Channel-Based Detection of Sybil Attacks in Wireless Networks

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

***Abstract*—Due to the broadcast nature of the wireless medium, wireless networks are especially vulnerable to Sybil attacks, where a malicious node illegitimately claims a large number of identities and thus depletes system resources. We propose an enhanced physical-layer authentication scheme to detect Sybil attacks, exploiting the spatial variability of radio channels in environments with rich scattering, as is typical in indoor and urban environments. We build a hypothesis test to detect Sybil clients for both wideband and narrowband wireless systems, such as WiFi and WiMax systems. Based on the existing channel estimation mechanisms, our method can be easily implemented with low overhead, either independently or combined with other physical-layer security methods, e.g., *spoofing* attack detection. The performance of our Sybil detector is verified, via both a propagation modeling software and field measurements using a vector network analyzer, for typical indoor environments. Our evaluation examines numerous combinations of system parameters, including bandwidth, signal power, number of channel estimates, number of total clients, number of Sybil clients, and number of access points. For instance, both the false alarm rate and the miss rate of Sybil attacks are usually below 0.01, with three tones, pilot power of 10 mW, and a system bandwidth of 20 MHz.**

***Index Terms*—Authentication, radio propagation, Sybil attacks, wireless networks.**

I. Introduction

WIRELESS networks mostly lack the ability to reliably identify clients, and fail to sufficiently protect management frames and control messages. For example, IEEE 802.11 (WiFi) systems do not provide reliable "mutual" authentication between access points (APs) and clients, even when equipped with security standards such as 802.11i [1]. One serious consequence is that such networks are vulnerable to various identity-based attacks, such as Sybil attacks [2].

Sybil attacks were first introduced in the context of peer-to-peer networks [3] as a form of resource depletion attack, and then analyzed in the context of wireless networks [2], [4]. In Sybil attacks, a malicious node claims a large number of client identities, either by impersonating other legal nodes or claiming false identities. For instance, a Sybil node may send a high rate of association request messages to an AP, using random medium access control (MAC) values to emulate a large number of clients. The result is that legal clients are denied access once the Sybil node has consumed an AP's association slots or channel slots. As a special kind of denial-of-service attack, Sybil attacks seriously endanger the availability of network services for wireless systems [4].

In order to address these problems, we propose a cross-layer approach to detect Sybil attacks in wireless networks, exploiting the spatial variability of the wireless channel. As illustrated in [5], the channel response decorrelates rapidly in space, in typical wireless scenarios with rich scatterers. Hence, two clients with similar channel responses are very likely to be in the same location (and thus from the same Sybil node). Based on this observation, we propose an authentication scheme, which utilizes the channel measurement mechanisms naturally existing in most wireless systems. Our scheme can be easily implemented in a wide range of wireless systems, such as IEEE 802.11, 802.15 (wireless PAN), and 802.16 (WiMax), and can be naturally integrated with a physical-layer spoofing detector with minimal extra overhead. In spoofing attacks, a malicious device claims to be a *specific* client or AP other than itself [1], [6]–[8].

Assuming stationary terminals and time-invariant channels, we suppose a Sybil node may use different policies in building the challenge frames. We analyze the detection performance of Sybil attacks, including the miss rate and false alarm rate for a given test threshold, as well as the corresponding receiver operating characteristic (ROC), for various combinations of system bandwidth, frequency sample size, pilot power, number of channel estimates, number of total clients, number of Sybil clients, and number of APs.

We begin by presenting our Sybil attack model in Section II. In Section III, we describe the channel-based Sybil detection strategy with one witnessing AP, and then discuss the case of multiple monitoring APs in Section IV. We discuss implementation in Section V. We then present simulation results and experimental results in Sections VI and VII, respectively. A brief overview of some related work is given in Section VIII. Finally, we provide a short conclusion, in Section IX.

II. Sybil Attack Model

We present a generalized Sybil attack model in Fig. 1, where the serving AP (AP 1) receives service requests from N clients, during a specified period of time. A Sybil node attempts to claim $N_s \leq N$ identities, in hopes of consuming the AP's resources.

Manuscript received April 24, 2008; revised May 18, 2009. First published July 07, 2009; current version published August 14, 2009. This work was supported, in part, through a grant CNS-0626439 from the National Science Foundation. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. M. Kivanc Mihcak.

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

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

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2009.2026454

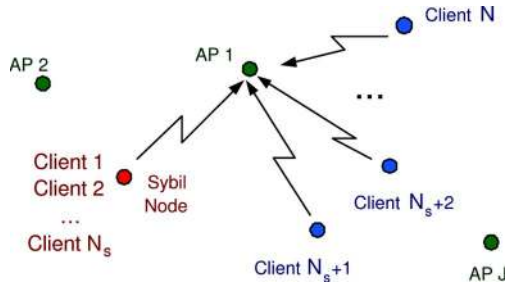

Fig. 1. Sybil attack model with AP 1 receiving messages from N clients, where the first N_s clients are actually in the same terminal (i.e., Sybil node), while the remaining $N-N_s$ clients are legal users in distinct terminals. Sometimes, more than one (i.e., $J>1$) AP cooperates to track channels from these clients.

The remaining $N-N_s$ clients are legal users at distinct terminals.

For convenience of notation, we will refer to the first N_s clients as being from the Sybil node. If the AP does not catch enough Sybil clients, it is likely that some of the legal clients will fail to access network services, especially when N_s is large. The special cases with $N_s=1$ and $N_s=N$, respectively, indicate no Sybil and no legal client.

Some wireless networks deploy more than one AP (i.e., $J>1$) in the area to improve the quality of service and to increase the number of clients allowed. Without loss of generality, we assume each AP can receive some of the service requests and is able to track the channel from some of the clients.

III. Single-AP Sybil Detection

A. Channel Measurements

We propose a channel-based Sybil detection technique that relies on existing channel estimation mechanisms in wireless systems. We first consider a single AP that utilizes pilots or preamble sequences to estimate channel frequency responses. Denote the true channel response at frequency f as $H_n(f)$, $1\le n\le N$, where N is the number of active clients. The AP obtains and stores the noisy version $\hat{H}_n(f)$, which is noisy due to three types of channel estimation errors: 1) the receiver thermal noise, which is modeled as white Gaussian noise; 2) the phase measurement rotation, due to the phase drifting of the receiver local oscillator between one measurement and another; 3) the scaling error of the amplitude measurement, which results from the deliberate change of the transmission power by an attacking Sybil node.

By sampling $\hat{H}_n(f)$ at M tones, $f\in(f_0-W/2, f_0+W/2]$, the AP obtains an M-dimension channel (row) vector $\hat{\mathbf{H}}_n$

$$\hat{\mathbf{H}}_n=\mathbf{H}_n a_n e^{j\phi_n}+\mathbf{N}_n,\qquad 1\le n\le N \tag{1}$$

where the elements of arbitrary vector $\mathbf{A}=[A_1,\ldots,A_M]$ are samples from $A(f)$. More specifically, $A_m=A(f_0+W(m/M-0.5))$; M is the frequency sample size; f_0 is the center frequency of the measurement; and W is the system bandwidth. All elements of $\mathbf{N}_n$ are independent identically distributed (i.i.d.) complex Gaussian noise samples $CN(0,\sigma^2)$; $\phi_n\in[0,2\pi)$ represents the phase measurement rotation; and a_n denotes the scaling error in the amplitude measurement, if $a_n\neq 1$.

B. Baseline Case: Two Clients

To gain insight, we first study the Sybil detection problem with $N=2$ clients. Since channel responses decorrelate rapidly in space, two clients with similar channel vectors are very likely to be at the same location (and thus from the Sybil node).

We can build a simple hypothesis test: In the null hypothesis $\mathcal{H}_0$ there is no Sybil node, i.e., two clients come from distinct terminals; while the alternative hypothesis $\mathcal{H}_1$ represents the presence of Sybil attacks, i.e., these two clients are actually the same terminal. So, we have

$$\mathcal{H}_0:\quad \mathbf{H}_1\neq\mathbf{H}_2 \tag{2}$$
$$\mathcal{H}_1:\quad \mathbf{H}_1=\mathbf{H}_2. \tag{3}$$

The test statistic is chosen according to an *a priori* assumption regarding the power control strategy of the Sybil nodes. There are two natural strategies.

1) Sybil Nodes With Constant Power: When Sybil nodes use the correct pattern for pilot transmission and keep their power levels fixed for different identities, the scaling error of the channel amplitude measurement can be ignored, i.e., $a_n=1$. Hence, we claim Sybil clients, if their channel responses are similar. The pair-wise test statistic is chosen as

$$L(\hat{\mathbf{H}}_1,\hat{\mathbf{H}}_2)=\frac{1}{\sigma^2}\|\hat{\mathbf{H}}_1-\hat{\mathbf{H}}_2e^{j\phi}\|^2 \tag{4}$$

where

$$\phi=\arg\min_x\|\hat{\mathbf{H}}_1-\hat{\mathbf{H}}_2e^{jx}\|=\mathrm{Arg}\left(\hat{\mathbf{H}}_1\hat{\mathbf{H}}_2^H\right). \tag{5}$$

This test statistic is approximately a generalized likelihood ratio test (GLRT), as shown in Appendix I. The minimization over the phase x is introduced to overcome phase measurement rotation. This step is necessary as otherwise we may fail to catch the Sybil node, since its channel vectors change with phase rotation.

2) Sybil Nodes With Adaptive Power: In order to increase the chance of fooling an AP and avoid detection, a clever Sybil node may change the power of its pilots as it attempts to claim different identities. As a result, the Sybil node will cause the scaling error a_n to vary across the different claimed identities, thus resulting in different channel vectors for different claimed identities. In this case, the AP should compare the relative shape of channel response sequences, i.e., it checks whether the scaled channel vectors of the clients can be matched up. Thus, as shown in Appendix II, an approximate likelihood ratio test statistic becomes

$$L(\hat{\mathbf{H}}_1,\hat{\mathbf{H}}_2)=\frac{2\|\hat{\mathbf{H}}_1-w\hat{\mathbf{H}}_2\|^2}{(1+|w|^2)\sigma^2} \tag{6}$$

where

$$w=\arg\min_x\|\hat{\mathbf{H}}_1-x\hat{\mathbf{H}}_2\|=\frac{\hat{\mathbf{H}}_1\hat{\mathbf{H}}_2^H}{\|\hat{\mathbf{H}}_2\|^2}. \tag{7}$$

Note that w is a complex number: its phase counteracts the phase measurement rotation (otherwise, we may fail to catch

the Sybil nodes); while its magnitude counteracts the change of the scaling error (this helps detect Sybil nodes that vary their power).

In both cases, we define the rejection region of the null hypothesis $\mathcal{H}_0$ as those cases where L falls below some threshold k. Given an environment and the locations of the terminals, we can study the performance of the detector, averaged over the channel measurement errors. More specifically, for a given test threshold (k) and true channel vectors ($\mathbf{H}_1$ and $\mathbf{H}_2$), the false alarm rate (or Type I error) and the miss rate (or Type II error) in the Sybil detection are defined, respectively, by

$$\alpha(k) = Pr(L \le k|\mathcal{H}_0) \tag{8}$$

$$\beta(k) = Pr(L > k|\mathcal{H}_1). \tag{9}$$

The probabilities are taken over all realizations of channel measurement error.

Theorem 1: In a Sybil detection scenario with two clients, given the miss rate β, the false alarm rate is

$$\alpha(\beta) = F_{\chi^2_{2M,\mu}}\left(F^{-1}_{\chi^2_{2M,0}}(1-\beta)\right) \tag{10}$$

where $F_X(\cdot)$ is the cumulative distribution function (CDF) of the random variable X, $F_X^{-1}(\cdot)$ is the inverse function of $F_X(\cdot)$, $\chi^2_{2M,0}$ denotes the Chi-square random variable with $2M$ degrees of freedom, $\chi^2_{2M,\mu}$ is the noncentral Chi-square random variable with a noncentrality parameter μ and $2M$ degrees of freedom [9], and

$$\mu = \frac{||\mathbf{H}_1 - \mathbf{H}_2 e^{j\mathrm{Arg}(\mathbf{H}_1\mathbf{H}_2^H)}||^2}{\sigma^2} \tag{11}$$

when the Sybil node is known to employ constant power, or

$$\mu = \frac{2||\mathbf{H}_1 - w\mathbf{H}_2||^2}{(1+|w|^2)\sigma^2} \tag{12}$$

when the Sybil node is known to possibly adapt its power, with $w = \mathbf{H}_1\mathbf{H}_2^H/||\mathbf{H}_2||^2$.

Proof: See Appendix III. ∎

C. Generalized Case: Multiple Clients

For a generalized case with N active clients, we represent the decision result of the Sybil detection with a decision indicator $I(\cdot)$, which is given by

$$I(m) = \begin{cases} 1, & \text{Client } m \text{ is a Sybil} \\ 0, & \text{Client } m \text{ is legal.} \end{cases} \tag{13}$$

If the AP claims the mth client to be Sybil, we have $I(m) = 1$; otherwise, $I(m) = 0$.

The authentication decision for one client may depend on the channel vectors of all N clients. The goal is to detect as many Sybil clients as possible, while reducing the false alarm rate, i.e., the probability of claiming a legal client as a Sybil client. In our problem model, where the first N_s clients come from the same Sybil terminal, i.e., $\mathbf{H}_1 = \mathbf{H}_n$, $n \le N_s$, an ideal error-free decision is

$$I(m) = \begin{cases} 1, & 1 \le m \le N_s \\ 0, & N_s < m \le N. \end{cases} \tag{14}$$

Given a (N, N_s) system with specified channel realizations, the false alarm rate α and the miss rate β, are given, respectively, by

$$\alpha(N, N_s) = \begin{cases} \frac{1}{N-N_s}\sum_{m=N_s+1}^{N} E[I(m)], & N > N_s \\ 0, & N = N_s \end{cases} \tag{15}$$

$$\beta(N, N_s) = \begin{cases} 0, & N_s = 1 \\ 1 - \frac{1}{N_s}\sum_{m=1}^{N_s} E[I(m)], & N_s > 1 \end{cases} \tag{16}$$

where $E[\cdot]$ is the average over all realizations of channel measurement error.

We note that the detection with multiple clients is no longer a simple hypothesis test, and thus the performance criteria are slightly different from those in Section III-B. More specifically, α in (8) and β in (9), correspond to $\alpha(2,0)$ in (15) and $\beta(2,2)$ in (16), respectively.

A heuristic solution would be to claim that two clients are Sybil, if their channel responses are similar. Thus the detection rule can be written as

$$I(m) = \begin{cases} 1, & \exists L(m,n) \le k, 1 \le n \le N, n \ne m \\ 0, & \text{otherwise.} \end{cases} \tag{17}$$

The test statistic L is chosen according to the *a priori* knowledge of the power strategy of the Sybil nodes

$$L(m,n) = \begin{cases} \frac{||\hat{\mathbf{H}}_m - \hat{\mathbf{H}}_n e^{j\phi}||^2}{\sigma^2}, & \text{constant power} \\ \frac{2||\hat{\mathbf{H}}_m - w\hat{\mathbf{H}}_n||^2}{(1+|w|^2)\sigma^2}, & \text{adaptive power} \end{cases} \tag{18}$$

where $\phi = \mathrm{Arg}(\hat{\mathbf{H}}_m\hat{\mathbf{H}}_n^H)$, and $w = \hat{\mathbf{H}}_m\hat{\mathbf{H}}_n^H/||\hat{\mathbf{H}}_n||^2$. It is actually based on (4) and (6).

For convenience of discussion, in the remainder of the paper, we suppose the APs do not know the power strategy that the Sybil nodes employ.

Theorem 2: Assume an AP receives requests from N clients, where N_s of them actually come from the same Sybil node. Given the test threshold k, the proposed Sybil detector has the false alarm rate and miss rate given by, respectively,

$$\alpha(N, N_s) = 1 - \frac{1}{N-N_s}\sum_{m=N_s+1}^{N}\left(1 - F_{\chi^2_{2M,\mu(m,1)}}(k)\right)^{N_s} \times \prod_{N_s+1\le n\le N, n\ne m}\left(1 - F_{\chi^2_{2M,\mu(m,n)}}(k)\right) \tag{19}$$

$$\beta(N, N_s) = (1 - F_{\chi^2_{2M}}(k))^{N_s-1} \cdot \prod_{N_s+1\le n\le N}\left(1 - F_{\chi^2_{2M,\mu(1,n)}}(k)\right) \tag{20}$$

where $\mu(m,n) = 2||\mathbf{H}_m - w\mathbf{H}_n||^2/(1+|w|^2)\sigma^2$.

Proof: See Appendix IV. ∎

As a special case, if there is no Sybil client, the false alarm rate is given by

$$\alpha(N,1) = 1 - \frac{\sum_{m=2}^{N}\prod_{n\ne m}\left(1 - F_{\chi^2_{2M,\mu(m,n)}}(k)\right)}{N-1}. \tag{21}$$

As another special case, if all clients are Sybil, the miss rate can be written as

$$\beta(N,N) = \left(1 - F_{\chi^2_{2M}}(k)\right)^{N-1}. \tag{22}$$

These cases illustrate in a simple way how the miss rate decreases with N, while the false alarm rate rises with it.

IV. Multiple-AP Sybil Detection

It is common practice that wireless networks are deployed with multiple APs (i.e., $J > 1$). If additional APs are available, they may cooperate to improve detection performance. For simplicity, we assume that no AP is outside the coverage area of the clients, i.e., we assume all channel response vectors are nonzero, and denote the estimated channel response between the nth client and the jth AP as $\hat{\mathbf{H}}_n(j)$, where $1 \le n \le N$ and $1 \le j \le J$.

Suppose the APs cooperate in the Sybil detection process, using (17) to make a decision. The APs can either be asynchronous or synchronous in configuration: If the APs are connected together and served by the same receiver oscillator, they may be synchronized to have the same (but unknown) phase measurement drifting. Otherwise, if using different oscillators, their phase rotations are assumed to be independent. With the size of the estimated channel samples rising from M to JM, we now build the tests according to each system configuration.

A. Synchronous APs

The channel frequency responses from synchronous APs have the same phase drifting and magnitude scaling factor. Hence, we can ignore which AP the channel vector comes from, and combine them into an extended channel (row) vector, $\underline{\hat{\mathbf{H}}}_n = [\hat{\mathbf{H}}_n(1), \ldots, \hat{\mathbf{H}}_n(J)]$. It is clear that it is the same as the case with a single AP, only with the dimension of the channel vectors changing from M to MJ. Thus, we choose a test statistic that is similar to (6)

$$L(m,n,J) = 2\frac{||\underline{\hat{\mathbf{H}}}_m - w\underline{\hat{\mathbf{H}}}_n||^2}{(1+|w|^2)\sigma^2} \tag{23}$$

$$w = \frac{\underline{\hat{\mathbf{H}}}_m \underline{\hat{\mathbf{H}}}_n^H}{||\underline{\hat{\mathbf{H}}}_n||^2}. \tag{24}$$

B. Asynchronous APs

Since the channel vectors have independent and unknown phase shifts among asynchronous APs, we choose the pair-wise test statistic as the sum of the metrics (6) from the J APs, i.e.,

$$L(m,n,J) = 2\sum_{j=1}^{J} \frac{||\hat{\mathbf{H}}_m(j) - w(j)\hat{\mathbf{H}}_n(j)||^2}{(1+|w(j)|^2)\sigma^2} \tag{25}$$

$$w(j) = \frac{\hat{\mathbf{H}}_m(j)\hat{\mathbf{H}}_n^H(j)}{||\hat{\mathbf{H}}_n(j)||^2}. \tag{26}$$

Theorem 3: Assume J APs work together to detect a Sybil node that claims N_s clients, with the existence of $N - N_s$ legal clients. Given test threshold k, the false alarm rate $\alpha(N, N_s, J)$ and the miss rate $\beta(N, N_s, J)$ are given by (27) and (28), respectively, shown at the bottom of the page, where

$$\mu(m,n) = \frac{2||\underline{\mathbf{H}}_m - w\underline{\mathbf{H}}_n||^2}{(1+|w|^2)\sigma^2} \tag{29}$$

$\underline{\mathbf{H}}_n = [\mathbf{H}_n(1), \ldots, \mathbf{H}_n(J)]$, when the APs are synchronous; otherwise, when using asynchronous APs

$$\mu(m,n) = \sum_{j=1}^{J} \frac{2||\mathbf{H}_m(j) - w(j)\mathbf{H}_n(j)||^2}{(1+|w(j)|^2)\sigma^2} \tag{30}$$

where w and $w(j)$ are given by (24) and (26), respectively.

Proof: See Appendix V. ∎

V. Implementation Issues

A. Frame Structure

In most wireless systems, each data/control message contains pilots/preambles, payload, and a cyclic redundancy check (CRC) field. The accuracy of the pilots or preamble-based channel estimation significantly influences the quality of the channel decoding. If there is too much decoding error, the message will fail the CRC parity check and the frame will be discarded.

If a Sybil alters its pilot transmission scheme, it can make the channel estimates of its corresponding claimed clients different. Thus the Sybil node has an increased chance to fool the monitoring APs. The modification of pilot patterns, however, is very likely to be noticed by the receiver. The reason is that

$$\alpha(N,N_s,J) = 1 - \frac{1}{N-N_s}\sum_{m=N_s+1}^{N}\left(1 - F_{\chi^2_{2JM,\mu(m,1)}}(k)\right)^{N_s} \times \prod_{N_s+1\le n\le N, n\ne m}\left(1 - F_{\chi^2_{2JM,\mu(m,n)}}(k)\right) \tag{27}$$

$$\beta(N,N_s,J) = \left(1 - F_{\chi^2_{2JM}}(k)\right)^{N_s-1}\prod_{N_s+1\le n\le N}\left(1 - F_{\chi^2_{2JM,\mu(1,n)}}(k)\right) \tag{28}$$

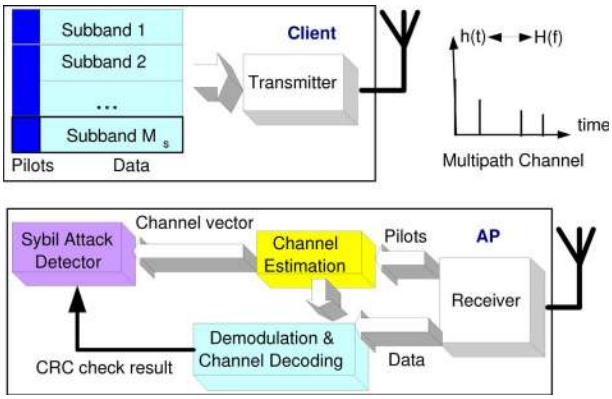

Fig. 2. Implementation of Sybil detector in OFDM systems. Each frame with M_s frequency subbands consists of one pilot and several data symbols in each subband.

it seriously degrades the channel decoding and thus leads to a CRC check failure with high probability. Hence, the Sybil node cannot send patterns that differ greatly from what is specified for normal communication. Thus, a clever Sybil node should keep the shape of the pilots the same and strive to fool an AP verifier by just changing the amount of power it uses to transmit pilots.

B. Wideband Systems

The underlying assumption of the proposed authentication scheme is that the system bandwidth is greater than the coherence bandwidth in current wireless systems and environments. We now examine practical issues for two types of wideband systems.

1) Orthogonal Frequency-Division-Multiplexing (OFDM)-Based Systems: The proposed Sybil detection scheme can be conveniently implemented in OFDM-based systems, like IEEE 802.11 (WiFi), 802.15 (wireless PAN), and 802.16 (WiMax) [10], [11]. As shown in Fig. 2, the Sybil detector utilizes the existing pilot-based channel estimation on M_s frequency subbands.

The number of pilot symbols M can in fact be less than the number of subbands M_s with the remainder of the subbands used for data. For concreteness, however, we assume initially that all subbands on the first symbol are used for pilots. In our numerical examples later, we relax this assumption. Simulation results will show that the detector only needs to consider channel estimation on $M < M_s$ subbands, where the tone spacing W/M is chosen to be greater than the coherence bandwidth of the channel. Moreover, as discussed in Section V-A, the CRC parity check result is utilized to catch Sybil nodes who change the pilot transmission patterns.

2) Single-Carrier-Based Systems: The proposed scheme can also be implemented in the wideband single carrier systems, e.g., code-division multiple access cellular systems. Each frame consists of M_s training symbols for channel estimation. The training sequence can be thought of as an impulse sequence convolved with $p(t)$, the pulse shape with a nominal width of T. Note that $1/T$ is large compared to the correlation bandwidth in wideband systems by definition. After going through the channel, with frequency-selective response $H(f)$, the receiver samples the M_s-pulse sequence and performs a discrete Fourier transform (DFT) on it.

In order to constrain the two-sided spectrum within the bandwidth W, $p(t)$ is typically chosen to be a root Nyquist pulse; specifically, we assume a $p(t)$ such that its matched filter response is a cosine rolloff pulse whose Fourier transform has a half-amplitude width of $1/T$ (the symbol rate) and a cosine rolloff factor $\mathcal{B}$. In this case, T, W, and $\mathcal{B}$ are related by $W = (1+\mathcal{B})/T$[12]. The choice of $\mathcal{B}$ is typically between 0.1 and 0.3, as a compromise between robustness of design and spectral efficiency. In any such case, the bulk of the transmission pulse $p(t)$ spans a time interval of about T second.

We use an M_s-symbol training sequence of $[1,0,0,\ldots,0]$, and every T second we sample the received version out of the matched filter. In this way, we obtain the channel impulse response sequence, whose DFT corresponds to the channel frequency response at a discrete set of frequencies (with aliasing, of course, the extent of which depends on the rolloff factor $\mathcal{B}$).

C. Narrowband Systems

Although the proposed authentication scheme is based on multipath propagation and hence actually applicable to wideband systems, it can as well be implemented in a narrowband system, where the system bandwidth is less than the coherence bandwidth [13]. In this case, all the channel samples within the system bandwidth are highly correlated, and thus we set $M = 1$.

If Sybil nodes use constant pilot power, our scheme can work with a single AP, and its performance degrades compared to the wideband system. On the other hand, under unknown power control strategy, the cooperation among multiple synchronized APs is required for the narrowband system to overcome the magnitude changes (23).

D. Integration With Spoofing Detection

We can integrate the proposed Sybil detection scheme with a spoofing detector with small additional overhead. When a client initiates a service request, the APs first start the Sybil detections. Once a client is verified to be non-Sybil, the APs continue to track its channel response and initiate the channel-based spoofing detection that also utilizes the existing channel measurement mechanism [14].

More specifically, without any change to the system structure above, the APs perform channel estimation and compare the channel vectors with the reference vectors, reusing the test statistic of (4). The service request is rejected on suspicion of spoofing, when the test statistic lying *above* some threshold k'. If a client has a similar channel response in consecutive time, APs update their reference channel vectors; otherwise, a spoofing attack alarm is reported.

The integrated channel-based detection can efficiently catch mobile Sybil attackers. If a Sybil node moves rapidly so as to yield a different channel response, it may be caught by the spoofing detector, since it has difficulty in generating the channel response of the corresponding client in the previous handshake process.

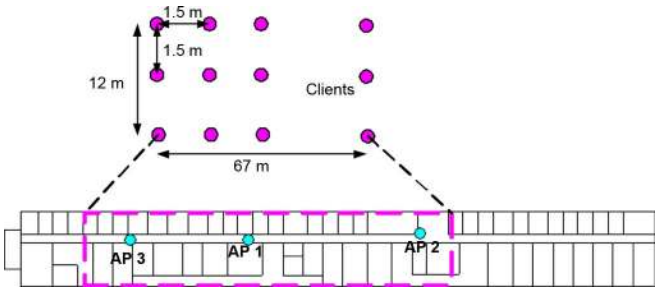

Fig. 3. System topology assumed in the simulations. Three APs are located at $[45.6, 6.2, 3.0]$ m, $[77.0, 5.0, 3.0]$ m, and $[24.0, 6.2, 3.0]$ m, respectively, in a 120 m × 14 m × 4 m office building. All clients, including both legal clients and Sybil, are located on dense grids at a height of 2 m. There are a total of 405 grid points.

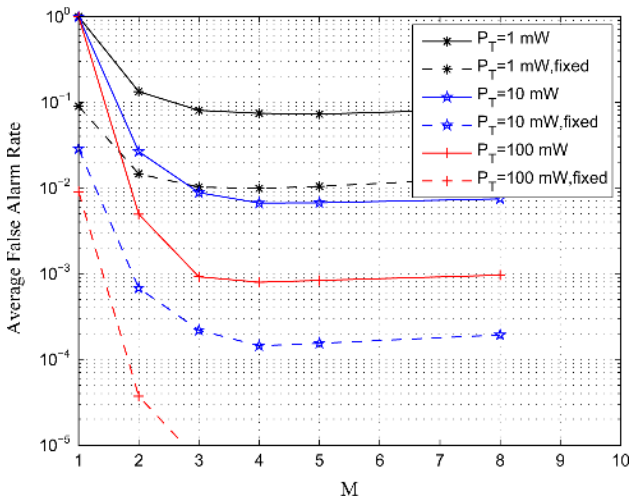

Fig. 4. Average false alarm rate of Sybil detection in wideband systems α for a given miss rate $\beta = 0.01$ with two clients, one AP, $W = 20$ MHz, and $b = 0.25$ MHz. The curves with notation "fixed" correspond to the cases where the receiver knows that the Sybil node uses constant power.

VI. Simulation and Numerical Results

A. Simulation Model

We conducted simulations to validate the efficacy of our strategy. Our simulation was carried out with a 3-D propagation prediction software package developed by Bell Laboratories, called the wireless system engineering (WiSE) tool [15]. The program uses ray-tracing to model typical channel responses for both indoor and outdoor environments, as well as the spatial variability of these responses. One input to WiSE is the 3-D 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 transmitter–receiver frequency response over any specified interval.

We have done this for a typical office building, for which a top view of the first floor is shown in Fig. 3. This floor of the building is 120 m long, 14 m wide, and 4 m high. For our experiments, we placed the APs in the hallway (the filled-in circles) at a height of 3 m, including AP 1 (the serving AP), AP 2, and AP 3, located at $[45.6, 6.2, 3.0]$ m, $[77.0, 5.0, 3.0]$ m, and $[24.0, 6.2, 3.0]$ m, respectively.

For the positions of clients, we considered a $12\,\text{m} \times 67\,\text{m}$ area, (outlined with a dashed line), and placed the clients randomly on a uniform grid of points with 1.5-m separations (with 405 grid points), at a height of 2 m. We randomly chose one position as the Sybil adversary who attempted to claim N_s identities, and randomly selected another $N - N_s$ points as legal clients. We then used WiSE to generate the corresponding channel impulse responses.

The hypothesis test was performed, and the performance including α and β was evaluated for the scenario. We repeated the experiment 10 000 times, and computed the average false alarm rate and miss rate over the whole area, for each of several selected combinations of system parameters.

The noise variance σ^2 is defined as the receiver noise power per tone P_N divided by the signal power per tone P_T/M, where P_T is the total power over M tones in milliwatts. Noting that $P_N = \eta N_F b$, where η is the thermal noise density in milliwatts per hertz, N_F is the receiver noise figure, and b is the measurement noise bandwidth per tone in hertz, we can write

$$\sigma^2 = \frac{\eta N_F b}{\frac{P_T}{M}}. \tag{31}$$

B. Simulation Results

In the simulations, we calculated the average false alarm rate for Sybil attacks α given a miss rate of $\beta = 0.01$ with center frequency $f_0 = 5$ GHz, $N_F = 10$, $b = 0.25$ MHz, $M = 1, \ldots, 8$, bandwidth $W = 0.025 \sim 100$ MHz and $P_T = 1 \sim 100$ mW, if not specified otherwise. The per tone signal-to-noise ratio (SNR) ranges from 1.7 to 80 dB, with a median value of 35 dB, for $P_T = 10$ mW and $M = 1$.

Fig. 4 shows the effectiveness of the proposed Sybil detector in a wideband system, with $N = 2$ clients and one AP. For example, both the average false alarm and miss rate are as small as 0.01, when the power is $P_T = 10$ mW, $M = 3$ tones, and $W = 20$ MHz. The performance improves with higher power, since the channel measurement error decreases with increasing P_T [see (31)]. The use of more frequency samples has a two-fold impact: it increases the channel resolution, while reducing the power per tone. Thus our scheme does not require too many frequency samples, and $M = 3$ is a good choice. It is also shown that if a Sybil node varies the power of pilots, it has a larger false alarm rate, i.e., it has a greater chance to hurt the system performance.

Proceeding further, Fig. 5 shows that our Sybil detector works in a narrowband system ($W = 300$ kHz), and its performance improves as we increase the number of APs. In other words, less pilot power is required for systems with more APs. For instance, systems with a single and two APs, require 100- and 1-mW pilot power, respectively, in order to make $\alpha < 0.01$ and $\beta = 0.01$. In addition, our scheme requires at least two APs, in order to work properly in narrowband systems, unless we know in advance that Sybil nodes use constant pilot power.

Next, we find in Fig. 6 that the false alarm rate decreases with the system bandwidth in wideband systems, and remains

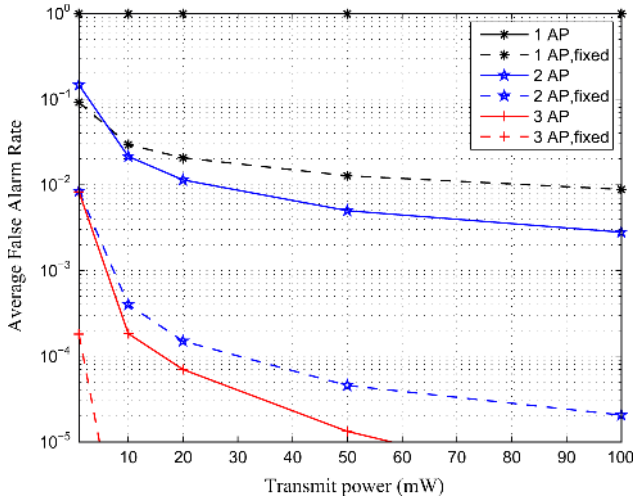

Fig. 5. Average false alarm rate α for a given miss rate of $\beta = 0.01$, in narrowband systems, with two clients, $W = 300$ kHz, $M = 1$, and $b = 0.25$ MHz. The J APs are synchronous to each other. The curves with notation "fixed" correspond to the cases where the receiver knows that the Sybil node uses constant power.

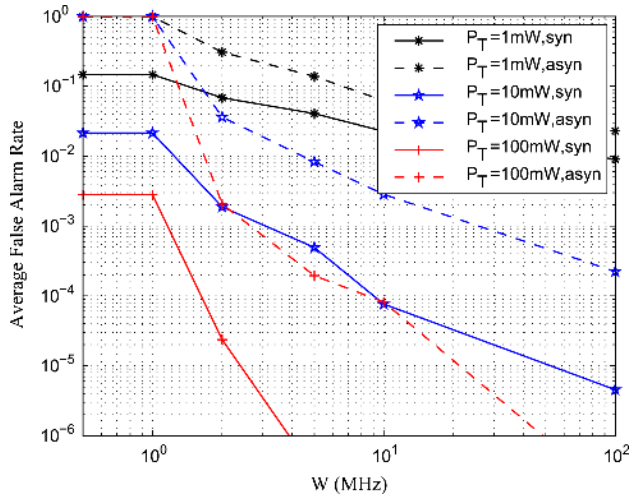

Fig. 6. Impact of system bandwidth on Sybil detection, with two clients, two APs, $b = 0.25$ MHz, and $\beta = 0.01$. We set $M = 1$ when $W \leq 1$ MHz, $M = 2$ for $W = 2$ MHz, and $M = 3$, otherwise. The curves with notations "syn" and "asyn" correspond to synchronous APs and asynchronous APs, respectively.

within an acceptable range in narrowband systems with two synchronous APs. As predicted, the synchronous system has a lower false alarm rate than the asynchronous system, and only synchronous multiple-AP systems work well in the narrowband regime.

Finally, Fig. 7 presents the performance with multiple clients (four legal clients), including the ROC curves. As indicated in (19) and (20), the miss rate decreases with the threshold k, while the false alarm rate rises. Moreover, for a given test threshold and number of legitimate clients, the false alarm rate slightly increases with N_s (number of Sybil clients), while the miss rate dramatically decreases. As shown in the ROC curves, the detection performance improves as the Sybil node claims more clients. In other words, the more harmful a Sybil node is to a network, the more likely it is to be caught by the proposed system.

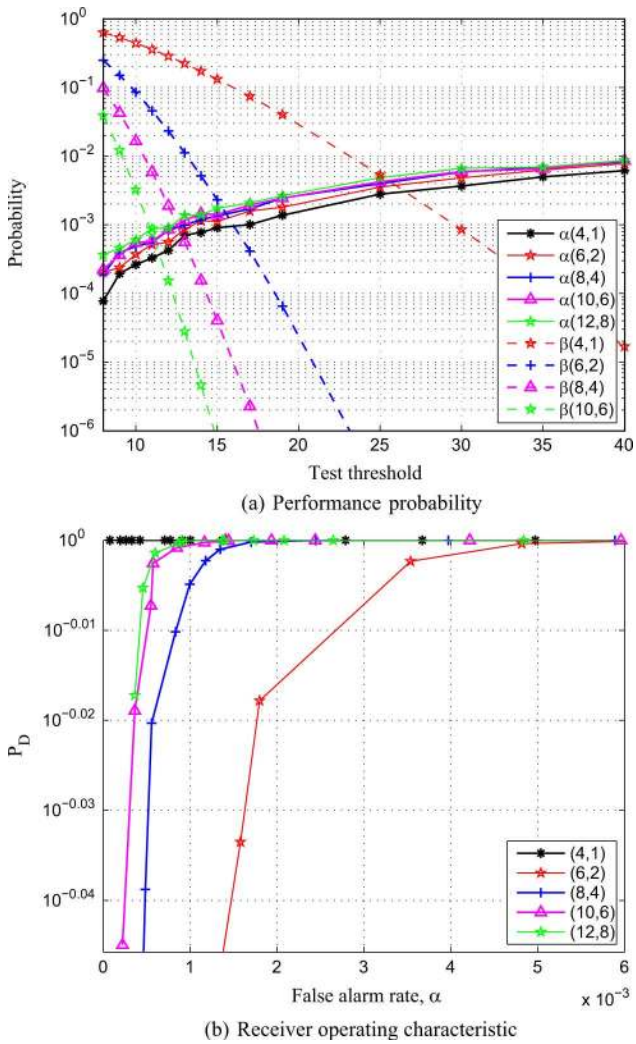

Fig. 7. Performance of Sybil detection in the (N, N_s) systems, where there is one AP, four legal clients, and N_s $(= N - 4)$ Sybil clients. We assume $M = 5$ tones, $W = 50$ MHz, $P_T = 50$ mW, and $b = 0.25$ MHz.

VII. Experimental Verification

We verified the proposed scheme via field measurements in a different office building, for which a top view is shown in Fig. 8. The experimental settings were similar to those in Section VI, except that the client grids were in a 4.55 m $\times$ 12.80 m area with 0.91-m separations (with 89 grid points). Both the AP and clients were at a height of 1.5 m.

We randomly chose $N - N_s + 1$ points as clients and measured the corresponding channel responses. The measurement system was comprised of an Agilent E5071B vector network analyzer (VNA), HG2458RD-RSP Rubber Duck vertically polarized omni-directional antennas, and low-loss, double-shielded, 60-ft cables, with a maximum loss of 6 dB at 6 GHz.

We used the same thermal noise model as in Section VI, and set $M = 5$, $W = 20$ MHz and $P_T = 1$ μW. The corresponding per tone SNR in the channel estimation ranged from 12.9 to 43.7 dB, with a median value of 28 dB. The value of P_T was smaller than 0.1 mW, since the average distance between transmitter and receiver was much less than that in Fig. 3.

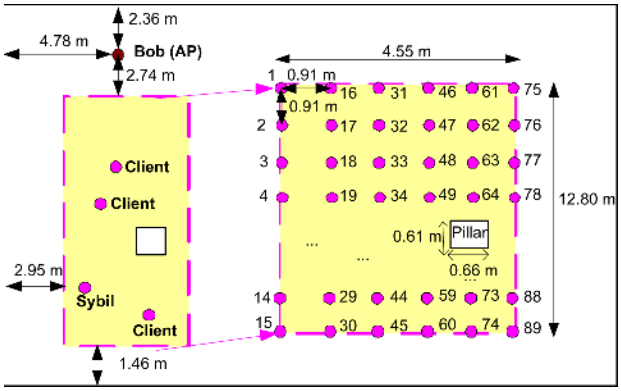

Fig. 8. System topology assumed in the verifications. The serving AP is located at one corner in a large room. All clients, including both legal clients and Sybil, are located on a rectangular grid of size 4.55 m $\times$ 12.80 m, with a spacing of 0.91 m (89 grid points). Both AP and clients are at a height of 1.5 m.

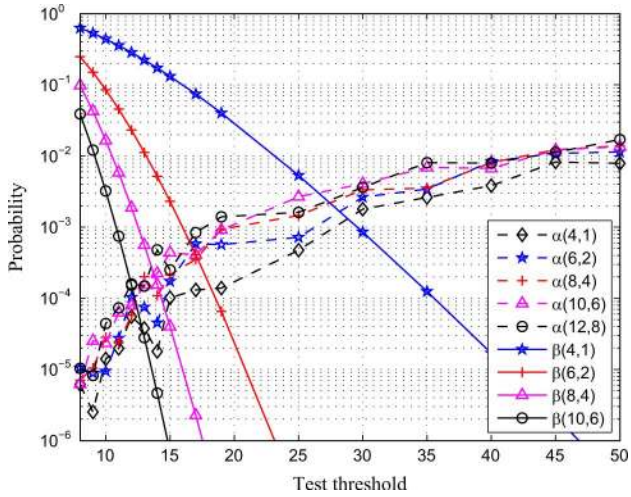

Fig. 9. Performance of Sybil detection with one AP, in the (N, N_s) systems shown in Fig. 8, where there is one AP, 4 legal clients, and N_s $(= N-4)$ Sybil clients. We assume $M = 5$, $W = 20$ MHz, $P_T = 1$ μW, and $b = 0.25$ MHz.

Fig. 9 presents the performance metrics as a function of test threshold k, given four legitimate clients. The figure verifies the performance of our Sybil detector; it shows that both the false alarm rate and the miss rate are below 0.01 for the test threshold $k = 25$. The results agree with the trend observed in Fig. 7.

VIII. Related Work

A traditional approach to address network attacks is secret-key-based authentication and encryption. Several pairwise key management schemes have been proposed for wireless sensor networks, based on probabilistic key sharing for authentication [16]–[19]. Their performance was improved by exploiting the location information of sensor nodes [20]. The use of pairwise keys to prevent Sybil attacks was briefly discussed in [21]. These key management schemes, however, usually incur a large system overhead associated with key management, which is not desirable. In contrast, after an initial association, our method does not require key management as it exploits the inherent properties of the channel (and not keys) to discriminate between entities.

In order to reduce the system overhead, the use of physical layer information has been proposed to enhance security in wireless networks. One group of work is based on the received signal strength (RSS) [2], [22], [23]. This work proposes to utilize large-scale channel fading and has three main limitations: 1) the monitor network has to be densely deployed, since each client must be measured by multiple landmarks; 2) the monitoring network may fail to discriminate terminals with small spatial separation, and may have performance degradation in rich-scattering environments; 3) the RSS information may be eavesdropped and spoofed in some circumstances [24].

To address these problems, the spatial variability of multipath propagation has been utilized in enhancing wireless security. A scheme based on channel frequency response was first proposed in [25]. An authentication method to detect spoofing attacks using hypothesis testing was defined and further explored in [14] and [26]–[28]. Meanwhile, Patwari and Kasera propose the use of the channel impulse response to discriminate between the terminal locations in [24].

IX. Conclusion

We have proposed a channel-based authentication technique to detect Sybil attacks in wireless networks, utilizing the uniqueness of channel responses in rich-scattering environments. By exploiting channel estimation, which is already performed in most wireless systems, we can build a hypothesis test that can detect Sybil attacks. Our Sybil detector involves a test statistic that is chosen based on the number of claimed identities, the number of APs, whether the APs are synchronized, as well as the attack strategy used by Sybil nodes. The technique takes into account measurement errors in channel estimation, including the receiver thermal noise, phase rotation of the receiver oscillator, and the variation of pilot power of Sybil clients. Our Sybil detector can be conveniently implemented in most existing wireless systems with low overhead, and can be naturally integrated with other physical layer security methods, such as spoofing detection, with minimal changes.

We derived the closed-form expression of the average miss detection rate and false alarm rate of the Sybil detection. We verified the efficacy of our scheme using the channel data generated from both propagation modeling software and field measurements via a VNA. Our scheme achieves high detection accuracy with a single AP in typical indoor environments. For instance, both the false alarm rate and the miss rate are below 0.01, when we use three tones, 10-mW pilot power, and a system bandwidth 20 MHz. Such a configuration is comparable to what is used in current WLAN deployments. It also works well in narrowband systems when there are multiple APs that are synchronized. The performance improves as we increase the number of APs, signal power, and system bandwidth. In addition, using ROC curves, we show that a Sybil node is more likely to be caught if it claims more identities, indicating that the Sybil nodes that hurt the network performance more seriously are more likely to be caught.

The spatial variability of wireless channels, which serves as the basis of our detection scheme, is most prevalent in environments with many scatterers and reflectors. As a result, our scheme achieves better performance if the terminals are inside

buildings or in crowded urban areas, and if the system bandwidth is greater than the coherence bandwidth of the channel. For narrowband systems, however, channel-based authentication has to rely on the limited spatial information associated with channel path loss, and thus the performance degrades in this case. We have shown, however, that employing multiple APs can overcome this limitation, and make channel-based authentication viable for narrowband systems.

APPENDIX I
DERIVATION OF (4)

When $\mathcal{H}_0$ is true, $\hat{\mathbf{H}}_1$ and $\hat{\mathbf{H}}_2$ come from different transmitters. We assume the elements of $\hat{\mathbf{H}}_1$ to be Gaussian random variables, i.e., $\mathbf{H}_1 \sim CN(\underline{0}, \sigma_H^2\mathbf{I})$, where $\mathbf{I}$ is an $M \times M$ identity matrix, and σ_H^2 is the channel variance as the transmitter roams within the coverage area of the AP. From (1) and (2), it is clear that given $\mathcal{H}_0$

$$\hat{\mathbf{H}}_1 \sim CN(\underline{0}, (\sigma_H^2 + \sigma^2)\mathbf{I}). \tag{32}$$

On the other hand, when $\mathcal{H}_1$ is true, from (1) and (3), we have

$$\hat{\mathbf{H}}_1 = (\hat{\mathbf{H}}_2 - \mathbf{N}_2)e^{j(\phi_1-\phi_2)} + \mathbf{N}_1 \sim CN(\hat{\mathbf{H}}_2 e^{j\phi}, 2\sigma^2\mathbf{I}). \tag{33}$$

Note that $\phi = \phi_1 - \phi_2$ is usually unknown, and thus we build a GLRT

$$\Lambda_g = \frac{\max_\phi Pr(\hat{\mathbf{H}}_1; \phi, \mathcal{H}_1)}{Pr(\hat{\mathbf{H}}_1; \mathcal{H}_0)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_1 \tag{34}$$

which can be further simplified to

$$L_g = \frac{||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 e^{j\phi'}||^2}{2\sigma^2} - \frac{||\hat{\mathbf{H}}_1||^2}{\sigma_H^2 + \sigma^2} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \eta_2 \tag{35}$$

$$\phi' = \arg\max_\phi P(\hat{\mathbf{H}}_1; \phi, \mathcal{H}_1) \tag{36}$$

$$= \arg\min_\phi ||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 e^{j\phi}|| = \mathrm{Arg}(\hat{\mathbf{H}}_1 \hat{\mathbf{H}}_2^H). \tag{37}$$

Since $\sigma_H^2 \gg \sigma^2$, we choose $L = ||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 e^{j\phi'}||^2/\sigma^2$ to approximate the GLRT.

APPENDIX II
DERIVATION OF (6)

In the adaptive power case, we have $\hat{\mathbf{H}}_1 \sim CN(\hat{\mathbf{H}}_2 w, 2\sigma^2\mathbf{I})$, where $w = w_1/w_2$, $w_n = a_n e^{j\phi_n}$, given $\mathcal{H}_1$. Similar to Appendix I, the GLRT in this case is given by

$$L_g = \frac{||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 w'||^2}{2\sigma^2} - \frac{||\hat{\mathbf{H}}_1||^2}{\sigma_H^2 + \sigma^2} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \eta_3 \tag{38}$$

$$w' = \arg\max_w P(\hat{\mathbf{H}}_1; w, \mathcal{H}_1) = \arg\min_w ||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 w|| = \frac{\hat{\mathbf{H}}_1 \hat{\mathbf{H}}_2^H}{||\hat{\mathbf{H}}_2||^2}. \tag{39}$$

For convenience of analysis, we choose $L = 2||\hat{\mathbf{H}}_1 - w'\hat{\mathbf{H}}_2||^2/(1 + |w'|^2)\sigma^2$, since $\sigma_H^2 \gg \sigma^2$.

APPENDIX III
PROOF OF THEOREM 1

First, we consider the case that the Sybil node uses constant signal power, i.e., $a_n = 1$. When $\mathcal{H}_1$ is true, we have $\mathbf{H}_1 = \mathbf{H}_2$, (3). From (1) and (5), and the assumption that $\mathrm{Arg}(\hat{\mathbf{H}}_n) \approx \mathrm{Arg}(\mathbf{H}_n e^{j\phi_n})$, which is reasonable for the high-SNR conditions where the system must operate, we can obtain

$$\begin{aligned}
&\mathbf{H}_1 e^{j\phi_1} - \mathbf{H}_2 e^{j\phi_2} e^{j\phi} \\
&= \mathbf{H}_1 e^{j\phi_1}(1 - e^{j(\phi_2 - \phi_1 + \mathrm{Arg}(\hat{\mathbf{H}}_1 \hat{\mathbf{H}}_2^H))}) \\
&\approx \mathbf{H}_1 e^{j\phi_1}(1 \\
&\quad - e^{j(\phi_2 - \phi_1 + \mathrm{Arg}(\mathbf{H}_1) + \phi_1 - \mathrm{Arg}(\mathbf{H}_2) - \phi_2)}) \\
&= e^{j\phi_1}\mathbf{H}_1(1 - e^{j(\mathrm{Arg}(\mathbf{H}_1) - \mathrm{Arg}(\mathbf{H}_2))}) = \mathbf{0}.
\end{aligned} \tag{40}$$

The elements in the M-dimensional vectors, $\mathbf{N}_1$ and $\mathbf{N}_2$, are i.i.d. complex Gaussian random variables $CN(0, \sigma^2)$. Thus $\mathbf{N}_m = \mathbf{N}_{1,m} - e^{j\phi}\mathbf{N}_{2,m} \sim CN(0, 2\sigma^2), m = 1, \ldots, M$. From (1), (4), and (40), the test statistic L under $\mathcal{H}_1$ can be written as

$$\begin{aligned}
L &= \frac{1}{\sigma^2}||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 e^{j\phi}||^2 \\
&= \frac{1}{\sigma^2}||\mathbf{H}_1 e^{j\phi_1} + \mathbf{N}_1 - \hat{\mathbf{H}}_2 e^{\phi_2 + j\phi} - e^{j\phi}\mathbf{N}_2||^2 \\
&= \frac{1}{\sigma^2}||\mathbf{N}_1 - e^{j\phi}\mathbf{N}_2||^2 \\
&= \frac{1}{\sigma^2}\left(\sum_{m=1}^{M}(\mathrm{Re}(\mathbf{X}_m))^2 + \sum_{m=1}^{M}(\mathrm{Im}(\mathbf{X}_m))^2\right) \\
&\sim \chi_{2M}^2
\end{aligned} \tag{41}$$

which is a Chi-square random variable with $2M$ degrees of freedom [9].

Similarly, when $\mathcal{H}_0$ is true, we usually have $\mathbf{H}_1 \neq \mathbf{H}_2$. From (1) and (4), the test statistic L under $\mathcal{H}_0$ can be written as

$$\begin{aligned}
L &= \frac{1}{\sigma^2}||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 e^{j\phi}||^2 \\
&= \frac{1}{\sigma^2}||\mathbf{H}_1 e^{j\phi_1} - \mathbf{H}_2 e^{j(\phi+\phi_2)} + \mathbf{N}_1 - e^{j\phi}\mathbf{N}_2||^2 \\
&= \frac{1}{\sigma^2}||\mathbf{H}_1 - \mathbf{H}_2 e^{j(\phi+\phi_2-\phi_1)} \\
&\quad + e^{-j\phi_1}\mathbf{N}_1 - e^{j(\phi-\phi_1)}\mathbf{N}_2||^2 \\
&\approx \frac{1}{\sigma^2}||\mathbf{H}_1 - \mathbf{H}_2 e^{j(\mathrm{Arg}(\mathbf{H}_1\mathbf{H}_2^H))} + e^{-j\phi_1}\mathbf{N}_1 \\
&\quad - e^{j(\phi_2 + \mathrm{Arg}(\mathbf{H}_1\mathbf{H}_2^H))}\mathbf{N}_2||^2 \sim \chi_{2M,\mu}^2
\end{aligned} \tag{42}$$

where $\mu = ||\mathbf{H}_1 - \mathbf{H}_2 e^{j\mathrm{Arg}(\mathbf{H}_1\mathbf{H}_2^H)}||^2/\sigma^2$, which is a noncentral Chi-square variable with a noncentrality parameter μ and $2M$ degrees of freedom.

Given a test threshold k, the false alarm rate α and the miss rate β, respectively, are given by

$$\alpha = Pr(L \leq k|\mathcal{H}_0) = F_{\chi_{2M,\mu}^2}(k) \tag{43}$$

$$\beta = Pr(L > k|\mathcal{H}_1) = 1 - F_{\chi_{2M}^2}(k) \tag{44}$$

where $F_X(\cdot)$ is the CDF of the random variable X. From (43) and (44), the false alarm rate for a given miss rate can be written

as

$$\alpha(\beta) = F_{\chi^2_{2M,\mu}}\left(F^{-1}_{\chi^2_{2M,0}}(1-\beta)\right) \tag{45}$$

where $F_X^{-1}(\cdot)$ is the inverse function of $F_X(\cdot)$.

Next, we assume that the Sybil node may change its transmission power, i.e., $a_n \neq 1$ holds in most cases, and denote $x_n = a_n e^{j\phi_n}$, $n = 1, 2$. When $\mathcal{H}_1$ is true, from (1), (3), (7), we can assume that when the SNR is high, $\hat{\mathbf{H}}_1\hat{\mathbf{H}}_2^H/||\hat{\mathbf{H}}_2||^2 \approx \mathbf{H}_1 x_1 \mathbf{H}_2^H x_2^*/||\mathbf{H}_2||^2 x_2 x_2^*$. Thus we have

$$\begin{aligned}\mathbf{H}_1 x_1 - w\mathbf{H}_2 x_2 &= \mathbf{H}_1 x_1 - \frac{x_2\hat{\mathbf{H}}_1\hat{\mathbf{H}}_2^H\mathbf{H}_2}{||\hat{\mathbf{H}}_2||^2} \\ &\approx \mathbf{H}_1 x_1 - \frac{x_2\mathbf{H}_1 x_1\mathbf{H}_2^H x_2^*\mathbf{H}_2}{||\mathbf{H}_1||^2 x_2 x_2^*} = \mathbf{0}.\end{aligned} \tag{46}$$

From (6) and (46), we have

$$L_{\mathcal{H}_1} \approx \frac{2||\mathbf{N}_1 - w\mathbf{N}_2||^2}{(1+|w|^2)\sigma^2} \sim \chi^2_{2M}. \tag{47}$$

Otherwise, when $\mathcal{H}_0$ is true, L can be written as

$$L = \frac{2||\mathbf{H}_1 - w\mathbf{H}_2 + \mathbf{N}_1 - w\mathbf{N}_2||^2}{(1+|w|^2)\sigma^2} \sim \chi^2_{2M,\mu} \tag{48}$$

where

$$\mu = \frac{2||\mathbf{H}_1 - w\mathbf{H}_2||^2}{(1+|w|^2)\sigma^2}. \tag{49}$$

The rest of the proof is the same as the case with constant power.

Appendix IV
Proof of Theorem 2

Given a test threshold k, the false alarm rate averaged over all channel estimation noise can be written as

$$\begin{aligned}\alpha(N, N_s) &= \frac{\sum_{m=N_s+1}^{N} E[I(m)]}{N - N_s} \\ &= \frac{1}{N-N_s}\sum_{m=N_s+1}^{N} Pr[I(m)=1] \\ &= 1 - \frac{1}{N-N_s}\sum_{m=N_s+1}^{N} Pr[I(m)=0] \\ &= 1 - \frac{1}{N-N_s}\sum_{m=N_s+1}^{N} \\ &\quad Pr[L(m,n) > k,\ \forall n \neq m] \\ &= 1 - \frac{1}{N-N_s}\sum_{m=N_s+1}^{N} \\ &\quad \prod_{1\leq n\leq N, n\neq m} Pr[L(m,n) > k] \\ &= 1 - \frac{1}{N-N_s}\sum_{m=N_s+1}^{N} \\ &\quad \prod_{1\leq n\leq N, n\neq m}\left(1 - F_{\chi^2_{2M,\mu(m,n)}}(k)\right) \\ &= 1 - \frac{1}{N-N_s}\sum_{m=N_s+1}^{N} \\ &\quad \left(1 - F_{\chi^2_{2M,\mu(m,1)}}(k)\right)^{N_s} \\ &\quad \times \prod_{N_s+1\leq n\leq N, n\neq m}(1 - F_{\chi^2_{2M,\mu(m,n)}}(k))\end{aligned} \tag{50}$$

where

$$\mu(m,n) = \frac{2||\mathbf{H}_m - w\mathbf{H}_n||^2}{(1+|w|^2)\sigma^2}. \tag{51}$$

Similarly, we get the miss rate for a given k

$$\begin{aligned}\beta(N, N_s) &= 1 - \frac{\sum_{m=1}^{N_s} E[I(m)]}{N_s} \\ &= 1 - \frac{\sum_{m=1}^{N_s} Pr[I(m)=1]}{N_s} \\ &= Pr[I(1)=0] \\ &= Pr[L(1,n) > k, \quad \forall n = 2, \ldots, N] \\ &= (1 - F_{\chi^2_{2M}}(k))^{N_s - 1} \\ &\quad \times \prod_{n=N_s+1,\ldots,N}(1 - F_{\chi^2_{2M,\mu(1,n)}}(k)).\end{aligned} \tag{52}$$

Appendix V
Proof of Theorem 3

It is clear that the synchronous-AP case is the same as the single-AP case, only with the dimension of the channel vectors changing from M to MJ. Thus we only discuss the asynchronous case here. It is easy to show that, when two clients come from different terminals, i.e., their true channel responses are different, the pair-wise test statistic L is a noncentral Chi-square variable with a noncentrality parameter μ, i.e.,

$$\begin{aligned}L &= 2\sum_{j=1}^{J}\frac{||\mathbf{H}_1(j) - w(j)\mathbf{H}_2(j) + \mathbf{N}_1(j) - w(j)\mathbf{N}_2(j)||^2}{(1+|w(j)|^2)\sigma^2} \\ &\sim \chi^2_{2JM,\mu}\end{aligned} \tag{53}$$

where

$$\mu = 2\sum_{j=1}^{J}\frac{||\mathbf{H}_1(j) - w(j)\mathbf{H}_2(j)||^2}{(1+|w(j)|^2)\sigma^2}. \tag{54}$$

Otherwise, when two clients come from the same Sybil node, the test statistic L is a Chi-square random variable with $2JM$ degrees of freedom, i.e.,

$$L = 2\sum_{j=1}^{J}\frac{||\mathbf{N}_1(j) - w(j)\mathbf{N}_2(j)||^2}{(1+|w(j)|^2)\sigma^2} \sim \chi^2_{2JM}. \tag{55}$$

Similar to the proof of Theorem 2, the false alarm rate α and the miss rate β, respectively, are given by

$$\begin{aligned}\alpha(N,N_s,J) &= 1-\frac{1}{N-N_s} \\ &\quad\times\sum_{m=N_s+1}^{N}(1-F_{\chi^2_{2JM,\mu(m,1)}}(k))^{N_s} \\ &\quad\times\prod_{n=N_s+1,\ldots,N,\ n\neq m}(1-F_{\chi^2_{2JM,\mu(m,n)}}(k)) \qquad (56)\\ \beta(N,N_s,J) &= (1-F_{\chi^2_{2JM}}(k))^{N_s-1} \\ &\quad\times\prod_{n=N_s+1,\ldots,N}(1-F_{\chi^2_{2JM,\mu(1,n)}}(k)) \qquad (57)\end{aligned}$$

where

$$\mu(m,n)=2\sum_{j=1}^{J}\frac{\|\mathbf{H}_m(j)-w(j)\mathbf{H}_n(j)\|^2}{(1+|w(j)|^2)\sigma^2} \qquad (58)$$

and $w(j)=\hat{\mathbf{H}}_m(j)\hat{\mathbf{H}}_n^H(j)/\|\hat{\mathbf{H}}_n(j)\|^2$.

REFERENCES

[1] A. Mishra and W. A. Arbaugh, An Initial Security Analysis of the IEEE 802.1x Standard University of Maryland, College Park, Tech. Rep. Cs-tr-4328, 2002.

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

[3] J. R. Douceur, "The sybil attack," in *Proc. First Int. Workshop on Peer-To-Peer Systems (IPTPS)*, Mar. 2002, pp. 251–260.

[4] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," in *Proc. Int. Symp. Information Processing in Sensor Networks (IPSN)*, Apr. 2004, pp. 259–268.

[5] W. C. Jakes , Jr, *Microwave Mobile Communications*. Hoboken, NJ: Wiley, 1974.

[6] A. Wood and J. Stankovic, "Denial of service in sensor networks," *IEEE Comput.*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[7] 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.

[8] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Commun.*, vol. 11, pp. 38–43, Dec. 2004.

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

[10] C. Snow, L. Lampe, and R. Schober, "Performance analysis and enhancement of multiband OFDM for UWB commmunications," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2182–2192, Jun. 2007.

[11] A. Ghosh, D. Wolter, J. Andrews, and R. Chen, "Broadband wireless access with WiMax/802.16: Crrent performance benchmarks and future potential," *IEEE Commun. Mag.*, vol. 43, no. 2, pp. 129–136, Feb. 2005.

[12] J. Proakis, *Digital Communications*. New York: McGraw-Hill, 1995.

[13] T. S. Rappaport, *Wireless Communications—Principles and Practice*. Englewood Cliffs, NJ: Prentice-Hall, 2001.

[14] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. IEEE Int. Conf. Communications (ICC)*, Jun. 2007, pp. 4646–4651.

[15] S. J. Fortune, D. H. Gay, B. W. Kernighan, O. Landron, R. A. Valenzuela, and M. H. Wright, "WiSE design of indoor wireless systems: Practical computation and optimization," *IEEE Comput. Sci. Eng.*, vol. 2, no. 1, pp. 58–68, Spring 1995.

[16] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Security and Privacy*, May 2003, pp. 197–213.

[17] D. Liu and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks," in *Proc. ACM Conf. Computer and Communications Security*, 2003, pp. 263–276.

[18] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. IEEE INFOCOM'04*, Hongkong, China, 2004, pp. 586–597.

[19] S. Jajodia, S. Zhu, and S. Setia, "Efficient security mechanisms for large-scale distributed sensor networks," in *Proc. ACM Conf. On Computer and Communications Security*, 2003, pp. 62–72.

[20] H. Yang, F. Ye, Y. Yuan, S. Liu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," *Proc. ACM Mobihoc'05*, pp. 34–44, 2005.

[21] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Elsevier Ad Hoc Netw. J.*, vol. 1, pp. 293–315, Sep. 2003.

[22] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in *Proc. IEEE Int. Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Jun. 2006.

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

[24] N. Patwari and S. Kasera, "Robust location distinction using temporal link signatures," in *Proc. ACM Int. Conf. Mobile Computing and Networking*, 2007, pp. 111–122.

[25] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proc. ACM Workshop on Wireless Security*, 2006, pp. 193–202.

[26] 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, no. 7, pp. 2571–2579, Jul. 2008.

[27] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," in *Proc. IEEE Conf. Information Sciences and Systems (CISS)*, Mar. 2008, pp. 642–646.

[28] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. IEEE Int. Conf. Communications (ICC)*, May 2008, pp. 1520–1524.

Liang Xiao (S'09) received the B.S. degree in communication engineering in 2000 from Nanjing University of Posts & Telecommunications, China, the M.S. degree in electrical engineering in 2003 from Tsinghua University, China, and the Ph.D. degree in electrical engineering from Rutgers University, NJ, in 2009.

From 2003 and 2004, she was with North Carolina State University, N.C. She is currently and associate professor in the Department of Communication Engineering, Xiamen University, Fujian, China. Her research interests include network security, localization, cognitive radio, radio resource managements, and wireless communications.

Larry J. Greenstein (M'67–SM'80–F'87–LF'03) received the B.S., M.S., and Ph.D. 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 anticlutter 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 (S'90–M'95–SM'00–F'09) 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), Rutgers University, North Brunswick, NJ, 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 corecipient (with O. Ileri) of the Fred W. Ellersick Prize from the IEEE Communications Society in 2009 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, Kharagpur, 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* (New York: Springer). 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).

Wade Trappe (S'98–A'02–M'03) received the B.A. degree in mathematics from The University of Texas at Austin, in 1994, and the Ph.D. degree in applied mathematics and scientific computing from the University of Maryland, in 2002.

He is currently Associate Professor in the Electrical and Computer Engineering Department, Rutgers University, and is Associate Director of the Wireless Information Network Laboratory (WINLAB), North Brunswick, NJ. 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. He is a coauthor of the textbook *Introduction to Cryptography with Coding Theory* (Englewood Cliffs, NJ: 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.