples, a channel estimation SINR of 20 dB, and a relative time variation power $b = 0.2$, that a test using L_g can still achieve a good result, e.g., $\alpha = \beta = 4\%$. Also, as κ in dB grows very large (either positive or negative), the test moves in the direction of near-perfect performance (i.e., towards $\alpha = \beta = 0$).

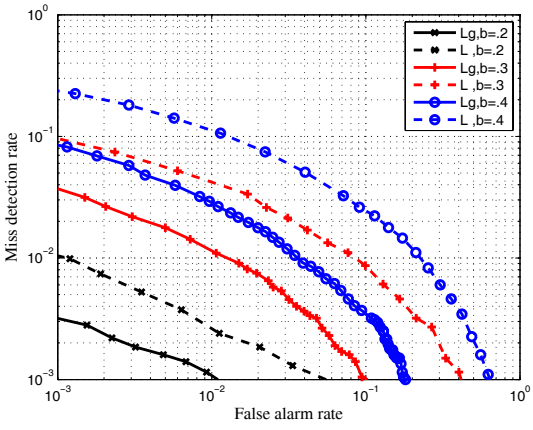
For the simpler test statistic L, negative dB values of κ yield worse results than positive ones, indicating that a "smart" intruder Eve would seek a position where $10\log_{10}(\kappa) < 0$ dB. The worst-case dB value for κ under this test is seen to be about -10 dB. At this value, the test can still achieve the reasonably good performance result $\alpha \approx \beta \approx 10\%$.



(a) $M = 4$ and $b = 0.2$



(b) $\rho = 10$ dB and $b = 0.2$



(c) $M = 8$ and $\rho = 20$ dB

Fig. 3. Miss detection rate (β) vs. false alarm rate (α) for channel-based spoofing detectors, including the GLRT, L_g, a simplified version, L. Results are shown as a function of the number of independent channel samples in each message, M; the SINR of the channel estimation for Alice, ρ; and the channel's relative time variation power, b. All results are for zero terminal speed ($v = 0$).

Figure 3 shows results for L_g and L to highlight the influences of SINR (ρ), degrees of freedom (M), and relative time variation power (b), all for the case when Alice is fixed ($v = 0$) and Alice and Eve deliver to Bob the same average power $10\log_{10}(\kappa) = 0$ dB. These curves quantify the superiority of the test L_g. They also show how the performances of both tests improve with higher ρ, lower M, and higher b; and how the benefit of using L_g diminishes for lower ρ, lower M and higher b.

Figure 3 (a) assumes a substantial channel time variation, $b = 0.2$, and $M = 4$ independent channel samples. The latter may be interpreted as using $M' = 4$ independent tones in a single-antenna (SISO) system; $M' = 2$ tones in a 2×1 MISO system; $M' = 2$ tones in a 1×2 SIMO system; or 1 tone in a 2×2 MIMO system. For $\alpha = 5\%$, we obtain $\beta \approx 2\%$ for L_g and $\beta \approx 4\%$ for L. Moreover, the performance gain is not significant as ρ increases from 20 dB.

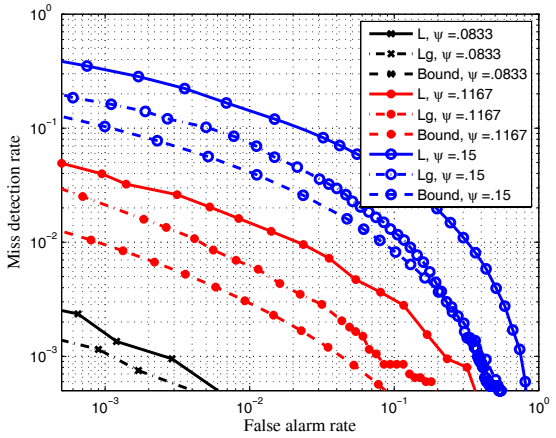
In Fig. 3 (b), we consider the case of a moderate SINR, $\rho = 10$ dB, with $b = 0.2$. The use of a larger M is a more efficient way to improve performance than to increase ρ, especially if ρ is already not very low. If M is large enough (e.g., $M \geq 12$), both tests perform extremely well, e.g., achieving $\alpha = 1\%$ and $\beta < 0.3\%$.

Figure 3 (c) shows how the performance degrades as the channel time variation rises. It is seen that L_g is more robust against channel time variation than L, and that these two tests achieve $\alpha = \beta \approx 2.5\%$, and $\alpha = \beta \approx 7.5\%$, respectively, when $b = 0.5$, $M = 8$, and $\rho = 20$ dB.

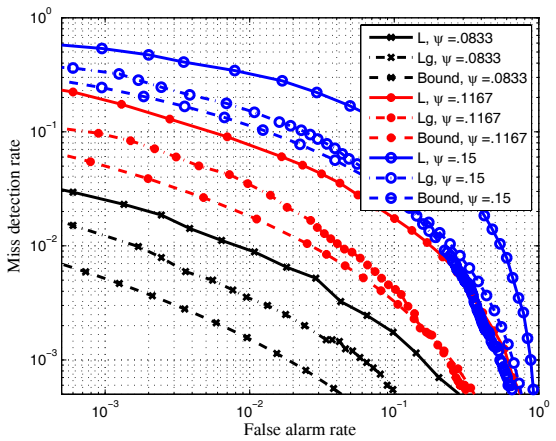
Figure 4 compares α vs. β for the three test statistics L_g, L and L', the latter being for the ideal case where no phase adjustment is needed or made. Results for each tests are shown for three values of $\psi = vT/\lambda$. Assuming an RF frequency of 5 GHz ($\lambda = 6$ cm) and a frame rate of 300 per second ($T = 3.33$ ms), the top, middle and lower sets of curves correspond, respectively, to $v = 2.7$, 2.1 and 1.5 meters per second; or, in terms of human walking speeds, fast, brisk and moderate. Note that the simple test with no phase adjustment needed or made outperforms the ideal test *with* phase adjustment. Also, for even the most extreme terminal speeds, performance results on the order of $\alpha = \beta = 10\%$ can be achieved or exceeded. Finally, a comparison between Figs. 4a and 4b shows the impact of the environment-caused gain variations, though it is not as strong here as for the case of no mobility ($v = 0$); its relative impact is diminished by the presence of the variance component $\sigma_1^2 = (1 - a^2)\sigma_A^2$ in (28).

Finally, let us consider the reality that κ is a random quantity over all possible joint locations of Alice and Eve. To get an idea of the "average" performance over the range of κ, we invoke the conditions cited earlier, i.e., there is no shadowing, $s_E - s_A = 0$; and the coverage area is a circular region centered on Bob. Assume further that ρ can be maintained fixed at 20 dB, say, by using power control; and that Eve, receiving the same power control commands as Alice, continues to transmit the same power level as Alice. In this case and the test statistic L', (27), we can get a near-analytical solution for the average β as a function of α, using (37) for the PDF of κ and combining it with (32) for β.

The results, Fig. 5, cover a wide practical range of the path loss exponent, γ. The robustness of spoofing detection with respect to pathloss exponent is clear. For example, the average false alarm rate (α) and miss detection rate (β) are around 2% and 1%, respectively, when $M = 8$, $\rho = 20$ dB, and $b = 0.2$, for $\gamma \in [2, 5]$.



(a) $b = 0$



(b) $b = 0.1$

Fig. 4. Miss detection rate (β) vs. false alarm rate (α) with terminal mobility. For each of three values of $\psi = vT/\lambda$, results are shown for each of three spoofing tests: L_g, L and L' (best-case bound). For this example, $M = 8$, $\rho = 20$ dB and $\kappa = 1$.

VIII. Conclusion

We have proposed a generalized channel-based spoofing detection for wireless networks, utilizing a channel estimation mechanism to detect spoofing messages with low overhead. For this framework, we presented an optimized generalized likelihood ratio test, L_g, and a practical test, L, which does not require knowledge of the channel parameters. The efficacy of the scheme was verified via numerical analysis using a generic frequency-selective Rayleigh channel model.

Considering relevant issues such as terminal mobility, interference, channel time variation, channel estimation errors, etc, we found that the simple test L is almost as good as the more optimal L_g in many cases. We found that, for either test over a wide range of practical conditions (system and channel parameters), the false alarm rate α and miss detection rate β can both be held to levels of 10% or lower.

Appendix A
Proof of Equation (37)

Assume that Alice and Eve are randomly uniformly distributed in a circular area centered on Bob with radius R.

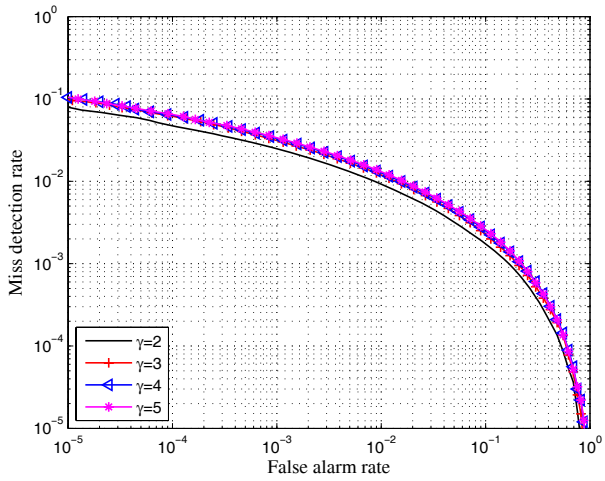


Fig. 5. Analytical result for β vs. α using the test L' (best case bound). Results shown are averaged over all realizations of κ, when Alice and Eve are randomly placed in the circle area centered on Bob. In this example, $M = 8$, $\rho = 20$ dB, $v = 0$ and $b = 0.2$. Performance is seen to be insensitive to path loss exponent γ.

Denote $D_1 = d_A^2$ and $D_2 = d_E^2$, and assume that both D_1 and D_2 are independent and uniformly distributed between 0 and R^2, i.e., $D_i \sim U(0, R^2)$, $i = 1, 2$. For $s_E - s_A = 0$ and using (36), we easily get $K = 5\gamma \log(D_2/D_1)$.

Since Alice and Eve can exchange their locations, it is clear that the PDF of K, $f_K(x)$, is symmetric about $x = 0$. For $x < 0$, the CDF can be written as

$$\begin{aligned} F_K(x) &= Pr(K \le x) = Pr(5\gamma \log(D_2/D_1) \le x) \\ &= \int_{-\infty}^{\infty} Pr\left(D_1 = x_1\right) Pr(5\gamma \log\left(D_2/x_1\right) \le x)\, dx_1 \\ &= \int_0^{R^2} \frac{1}{R^2} Pr\left(D_2 \le x_1 10^{x/5\gamma}\right) dx_1 \\ &= \int_0^{R^2} \frac{1}{R^2} \frac{x_1 10^{x/5\gamma}}{R^2} dx_1 = 0.5 \cdot 10^{x/5\gamma} \end{aligned} \tag{38}$$

Given the symmetry about $x = 0$, we have the result that the PDF of K is

$$f_K(x) = \frac{dF_K(x)}{dx} = \frac{\ln(10)}{10\gamma} 10^{-|x|/5\gamma} \tag{39}$$

References

[1] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in *Proc. MobiCom '01: Proc. 7th Annual International Conf. Mobile Computing Networking*, 2001, pp. 180-189.

[2] A. Mishra, M. Shin, and W. A. Arbaugh, "Your 802.11 network has no clothes," *IEEE Commun. Mag.*, pp. 44-51, 2002.

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

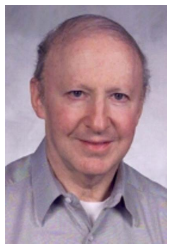
[4] Y. Chen, W. Trappe, and R. Martin, "Detecting and localizing wireless spoofing attacks," in *Proc. Sensor, Mesh Ad Hoc Commun. Networks*, 2007, pp. 193-202.

[5] 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.

[6] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in *Proc. USENIX Security Symp.*, 2003, pp. 15-28.

[7] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proc. ACM Workshop Wireless Security*, 2006, pp. 43-52.
[8] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proc. IEEE International Symp. World Wireless, Mobile Multimedia Networks (WoWMoM)*, June 2006.
[9] N. Patwari and S. Kasera, "Robust location distinction using temporal link signatures," in *Proc. ACM International Conf. Mobile Computing Networking*, 2007, pp. 111-122.
[10] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: using the physical layer for wireless authentication," in *Proc. IEEE International Conf. Commun. (ICC)*, June 2007, pp. 4646-4651.
[11] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2571-2579, July 2008.
[12] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," in *Proc. IEEE Conf. Inform. Sciences Syst. (CISS)*, Mar. 2008, pp. 642-646.
[13] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. IEEE International Conf. Commun. (ICC)*, May 2008, pp. 1520-1524.
[14] P. Yu, J. Baras, and B. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 1, pp. 38-51, Mar. 2008.
[15] W.C. Jakes Jr., *Microwave Mobile Communications*. Wiley, 1974.
[16] 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 Engineering*, Mar. 1995.
[17] IEEE Std 802.11i 2004, "IEEE 802.11i-2004: Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. Amendment 6: Medium access control (MAC) security enhancements," June 2004.
[18] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *IEEE Wireless Personal Commun.*, vol. 6, pp. 311-335, Mar. 1998.
[19] A. O. Kaya, L. Greenstein, and W. Trappe, "Characterizing indoor wireless channels via ray tracing combined with stocahstic modeling," *IEEE Trans. Wireless Commun.*, to appear.
[20] A. O. Kaya, L. Greenstein, and W. Trappe, "Modeling temporal channel variations in wireless environments," in *Proc. IEEE MILCOM*, 2008.
[21] S. M. Kay, *Fundamentals of Statistical Signal Processing*. Englewood Cliffs, NJ: Prentice Hall, 1993.
[22] L. Xiao, "PHY-techniques to improve higher-layer functions in wireless networks," Ph.D. thesis, Rutgers Univ., New Brunswick, May 2009.
[23] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions, with Formulas, Graphs, and Mathematical Tables*. New York: Dover, 1965.
[24] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005: ch. 2.8, eq. (2.51).

Liang Xiao received the B.S. in communication engineering in 2000 from Nanjing University of Posts & Telecommunications, China, the M.S. in electrical engineering in 2003 from Tsinghua University, China, and the PhD degree in electrical engineering from Rutgers University, NJ, in 2009. She is currently an associate professor in the Department of Communication Engineering, Xiamen University, Fujian, China. From 2003 and 2004, she was with North Carolina State University, NC. Her research interests include network security, localization, cognitive radio, radio resource managements, and wireless communications.



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, where he conducted research 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 on 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 Associate at Rutgers-WINLAB, North Brunswick, NJ, working in the areas of cognitive radio, 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 four best paper awards. He is currently Director of Journals for the IEEE Communications Society 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, all in electrical engineering. From 1994 to 1996, he was a Research Associate at the Wireless Information Network Laboratory (WINLAB), Rutgers University before joining the faculty of the Electrical and Computer Engineering 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 2002 and a visiting faculty at the Indian Institute of Science in 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 networks.

Dr. Mandayam is a recipient of the Fred W. Ellersick Prize from the IEEE Communications Society in 2009 along with O. Ileri for their work on dynamic spectrum access models and spectrum policy. He is also a recipient of the Institute Silver Medal from the Indian Institute of Technology in 1989 and the National Science Foundation CAREER Award in 1998. He is a coauthor with C. Comaniciu and H. V. Poor of the book *Wireless Networks: Multiuser Detection in Cross-Layer Design* (Springer, New York). He has served as an Editor for the journals IEEE COMMUNICATION LETTERS and IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He has also served as a guest editor of the IEEE JSAC Special Issues on Adaptive, Spectrum Agile and Cognitive Radio Networks (2007) and Game Theory in Communication Systems (2008). He is a Fellow of the IEEE.

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.