PHY-TECHNIQUES TO IMPROVE HIGHER-LAYER FUNCTIONS IN WIRELESS NETWORKS

by

LIANG XIAO

A Dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Electrical and Computer Engineering

Written under the direction of

Profs. Narayan Mandayam and Wade Trappe and Larry Greenstein

and approved by

_____

_____

_____

_____

New Brunswick, New Jersey

May, 2009

ABSTRACT OF THE DISSERTATION

PHY-Techniques to Improve Higher-Layer Functions in Wireless Networks

By Liang Xiao

Dissertation Directors:

Profs. Narayan Mandayam and Wade Trappe and Larry Greenstein

The wireless medium contains location-specific information at various scales, and thus it can serve in multiple ways to enhance the performance of wireless networks. In this thesis we study the use of physical-layer information to improve higher-layer functions in the following categories: (1) the use of the measured large-scale channel gain variations (due to power spreading and shadowing) to estimate signal outage and to perform mobile localization; and (2) the use of the measured small-scale channel gain variations (due to multipath) to improve wireless network security.

We first consider sensor networks that record received signal strength for estimating and updating network performance. Using a generic path-loss model incorporating distance effects and shadow fading, we apply the principle of importance sampling to the sensor placements. This helps to minimize measurement costs while accurately estimating outage probability and coverage holes, thereby improving the radio resource management of wireless systems. We also analyze the use of sensor networks to locate mobiles, and we

propose four simple-yet-accurate localization algorithms that meet E-911 requirements in most environments. The localization performance can be further improved by implementing a minimum mean square error (MMSE) algorithm which meets the Cramer-Rao lower bound. However, the four simple proposed algorithms have much lower numerical complexity than MMSE for real-time operation and require little *a priori* knowledge of the channel parameters.

Next, we exploit the rapid-decorrelation property of the multipath channel to enhance security in environments with rich scattering. We propose a channel-based authentication scheme to detect both spoofing attacks (a spoofing node pretends to be another node to gain access to network resources); and Sybil attacks (a Sybil node maliciously sends multiple service requests with different identities, in hopes of depleting network resources). The scheme uses little additional system overhead, as it exploits pilots or preambles that already exist in most wireless systems. A double-layer authentication protocol is devised, whereby the scheme either combines with higher-layer security mechanisms, such as 802.11i or works independently with some performance degradation. Verification that PHY-based authentication provides good performance is performed using several methods, specifically, stochastic channel modeling, site-specific ray-tracing and field tests.

Acknowledgements

First, I would like to thank my thesis advisor, Prof. Narayan Mandayam, for his inspiring guidance, strong support and great help that he has given me throughout my PhD studies. He has given me invaluable advice on my research, introduced me to the area of statistical signal processing, and has provided me many precious professional opportunities. This thesis would not have been possible without his guidance.

I am also greatly indebted to my co-advisor Prof. Wade Trappe, who has been a constant and important source of guidance, support and encouragement. I have benefited tremendously from his extensive knowledge and technical insight, especially in his primary research area of wireless security and security protocols. Additionally, he has also provided me guidance that has helped steer my professional development.

I am especially grateful to my co-advisor Prof. Larry Greenstein, who has opened my horizons with his tremendous expertise on propagation theory and channel modeling. I will not forget his efforts to help me improve my research, as well as help me develop many other skills. In spite of his tight schedule as a leader in his field, he always carefully read each of my work reports, offered to give me talk rehearsals, and promptly gave constructive comments. I feel very lucky to have these three caring advisors.

I also wish to thank the fourth member of my thesis committee, Dr. Reinaldo Valenzuela, for his Wireless Systems Engineering (WiSE) tool, which has significantly helped my thesis work. I have benefited from his knowledge of WiSE and, more generally, the area of

wireless communications. I also would like to thank Dr. Alex Reznik and my colleagues in InterDigital for their constructive suggestions on Chapter 4.7-4.8. I am grateful to Dr. Qi Bi for hiring me as a research intern at Bell Labs, and the generous help that he has continued to provide since then.

I would like to express my gratitude to the many professors at Rutgers who have given me generous help and constructive suggestions, especially Prof. Dipankar Raychaudhuri, Prof. Predrag Spasojevic, Prof. Zoran Gajic, Prof. Yanyong Zhang, and Prof. Roy Yates. I am also thankful to all WINLAB graduate students, and especially indebted to Prof. Trappe's research group. Beyond my immediate group, I really appreciate the helpful technical discussions and nontechnical conversations with Ruoheng Liu, Xiaojun Tang, Haris Kremo, Hongbo Liu, Suli Zhao, Jing Lei, Zhibin Wu, Xiangpeng Jing, Bin Zan, Kuo-Chun Huang, Goran Ivkovic, Chandrasekharan Raman, Hithesh Nama, and all my WINLAB colleagues.

Finally, I would like to thank my parents and sister, for their lifelong encouragement, support and love.

Dedication

To my parents, my sister, and my niece Maggie

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

Wireless communications are susceptible to interference and channel fading, which vary over time in an unpredictable way. In general, interference from other radios can be controlled by techniques, such as appropriate radio resource management, while the property of the radio channel places fundamental limitations on the system performance.

Radio propagation is usually characterized by two models: The *large-scale* path gain variation indicates how the locally averaged received signal strength (RSS) changes over large transmitter-receiver (T-R) separation, and is usually described by the pathloss and shadow fading models; and the *small-scale* gain variation, modeled in terms of multipath and Doppler, captures the rapid fluctuations of path gain over very short distances (a few wavelengths) or short time duration [1].

We study how to exploit the properties of the radio channel to improve higher-layer functions for wireless networks, notably, cellular networks and wireless local area networks (WLANs). We focus on four applications: The estimation of the signal coverage outages of cellular systems and the localization of mobile terminals (MT), both using large-scale variation information; and the detection of spoofing attacks and Sybil attacks, both based on using small-scale variation information.

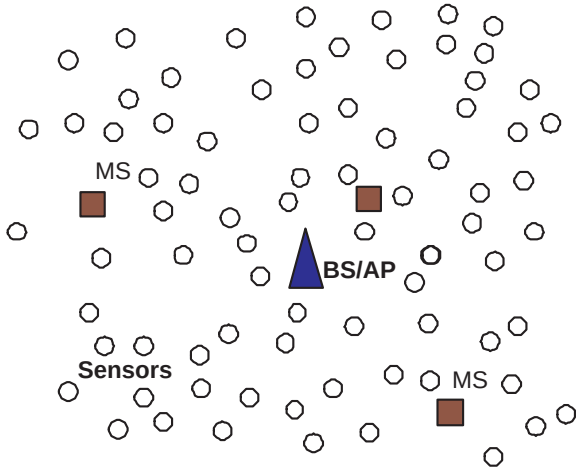


Figure 1.1: System topology of the distributed measurements that use a large number of sensors with known locations to measurement the recieved signal strength for wireless systems, such as cellular systems and WLAN.

1.2 The Use of Large-Scale Variations Measurements

The first two applications, signal coverage estimation and mobile localization, are both accomplished by using distributed measurements. As shown in Fig. 1.1, the distributed measurements can be performed via many low-cost sensors over the area of interest. Each sensor is located at known locations and estimates and updates the received signal strength information. While we focus here on applications to cellular, the technique also has the potential to work in cognitive radio systems.

The sensor-based distributed measurements provide round-the-clock services, and can react to gradual changes in propagation, e.g., new structures, especially in cities, or interference which may change due to adaptive beamforming. The use of distributed measurements is not labor-intensive, and moreover, it is easy to ensure that data is available at all times, so as to facilitate slow adaptive changes in radio resources. The sensors can be numerous and measurements can be gathered more-or-less uniformly from known locations, facilitating

reliable outage evaluations. In fact, the potential exists to accurately pinpoint chronically poor service areas that arise after initial planning, and to identify the need for new or reengineered sites. Additionally, the sensor network could be extended to support multiple air interfaces within overlapping coverage regions (e.g., wireless LAN, DVB-H deployments).

The first application of distributed measurements, coverage outage estimation in cellular environments, can be used not only for medium-term radio resource management, but also for longer-term engineering, e.g., identifying the need for new cell sites.

The second application, the collection of the location information of mobile terminals, can be used to improve radio resource management, mobility management, and overall cellular system design [2]. Also, the Federal Communications Commission (FCC) initially required all wireless carriers to report the location of E-911 callers with an accuracy of 125 m in at least 67% of cases [3]. This rule was later adjusted to 100 m or less in 67% of all cases, and 300 m or less in 90% of all cases [4].

1.3 The Use of Small-Scale Variation Measurements

The rapid proliferation of wireless networks has changed the landscape of network security. Security has become a significant concern in wireless networks and subscribers demand protection of their privacy, as wireless platforms are being used to access an increasing amount of security-sensitive services, such as e-commerce and online banking. Security in wired networks has been thoroughly studied, resulting in many encryption and authentication mechanisms proposed for multiple layers in the communication OSI protocol stacks. Although conventional cryptographic security mechanisms are essential to securing wireless networks, these techniques do not directly leverage the unique properties of the wireless domain to address security threats.

1.3.1 Security Mechanisms in Wireless LAN

In a typical wireless LANs, the mobile wireless devices communicate though the wireless channel with a centralized, stationary access point (AP) that might be connected to a wired network.

The first link-layer security protocol developed for WLAN is the wired equivalent privacy (WEP) scheme, which was aimed at providing a security level comparable to that with a wired network. An RC4-based stream cipher is used for the encryption and a cyclic redundancy check (CRC) is utilized as the integrity checksum. A challenge-response handshake is used to authenticate the stations. Unfortunately, WEP has been proved to have severe flaws, such as key reuse, weak RC4 keys, linear checksum, and one-way authentication.

In order to amend these flaws of WEP, the Wi-Fi alliance released a second standard called Wi-Fi Protected Access (WPA) in 2002. The important new features introduced by WPA include the temporal key integrity protocol (TKIP), which addresses the key reuse and weak key attack problems, message integrity codes (MICs), which provide better data integrity protection; and 802.1x authentication, which provides stronger authentication, authorization, and key management.

Later, in 2004, a next-generation WPA, or WPA2, or 802.11i was released by IEEE 802.11 Task Group i. This standard is based on WPA and retains many WPA features, such as TKIP/Michael and 802.1x. On the other hand, instead of the RC4 steam cipher, 802.11i utilizes the Advanced Encryption Standard (AES) in counter mode with CBC-MAC Protocol (CCMP) for data encryption [5]. In spite of all these efforts, 802.11 systems still have security vulnerabilities, as shown in [6, 7].

1.3.2 Security Threats to Wireless Networks

Compared to their wired counterparts, wireless networks are especially vulnerable to security threats. First of all, the broadcast nature of radio implies that no physical connection is required for access to a wireless network. As consequence, wireless networks are open to intrusion from the outside without the need for a physical connection.

Second, mobile devices usually identify themselves with their MAC address. In commodity networks, such as 802.11, it is easy for a device to alter its MAC address and claim to be another device by simply issuing an `ifconfig` command. The development of new wireless platforms, such as cognitive radio, provides attackers even more power to implement attacks.

Furthermore, mobile nodes in a wireless network require high energy efficiency and can not support algorithms with high complexity and computation costs. For example, in sensor networks, low-power/low-cost algorithms are highly desirable. Moreover, time-variant fading of the wireless medium, due to both node mobility and environment changes, introduces new challenges to network security.

As a result, techniques that would provide a high level of security in a wired network have proven inadequate in a wireless network, as many motivated groups of students have readily demonstrated [8–10]. Let us review some attacks that seriously threaten wireless networks:

- Spoofing/masquerading: An attacker can claim to be given mobile or access point (AP) by using their identities, such as the MAC address.
- Sybil attacks: An attacker claims to be multiple users in hopes of depleting the network resources.

- Jamming: An attacker can jam the wireless network at the physical layer by transmitting while a nearby user is sending or receiving signals and thus prevent nearby legal users from accessing the network.

- Man-in-the-middle attacks: If an attacker manages to stay between a mobile and a AP, and can intercept and spoof the messages on-the-fly, then he/she can act as a rogue AP, replaying false messages between the mobile and the AP.

- Session hijacking: An attacker can hijack an established session by first breaking the session connection, and then spoofing the mobile/AP and replaying the previous authentication messages.

Wireless networks are vulnerable to these attacks because the MAC-layer or even higher-layer security mechanisms do not offer mutual authentication or protection before the establishment of authentication. More specifically, an adversary device can perform Sybil attacks and/or spoof management frames/control messages in a wireless system. Possible results include session hijacking, Man-in-the-middle attacks and denial-of-service (DoS) attacks, even in presence of the advanced security mechanisms, such as 802.11i [6, 7].

1.3.3 Channel-based Authentication

The physical properties of the wireless medium are a powerful source of domain-specific information that can be used to complement and enhance traditional security mechanisms.

In rich multipath environments typical of wireless scenarios, the response of the medium along any transmit-receive path is *frequency-selective* (or in the time domain, *dispersive*) in a way that is *location-specific*. This means:

- The channel can be specified by a number of complex samples either in the frequency

domain, i.e., a set of complex gains at a set of frequencies, or the time domain, i.e., a set of impulse response samples at a set of time delays.

- Such sets of numbers decorrelate from one transmit-receive path to another if the paths are separated by the order of an RF wavelength or more.

Therefore, we could use the channel response to discriminate among transmitters, and thus detect various identity-based attacks, such as spoofing attacks and Sybil attacks. While using the physical layer to enhance security might seem to be a radical paradigm shift for wireless systems, we note that this is not the first time that multipath and advanced physical layer methods have proven advantageous. Specifically, we are encouraged in our belief by two notable parallel paradigm shifts in wireless systems:

- Code division multiple access (CDMA) systems [11], where the use of Rake processing transforms multipath into a diversity-enhancing benefit; and
- Multiple-input multiple-output (MIMO) antenna techniques [12], which transform scatter-induced Rayleigh fading into a capacity-enhancing benefit.

1.4 Thesis Roadmap

In Chapter 2, we consider a received signal strength (RSS)-based distributed measurements that estimate the signal coverage for cellular systems. A large number of sensors are placed in the area and they measure the received signal strength. By applying the principle of importance sampling and a generic path-loss model, we propose an efficient sensor placement method, which reduces the required number of nodes for a given measurement accuracy. A higher measurement efficiency can have a substantial payoff, in terms of both the drain on sensor batteries and the information bandwidth needed by sensor networks.

In Chapter 3, we investigate the localization of MTs, using distributed measurements. Each sensor has an identifying code and a fixed and known location, and it measures the received signal power from transmitting MTs to estimate their locations. Our work is based on RSS or power measurement approach, which is relatively inexpensive and simple to implement in hardware [13]. In the system we consider, it is very likely that some sensors are located very close to the MT, and thus simple-yet-accurate localization schemes are possible.

In Chapter 4, we exploit the rapid spatial-decorrelation property of the channel response in environments rich with scatterers to detect spoofing attacks in wireless networks. We describe a physical-layer authentication technique that combines channel probing with hypothesis testing. More specifically, the channel frequency response is used to discriminate among transmitters, e.g., to determine whether current and prior communication attempts are made by the same user (same channel response). We consider practical issues, such as environmental changes, terminal mobility, channel estimation errors, and multiple antenna techniques. The performance of scheme is analyzed based on stochastic channel modeling, site-specific ray tracing, and experiments using 802.11 testbench within typical indoor environments.

We apply the channel-based authentication technique to detect Sybil attacks in Chapter 5. We build a hypothesis test to detect Sybil clients for both wideband and narrowband wireless systems, such as WiFi and WiMax systems with low overhead. This Sybil detection scheme can be implemented either independently or combined with the channel-based spoofing detection. The performance of our Sybil detector is verified, via both propagation modeling software and field measurements using a vector network analyzer. 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 APs.

In the last part of the thesis, in Chapter 6, we conclude and discuss future work.

Chapter 2

RSSI-based Coverage/Outage Estimation for Cellular Systems

In a coverage outage area, the mobiles have inadequate signal-to-noise ratio (SNR) or signal-to-interference ratio (SIR), and consequently call drops or handovers are very likely to take place. The knowledge of the outages is important for radio resource management and longer-term engineering, such as site planning, for commercial wireless networks, such as cellular systems, WLAN and DVB-H (digital video broadcasting - handheld).

To estimate the outages for wireless networks, we propose a distributed measurement via a number of low-price power-measuring nodes, such as sensors, at known locations. This method is not labor-intensive and is available at all times to accommodate slow adaptive changes in radio resources. Our focus is to improve the efficiency of the distributed measurement, which reduces the overall costs of the measurements.

2.1 System Model

We consider a scenario involving distributed measurements with N sensors in a given cellular cell with radius R, where the sensors measure the power of a downlink (DL) pilot signal from the base station (BS). We assume that the sensors perform the measurement over a bandwidth sufficiently wide (5 MHz or more) that multipath fading is essentially averaged out. Thus, the measurement of the signal power received by the i-th sensor, P_i, combined

with knowledge of the DL transmit power per user and the antenna gains, permits the network to estimate the DL path loss, PL_i, $i = 1, \cdots, N$.

For our purposes, it is fair to assume that the antenna gains are independent of sensor position, so that the variation of P_i precisely tracks the variation of PL_i, i.e., $P_i = C - PL_i$, where C is the same for all sensors.

For *SNR*-based estimation of outage probability, we compare the path loss, PL_i, to a threshold value PL_0. That threshold is the value at which a mobile receiver near the sensor would have just enough fade-averaged SNR for good reception[1]. A hole in coverage (i.e., an outage) is defined as a location whose path loss from the BS is greater than the threshold, i.e., $PL > PL_0$. The fraction of sensors measuring power below the threshold is the sensor network's estimate of the cell's SNR-based outage probability. The SNR-based approach is the same for the downlink and uplink, while the value of PL_0 may differ for the two directions, due to differences in transmit power, receiver noise level or air interface.

Placing the i-th sensor in a location with a distance d_i from the BS at an azimuth angle φ_i, we assume that the squared distance, $D_i = d_i^2$, is drawn from a set of possible values on $(0, R^2]$, whose underlying probability density function (PDF) is $f(D)$; that each φ_i has a uniform PDF on $[0, 2\pi)$; and that all the D_i and φ_i are mutually independent. Thus, in populating a given cellular cell with N sensors, each sensor can be said to be placed independently and randomly according to the underlying PDF $f(D)$.

---

[1]The multipath-averaged SNR is a valid determinant of link performance (e.g., see [14] and [15]), which is why our method is based on fade-averaged measurements.

2.2 Large-Scale Path Loss

Assuming the model of [16], the path loss (PL) from a transmitter (Tx) to a location of the receiver (Rx) in the environment is

$$PL[dB] = A + 10\gamma \log(d/d_0) + s, \qquad d > d_0, \tag{2.1}$$

where d is the T-R separation distance; d_0 is a reference distance (typically, 1 m indoors and 100 m outdoors); the intercept A is given by $20\log(4\pi d_o/\lambda)$, where λ is the wavelength [16]; the path loss exponent γ can range from 3 to 6, depending on the environment; the dB shadow fading, s, is a Gaussian random variable with zero mean and standard deviation σ; and σ can range from 3 dB to 10 dB, depending on the environment [17].

We assume that the autocorrelation of the spatial process s depends only on the separation distance. More specially, if we consider one transmitter and two receivers (denoted as the i-th Rx and j-th Rx), we have

$$E[s_i s_j] = \sigma^2 e^{-d_{ij}/X_c}, \qquad i, j = 1, \cdots, N, \tag{2.2}$$

where d_{ij} is the distance between these receivers; and X_c, the shadow fading correlation distance, ranges from several to many tens of meters [17].

2.3 Importance Sampling (IS) for Outage Probability Estimation

2.3.1 IS Concept and Analysis

We first consider a *full-cell* (FC) placement of sensors, based on a Monte Carlo method, where N sensors are distributed randomly and uniformly over the full cell, with D_i following

the distribution of

$$f(D) = \begin{cases} 1/R^2, & 0 < D < R^2 \\ 0, & \text{otherwise} \end{cases} . \tag{2.3}$$

For given channel realizations, the outage probability estimated by a FC placement is an average over measurements by N sensors, given by

$$\hat{p}_{FC} = \frac{1}{N} \sum_{i=1}^{N} \phi(\xi_i), \tag{2.4}$$

where $\phi(\cdot)$ is an indicator function, i.e., $\phi(\xi_i) = 1$ if $PL_i > PL_0$, otherwise, $\phi(\xi_i) = 0$.

Now we utilize important sampling (IS) theory in the sensor placement, where more sensors are placed in areas where the outage is more likely to happen. We denote the corresponding PDF of D and d as $f^*(D)$ and $f_d^*(d)$, respectively. The estimated outage probability is

$$\hat{p}_{IS} = \frac{1}{N} \sum_{i=1}^{N} \phi(\xi_i')W(\xi_i'), \tag{2.5}$$

where ξ_i' is the location of the i-th sensor, generated according to $f^*(D)$. The weight function $W(\cdot)$ seeks to "undo" the bias due to sampling with the biased placement.

The estimate of outage probability must be unbiased, i.e., $E[\hat{p}_{IS}] = E[\hat{p}_{FC}]$. Also, the variance should be smaller, i.e., $Var[\hat{p}_{IS}] < Var[\hat{p}_{FC}]$, which means that its estimate is *sharper* than that for full-cell placement with same amount of sensors, or equivalently, requires fewer sensors for the same estimate sharpness. The average and the variance are taken over different random selections of the sensor positions and the shadow fading realizations. This is the essence of *importance sampling* [18].

We now consider how to satisfy the two conditions: (1) unbiased estimates of the outage probability, P_0, and (2) minimal estimator variance. To gain insight with minimal complexity, we assume $X_c = 0$ in the current analysis, i.e., the dB shadow fadings are i.i.d. Gaussian

variables $N(0,\sigma^2)$. In our later computations, we will take shadow fading correlations into account.

Following Eq. (2.1) and (2.4), we have the average outage probability of FC placement over all realizations of the shadow fading as

$$\begin{aligned}\hat{P}_{FC} &= \frac{1}{N}\sum_{i=1}^{N} Pr(A + 10\gamma\log(d_i/d_0) + s_i > PL_0) \\ &= \frac{1}{N}\sum_{i=1}^{N} Q(\frac{\beta - \alpha\log(D_i)}{\sigma}),\end{aligned} \tag{2.6}$$

where $\alpha = 5\gamma$, $\beta = PL_0 - A + 10\gamma\log(d_0)$.

Similarly, by Eq. (2.5), the average outage probability of IS placement is given by

$$\hat{P}_{IS} = \frac{1}{N}\sum_{i=1}^{N} Q(\frac{\beta - \alpha\log(D_i^*)}{\sigma})W(D_i^*). \tag{2.7}$$

Condition 1 above amounts to $E[\hat{P}_{FC}] = E[\hat{P}_{IS}] = P_0$, and by Eq. (2.6)(2.3), we have

$$\begin{aligned}P_0 = E_{f(D)}[\hat{P}_{FC}] &= E[Q(\frac{\beta - \alpha\log(D)}{\sigma})] \\ &= \frac{1}{R^2}\int_0^{R^2} Q(\frac{\beta - \alpha\log(D)}{\sigma})dD.\end{aligned} \tag{2.8}$$

By (2.7), we also require that

$$W(D) = \frac{f(D)}{f^*(D)} = \begin{cases} \frac{1}{R^2 f^*(D)}, & 0 < D < R^2 \\ 0, & \text{o.w.} \end{cases}, \tag{2.9}$$

which indicates that $f^*(D) > 0$, for any $D \in (0, R^2]$.

Condition 2 amounts to minimizing $Var[\hat{P}]$. By (2.7) and (2.9), we have

$$\begin{aligned}&Var_{f^*(D)}[\hat{P}] = E_{f^*(D)}[\hat{P}^2] - P_0^2 \\ &= \frac{1}{N^2}E[\sum_{i=1}^{N}\sum_{j=1}^{N} Q(\frac{\beta - \alpha\log(D_i^*)}{\sigma})W(D_i^*)Q(\frac{\beta - \alpha\log(D_j^*)}{\sigma})W(D_j^*)] - P_0^2 \\ &= \frac{1}{N}E_{f^*(D^*)}[(Q(\frac{\beta - \alpha\log(D^*)}{\sigma})W(D^*))^2] - \frac{P_0^2}{N} \\ &= \frac{1}{NR^4}\int_0^{R^2} \frac{Q^2(\frac{\beta - \alpha\log(D)}{\sigma})}{f^*(D)}dD - \frac{P_0^2}{N},\end{aligned} \tag{2.10}$$

where the third line follows from the independence of $W(D_i^*)$ and $W(D_j^*)$, for $i \neq j$.

Based on these two conditions, we can derive $f^*(D)$ for the optimal sensor placement. Noting that $\int_0^{R^2} f^*(D)dD = 1$ and $f^*(D) \geq 0$ by definition, we have

$$\begin{array}{ll} \min & Var_{f^*(D)}[\hat{P}] \\ \text{s.t.} & \int_0^{R^2} f^*(D)dD = 1, \end{array} \tag{2.11}$$

where $f^*(D) > 0$, for $0 < D < R^2$. Its Lagrangian form is

$$L(f^*, \lambda) = \int_0^{R^2} \frac{Q^2(\frac{\beta - \alpha \log(D)}{\sigma})}{f^*(D)} + \lambda f^*(D)dD. \tag{2.12}$$

Then the optimization reduces to minimizing

$$L_2(f^*, \lambda) = \frac{Q^2(\frac{\beta - \alpha \log(D)}{\sigma})}{f^*(D)} + \lambda f^*(D), \tag{2.13}$$

leading to the following solution for the PDF of D:

$$f^*(D) = \begin{cases} Q(\frac{\beta - \alpha \log(D)}{\sigma})/\eta, & 0 < D < R^2 \\ 0, & \text{otherwise} \end{cases}, \tag{2.14}$$

where $\eta = \int_0^{R^2} Q(\frac{\beta - \alpha \log(x)}{\sigma})dx$, according to the constraint in (2.11). The corresponding optimal PDF for d is

$$f_d^*(x) = \begin{cases} 2xQ(\frac{\beta - 2\alpha \log(x)}{\sigma})/\eta, & 0 < d < R \\ 0, & \text{otherwise} \end{cases}. \tag{2.15}$$

This is a parametric scheme in that it requires knowledge of channel parameters, such as σ and γ ($= 0.2\alpha$). Further, this optimal placement essentially requires knowledge of the outage probability P_0, as can be seen from (2.8) and the above definition of η. In traditional IS methods, such an optimal solution is referred to as degenerate, since it requires knowledge of the true value of the quantity being estimated.

2.3.2 Semi-Parametric Placement Schemes

Motivated by the importance sampling idea above and to overcome the degenerate problem, we propose three sensor placement schemes that are *semi-parametric*, that is, each exploits the knowledge that power generally falls off with distance but does not attempt to know or exploit the precise nature of that falloff. Each scheme is defined by the PDF it uses for the base-to-sensor distance, d; the *angular* PDF in each case is uniform on $[0, 2\pi]$, as before. The three distance PDFs we consider are the following:

$$\text{Scheme} \quad 1: \quad f_d(x) = \begin{cases} 4x^3/R^4, & 0 < x < R \\ 0, & \text{otherwise} \end{cases} \tag{2.16}$$

$$\text{Scheme} \quad 2: \quad f_d(x) = \begin{cases} 6x^5/R^6, & 0 < x < R \\ 0, & \text{otherwise} \end{cases} \tag{2.17}$$

$$\text{Scheme} \quad 3: \quad f_d(x) = \begin{cases} \frac{2x}{R^2 - R_{min}^2}, & R_{min} < x < R \\ 0, & \text{otherwise} \end{cases} \tag{2.18}$$

Unlike the first two schemes, Scheme 3 is based on the assumption that there are no holes in the cell center area, i.e., at locations with distances smaller than R_{min}. Here, all the sensors are distributed uniformly in the outer ring of the cell, i.e., at locations with distances between R_{min} and R. Accordingly, we call Scheme 3 *partial-cell* (PC) placement. From Fig. 3, we see that these PDFs, and especially the one for Scheme 2, are good approximations to the PDF that was shown to be optimal for the case $\gamma = 3.8$, $\sigma = 8$ dB, $X_c = 0$ and $P_0 = 0.05$. How this translates into performance is a topic we address next.

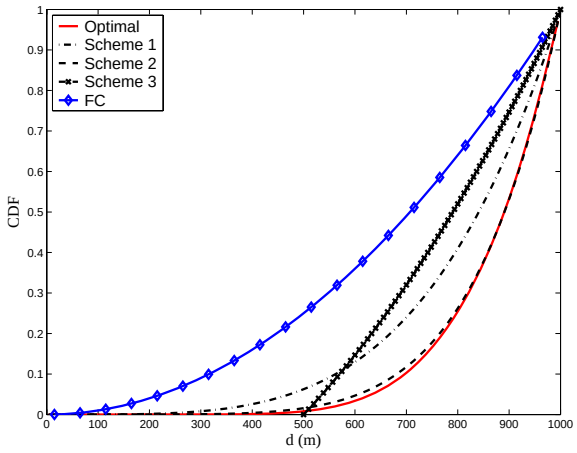


Figure 2.1: CDF of the distance between sensor and BS (d) for five sensor placement schemes, including full-cell (FC) placement. The "optimal" scheme is for the case $\gamma = 3.8$, $\sigma = 8$ dB, $X_c = 0$, $R = 1000$ m, and $P_0 = 0.05$. Scheme 3 is partial-cell (PC) placement with $R_{min} = 0.5R$.

2.4 Simulation Results on Outage Probability Estimation

2.4.1 Preliminary Result

Figure 2.2 presents the probability that the error in estimating P_o falls within $\pm 20\%$ of the true value, which is 0.05 in this example. Similar results are obtained for $P_o = 0.10$. It is seen that the three IS-based schemes cited above have similar performance, and all of them are better than full-cell placement. Among the IS-based schemes, Scheme 3, partial-cell placement given by (2.18), is easy to implement and has very good performance. In the remainder of this section, we will compare it with full-cell placement for both *SNR*-based and *SIR*-based outages and for both indoor and outdoor environments.

2.4.2 Simulation Approach

In our simulations, we initially assume a circular cell of radius R (later, we discuss circular vs. hexagonal cell shapes), and we assign values to R and the propagation parameters in

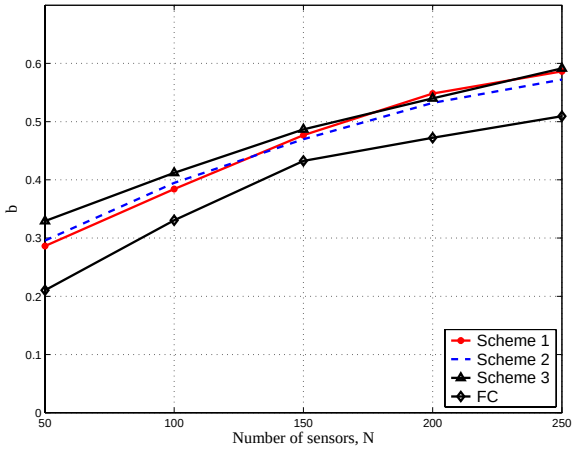


Figure 2.2: Estimation performance, $b = Pr[|\hat{P}_0 - P_0| < 0.2P_0]$, vs. the number of sensors in a cell, N, with cell radius $R = 1000$ m, $\gamma = 3.8$, $\sigma = 8$ dB, $X_c = 50$ m, and $P_0 = 0.05$.

Eq. (2.1) and (2.2). We simulate some number, N_{sh}, of statistically similar cells, with each having a different spatial variation of s, the dB shadow fading. We start by simulating $s(\xi)$ for Cell 1, where ξ denotes position within the cell. This random spatial variation is simulated using (2.2) and Cholesky decomposition described in [19]. The next step is to choose a value for N, the number of sensors per cell; a placement for the N sensors; and a path-loss threshold, PL_0, the determination of which is described below. Finally, the path-loss at each of the sensors is computed, and the outage probability in Cell 1, $p_0(1)$, is determined as the fraction of sensors for which $PL > PL_0$.

With $s(\xi)$ fixed, the N-sensor placement is chosen a total of M times and, if M is sufficiently large, the mean and standard deviation of $p_0(1)$, μ_1 and σ_1, respectively, can be estimated. (Note that these are the mean and standard deviation taken over the random placements of the N sensors within the cell.) This procedure is repeated for a total of N_{sh} generations of the shadow fading variation $s(\xi)$, corresponding to Cells $1, \cdots, N_{sh}$. The average of μ_j over j is the network's estimate, denoted by P_0^*, of the true outage probability; and the average of σ_j over j, denoted by ρ, is the network's estimate of the intra-cell standard

deviation due to the random N-sensor placement. We call ρ the "sharpness" of the estimate, and seek to make it as small as $0.25P_0$ or less.

The baseline value of P_0, i.e., what we assume to be the true one, is obtained by first assigning an extremely large value for N. We have found, by a combination of analysis and simulation not shown here, that $N = 4000$ would yield precise estimates in any cell, with negligible variation from one placement of N sensors to another. For that N, we (1) computed outage probability for each of N_{sh} realizations of $s(\xi)$, for each of several values of path-loss threshold, PL_0; (2) averaged over the N_{sh} values for each PL_0; and (3) took the result to be the "true" outage probability, P_0, for that path-loss threshold. We were thus able to identify the values of PL_0 producing average outage probabilities of 0.05 and 0.10. We applied the procedure described in the previous paragraph for each of these P_0-values, using practical values of N (namely, $50, 100, 200, 300$, and 400). For each of these N, we did $M = 200$ placements for each of $N_{sh} = 10$ realizations of the shadow fading variation, $s(\xi)$.

2.4.3 Simulation Performance

First, we investigate an outdoor system with the usual hexagonal cells, in particular, a center cell and six surrounding cells. The center cell, for which we will analyze outage probability estimation, is conveniently assumed to be circular, with a radius, R, chosen such that the circle has the same area as the actual hexagonal cell. This will simplify analysis with no loss in accuracy; other studies (e.g., [20]) have shown cell shape to be a negligible factor so long as cell area is preserved[2]. The shadow fading parameters (σ, X_c) are initially set at (8 dB, 50 m). We set PL_0 at values that yield "true" outage probabilities, P_0, of 0.05 and 0.10. For each of these two values, we have computed the corresponding estimate, P_0^*, for

[2]We note further that the regular hexagon closely approximates a circle, which is why early investigators chose it as the tessellating shape to use in cellular studies [21], [22].

both full-cell sensor placement ($R_{min} = 0$) and partial-cell placement ($R_{min} = 0.5R$ and $0.7R$).

Simulation results for P_0^* are shown in Table 2.1. The estimates obtained are independent of N except for a slight fluctuation due to finite simulation, so the numbers shown are averages of those obtained for several values of N. We see that the estimation of P_0 is virtually unbiased for R_{min} up to at least $0.5R$, i.e., there are virtually no outages to be counted at smaller distances. At $R_{min} = 0.7R$, however, the estimation is biased downward because outages can occur at base-terminal distances between $0.5R$ and $0.7R$ and are not counted.

For the same case, we obtained simulation results for ρ, the average standard deviation of the estimate resulting from the random placement of N sensors. Here, we expect to see a decrease with N, as is confirmed by the plots in Fig. 2.3. The "sharpness" of the estimates improves not only with increasing N, but also with increasing R_{min}, because larger R_{min} leads to a higher density of sensors in the area containing them. A near-best tradeoff between small bias error and maximum "sharpness" occurs for $R_{min} = 0.5R$, at least for the assumed model. For ρ to be no greater than $0.25P_0$, the figure shows that the required N for $P_0 = 0.05$ is about 200 for $R_{min} = 0.5R$ and around 300 for $R_{min} = 0$ (full placement). For $P_0 = 0.10$, the required N-values are around 100 and 150, respectively. Thus, a simplified form of importance sampling reduces the required number of sensors by about 33%. The general rule is that, with $R_{min} = 0.5R$, the required N is $\sim 10/P_0$, which is consistent with binomial statistics.

While the above study of SNR-based outage probability was generic, the study of *SIR*-based outage probability requires specificity about the radio interface. For this purpose, we assume a CDMA system with a spreading factor of 128 and a required receiver output

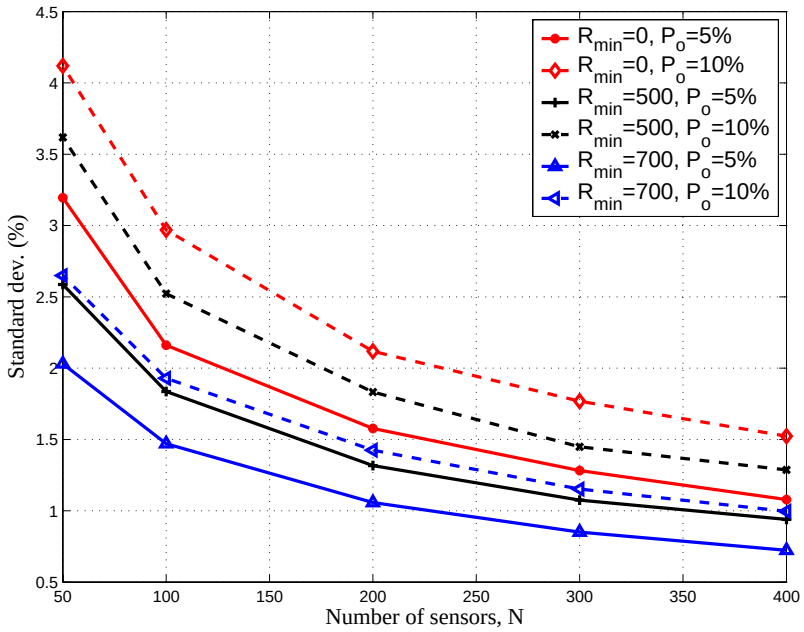


Figure 2.3: Standard deviation of estimate for $P_0 = 0.05$ and 0.10, $R = 1000$ m, and (X_c, σ)=(50 m, 8 dB).

SIR of 5 dB. For simplicity, we assume that the downlink co-channel interference from the six surrounding cells is dominant. Also, we assume that each sensor is able to identify, from downlink pilots, the power from each base (its own plus the six nearest interfering bases) [23]; that each base is transmitting its full rated power; and that an "outage" occurs for a mobile if its serving base runs out of power before it is able to meet that mobile's *SIR* requirement. These assumptions, combined with the above path-loss model, enable us to compute outage probability for a given number, K, of active mobiles per cell (or sector). Some results are given in Table 2.1, where the increase in P_0 with K, due to the dividing of transmit power among more mobiles, is evident but mild.

Table 2.1: Estimated Downlink Outage Probability.

CASE	$R_{min} = 0$	$R_{min} = 0.5R$	$R_{min} = 0.7R$
SNR-Based; Outdoor Cell ($R = 1000$ m); (σ, X_c)=(8 dB, 50 m)			
"True" $P_0 = 0.05$	0.050	0.050	0.044
"True" $P_0 = 0.10$	0.100	0.098	0.086
SNR-Based; Indoor Cell ($R = 100$ m); *"True"* $P_0 = 0.10$			
(σ, X_c)=(8 dB,8 m)	0.100	0.099	0.089
(σ, X_c)=(8 dB,50 m)	0.099	0.100	0.092
(σ, X_c)=(10 dB,50 m)	0.100	0.099	0.089
SIR-Based; Outdoor Cell ($R = 1000$ m); *CDMA System;* (σ, X_c)=(8 dB, 50 m)			
$K = 4$ ($P_0 = 0.076$)	0.075	0.074	-
$K = 8$ ($P_0 = 0.088$)	0.088	0.087	-
$K = 12$ ($P_0 = 0.103$)	0.103	0.100	-

2.5 Conclusion

We applied the principle of importance sampling to improve the efficiency of the distributed measurements in cellular systems. Specifically, we investigated ways to minimize the number (N) of sensors needed to estimating the signal coverage of the cells. We derived, for a particular set of parameters, an optimal sensor placement scheme for estimating cell outage probability; and we used it to postulate schemes that require no specific parameter information. Among them, we emphasize a version of partial-cell placement, wherein the power-measuring sensors are distributed in a random uniform way over base-mobile distances from 50% to 100% of the cell radius. Its performance was compared with that of full-cell placement. It was shown that a cell outage probability of P_0 can be accurately estimated using $\sim 10/P_0$ sensors with partial-cell placement; and that this represents a reduction, relative to full-cell placement, of $\sim 33\%$. This result applies to both *SNR*-based and *SIR*-based outage estimation for both indoor and outdoor environments [24, 25].

Chapter 3

RSSI-based Mobile Localization for Cellular Systems

In cellular systems, location information associated with mobile terminals (MTs) is collected to improve radio resource management, mobility management, and overall cellular system design [2]. Further, the Federal Communications Commission (FCC) initially required all wireless carriers to report the location of E-911 callers with an accuracy of 125 m in at least 67% of cases [3]. This rule was later adjusted to 100 m or less in 67% of all cases, and 300 m or less in 90% of all cases [4].

To address this problem, we investigate the localization of MTs using the distributed measurements described in previous chapter. For this chapter, we note that the sensors measure the received signal power from transmitting *mobiles*, instead of from the *BS*. In this system, it is very likely that some sensors are located very close to the MT, so that simple-yet-accurate localization schemes should be possible.

3.1 Related Work

Related work in the area of user localization based on received power falls roughly into four categories: (1) In-building infrared networks, (2) cellular networks based on RF, (3) global positioning system (GPS) and (4) sensor networks [26–30].

Accordingly, the MinMax algorithm was proposed for N-hop sensor networks to obtain an initial coarse estimate of sensor locations [28]. The least squares (LS) algorithm linearizes

the triangulation formulas of the distance between anchors (i.e., the sensors with known locations) and the unknown sensor, and then uses the standard least-squares approach to solve the linearized equations [29]. Similarly, in the Euclidean algorithm, up to two possible sensor positions are obtained by strictly solving the triangulation formulas of two anchors, and then the position of the unknown sensor is determined by the vote of the third anchor if necessary [30]. It often *flags* the case with large distance estimation error, through a failure to achieve intersecting circles. Such a flag can signal the location algorithm to switch to a more robust scheme.

3.2 System Model of Sensor-Assisted Localization

The model of the sensor network is almost the same as described in the previous chapter, though the sensors measure the power of signals coming from mobiles instead of BSs. We denote the sensor locations as $\underline{L}_1, \cdots, \underline{L}_N$, where $\underline{L}_i = [x_i, y_i]^T$, $i = 1, 2, \cdots, N$. The received power and path-loss associated with location L_i are P_i and PL_i, respectively.

Power-based localization in a sensor-assisted cellular system can be implemented in two steps:

Step 1: The system collects the received signal power information P_i from N sensors. For convenience, i is ordered such that P_i decreases with i ($P_1 \geq P_2 \geq \cdots \geq P_N$).

For most of the schemes considered here, the distances d_i is estimated from PL_i via (2.1), assuming that A and γ are known and the shadow-fading components s_i are unknown. Estimating d_i is possible by assuming that $s_i = 0$, leading to

$$\hat{d}_i = d_0 \cdot 10^{(PL_i - A)/(10\gamma)}. \tag{3.1}$$

The estimation error for d_i results from the existence of unknown shadow fading and any

errors in estimating A and γ.

Step 2: To estimate the location of the MT, $\underline{\theta} = [\theta_1, \theta_2]^T$, we select the first n data values, estimated by sensors with the n strongest powers. Compared with localization algorithms using data from all N sensors [26], this not only simplifies the implementation and saves energy, but also improves the estimate accuracy, as we will discuss in Section 3.3.

The postulated sensor-based system can use existing localization algorithms, such as MinMax [28] and Least Squares [29], but we also consider two new schemes (*Weighted Average* and *Modified Euclidean*), as follows:

Weighted Average (WtdAv) Method: This method requires no *a priori* information on A or γ, and does not need to estimate the distances between the MT and the sensors. The location of the MT is assumed to be an average of the locations of the nearby sensors, weighted by their received signal powers, i.e., $\hat{\underline{\theta}} = [\sum_{i=1}^{n} x_i w_i, \sum_{i=1}^{n} y_i w_i]^T$, where $w_i = P_i / \sum_{j=1}^{n} P_j$.

Modified Euclidean (ModEuc) Method: This method is an extension of the Euclidean algorithm [30], wherein WtdAv with $n \geq 3$ is invoked if and only if the Euclidean algorithm fails to produce intersecting circles. We will see that ModEuc provides a good combination of accuracy and robustness to conditions; and obviously, it has better coverage than the Euclidean algorithm, especially under heavy shadow fading. For example, with $\gamma = 3.8$, $\sigma_s = 8$ dB, $X_c = 80$ m, and $N = 200$ sensors in an outdoor cell with a radius of 1000 m, the Euclidean algorithm fails in 63% of the cases where ModEuc succeeds.

3.3 Simulations, Results and Discussion

3.3.1 Simulation Approach

We developed a simulation platform for determining the error statistics for different propagation conditions and system parameters. If not specified otherwise, the numerical results we present will be for the specific case of an outdoor cell, with a cell radius of 1 km; a reference distance $d_0 = 100$ m; a frequency of 2.4 GHz; a path-loss exponent, γ, of 3.8; and a correlation distance $X_c = 80$ m.

In the simulations, we first generate a total of N_{sh} "scenarios", a scenario consisting of a randomly chosen MT location and a spatial distribution of the dB shadow fading component, s, as characterized by (2.2). For each scenario, we generated M random placements of N sensors, with M being a program variable. We chose $N_{sh} = 50$ and $M = 300$, for a total of 15,000 trials. In each trial, we determined the location estimate for each of the methods, compared it with the true MT location, and thus determined the location error, ε, in meters. From the 15,000 values of ε for each method, we obtained a CDF, determined the $67th$ percentile value, and also computed the RMS value.

3.3.2 Numerical Results

As noted, the localization schemes select n out of N data values, i.e., the data collected by those sensors with the n strongest powers. Figure 3.1 presents the impact of n on the $67th$ percentile and the RMS estimation error, with $3 \leq n \leq 32$ and the parameters indicated in the caption. We see that WtdAv is not sensitive to n, because the additional data brought in by a larger n are weighted by smaller values $(P_i / \sum_j P_j)$. ModEuc is also insensitive to n, since the Euclidean method itself is based solely on the three nearest sensors; thus, $n > 3$

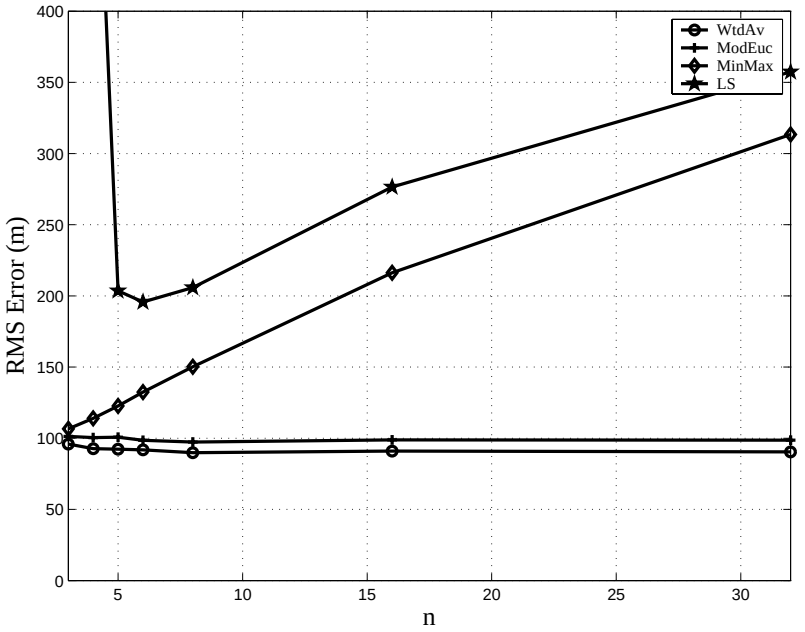
only applies when WtdAv is brought in.

MinMax tends to be less accurate as n rises. From Eq. (2.1) and Eq. (3.1) we see that the absolute estimation error of the distance between MT and the i-th sensor, $|\hat{d}_i - d_i| = d_i|10^{s_i/(10\gamma)} - 1|$, is approximately proportional to the distance d_i itself. Thus the distance estimate from a farther sensor is usually less accurate, especially in these sparsely distributed sensor networks. Since MinMax does not weight the measurements, its performance degrades when taking into account more "bad" data.

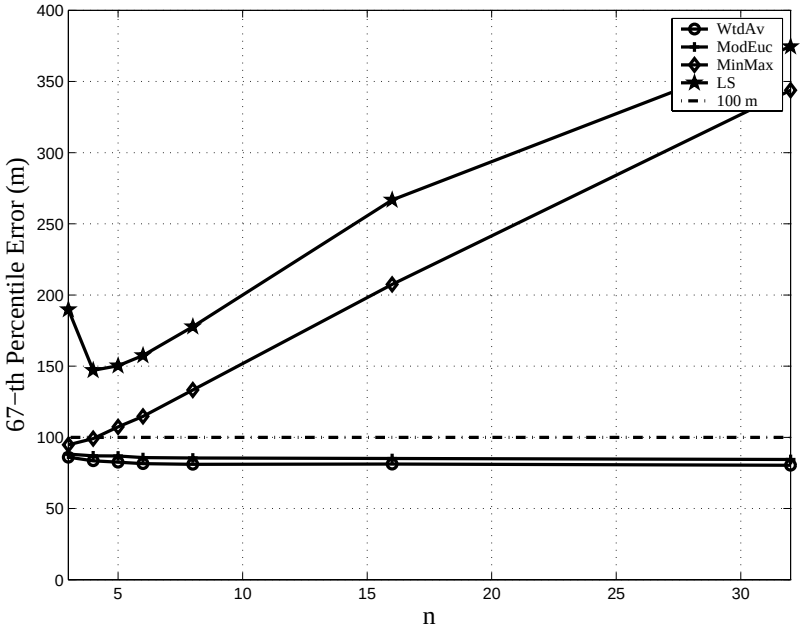
Similar comments apply to the LS scheme as well. The choice of n in that case is a bit complicated: $n = 4$ and 5 yield the lowest $67th$ percentile, while $n = 6$ yields the lowest RMS error. The large RMS errors seen for $n < 5$ arise from the occasional flip ambiguity (illustrated in [31]), where the sensors line up and cause the estimated and true MT location to be approximately symmetric about the line of sensors. We can assume that a practical algorithm would avoid these cases, but to simplify our study (and since the $67th$ percentiles are hardly different for $n = 4$, 5 and 6), we will assume $n = 6$ for the LS method.

Now we consider the selection of N, the number of sensors in each cell. Figure 3.2 shows that the estimation error decreases with N for each scheme. Under large shadow fading ($\sigma = 8$ dB), LS is the worst algorithm and all the other three schemes satisfy the FCC requirement that the estimation error be less than 100 m for 67% of cases with $N > 150$. For the case with negligible shadow fading ($\sigma = 0.1$ dB), all schemes satisfy the FCC requirement using very small N. Note that the LS and ModEuc schemes yield almost zero error with small shadow fading (assuming A and γ are precisely known).

From Fig. 3.3 we can see that the LS scheme is the most sensitive to σ among the four schemes, followed by the ModEuc scheme. However, the latter has smaller $67th$ percentile errors than others, as σ ranges from 0 to 8 dB. The performance of the WtdAv scheme is

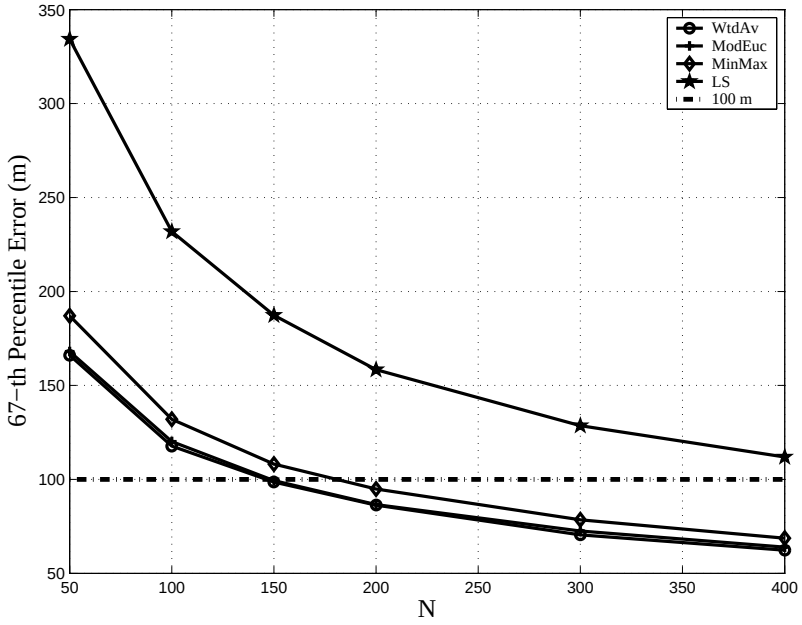


(a) RMS Error (m)

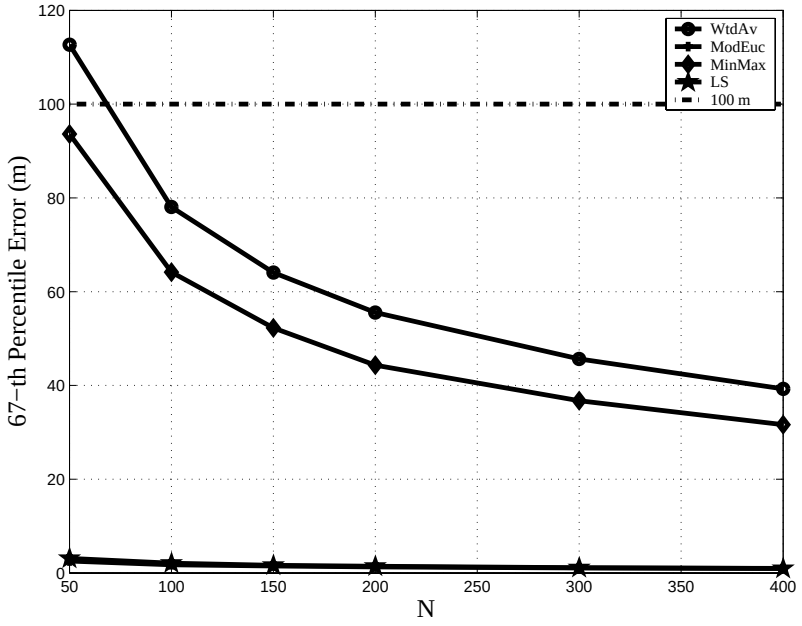


(b) 67% Error (m)

Figure 3.1: Error metrics vs. n, the number of strongest-power sensors used in the algorithm ($\gamma = 3.8$, $\sigma = 8$ dB, $X_c = 80$ m, $N = 200$, outdoor cell with a radius of 1000 m). Note the rough similarity of the RMS error to the 67% error in most cases.



(a) $\sigma = 8$ dB



(b) $\sigma = 0.1$ dB

Figure 3.2: 67% error vs. N, the number of sensors in a a cell ($\gamma = 3.8$, $X_c = 80$ m, outdoor cell with a radius of 1000 m).

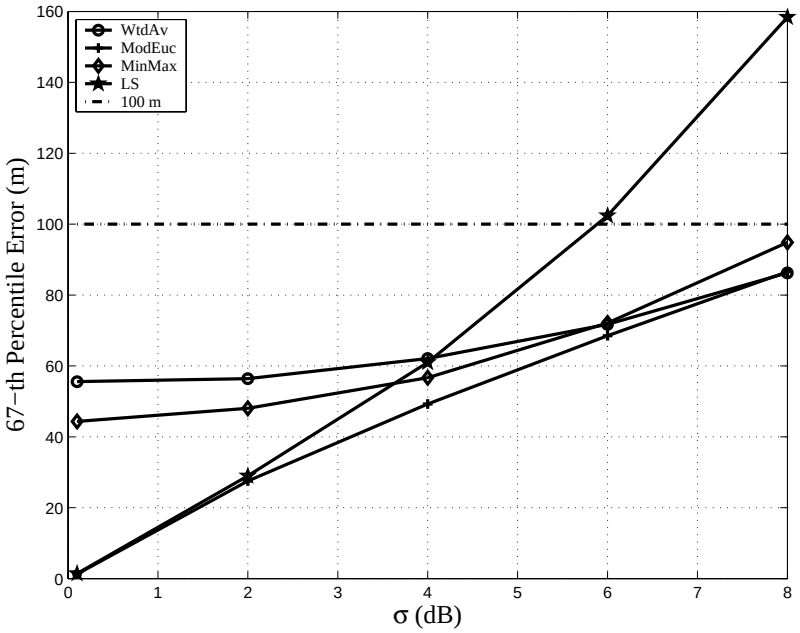


Figure 3.3: 67% error vs. σ ($N = 200$, $\gamma = 3.8$, $X_c = 80$ m, outdoor cell with a radius of 1000 m).

similar to that of MinMax, although the former does not require any *a priori* information about A and γ. Besides, we can see that $N = 200$ is large enough (for a 1-km radius) to find a scheme satisfying the FCC requirement over a wide range of σ. In the previous chapter, we found that 200 sensors also enable the system to obtain accurate estimates of outage probability.

Simulation results not presented here show that the estimation error of the algorithms decreases with increasing γ. For example, the $67th$ percentile errors of MinMax are 90 m and 140 m, respectively, for $\gamma = 3.8$ and 3, with $\sigma = 8$ dB, $X_c = 80$ m, and $N = 200$. This is because the distance estimate is less accurate with a smaller γ for the same shadow fading value.

3.4 Lower Bounds and Parameter Estimation

To better assess the above results, we first invoke the CRB, which is the theoretical lower limit on the variance of an unbiased estimator. We then describe the MMSE estimator, which meets the CRB if the path-loss model parameters are perfectly known; and we show how these parameters can be estimated using the N deployed sensors. Finally, we compare RMS errors corresponding to the CRB, the MMSE estimator and the four simple schemes when the parameter estimates are imperfect. We do this for a situation specifically devised to simplify analysis, i.e., for spatially white shadow fading ($X_c = 0$). To simplify computations as well, we further assume that N and the cell radius are reduced ($N = 20$ and the radius is 316 m), thereby keeping sensor density the same while significantly reducing the running time.

3.4.1 Cramer-Rao Bound (CRB)

The CRB is the lower bound for the *variance* of any *unbiased* estimator, and provides a benchmark for determining how far practical location algorithms are from ideal [32]. Following the derivation in [33], we compute the Fisher information matrix for the estimator of $\underline{\theta}$ with observation $\underline{z} = [PL_1, \cdots, PL_N]^T$, which is given by

$$\mathbf{F} = (\frac{10\gamma}{\sigma_s \log 10})^2 E_{\underline{\theta},\underline{L}_1,\cdots,\underline{L}_N}(\begin{bmatrix} \Sigma_i \frac{(\theta_1 - x_i)^2}{d_i^4} & \Sigma_i \frac{(\theta_1 - x_i)(\theta_2 - y_i)}{d_i^4} \\ \Sigma_i \frac{(\theta_1 - x_i)(\theta_2 - y_i)}{d_i^4} & \Sigma_i \frac{(\theta_2 - y_i)^2}{d_i^4} \end{bmatrix}). \tag{3.2}$$

For any unbiased estimator based on power measurements, we have

$$E\{||\underline{\theta} - \hat{\underline{\theta}}||^2\} \geq CRB = (\mathbf{F}^{-1})_{1,1} + (\mathbf{F}^{-1})_{2,2}. \tag{3.3}$$

Note that the MT and sensor locations $(\underline{\theta}, \underline{L}_1, \cdots, \underline{L}_N)$ are viewed here as random variables, instead of as nonrandom parameters as in [33]. This is because most existing estimators,

including the bias-corrected ML estimator in [34], are usually *biased* for a specific asymmetric MT-sensors topology. Meanwhile, most estimates of $\underline{\theta}$ become *unbiased*, if averaged over all possible topologies, because of the symmetry. Assuming that the MT and N sensors are uniformly distributed in the cell, we can use (3.2) to numerically calculate the CRB. If an efficient estimate exists, the CRB can be approached by the MMSE estimator [32], discussed next.

3.4.2 MMSE Estimator

For the channel model in Sector 2.2, the minimum-mean-square error (MMSE) estimate of $\underline{\theta}$ with observations of $\underline{z}$ and known sensor locations is given by

$$\hat{\theta}_i = \int_{-\infty}^{\infty} \theta_i p(\theta_i|\underline{z}) d\theta_i = \frac{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \theta_i p(\underline{z}|\underline{\theta}) p(\underline{\theta}) d\theta_1 d\theta_2}{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(\underline{z}|\underline{\theta}) p(\underline{\theta}) d\theta_1 d\theta_2}, \quad i = 1, 2, \tag{3.4}$$

where

$$p(\underline{z}|\underline{\theta}) = \frac{\exp(-\sum_{1\le i\le N} \frac{(PL_i - A + 10\gamma \log_{10}(d_0) - 5\gamma \log_{10}((\theta_1 - x_i)^2 + (\theta_2 - y_i)^2))^2}{2\sigma_s^2})}{(\sqrt{2\pi}\sigma_s)^N}, \tag{3.5}$$

and $p(\underline{\theta})$ has a value equal to the inverse of the cell area if $\underline{\theta}$ is inside the cell, and is zero otherwise. Implementation of the MMSE algorithm clearly requires knowledge of the channel model parameters, A, γ, and σ. We now discuss their estimation from finite measurements.

3.4.3 Estimating the Model Parameters

Among the four described schemes, only WtdAv can operate without knowledge of the model parameters, (2.1), which are known to vary from cell to cell. The other three rely on knowledge of A and γ, and Figs. 3.1-3.3 are based on perfect information. The MMSE estimator, moreover, requires knowledge of σ as well. It also requires an inordinate amount

of computation, (3.4), which is not readily accomplished in a real-time operation like localization. Quantifying this computational problem is beyond the scope of this work, but we *can* address the method, and impact, of parameter estimation.

We assume that the N sensors in a cell measure the $N(N-1)/2$ path-losses among them. The sensor network knows their locations, and thus the distance between each node pair. A scatter plot of path-loss versus distance, with $N(N-1)/2$ points, can therefore be constructed; and (A, γ, σ) can be estimated via least-squares fitting using (2.1). This was done for the case of the smaller cell with 20 sensors and spatially white shadow fading described above, and the results were used to compare RMS errors for various cases.

3.4.4 Numerical Results

Figure 3.4 compares RMS location error that include the four simple schemes, the MMSE estimator, and the CRB given by (3.3). We see that, with only 20 sensors, the errors in estimating (A, γ, σ) lead to but a minor degradation in performance. For larger cells with more sensors, the results should be even better. What penalizes the MMSE estimator is its computation-intensive nature.

Comparing the four simple schemes, with each other and with the MMSE estimator, we see that, over the typical range of σ ($\sigma > 4$ dB), there is little difference among WtdAv, MinMax and ModEuc. Further, the RMS errors for these schemes are above that for the MMSE estimator by a factor between 2 and 3. Choosing among approaches then comes down to balancing location accuracy against computation cost (running time, battery energy). The WtdAv scheme seems to provide the best tradeoff while meeting the FCC accuracy requirements under most conditions.

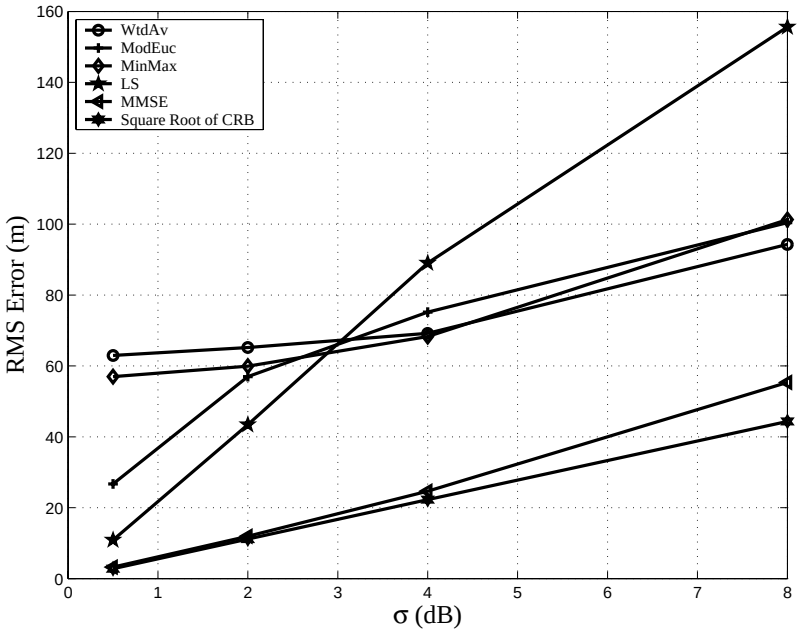


Figure 3.4: RMS error vs. σ, with channel parameters (A, γ and σ) estimated via least-squares fitting of $N(N-1)/2$ inter-sensor path-loss measurements ($N = 20$, $\gamma = 3.8$, $X_c = 0$, and outdoor cell with a radius of 316 m).

3.5 Conclusion

We have postulated a sensor-assisted localization approach for mobile terminals in cellular systems, where the power measurements obtained from $3 \sim 6$ sensors are used to locate the mobile station (MT). We have validated it by evaluating the performance of five algorithms in the system. Among them, a very simple scheme called WtdAv has performance similar to the MinMax algorithm, without requiring any channel parameter information. The MMSE estimator that ideally reaches the Cramer-Rao Bound, on the other hand, requires *a priori* knowledge of all the channel parameters and has prohibitive numerical complexity for real-time operation. Simulation results show that, in an outdoor cell with a radius of 1000 m, 200 sensors are sufficient for all these schemes to meet FCC E-911 requirements in most cases.

Although we have only discussed the localization of a single MT, our approach has great potential to work with multiple MTs. First, the interference between two MTs is small, unless they are too close to each other, because the localization of one MT solely depends on the measurements from the $3 \sim 6$ closest sensors. Moreover, Base Stations can roughly locate the MTs by sectoring, tracking records, etc; and then the sensors need only provide refinements of these localizations. Further effort is needed to more fully explore this approach [35].

Chapter 4

Channel-Based Spoofing Detection

In a typically rich scattering environment, the radio channel response decorrelates quite rapidly in space. Since the channel responses are difficult for others to predict and to spoof, we can call them "Fingerprint in the Ether", and use them to complement and enhance traditional authentication. To this end, we will consider a channel-based authentication scheme that exploits the channel estimation mechanism existing in most wireless systems. In this scheme, the channel response is used to discriminate among transmitters, e.g., to determine whether current and prior communication attempts are made by the same user (same channel response). This physical-layer authentication can help detect identity-based attacks, like spoofing attacks and Sybil attacks, with low additional system overhead. In this chapter, we analyze channel-based spoofing detection, considering practical issues, such as environmental changes, terminal mobility, channel estimation errors, and multiple antenna techniques. The performance of our physical-layer authentication scheme is analyzed using stochastic channel modeling, site-specific ray-tracing, and field tests using an 802.11 testbench.

4.1 Introduction

Due to the broadcast nature of wireless medium, intruders can access wireless networks without a physical connection. One serious consequence is that spoofing attacks (or masquerading attacks), where a malicious device claims to be a specific client by spoofing its MAC address, becomes possible. Spoofing attacks can seriously degrade network performance and facilitate many forms of security weakness. For instance, if attacking control messages/ management frames smartly, the intruder can corrupt services of legal clients [6, 36, 37].

It is desirable to conduct authentication at the lowest possible layer (i.e., physical layer). We note that in rich multipath environments typical of wireless scenarios, channel responses are *location-specific*. More specifically, channel responses decorrelate from one transmit-receive path to another, if the paths are separated by the order of an RF wavelength or more [38]. Hence it is difficult for an adversary to create or precisely model a waveform that is transmitted and received by entities that are more than a wavelength away from the adversary. This is the basis of "Fingerprints in the Ether", i.e., PHY-layer authentication for wireless networks [39–44].

Authentication is traditionally associated with the assurance that a communication comes from a specific entity [45]. Physical-layer authentication, however, is used to discriminate among different transmitters, and can be combined with a traditional handshake authentication process to completely identify an entity. If not specified otherwise, we assume that an entity's identity is obtained at the beginning of a transmission using traditional higher layer authentication mechanisms. Channel-based authentication is then used to ensure that all signals in both the handshake process and data transmission are actually from

the same transmitter. The cross-layer design of physical-layer authentication is discussed in Section 4.7.

4.2 Related Work

In commodity networks, such as 802.11 networks, it is easy for a device to alter its MAC address and claim to be another device by simply issuing an `ifconfig` command. This weakness is a serious threat, and there are numerous attacks, ranging from session hijacking [37] to attacks on access control lists [9], which are facilitated by the fact that an adversarial device may masquerade as another device.

In response, researchers have proposed using physical layer information to enhance wireless security. For example, spectral analysis has been used to identify the type of wireless network interface card (NIC), and thus to discriminate among users with different NICs [46]. A similar method, radio frequency fingerprinting, discriminates wireless devices according to the transient behavior of their transmitted signals [47]. For more general networks, the clock skew characteristic of devices has been viewed as a remote fingerprint of devices over the Internet [48]. In addition, the inherent variability in the construction of various digital devices has been used to detect intrusion [49].

More recently, the wireless channel has been explored as a new form of fingerprint for wireless security. The reciprocity and rich multipath of the radio channel has been used as a means to establish encryption keys [50, 51]. In [7], a practical scheme to discriminate among transmitters was proposed and identifies mobile devices by tracking measurements of signal strength from multiple access points.

Concurrent to these efforts, we have proposed a channel-based authentication scheme that exploits the spatial variability of channel frequency (or impulse) response to detect

spoofing attacks and Sybil attacks in wireless networks [39–44].

Another group of physical-layer authentication techniques have been proposed to detect identity-based attacks in wireless networks, exploiting the received signal strength (RSS) [7, 36, 52] and channel impulse response (CIR) [53]. We note that channel responses contain more location-specific information than RSS, and hence the channel response-based techniques can provide higher accuracy than those merely using RSS.

4.3 System & Channel Models

4.3.1 Problem Model

We shall borrow from the conventional terminology of the security community by introducing three different parties: Alice, Bob and Eve, which may be be thought of as wireless transmitters/receivers that are potentially located in spatially separated positions, as depicted in Fig. 4.1. Alice serves as the legitimate transmitter that initiates communication, while Bob serves as the intended receiver. Their nefarious adversary, Eve, serves as an active opponent who injects undesirable communications into the medium in the hopes of impersonating Alice.

Our security objective is to provide authentication between Alice and Bob, despite the presence of Eve. Authentication is traditionally associated with the assurance that a communication comes from a specific entity, while the objective of the channel-based authentication may be interpreted as follows: Since Eve, a potential adversary within range of Alice and Bob, is capable of injecting her own signals into the environment to impersonate Alice, it is desirable for Bob to have the ability to differentiate between legitimate signals from Alice and illegitimate signals from Eve. The physical-layer authentication provides Bob evidence that the signal he receives did, in fact, come from Alice.

To illustrate this, let us consider a simple transmitter identification protocol in Fig. 4.1, where Bob seeks to verify that Alice is the transmitter. Suppose that Alice probes the channel sufficiently frequently to assure temporal coherence between channel estimates and that, prior to Eve's arrival, Bob has estimated the Alice-Bob channel. Now, Eve wishes to convince Bob that she is Alice. Bob will require that each information-carrying transmission be accompanied by an authenticator signal. The channel and its effect on a transmitted signal between Alice and Bob is a result of the multipath environment.

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, while the second message, sent at $k+1$, is either a legal message from Alice or a spoofed 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: both Alice and Eve use $N_T \geq 1$ transmit antennas, while Bob uses $N_R \geq 1$ receive antennas. The antennas are placed in a way so that the channel paths of different antenna pairs are independent.

The distance from Bob to Alice (Eve) is denoted as d_A (d_E). We assume that the propagation environment may change, e.g., due to people walking by, and/or Alice moves in any direction with a velocity v. We note that our method is generic and our results can be easily extended to the case of mobility of all terminals. Finally, we allow the possibility that channel gain estimation may be corrupted by additive interference.

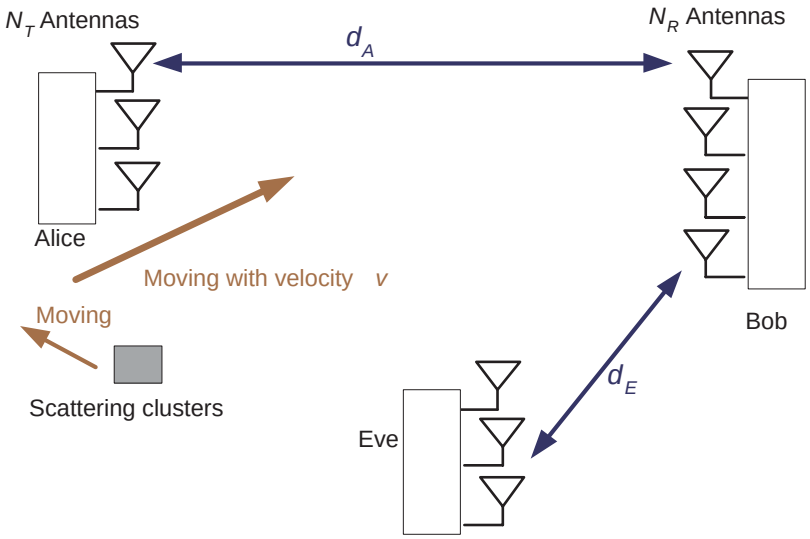


Figure 4.1: The multipath environment involving multiple scattering surfaces. The transmission from Alice with N_T antennas to Bob with N_R antennas, experiences different multipath effects than the transmission by the adversary, Eve. Bob has to discriminate between a legal message from Alice and the spoofing one from Eve. The distance between Alice (Eve) and Bob is denoted as d_A (d_E).

4.3.2 Channel Estimates

As we mentioned, the channel-based authentication scheme utilizes the rapid spatial decorrelation property of channel responses in multipath environments. Bob uses the received version of the authenticator signal to estimate the channel response, as in the existing channel estimation mechanisms in most wireless systems. More specifically, Bob first (at time k) measures and stores the frequency response of the channel connecting Alice with him, based on pilot or preamble symbols in the message. (The discussion can be easily extended to the case of the channel impulse response.)

The resulting channel vector contains M' independent channel samples. This assumption can be conveniently implemented in orthogonal frequency division multiplexing (OFDM) systems, where channel responses are measured at M' tones based on the pilots that are equally placed 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 over-sampled case where neighboring tones are correlated.

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.

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 Gaussian error component, $\underline{N}(k)$, to each channel gain estimate. This error is zero-mean, independent across paths and frequencies, and has a common variance given by

$$\sigma_N^2 = P_N / P_T, \tag{4.1}$$

where P_N is the average receiver noise power for each measured tone, and P_T is the transmitted power.

Another impairment is that due to the interference from other radio users. We can model the interference effect on channel estimation as contributing a random error component, $\underline{I}(k)$, to the true value of each measured channel gain. Again, we model these errors as zero-mean, Gaussian, independent across paths and frequencies, and having a common variance given by

$$\sigma_I^2 = P_I / P_T, \tag{4.2}$$

where P_I is the average received interference power for each measured tone. Thus we have

$$\underline{N} + \underline{I} \sim CN\left(\underline{0}, \left(\sigma_I^2 + \sigma_N^2\right)\mathbf{I}\right), \tag{4.3}$$

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

Combining these factors, the channel estimation vector at time k, $\underline{\hat{H}}(k)$, can be given by

$$\underline{\hat{H}}(k) = \underline{H}(k)e^{j\varphi(k)} + \underline{N}(k) + \underline{I}(k), \tag{4.4}$$

where $\underline{H}(k)$ is the "ideal" channel row 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 $k+1$.

4.3.3 Channel Gains

As noted, we assume in this section that the first message at time k is not spoofed, 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.,

$$\underline{H}_i(k) \sim CN\left(\underline{0}, \sigma_i^2 \mathbf{I}\right), \quad i = A, E, \tag{4.5}$$

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 [38]. We note that both Alice and Eve could be anywhere in the coverage region of Bob, and in practice, Eve cannot be close to Alice. If the terminals never move fast and the interval T is very short, we can assume

that Eve at time $k+1$ can not be close to Alice's previous location. Thus we assume that $\underline{H}_A(k)$ and $\underline{H}_E(k+1)$ are independent.

By (4.2), (4.4) and (4.5), we have

$$\begin{aligned}\hat{\underline{H}}_E(k+1) &= \underline{H}_E(k+1)e^{j\varphi(k+1)} + \underline{N}(k+1) + \underline{I}(k+1) \\ &\sim CN\left(\underline{0}, \left(\sigma_E^2 + \sigma_N^2 + \sigma_I^2\right)\mathbf{I}\right). \end{aligned} \tag{4.6}$$

Similarly,

$$\hat{\underline{H}}_A(k) \sim CN\left(\underline{0}, \left(\sigma_A^2 + \sigma_N^2 + \sigma_I^2\right)\mathbf{I}\right). \tag{4.7}$$

4.3.4 Channel Variations

Assuming a short enough interval T between successive transmissions, Alice at time $k+1$ is 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

$$\underline{H}_A(k+1) = a\underline{H}_A(k) + \underline{\Delta}(k), \tag{4.8}$$

where a is the correlation coefficient between channel gains spaced by T; and $\underline{\Delta}(k)$ is an M-dimensional vector in which each term is an i.i.d. zero-mean Gaussian process that is independent of $\underline{H}(k)$ and has a variance

$$\sigma_\Delta^2 = (1-a^2)\sigma_A^2. \tag{4.9}$$

Assuming that Alice moves with a speed of v, and using the Jakes model [38], we have

$$E\left[\underline{H}_A(k+1)\underline{H}_A^H(k)\right] = \sigma_A^2 J_0\left(2\pi v f_0 T/c\right)\mathbf{I}, \tag{4.10}$$

where c is the speed of light, f_0 is the carrier frequency, and J_0 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 $v \sim 0$, then it is clear that $a \sim 1$.

Finally, we consider the possibility that, even if Alice is stationary, there can be changes in the path gains due to movement of objects or people in the environment. We model this as a component added to the path gains for the static case, $\underline{H}_A(k)$. This added term is zero-mean, Gaussian, independent across paths and frequencies, and has a common variance σ_Δ^2. With this variation included, the channel time variation $\underline{\Delta}(k)$ in (4.8) can be modeled as the sum of two random, independent Gaussian terms, ϵ_1 and ϵ_2, due to the motion and the change in the environment [40], respectively, i.e.,

$$\underline{\Delta}(k) = \epsilon_1 + \epsilon_2 \sim CN\left(\underline{0}, \left(\sigma_A^2(1-a^2) + \sigma_\Delta^2\right)\mathbf{I}\right). \tag{4.11}$$

By (4.2)-(4.5), (4.8), and (4.11), we have

$$\underline{\hat{H}}_A(k+1) \sim CN\left(a\underline{\hat{H}}(k)e^{j\phi_0}, \varrho^2\mathbf{I}\right), \tag{4.12}$$

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

$$\varrho^2 = \left(1+a^2\right)\left(\sigma_N^2 + \sigma_I^2\right) + \left(1-a^2\right)\sigma_A^2 + \sigma_\Delta^2. \tag{4.13}$$

4.4 Channel-Based Spoofing Detection

In order to detect spoofing attacks, Bob compares the two resulting channel vectors: If the two channel estimates are "close" to each other, then Bob will conclude that the source of the second message is still Alice. If the channel estimates are not similar, then Bob should conclude that the second source is likely a would-be intruder, e.g., Eve.

The channel-based spoofing detector utilizes a simple hypothesis test:

$$\mathcal{H}_0 : \underline{H}(k+1) = \underline{H}_A(k+1), \tag{4.14}$$

$$\mathcal{H}_1 : \underline{H}(k+1) = \underline{H}_E(k+1). \tag{4.15}$$

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.

4.4.1 Generalized Likelihood Ratio Test (GLRT)

The generalized likelihood ratio test for the hypothesis (4.14) and (4.15) in the generalized system model given by the previous section can be written as

$$L_g = \frac{||\hat{\underline{H}}(k+1) - a\hat{\underline{H}}(k)e^{j\phi}||^2}{\varrho^2} - \frac{||\hat{\underline{H}}(k+1)||^2}{\sigma_E^2 + \sigma_N^2 + \sigma_I^2} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta', \tag{4.16}$$

where $||A||$ denotes the Frobenius norm of the matrix A, ϱ^2 is given by (4.13), $\phi = Arg(\hat{\underline{H}}(k+1)\hat{\underline{H}}(k)^H)$, and the superscript ^{H} represents Hermitian transformation.

Proof: Since the phase rotation, ϕ, is usually unknown, the generalized likelihood ratio test [54] for the system model can be written as a function of $\hat{\underline{H}}(k+1)$, i.e.,

$$\Lambda_g = \frac{Pr\left(\hat{\underline{H}}(k+1); \mathcal{H}_1\right)}{\max_{\phi_0} Pr\left(\hat{\underline{H}}(k+1); \phi_0, a, \mathcal{H}_0, \hat{\underline{H}}(k)\right)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_1. \tag{4.17}$$

By (4.6), (4.12), (4.14), and (4.15), we can rewrite (4.17) as

$$L_g = \frac{||\hat{\underline{H}}(k+1) - a\hat{\underline{H}}(k)e^{j\phi}||^2}{\varrho^2} - \frac{||\hat{\underline{H}}(k+1)||^2}{\sigma_E^2 + \sigma_N^2 + \sigma_I^2} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta', \tag{4.18}$$

where

$$\begin{aligned}
\phi &= \max_{\phi_0} Pr\left(\hat{\underline{H}}(k+1); \phi_0, a, \mathcal{H}_0, \hat{\underline{H}}(k)\right) \\
&= \arg\min_{\phi_0} ||\hat{\underline{H}}(k+1) - a\hat{\underline{H}}(k)\exp(j\phi_0)|| \\
&= Arg\left(\hat{\underline{H}}(k+1)\hat{\underline{H}}(k)^H\right).
\end{aligned} \tag{4.19}$$

■

The exponent term is introduced to adjust for the phase drift in the channel estimation. Otherwise, the messages belonging to Alice are likely to be mistaken for spoofing messages. The rejection region is defined as those cases where the test statistic falls above the test threshold, η'.

It is clear in (4.16) that the GLRT requires *a priori* knowledge of the channel parameters, such as σ_N, σ_I, σ_E, a, and σ_Δ. These parameters can be obtained via training, or from field measurements in a similar scenario before the start of the test.

4.4.2 Test with Unknown Channel Parameters

In practice, wireless systems are not always able to obtain the channel parameters in (4.16). 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 (4.16) can be simplified into a more practical test,

$$L = ||\hat{\underline{H}}(k+1) - a\hat{\underline{H}}(k)e^{j\phi}||^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta, \tag{4.20}$$

where the test threshold η usually differs from η' in (4.16), and a can be estimated by $J_0(2\pi v f_0 T/c)$. If the terminal velocity v is unknown at the receiver, we use $a = 1$ by assuming a very slow terminal velocity.

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, (4.20) can be further simplified into

$$L = \left\| \hat{\underline{H}}(k+1) - \frac{\hat{\underline{H}}^H(k)\hat{\underline{H}}(k+1)}{|\hat{\underline{H}}^H(k)\hat{\underline{H}}(k+1)|}\hat{\underline{H}}(k) \right\|^2, \tag{4.21}$$

indicating small computational overhead. For convenience of analysis, the test statistic L sometimes is normalized with some parameter, such as σ_N^2 [39, 40, 42].

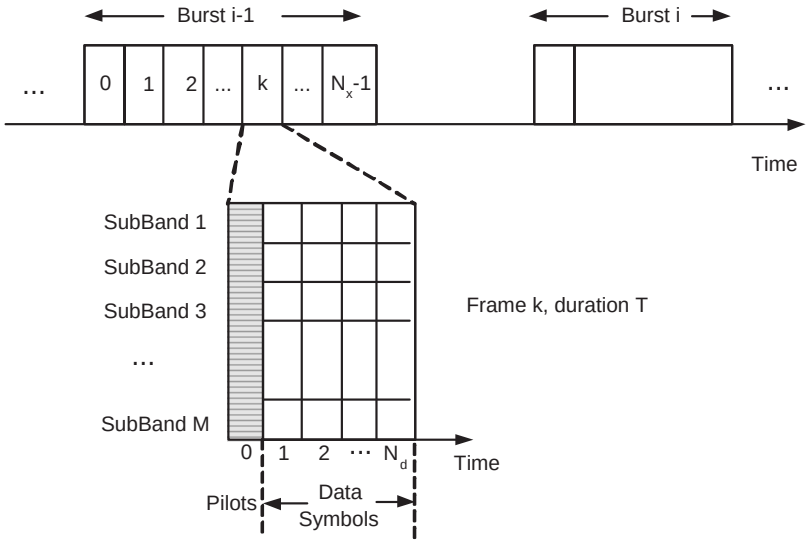


Figure 4.2: Frame structure of the transmission from Alice to Bob. Each data burst consists of an arbitrary number of frames, while each frame has one pilot and N_d data symbols on each of M subbands. Frame 0 in each data burst contains the channel response value in the previous burst as a key for the inter-burst authentication. Bob uses the intra-burst authentication method in the following frames to authenticate Alice, and saves at least one frequency response as the key for the next burst.

4.4.3 Implementation Issues

Although our scheme can be implemented in many wireless systems, we shall take orthogonal frequency division multiplexing (OFDM) systems as our example. Suppose Alice sends a signal to Bob with the frame structure shown in Fig. 4.2, where the whole session consists of several data bursts. Each burst has N_x frames (N_x may vary with the burst), while each frame, with M frequency subbands and duration T, consists of N_d data symbols and one pilot in each subband. The number of pilots in the first symbol can, in fact, be less than the number of subbands, with the rest used for data. For concreteness, however, we assume initially that all subbands in the first symbol are used for pilots.

As shown in Fig. 4.3, Bob uses the pilots for channel estimation, obtaining test vectors $\underline{\hat{H}}[k]$, where k is the frame index. The frame duration T is assumed to be small enough to make the displacement of the transmitter (Alice) per frame much smaller than the channel

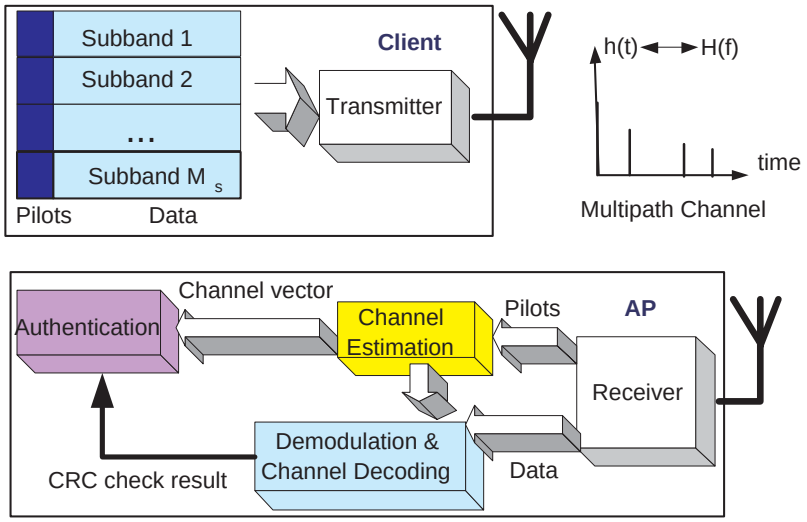


Figure 4.3: Implementation of spoofing detector in OFDM systems. Each frame with M frequency subbands, consists of one pilot and several data symbols in each subband.

decorrelation distance (i.e., $r = vT \ll \lambda/2$). Thus, two consecutive channel responses are highly correlated.

Terminal mobility may force the self-decorrelation of Alice's channel with respect to itself. Hence we must employ a different strategy to bridge the gap between bursts of communications. To accomplish this, an improved process consists of two consecutive parts: an inter-burst authentication phase and an intra-burst authentication phase.

The intra-burst authentication happens within a data burst, after the first frame passes the inter-burst authentication process. For any frame index $k > 1$, Bob is assumed to obtain the Alice-Bob channel gain in the previous frame, $\underline{\hat{H}}_A[k]$, and the observation of the current channel gain, $\underline{\hat{H}}[k+1]$. The GLRT, L_g, or the test of L, can be used to determine whether the current transmitter is still Alice.

The inter-burst authentication is carried out using the first frame of each data burst to determine whether the current transmitter is still Alice. At the outset of this protocol, in order for Bob to get an initial channel estimate for Alice, it is necessary to employ a higher-layer authentication protocol to bootstrap the association between Alice and and a

corresponding channel response. However, this is a one-time step, and generally the inter-burst process will focus on authenticating a subsequent data burst given that a prior data burst has been verified.

Thus we assume that Bob has an estimate of the Alice-Bob channel response of a particular frame in the previous data burst, which we shall denote as $\underline{\hat{H}}_A[-1]$. The time interval between two bursts may be so large that Alice has moved a significant distance. Thus the channel response of the first frame in the current burst, $\underline{\hat{H}}_A[0]$, may be totally uncorrelated with $\underline{\hat{H}}_A[-1]$.

To solve this problem, we assume that both Alice and Bob save at least one channel response in each data burst as the key in the authentication process for the next successive burst. Alice may obtain this $\underline{\hat{H}}_A[-1]$ either by feedback from Bob, or by measurement of the reverse link pilots in a time division duplexing (TDD) system. In the first frame of each burst, Alice sends the saved $\underline{\hat{H}}_A[-1]$ from the last burst to Bob. If it matches with Bob's version, Bob will assume it is from Alice. The channel response $\underline{\hat{H}}_A[-1]$ is not readily predicted by Eve. Thus she will fail the inter-burst authentication with high probability. We will present in Section 4.7 a double-layer authentication protocol to integrate the channel-based authentication scheme in wireless systems assuming a more generalized transmission pattern.

4.4.4 RLS Adaptive Filter-Based Test

We now explore an alternative hypothesis test, where M sets of linear least-squares adaptive filters are used independently to estimate the channel response for the M subbands. For the convenience of notion, we focus on the m-th subband, and ignore the frequency index m unless necessary.

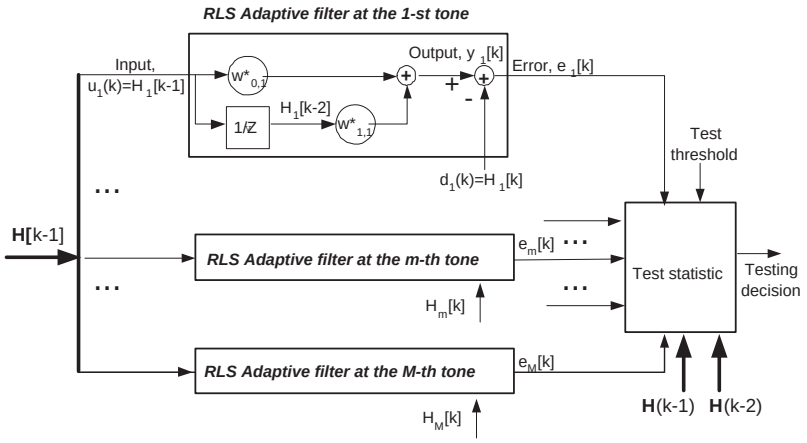


Figure 4.4: Illustration of the RLS adaptive filter-based spoofing detection.

As shown in Fig. 4.4, the estimated channel response at time k, which is the output of the m-th adaptive linear filter with order l, can be written as

$$y[k] = \sum_{l=0}^{l-1} w_n^* u(k-n), \tag{4.22}$$

where $u(k)$ is the input of the adaptive filter at time k, and w_n is the n-th tap weight of the filter, which can be determined using various adaptive algorithms, like the recursive least-squares (RLS) algorithm [55].

If it is Alice transmitting during the time interval $[k-L, k]$, the filter inputs are $\underline{\hat{H}}_A[k-L], \cdots, \underline{\hat{H}}_A[k-1]$, and the estimation error is $\underline{e}[k] = \underline{\hat{H}}_A[k] - \underline{y}[k]$. Because of the strong correlation of the inputs $\underline{\hat{H}}_A[k-L], \cdots, \underline{\hat{H}}_A[k]$, the ensemble-averaged squared error of the channel estimation filter is usually quite small.

If, on the other hand, Eve comes in at time k, due to the spatial variability of the channel response, the estimation error,

$$e_m[k] = \hat{H}_{E,m}[k] - \sum_{n=0}^{l-1} w_n^* \hat{H}_{A,m}[k-n-1], \tag{4.23}$$

is very likely to jump to a much larger value.

Therefore, we build another test statistic L_R, using M parallel adaptive channel estimators. The null hypothesis $\mathcal{H}_0$ is accepted if the normalized squared sum of estimation error from these filters is less than a certain threshold η_R; otherwise, the alternative hypothesis is chosen. Thus

$$L_R = \frac{||\underline{e}[k]||^2}{\sum_{n=0}^{l-1} ||\underline{u}[k-n]||^2/l} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_R. \tag{4.24}$$

We normalize the estimation error to make η_R easier to determine. It does not have a closed-form expression but can be obtained through simulations.

This test can be carried out only after the successful authentication of at least l frames, and even though the RLS algorithm converges fast, it still takes approximately $2l$ frames [55]. Since we have to take data after the algorithm converges, we usually choose $k > 3l$ in Eq. (4.24). Thus this method has larger system overhead ($3l$ frames) than the previous tests, L and L_g, (1 frame), as well as greater implementation complexity.

The use of RLS estimators in this context may not be practical or cost-effective, but the results we will present for this case are instructive. It is shown in [42] that, even under the most favorable assumptions (RLS estimation), using least-squares adaptive filtering is not measurably superior to using the tests, L_g or L.

4.5 Performance Evaluation based on Stochastic Channel Modeling

In order to evaluate the spoofing detection performance of the schemes, L_g and L, we consider the *false alarm rate* (or Type I error), α, the probability that the test declares Alice as Eve by mistake; and the *miss detection rate* (or Type II error), β, the probability

that the test misses the detection of Eve. These metrics are defined, respectively, by

$$\alpha = Pr(L > \eta|\mathcal{H}_0), \tag{4.25}$$

$$\beta = Pr(L \leq \eta|\mathcal{H}_1), \tag{4.26}$$

where the probabilities are taken over all channel vectors and measurement errors. The test may be actually L_g or L_R, and for convenience, we only use L as an example here.

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 [54]. Before the test, Alice first sends a number of training messages, based on which Bob computes α for several η, via (4.25). 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 term in (4.10). One is the signal-to-(interference-plus-noise) ratio (SINR) of the channel estimates for Alice, defined by

$$\rho = \frac{\sigma_A^2}{\sigma_I^2 + \sigma_N^2}. \tag{4.27}$$

We see that ρ increases with transmit power, since the estimation noise variance, σ_N^2, varies inversely with P_T. Another key parameter is the ratio of the locally averaged path gains for Alice and Eve,

$$\kappa = \sigma_E^2/\sigma_A^2. \tag{4.28}$$

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,

$$b = \sigma_{\Delta}^2/\sigma_A^2. \tag{4.29}$$

4.5.1 Performance Bound

The analysis of the performance of the test L can be greatly simplified if we assume zero phase drift, $\phi = 0$, whereupon (4.20) can be approximated as

$$L \approx ||\hat{\underline{H}}(k+1) - a\hat{\underline{H}}(k)||^2. \tag{4.30}$$

Since $L \leq ||\hat{\underline{H}}(k+1) - a\hat{\underline{H}}(k)||^2$, the assumption $\phi = 0$ generally increases the false alarm rate α, (4.25), and decreases the miss rate β, (4.26). Consequently, this simplified approach upper bounds α, and lower bounds β.

When the null hypothesis $\mathcal{H}_0$ is true, both channel samples are from Alice. By (4.2)-(4.5), (4.8), and (4.10), we can approximate $\hat{\underline{H}}_A(k+1) - a\hat{\underline{H}}(k)$ as a vector with M i.i.d. complex Gaussian elements. Each element has zero mean and a variance given by

$$Var[\hat{H}_{A,m}(k+1) - a\hat{H}_{A,m}(k)] = (1+a^2)(\sigma_I^2 + \sigma_N^2) + \sigma_{\Delta}^2 + (1-a^2)\sigma_A^2. \tag{4.31}$$

Thus, L under $\mathcal{H}_0$ is chi-square distributed with order $2M$ [56]. Given a test threshold η, the false alarm rate can be written as

$$\begin{aligned}
\alpha &= 1 - P[L \leq \eta | \mathcal{H}_0] \\
&= 1 - F_{\chi^2_{2M}}\left(\frac{2\eta}{(1+a^2)(\sigma_I^2 + \sigma_N^2) + \sigma_{\Delta}^2 + (1-a^2)\sigma_A^2}\right) \\
&= 1 - F_{\chi^2_{2M}}\left(\frac{2\eta/\sigma_A^2}{(1+a^2)/\rho + 1 - a^2 + b}\right),
\end{aligned} \tag{4.32}$$

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

σ_E. In addition, this equation also provides the test threshold for a given α:

$$\eta = 0.5\sigma_A^2 \left(\frac{1+a^2}{\rho} + 1 - a^2 + b \right) F^{-1}_{\chi^2_{2M}}(1-\alpha), \tag{4.33}$$

where F^{-1} 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, the channel vectors, $\underline{\hat{H}}(k+1)$ and $\underline{\hat{H}}(k)$, are independent. By (4.6) and (4.7), we have

$$\hat{H}_m(k+1) - a\hat{H}_m(k) \sim CN\left(0, \left(\left(1+a^2\right)\left(\sigma_I^2 + \sigma_N^2\right) + a^2\sigma_A^2 + \sigma_E^2\right)\right). \tag{4.34}$$

Hence the test statistic L is also chi-square distributed with order $2M$, and the miss rate is given by

$$\begin{aligned} \beta &= F_{\chi^2_{2M}}\left(\frac{2\eta}{\left(1+a^2\right)\left(\sigma_I^2+\sigma_N^2\right) + a^2\sigma_A^2 + \sigma_E^2} \right) \\ &= F_{\chi^2_{2M}}\left(\frac{2\eta/\sigma_A^2}{\left(1+a^2\right)/\rho + a^2 + \kappa} \right). \end{aligned} \tag{4.35}$$

As we see from (4.32) and (4.35), 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.

4.5.2 Simulation Method

We perform Monte Carlo simulations to provide the receiver operating characteristic (ROC) curves for the GLRT (L_g) and the more practical test (L), in a wide range of scenarios. ROC curves are widely used in the performance evaluation of spoofing detection, showing how the detection rate $P_d = 1 - \beta$ changes with the false alarm rate, α. The value of the test threshold, η (or η'), determines the working point on the ROC curve. Accordingly,

in our computations, we make the simplifying assumption (with no loss in generality) that $\sigma_A^2 = 1$.

For each scenario, we first use (4.6) and (4.7) to generate two channel vectors, $\underline{\hat{H}}_E(k+1)$ and $\underline{\hat{H}}_A(k)$. Then we obtain $\underline{\hat{H}}_A(k+1)$ via (4.12) and $\underline{\hat{H}}_A(k)$. Based on these M-element vectors, we calculate the test statistics of L_g via (4.16) and L via (4.20), for both $\mathcal{H}_0$ and $\mathcal{H}_1$. We repeat the experiment $N_s = 20,000$ times.

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

$$\alpha = \frac{1}{N_s} \sum_{k=1}^{N_s} I\left(L\left(\underline{\hat{H}}_A(k), \underline{\hat{H}}_A(k+1)\right) > \eta\right), \tag{4.36}$$

$$\beta = \frac{1}{N_s} \sum_{k=1}^{N_s} I\left(L\left(\underline{\hat{H}}_A(k), \underline{\hat{H}}_E(k+1)\right) \leq \eta\right), \tag{4.37}$$

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

path-loss Model: The emulation of $\underline{\hat{H}}_A(k)$ and $\underline{\hat{H}}_E(k+1)$ with (4.7) and (4.6) requires information about σ_A^2 and σ_E^2. We can model them as the ratio version of the generic dB formula for path-loss, [15], i.e.,

$$\sigma_i^2 = \Omega d_i^{-\gamma} S_i, \quad i = A, E, \tag{4.38}$$

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,

$$K = 10\gamma \log(d_A/d_E) + (s_E - s_A), \ (\kappa \text{ in dB}), \tag{4.39}$$

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 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. The PDF of K in this special case is a double-sided exponential given by

$$f_K(x) = \frac{\ln(10)}{10\gamma} 10^{-|x|/5\gamma}. \tag{4.40}$$

Proof: Assume that Alice and Eve are randomly uniformly distributed in a circular area centered on Bob with radius R. Denote $D_1 = d_A^2$ and $D_2 = d_E^2$, and we 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 (4.39), 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

$$\begin{aligned} F_K(x) &= Pr(K \le x) = Pr(5\gamma \log(D_2/D_1) \le x) \\ &= \int_{-\infty}^{\infty} Pr(D_1 = x_1) Pr(5\gamma \log(D_2/x_1) \le x) dx_1 \\ &= \int_0^{R^2} \frac{1}{R^2} Pr(D_2 \le x_1 10^{x/5\gamma}) dx_1 \\ &= \int_0^{R^2} \frac{1}{R^2} (x_1 10^{x/5\gamma})/R^2 dx_1 = 0.5 \cdot 10^{x/5\gamma} \end{aligned} \tag{4.41}$$

By symmetry about $x = 0$, we have the PDF of K as

$$f_K(x) = dF_K(x)/dx = \frac{\ln(10)}{10\gamma} 10^{-|x|/5\gamma} \tag{4.42}$$

■

4.5.3 Numerical Results

We first present in Fig. 4.5 the ROC curves of L_g and L with a parameter κ. The worst case for L_g is at $\kappa = 0$ dB. The corresponding performance can be $\alpha = \beta = 4\%$, when there are $M = 4$ independent channel samples in each message, the SINR of the channel estimation is $\rho = 20$ dB, and the (relative) channel time variation power is $b = 0.2$. When the absolute value (in dB) of κ is very large, i.e., ± 100 dB, the system achieves near-perfect performance.

As for L, negative dB values of κ yield worse results than positive ones, indicating that a "smart" Eve should stay in an area wherein $\kappa < 0$. As an example, let us fix the locations of Alice and Bob, and let Eve depart from a near-Bob location. The performance of L first degrades, until Eve reaches a location where $\kappa \approx -10$ dB. The performance slowly improves thereafter, and converges to an asymptotic value as κ goes to $-\infty$ dB. This value is still worse than for $\kappa \geq 0$ dB. The worst case, $\kappa \approx -10$ dB, corresponds to $\alpha \approx \beta \approx 10\%$.

Figure 4.6 presents the performance under various combinations of ρ, M, and b, given $\kappa = 0$ dB (worst case for L_g). It shows that both L_g and L have better detection performance, under a higher ρ, larger M, or smaller b. It is clear that L_g provides better detection performance than L, and the performance gain is more significant with less detection resources, i.e., for lower ρ and smaller M, and also for larger b.

Figure 4.6 (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 narrow band 2×2 MIMO system. Given $\alpha = 5\%$, we have $\beta \approx 2\%$ for L_g and $\beta \approx 4\%$ for L. Moreover, the performance gain is not significant if ρ increases from 20 dB.

In Fig. 4.6 (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, i.e., with $\alpha = 1\%$ and $\beta < 0.3\%$.

Figure 4.6 (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 tests have $\alpha = \beta \approx 2.5\%$, and $\alpha = \beta \approx 7.5\%$, respectively, when $b = 0.5$, $M = 8$, and $\rho = 20$ dB.

Figure 4.15 presents the performance of L_g and L in a scenario with both terminal mobility and environmental change, as functions of the velocity of Alice, v, for $b = 0.1$, $M = 8$, $\rho = 20$ dB, and carrier wavelength $\lambda = 6$ cm. The figure also shows the bounds given by (4.32) and (4.35), which upper bound α and lower bound β by assuming $\phi = 0$. It is seen that the bound can be used to approximately describe the performance of L_g, or to upper bound that of L. It is also shown that the performance degrades, of course, as Alice moves faster. These results can easily be generalized in terms of the dimensionless parameter vT/λ. For example, the three mobile speeds, $v = .05$, .07, and .09 meter per second (mps) translate, respectively, to vT/λ=0.0833, 0.1167, and 0.15.

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, we can get a near-analytical solution for the average β as a function of α, using (4.40) for the PDF of κ. The results, Fig. 4.8, cover a wide practical range of the path-loss exponent, γ.

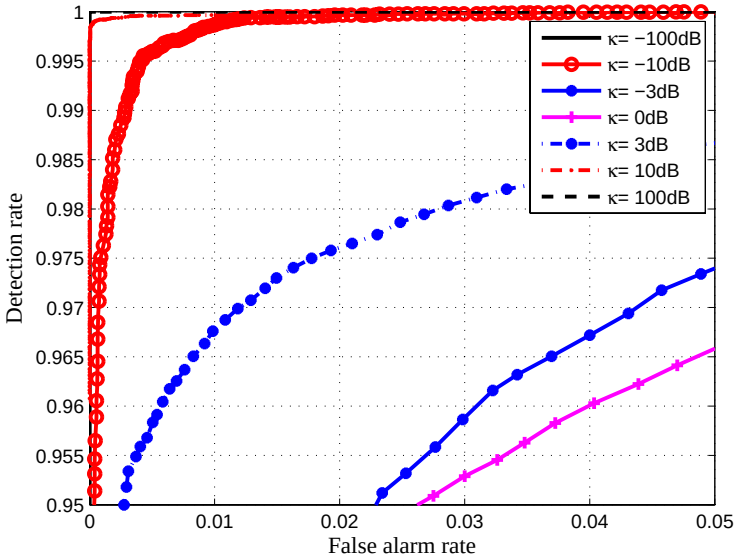
The efficacy of using L, for any likely value of γ, is confirmed. For example, $\bar{\alpha} \approx 2\%$ and $\bar{\beta} = 1\%$, when $M = 8$, $\rho = 20$ dB, and $b = 0.2$, for $\gamma \in [2, 5]$.

4.6 Performance Analysis based on Site-Specific Ray Tracing

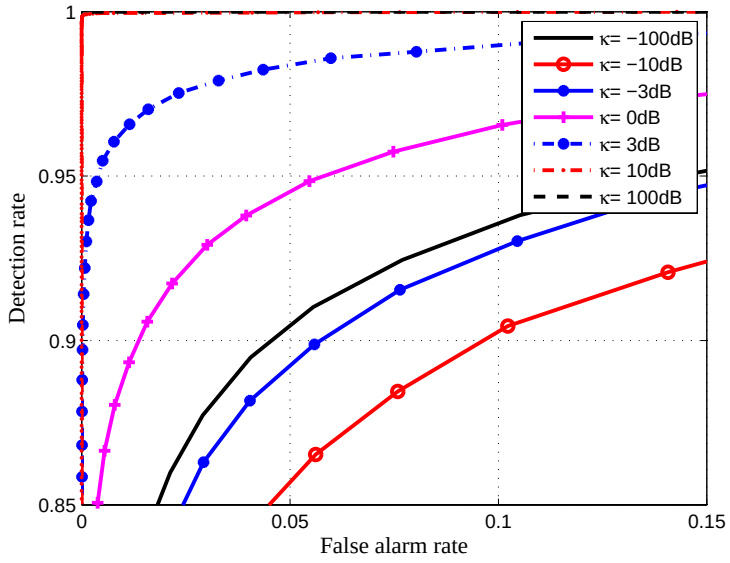
We now analyze the performance of the proposed channel-based spoofing detection for given typical indoor environments. It is necessary to model not only "typical" channel responses, but the spatial variability of these responses for the site. Only in that way can we discern the success in detecting would-be intruders like Eve. To that end, we make use of a 3-D propagation prediction software package developed by Bell Laboratories, called the Wireless System Engineering (WiSE) tool [57].

The WiSE 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-dimensional plan of a specific building, including walls, floors, ceilings and their material properties. With this information, WiSE can predict the rays at any receiver from any transmitter, including their amplitudes, phases and delays. From this, it is straightforward to construct the transmitter-receiver frequency response over any specified interval.

We have done this for one particular office building, for which a top view of the first floor is shown in Fig. 4.9. This floor of this building is 120 meters long, 14 meters wide and 4 meters high. For each Alice-Eve pair, (1) WiSE was used to generate the Alice-Bob and Eve-Bob channel responses ($\underline{H}_A$ and $\underline{H}_E$); and (2) we performed the Neyman-Pearson test to detect Eve. More specifically, we calculated the test statistics, such as L by (4.20) and L_R by (4.24), and used them to compute the miss detection rate, β, for a specified false alarm rate, α. The set of all β-values in a specific scenario were used to compute

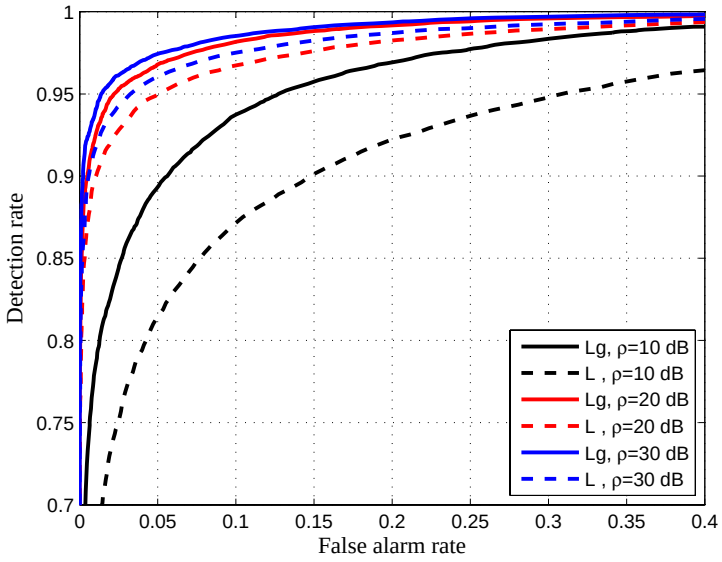


(a) L_g

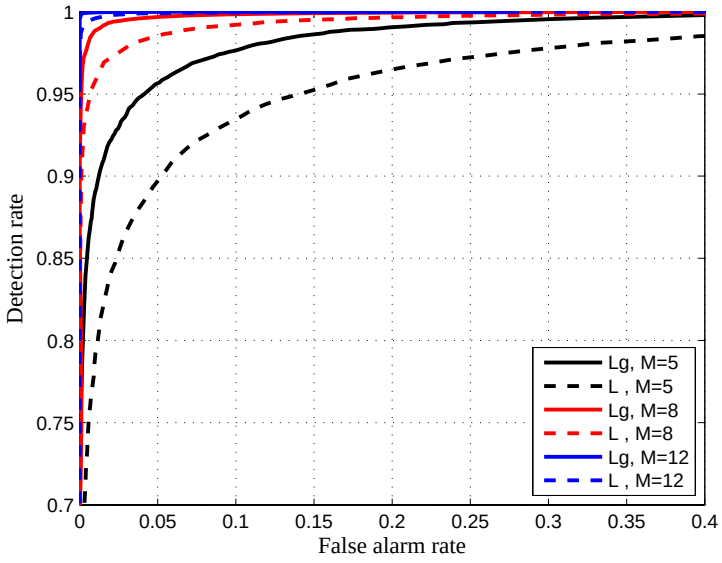


(b) L

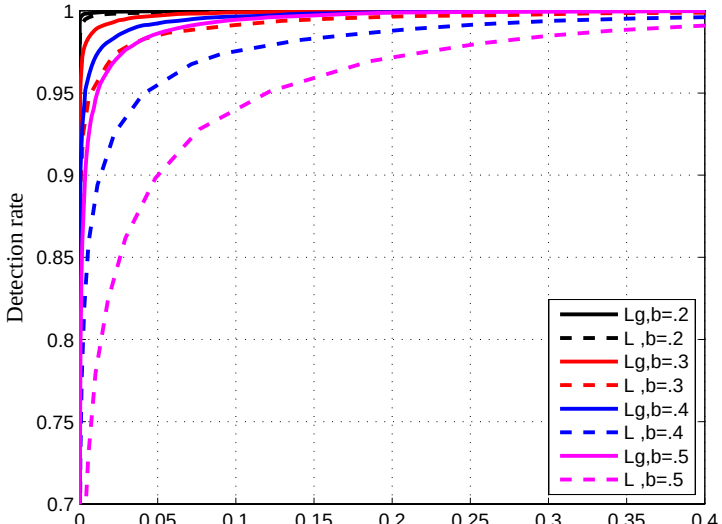
Figure 4.5: Receiver operating characteristic (ROC) of the channel-based spoofing detectors, including the GLRT L_g, (4.16), and a simplified version, L, (4.20), as a function of $\kappa(=\sigma_E^2/\sigma_A^2)$, with $M = 4$ independent channel samples in each message, SINR of the channel estimation $\rho = 20$ dB, zero terminal speed ($v = 0$), and the channel's relative time variation power, $b = 0.2$.



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



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



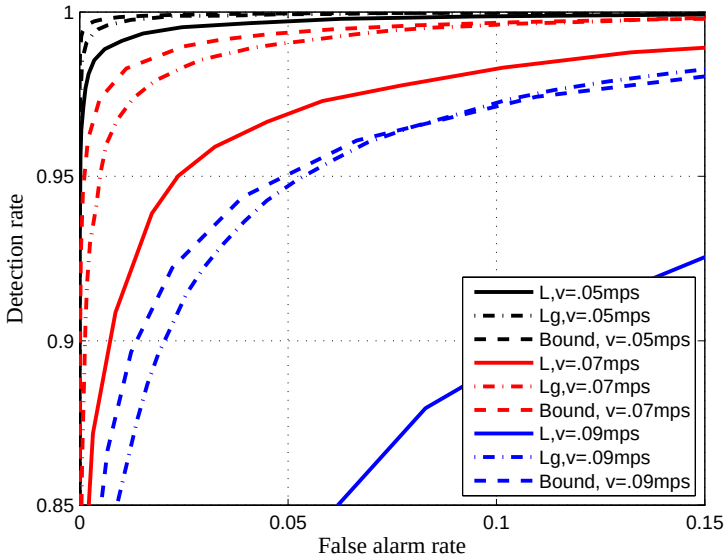


Figure 4.7: ROC of the spoofing detector, L, (4.20), where Alice moves with a speed of v, $b = 0.1$, $T = 100$ ms, $\rho = 20$ dB, carrier wavelength $\lambda = 6$ cm, $M = 8$ and $\kappa = 1$.

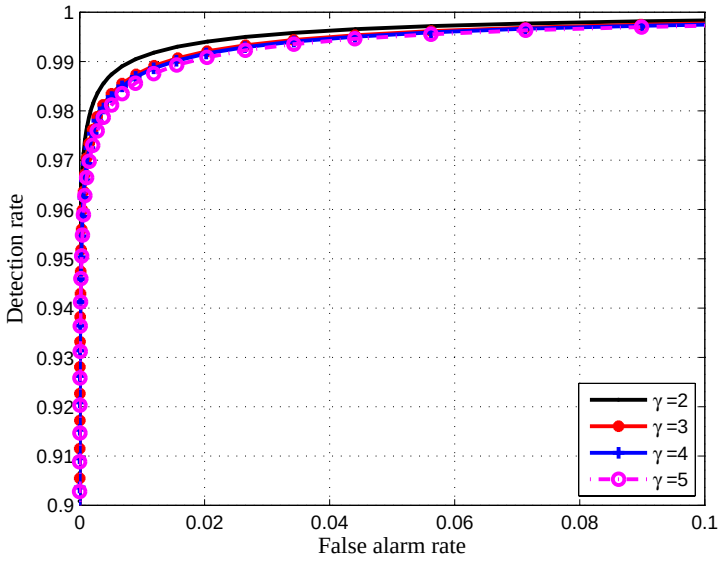


Figure 4.8: ROC of the spoofing detector, L, (4.20), averaged over all realizations of κ, when Alice and Eve are randomly placed in the circle area centered on Bob, with $M = 8$ independent channel samples in each message, SINR of the channel estimation $\rho = 20$ dB, $v = 0$ and $b = 0.2$.

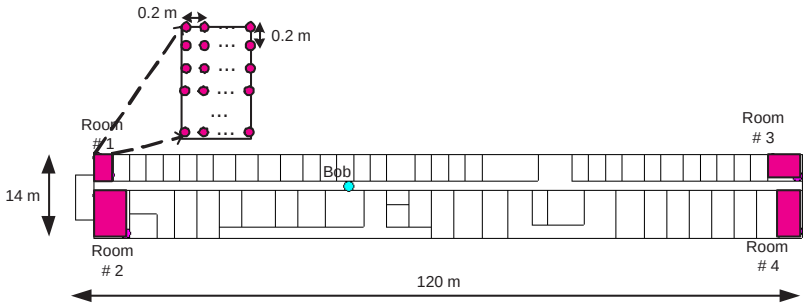


Figure 4.9: System topology assumed in the simulations. Bob is located at 3-m height near the center of a 120 m × 14 m × 4 m office building. Alice and Eve are located on dense grids at a height of 2 m. The sizes of the grids are $N_s = 150$, 713, 315, and 348, respectively, for Room # 1, 2, 3 and 4.

a site-specific mean, $\overline{\beta}$, for each of several selected combinations of scenarios and system parameters, such as bandwidth (W), number of tones (M) and transmit power (P_T).

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

4.6.1 Static Channel Test Scenario

We first performed a test for a static channel in this typical building. As shown in Fig. 4.9, we placed Bob in the hallway (the filled-in circle) at a height of 3 m. For the positions of Alice and Eve, we considered four rooms at the extremities of the building (shown shaded). For each room, we assumed Alice and Eve both transmitted from a height of 2 m, each of them being anywhere on a uniform horizontal grid of points with 0.2-meter separations. With N_s grid points in a room, there were $N_s(N_s-1)/2$ possible pairs of Alice-Eve positions. For Rooms 1, 2, 3 and 4, the numbers of grid points were $N_s = 150$, 713, 315 and 348,

respectively.

In the simulations, we set $\alpha = 0.01$, $f_0 = 5$ GHz, $N_F = 10$ (10 dB noise figure), $\kappa\mathcal{T} = 10^{-17.4}$ mW/Hz, $b_N = 2.5$ MHz and $P_T = 1$, 10 and 100 mW, respectively. We obtain a miss rate β for each Alice-Eve pair, and then calculate the mean value $\overline{\beta}$ for each room with $M = 1 \sim 10$ and $W = 20 \sim 500$ MHz. The per tone SNR in the channel estimation ranges from 5 dB to 26 dB, with a median value of 20 dB, given $P_T = 10$ mW and $M = 5$.

The results in Fig. 4.10 verify the utility of our algorithm and show that, if $P_T = 100$ mW, the average miss rate is usually below 0.05, even at Room 1, a corner of the building.

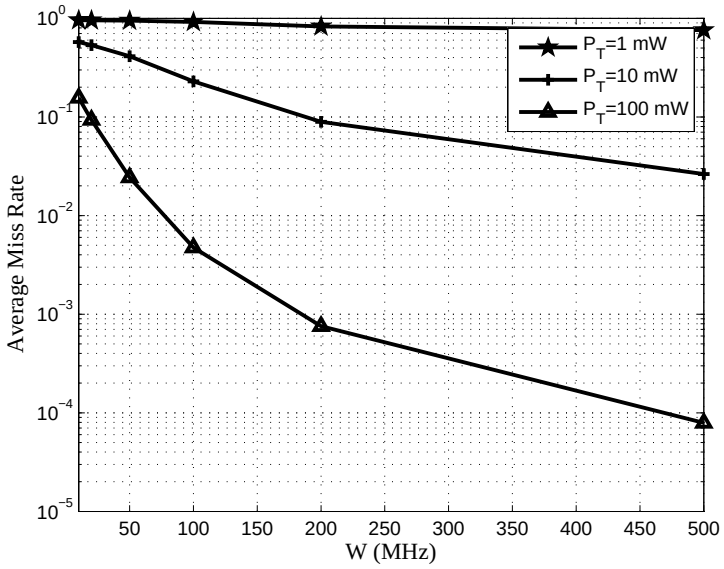
4.6.2 Test Scenario with Terminal Mobility

We next consider the mobility of the legal transmitter Alice, and multiple possible positions of Eve. For our experiment, we randomly and uniformly select N_A in-bulding locations for Alice, each corresponding to her position at the start (i.e., in Frame 0) of one of N_A data bursts. As shown in Fig. 4.11, for each such location, we consider a set of N_E possible locations for Eve, which are also randomly uniformly selected. We assume that each burst has the same number of frames, N_x.

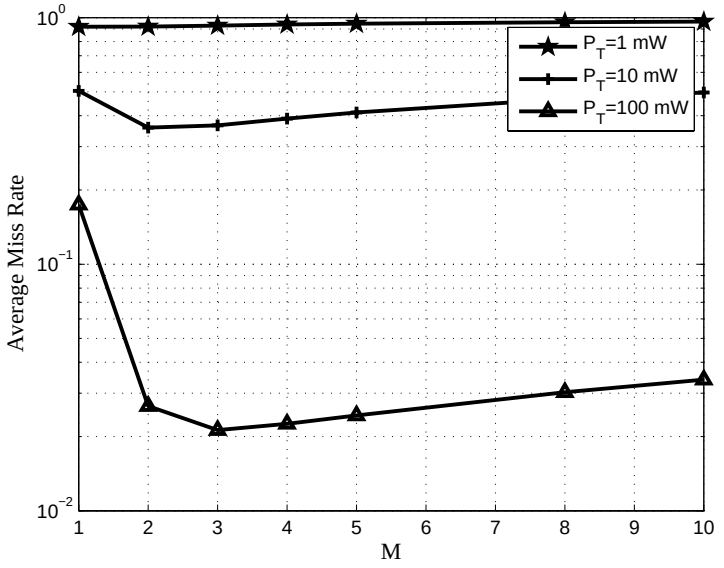
Alice moves r millimeter (mm) per frame in arbitrary directions, and an arbitrary distance between neighboring data bursts. For each r, we collect $N_A(N_x - 1)N_n$ samples to calculate the false alarm rate α of Λ_1, and $N_A N_E N_n$ samples for the miss rate β, for a given threshold η. For the case of Λ_2, we use $N_A(N_x - 3L)N_n$ and $N_A N_E N_n$ samples, respectively, to calculate α and β.

We assume $P_T = 10$ mW, $b_N = 0.25$ MHz, $M = 3$[1], $N_A = 50$, $N_E = 1000$, $N_n = 5$,

[1]Here we depart from our initial assumption that the number of pilots used to measure the channel is



(a) $M = 5$ tones



(b) Bandwidth $W = 50$ MHz

Figure 4.10: The average miss rate, $\overline{\beta}$, for Room 1, given false alarm rate of 0.01.

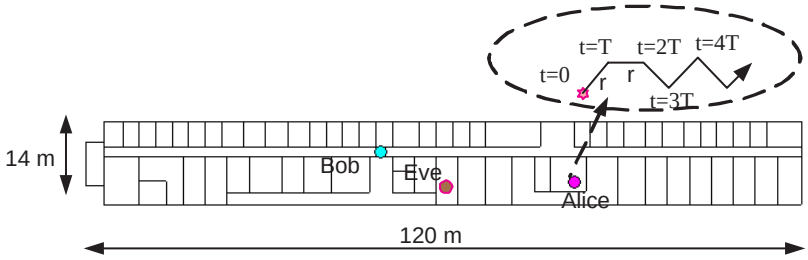


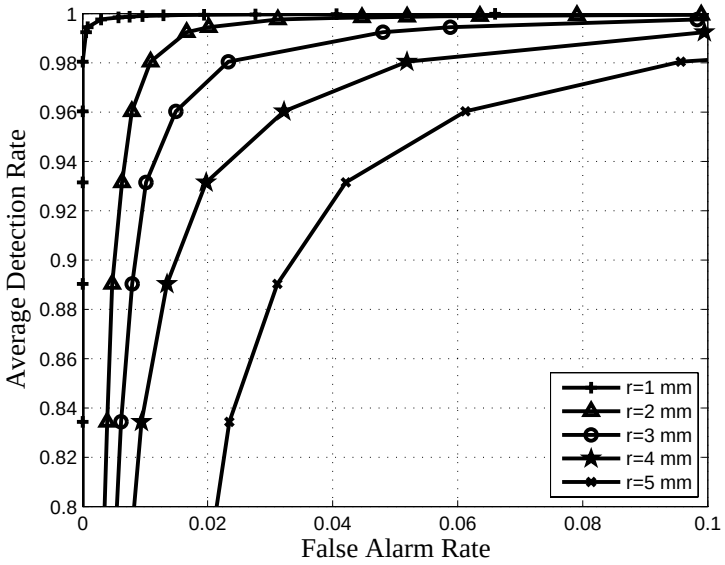
Figure 4.11: System topology assumed in the simulation scenario with terminal mobility. The receiver, Bob, is fixed at a location within the hall way. We randomly uniformly select N_A locations for Alice inside the building, representing her positions at the start of each of N_A data bursts. For each of these, we consider a set of N_E positions for Eve, which are also randomly uniformly selected. Each burst has the same number of frames, N_x, and Alice moves a distance of r from frame to frame, in an arbitrary direction. The independence among her N_A selected starting locations means that her position is independent from one burst to another.

and $N_x = 100$. The center frequencies of the subbands are at 4.75, 5.0, and 5.25 GHz. The per tone SNR in the channel estimation ranges from 1.7 dB to 69 dB, with a median value of 30 dB. To implement the L_R test, we use the RLS algorithm [55], with the filter order $L = 2$, forgetting factor $\lambda = 0.9995$, and regularization parameter $\delta = 10^{-10}$.

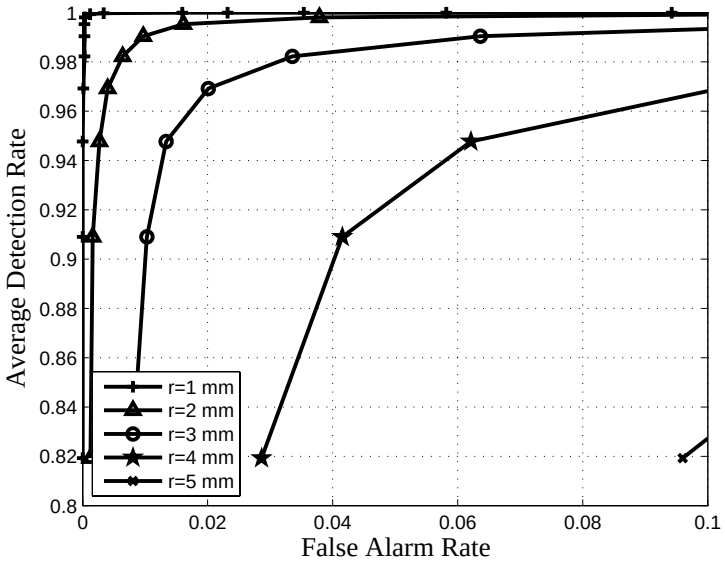
Figure 4.12 presents the receiver operating characteristic (ROC) curves of the intra-burst authentication method, i.e., the detection rate, $1 - \beta$, as a function of the miss detection rate, α, for the NP-based statistic L and the adaptive filter based statistic L_R, with Alice displacement per frame $r \in \{1, 2, 3, 4, 5\}$ mm. This corresponds to the frame duration $T \in \{0.70, 1.4, 2.1, 2.8, 3.5\}$ millisecond (ms) given a typical pedestrian velocity $v_a = 1.43$ mps.

It is shown in Fig. 4.12 that both L and L_R have good authentication performance, given that $r \leq 2$ mm. For example, L and L_R result in detection rate greater than 0.98 and 0.99, respectively, with $\alpha = 0.01$, $r \leq 2$ mm and $\eta = 0.1$. The performance degrades

equal to the number of subbands in the signal format. Previous studies [39, 40] have shown that only a few measurements say, 3-10, are needed; in an OFDM format, however, the number of subbands (tones) is generally much larger



(a) L.



(b) Adaptive filter based statistic, L_R.

Figure 4.12: Receiver operating characteristic (ROC) curves of the intra-burst authentication method, i.e., the average detection rate, $P_D = 1 - \beta$, as a function of false alarm rate, α, with Alice's displacement per frame $r \in \{1, 2, 3, 4, 5\}$ mm in arbitrary directions, and Eve randomly placed in the building with topology shown in Fig. 4.11.

as Alice moves faster, since it leads to a smaller correlation between successive channel realizations of Alice's channel to Bob. In addition, although L_R has better performance under smaller terminal velocity (e.g., $r \leq 2$ mm), L is more robust against terminal mobility. For instance, the detection rates of L and L_R are around 0.96 and below 0.8, respectively, given false alarm rate of 0.06, transmitter speed of 1.43 mps, and frame duration of 3.5 ms. Considering that L_R has larger system overhead than L, we believe L is a better statistic to use than L_R.

4.7 Protocol Design of FP

So far our analysis of the fingerprints authentication algorithm (called FP in this section) assumed a "reliable" reference channel response $\underline{\hat{H}}_0(k)$, where the subscript "0" indicates that it is a reference channel record for the corresponding user at time k. Channel response decorrelates after a channel coherent time [15], and thus the use of stale channel data in the FP test increases the false alarm of spoofing attacks. Hence, this assumption indicates that $\underline{\hat{H}}_0(k)$ comes from a *non-spoofing* message received within the channel coherent time.

However, this assumption does not always hold in practice. It is possible that the reference channel record corresponds to a spoofing message that successfully fools Bob. Moreover, unless an additional mechanism is taken, the FP test is prone to error propagation: once accepting one spoofing message from Eve, Bob is very likely to accept Eve and reject Alice in the following FP test. Finally, Bob does not have a valid reference channel if Alice has kept silence during the past channel coherence time or all her messages in that period have been rejected by Bob.

Therefore, it is important to analyze the performance of FP without assuming a reliable $\underline{\hat{H}}_0(k)$. To this end, we build a double-layer authentication protocol to integrate the FP test

with the higher-layer security process in the wireless systems, which might contain some key-based authentication or authorization. The higher-layer security mechanism can be chosen as sophisticated as IEEE 802.11i, to achieve maximal performance; or just a "nominal" process that enables FP to work independently, with an associated level of performance degradation.

4.7.1 Double-layer Authentication Protocol

We propose a double-layer authentication protocol that integrates the channel-based authentication algorithm FP, and the higher-layer authentication to detect spoofing attacks for wireless networks. The flow chart is shown in Fig. 4.13, where CIR is the channel impulse response vector.

As a built-in process in the specified system, the higher-layer function might provide security protection, e.g., the 802.11i in Section 1.3.1, while this higher-layer security mechanism has some weakness shown in Section 1.3.2. We do not intend to change the existing process when implementing the FP test. It is clear that the higher-layer process has less workload in this protocol, since FP filters out most spoofing messages. On the other hand, the system also has better performance in terms of spoofing detection by using FP, as we will see later.

When receiving a new message at time k, Bob identifies the sender by checking its MAC address of the message. In this Alice-Bob-Eve model, both Alice and Eve use Alice's MAC address in their messages. In order to perform the FP test, Bob utilizes the pilots/premables in the message to obtain a channel sample vector, $\underline{\hat{H}}_1(k)$, where the subscript "1" indicates that it belongs to the new message.

If Bob has a valid reference channel record, he performs the FP test to compare it with

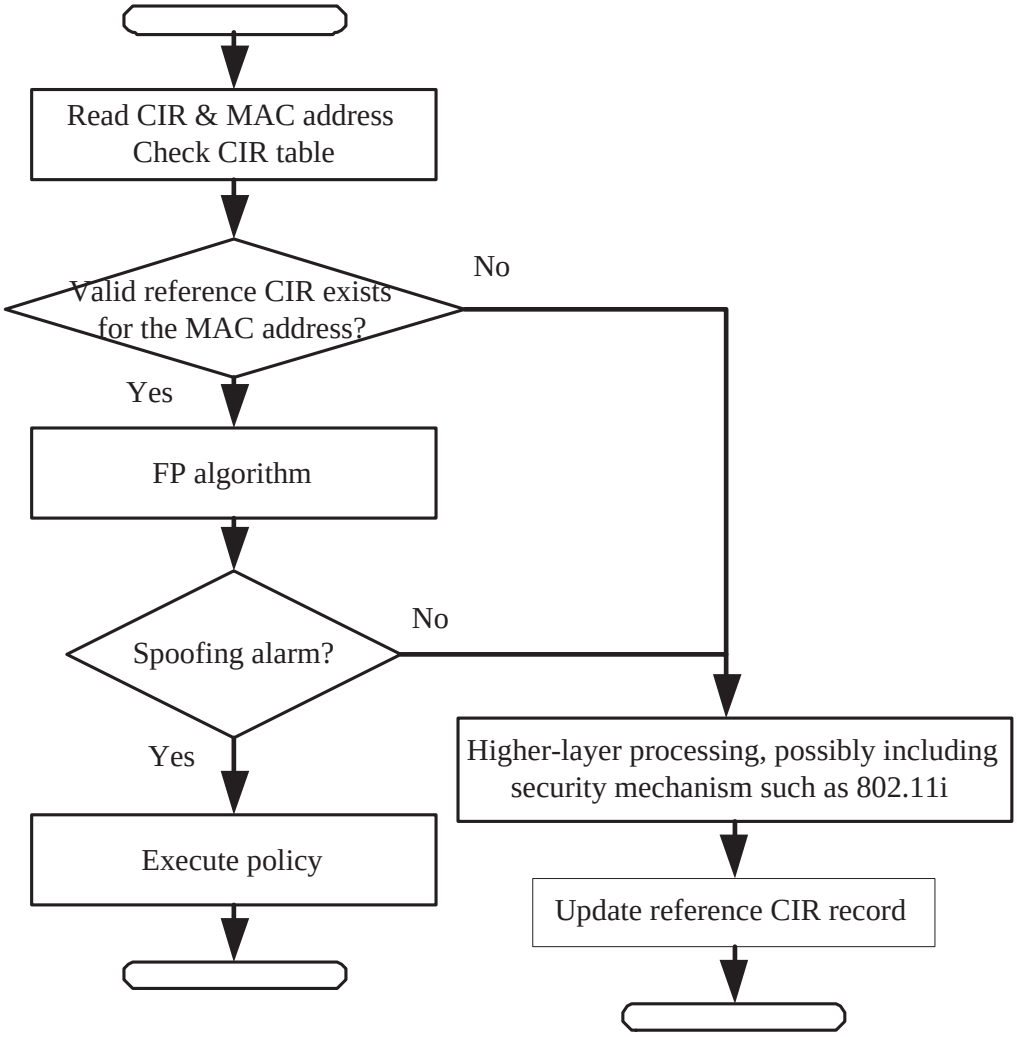


Figure 4.13: Flow chart of the double-layer authentication protocol that integrates the channel-based authentication (FP) and the higher-layer process, where CIR is the channel vector obtained by pilots/preambles of the message.

$\underline{\hat{H}}_1(k)$. Here, a test statistic L is calculated with (4.20) and compared with a test threshold η. Let $I_1(k)$ denote the FP decision, where the value "0" represents no alarm, "1" denotes a spoofing alarm, and "2" indicates a FP suspension due to the lack of $\underline{\hat{H}}_0(k)$. If the channel samples, $\underline{\hat{H}}_1(k)$ and $\underline{\hat{H}}_0(k)$, are so different that $L \geq \eta$, FP sends a spoofing alarm with $I_1(k) = 1$. In this way, the FP decision function can be written as

$$I_1(k) = \begin{cases} 0 \text{ (No alarm)}, & L(\underline{\hat{H}}_1(k), \underline{\hat{H}}_0(k)) < \eta \\ 1 \text{ (Spoofing alarm)}, & L(\underline{\hat{H}}_1(k), \underline{\hat{H}}_0(k)) \geq \eta \\ 2 \text{ (FP suspension)}, & \text{No } \underline{\hat{H}}_0(k) \end{cases} . \tag{4.43}$$

When FP sends a spoofing alarm, Bob processes the message according to one of the following two execution policies:

- Simply discard the message. In this strategy, the FP test threshold η has to be designed to ensure a low false alarm rate. We assume this policy in this section unless specified otherwise.

- Use a *simplified* higher-layer authentication algorithm to double-check the message, and discard the message if it fails this second check. This strategy has better detection accuracy, though at the expense of higher system overhead, compared to the previous policy.

As shown in Fig. 4.13, if FP does not send a spoofing alarm, i.e., $I_1(k) \neq 1$, the message then enters the higher-layer process, such as IEEE 802.11i. Let $I_2(k)$ denote the higher-layer authentication decision, which equals one if finding a spoofing, and zero otherwise.

In our double-layer authentication protocol, Eve can successfully spoof Alice if and only if both FP and the higher-layer test miss it, i.e., $I_1(k) \neq 1$ and $I_2(k) = 0$. Let $I_a(k)$ denote

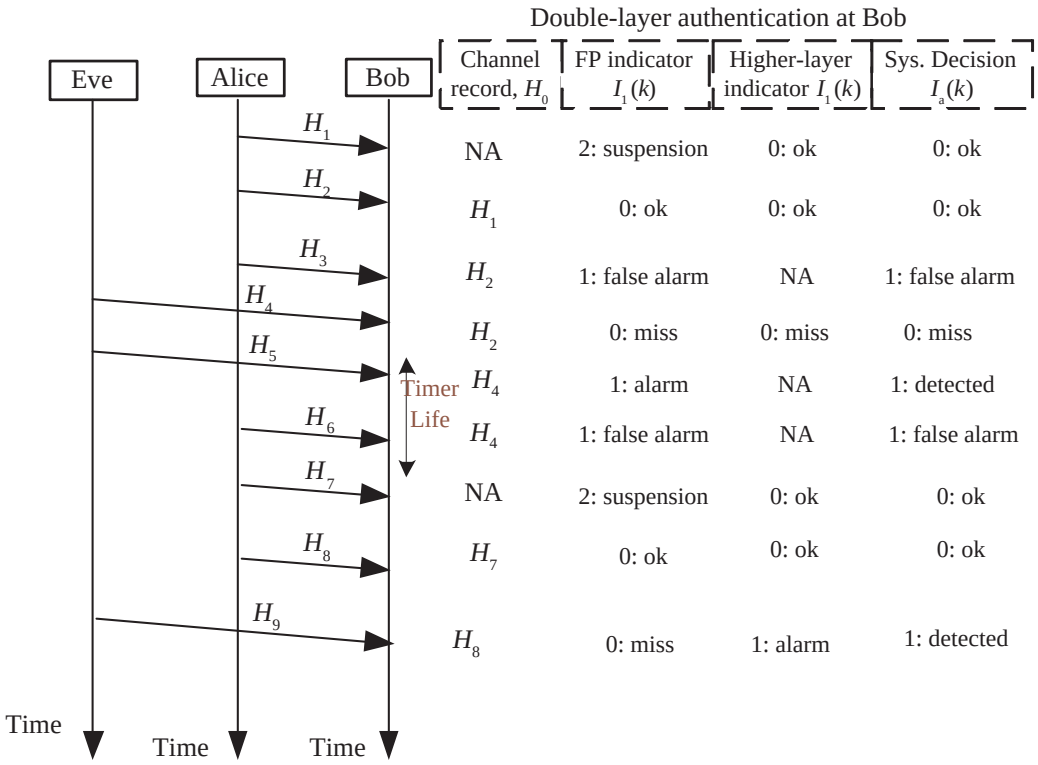


Figure 4.14: An example of how the double-layer authentication system works, where Bob receives six "legal" messages from Alice, and three spoofing messages from Eve with the identity of Alice. The overall system decision, $I_a(k)$, depends on both the channel-based FP algorithm, $I_1(k)$, and the back-up higher-layer authentication algorithm, $I_2(k)$. The reference channel H_0 is maintained according to previous overall system decisions, I_a, and a buffer timer with lifetime limit N_T.

the final system decision, which is given by

$$I_a(k) = \begin{cases} 1 \text{ (Reject)}, & \text{if } I_1(k) = 1 \text{ or } I_2(k) = 1 \\ 0 \text{ (Accept)}, & \text{o.w.} \end{cases} . \tag{4.44}$$

If Bob accepts the message with $I_a(k) = 0$, the channel sample $\underline{\hat{H}}_1(k)$ is saved as the new reference channel record at time $k+1$, i.e., $\underline{\hat{H}}_0(k+1) = \underline{\hat{H}}_1(k)$. The FP test maintains a channel table to record and update the reference channel data for active users, and sets a timer for each record. Since channel response decorrelates after the channel coherent time, the use of stale channel data increases the false alarm rate of FP. Accordingly, we delete the outdated channel data in the channel table, once their timers reach the maximum lifetime, N_T, which depends on the channel coherence time. The reference channel data is maintained according to the following rule:

$$\underline{\hat{H}}_0(k) = \begin{cases} \underline{\hat{H}}_1(k-1), & \text{if } I_a(k-1) = 0 \\ \underline{\hat{H}}_0(k-1), & \text{if } I_a(k-1) = 1, \text{ and Elapsed Time } \leq N_T \\ \text{No ref.}, & \text{o.w.} \end{cases} . \tag{4.45}$$

As an example, Fig. 4.14 shows how the protocol works in a scenario with Bob receiving three spoofing messages from Eve and six messages from Alice. A spoofing message can fool Bob only when both tests fail, such as the fourth message. The FP decision, $I_1(k)$, depends on the difference between the new channel vector and the reference channel H_0. The reference channel is updated according to the previous system decisions I_a and the timer lifetime limit N_T.

4.7.2 Performance Analysis

We consider the performance of FP in spoofing detection, without assuming a reliable reference channel. The FP false alarm rate α and the miss rate β, previously defined in

(4.25) and (4.26), assume a reliable reference channel. As noted above, this assumption does not hold in general, and the corresponding scenario can be viewed as a special "snapshot" case. Let $S(\underline{\hat{H}}) = A(\text{lice})$ or $E(\text{ve})$ denote the actual sender of the message from which the channel vector $\underline{\hat{H}}$ is derived. The "snapshot" assumption indicates $S(\underline{\hat{H}}_0(k)) \equiv A$, and the snapshot performance, α and β, can be rewritten as

$$\alpha = Pr(I_1(k) = 1 | S(\underline{\hat{H}}_1(k)) = S(\underline{\hat{H}}_0(k))) \tag{4.46}$$

$$\beta = Pr(I_1(k) = 0 | S(\underline{\hat{H}}_1(k)) \neq S(\underline{\hat{H}}_0(k))). \tag{4.47}$$

Let α_2 and β_2 denote the false alarm rate and miss rate of the higher-layer authentication test in the spoofing detection:

$$\alpha_2 = Pr(I_2(k) = 1 | S(\underline{\hat{H}}_1(k)) = A) \tag{4.48}$$

$$\beta_2 = Pr(I_2(k) = 0 | S(\underline{\hat{H}}_1(k)) = E). \tag{4.49}$$

In general, the FP test decision $I_1(k)$ has *three* possible states, (4.43). As shown in Fig. 4.13, the two decisions, $I_1(k) = 0$ and 2, lead to the same process afterwards in this double-layer protocol. Thus, we define the generalized *FP* false alarm rate, P_{FA}, and the miss detection rate, P_M, as:

$$P_{FA} = Pr(I_1(k) = 1 | S(\underline{\hat{H}}_1(k)) = A) \tag{4.50}$$

$$P_M = Pr(I_1(k) \neq 1 | S(\underline{\hat{H}}_1(k)) = E). \tag{4.51}$$

Let P_{FAA} and P_{MA} denote the spoofing detection performance of the double-layer protocol. By (4.44), (4.48)-(4.51), they can be written as

$$P_{FAA} = Pr(I_a(k) = 1 | S(\underline{\hat{H}}_1(k)) = A) = \alpha_2 + (1 - \alpha_2) P_{FA} \tag{4.52}$$

$$P_{MA} = Pr(I_a(k) = 0 | S(\underline{\hat{H}}_1(k)) = E) = P_M \beta_2. \tag{4.53}$$

It is clear that $P_{FAA} \geq \alpha_2$ and $P_{MA} \leq \beta_2$. For the FP with small P_{FA} and P_M, we have $P_{FAA} \approx \alpha_2$ while $P_{MA} \ll \beta_2$. Thus, the use of FP improves the system performance in spoofing detection. In order to limit the system false alarm rate, we should adjust the test threshold η to obtain a small P_{FA}, while a relatively large P_M does not hurt too much. Further, what matters here are the values of P_{FA} and P_M, instead of their "snapshot" counterparts.

In general, the performance of FP, P_{FA} and P_M, depends on the snapshot performance (α and β), the maximum timer lifetime (N_T), the higher-layer algorithm (α_2 and β_2), and the spoofing frequency (i.e., how often Eve injects spoofing messages). Both P_{FA} and P_M increase, as Eve injects more spoofing messages, even with constant α and β. Let $P_a \in [0, 1]$ denote the fraction of all messages from Alice. As an extreme case, if all the received messages are from Eve, i.e., $P_a = 0$, the FP test fails, even with small α and β.

It is very difficult to perform field tests to extensively measure P_{FA} and P_M, since they depend on the attack pattern and the performance of the higher-layer process. On the other hand, the snapshot performance of FP, α and β, are much easier to obtain via field tests. We will consider two extreme cases of the higher-layer test, in order to bound the performance of FP.

Ideal Higher-layer Test

For the double-layer protocol shown in Fig. 4.13, the performance of FP can be upper bounded by an "ideal" higher-layer authentication test with $\alpha_2 = \beta_2 = 0$. In this case, by (4.52) and (4.53), we see that $P_{FAA} = P_{FA}$ and $P_{MA} = 0$, indicating that the protocol does not provide Eve any chance to spoof Alice, with the ideal higher-layer test. Hence, the reference channel $\underline{\hat{H}}_0(k)$, if it exists, always comes from Alice's message.

For simplicity, we assume that the reference channel timer lifetime N_T to be an integer, and that Bob receives exactly one message at each discrete time. Suppose the senders of these messages are independent, and identically distributed with

$$P_a = Pr(S(\underline{\hat{H}}_1(k)) = A) = 1 - Pr(S(\underline{\hat{H}}_1(k)) = E). \tag{4.54}$$

The discussion can be also extended to a general case. By (4.45), if a valid reference channel record comes from the message received at time $k-n$, i.e., $\underline{\hat{H}}_0(k) = \underline{\hat{H}}_1(k-n)$, we have $S(\underline{\hat{H}}_1(k-n)) = A$, $n \leq N_T$, and that Bob rejects all the messages sent by Alice after $k-n$.

Theorem 4.7.1 *Without any assumption on the reference channel, we can upper-bound the performance of the FP test based on the Alice-Bob-Eve attack model given by (4.54) as:*

$$P_{FA} = \alpha - \alpha(1 - P_a(1 - P_{FA}))^{N_T} \tag{4.55}$$

$$P_M = \beta + (1-\beta)(1 - P_{FA}/\alpha). \tag{4.56}$$

Proof: In the i.i.d. attack model, (4.54), the FP decision $I_1(k)$ does not impact the sender of the following messages, and we have

$$\begin{aligned} Pr(\text{No } \underline{\hat{H}}_0(k)) &= \prod_{n=1,\cdots,N_T} (1 - Pr(S(\underline{\hat{H}}_1(k-n)) = A, I_1(k-n) \neq 1)) \\ &= \prod_{n=1,\cdots,N_T} (1 - Pr(S(\underline{\hat{H}}_1(k-n)) = A) Pr(I_1(k-n) \neq 1 | S(\underline{\hat{H}}_1(k-n)) = A)) \\ &= (1 - P_a(1 - P_{FA}))^{N_T}. \end{aligned}$$

As mentioned, with the ideal higher-layer test, the reference channel record, $\underline{\hat{H}}_0(k)$, if it exists, always results from a message sent by Alice, and thus

$$Pr(S(\underline{\hat{H}}_0(k)) = A) + Pr(\text{No } \underline{\hat{H}}_0(k)) = 1. \tag{4.57}$$

Hence, we can rewrite the false alarm rate of FP, (4.50), as

$$\begin{aligned} P_{FA} &= Pr(I_1(k)=1|S(\hat{\underline{H}}_1(k)) = S(\hat{\underline{H}}_0(k)))Pr(S(\hat{\underline{H}}_0(k)) = A) \\ &\quad + Pr(I_1(k)=1|\text{No } \hat{\underline{H}}_0(k))Pr(\text{No } \hat{\underline{H}}_0(k)) \\ &= \alpha(1 - Pr(\text{No } \hat{\underline{H}}_0(k))) \\ &= \alpha - \alpha(1 - P_a(1-P_{FA}))^{N_T}. \end{aligned} \tag{4.58}$$

We can also obtain the miss rate (4.51) with

$$\begin{aligned} P_M &= Pr(S(\hat{\underline{H}}_0(k)) = A)Pr(I_1(k) \neq 1|S(\hat{\underline{H}}_0(k)) \neq S(\hat{\underline{H}}_1(k))) + Pr(\text{No } \hat{\underline{H}}_0(k)) \\ &= (1 - P(\text{No } \hat{\underline{H}}_0(k)))\beta + P(\text{No } \hat{\underline{H}}_0(k)) = \beta + (1-\beta)P(\text{No } \hat{\underline{H}}_0(k)) \\ &= \beta + (1-\beta)(1 - P_a(1-P_{FA}))^{N_T} = \beta + (1-\beta)(1 - P_{FA}/\alpha). \end{aligned} \tag{4.59}$$

The last line is based on (4.58). ■

Equation (4.55) shows that P_{FA} is a function of α, β, P_a and N_T, but it does not provide a closed-form expression of P_{FA}. However, the value of P_{FA} can be easily derived from (4.55), especially for small N_T. For example, given $N_T = 2$, we have

$$\alpha P_a^2 P_{FA}^2 + (1 + 2\alpha(1-P_a)P_a)P_{FA} + ((1-P_a)^2 - 1)\alpha = 0. \tag{4.60}$$

On the other hand, as N_T approaches infinity (i.e., a static channel case), it is shown in (4.55) and (4.56) that $P_{FA} = \alpha$ and $P_M = \beta$.

Figure 4.15 provides an upper bound of the performance of FP, as a function of P_a and N_T, given $\alpha = 0.05$ and $\beta = 0.03$. It is shown that both P_{FA} and P_M improve with P_a, due to the high costs for FP to recover from the miss detection of a spoofing message. We also see that the FP test works efficiently, when Bob receives much more messages from Alice than from Eve, e.g., $P_a > 0.8$. In addition, the performance of FP improves with the timer limit N_T, and in particular $N_T = \infty$ results in the best performance. Actually, the

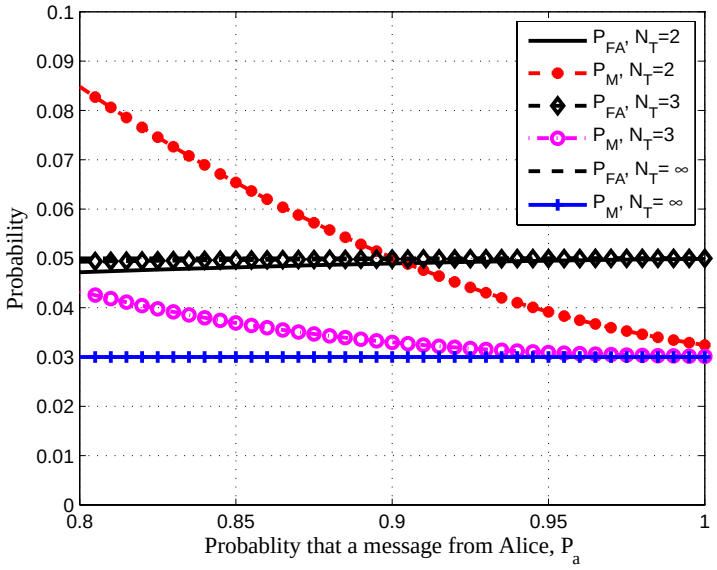


Figure 4.15: Upper bound of the performance of FP in spoofing detection, including the false alarm rate P_{FA} and the miss rate P_M, given $\alpha = 0.05$, and $\beta = 0.03$, by (4.55) and (4.56).

performance gap between $N_T = 3$ and $N_T = \infty$ is very small, indicating that FP works well if Bob can receives about three messages on average during a channel coherence time.

Nominal Higher-layer Test

As another extreme case, a nominal "empty" higher-layer authentication test with $I_2(k) \equiv 0$ lower bounds the performance. In certain cases, e.g. where low-power/lower-cost devices are desired, higher-layer authentication may be too expensive in terms of power, computation, or delay. In this case, the FP test works independently, as the only authentication process for the system. Bob accepts any message if no valid reference channel exists. Thus we have $I_a(k) = 1$, if and only if $I_1(k) = 1$; and zero otherwise.

The error propagation property of FP is even more significant here, since any "non-empty" higher-layer authentication can detect some spoofing messages that are missed

by FP and thus reduces the error propagation. That is why this case lower bounds the performance of FP.

On the other hand, the use of reference channel timers enables FP to recover from a miss detection of Eve. As shown in (4.45), an "invalid" channel record expires, if Bob does not accept any new message during a period of N_T. If Eve keeps silent during that time and the next message is sent by Alice, Bob accepts the new message and the FP test then returns to the normal status. Thus the FP test can work independently, if Bob receives far more legal messages than spoofing messages in the long run.

4.8 Field Test and Implementation Issues in 802.11

As a first step to implementing the FP algorithm in wireless systems, we verify the performance of FP, as well as the double-layer authentication protocol, for IEEE 802.11 systems [58]. To this end, we utilize an 802.11 testbench, which we call the InterDigital Physical Layer Security Validation Platforms (IPLSVP), with system parameters listed in Table 4.1. The experiment is performed in the security lab at InterDigital's King of Prussia office site, a typical indoor office environment, with horizontal building map shown in Fig. 4.16.

In the experiment, we use two or three IPLSVP boards, and call them Alice, Bob, and/or Eve. Mimicking a realistic deployment of the FP algorithm, our test in general operates as follows:

- A connection is first established between a transmitter IPLSVP board and a receiver board, according to the standardized 802.11 protocol.
- Then, the transmitter keeps sending probe signals to the receiver for a duration of several minutes. The transmission intervals between neighboring probe signals vary,

Table 4.1: System parameters for the field test of the channel-based spoofing detection in 802.11 testbed.

Type	Value
Bandwidth	16.6 MHz
Channel spacing/sampling rate	20 MHz
Number of subcarriers	52
Center frequency	5 GHz
Noise power	17-21 dB
Number of CIR vectors	3000
Measurement duration	4 min
Average interval between CIRs	60.3 ms
Std of the interval between CIRs	23 ms

with a mean of 60.3 ms and standard deviation of 23 ms.

- The receiver utilizes the preamble symbols in each probe signal to measure the channel impulse response (CIR). Each of the resulting CIR vector contains 64 channel samples, as the inverse fast Fourier transform (IFFT) of the channel frequency response, which is estimated from the preamble symbols at 52 subcarriers over the bandwidth of 16.6 MHz. The arrival time of each CIR vector is recorded with a time stamp.

  The IPLSVP receiver saves these CIR data as well as their time stamps in a large memory. We consider the CIR vectors from the first $N = 3000$ received probe signals, which lasts for about four minutes.

- We change the locations of the testbenches, and then repeat the measurements of the CIR data for the new scenario.

- By using these CIR data saved from field tests, we perform the FP test offline and analyze its performance based on various attack models.

More details about the experiments are presented in the following discussion.

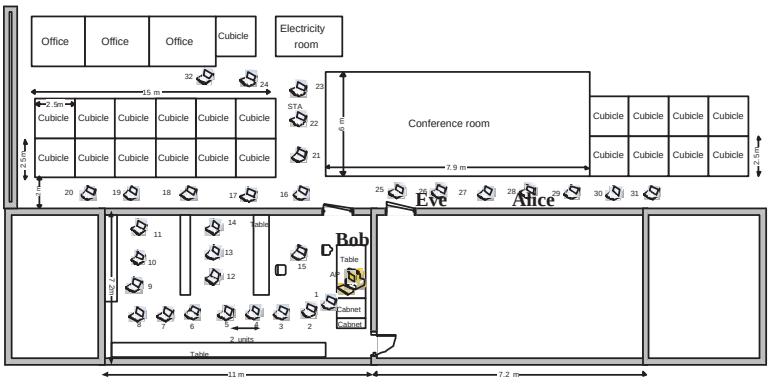


Figure 4.16: The layout of the two-board test for the channel-based authentication (FP) algorithm, at InterDigital's office. We place the receiver Bob on a table of a room, and the transmitter at 32 different locations. For each scenario, both terminals are stationary. The transmitter keeps sending probe signals, based on which the receiver Bob obtains CIR data.

4.8.1 Two-Board Test

In the two-board test, we perform the FP test by using the data collected by two IPLSVP boards: one acts as Bob, the intended receiver; and the other acting as Alice or Eve, periodically transmiting probe signals to Bob. We place Bob on a fixed location: a table inside the lab, and put Alice in 32 different locations, as shown in Fig. 4.16. In each test scenario, both the transmitter and the receiver are stationary, while people may walk around from time to time in this busy office site.

Let $\underline{\hat{H}}_l(k)$, $k = 1, \cdots, N$, $l = 1, \cdots, 32$, denote the CIR vector derived from the k-th message, when the transmitter is located at location l, as in Fig. 4.16. Each vector contains 64 complex channel impulse samples. For the offline FP test, there are totally 32 groups of these CIR data, each containing $N = 3000$ CIR vectors. We select one transmitter location as Alice and another one as Eve, and thus obtain $32 \times 31 = 992$ possible Alice-Eve pairs. In this way, the two-board experiment conveniently tests the performance of FP, with Alice and Eve covering a large area.

For each transmitter location (i.e., given l), we calculate $N-1$ test statistics with (4.20), based on the consecutive CIR pairs, $\underline{\hat{H}}_l(k-1)$ and $\underline{\hat{H}}_l(k)$, $k = 2, \cdots, N$. By comparing these $N-1$ test statistics with η, we obtain the "snapshot" false alarm rate, as Alice is located at the l-th location:

$$\alpha(l) = \frac{1}{N-1} \sum_{k=2}^{N} J(L(\underline{\hat{H}}_l(k-1), \underline{\hat{H}}_l(k)) \geq \eta), \tag{4.61}$$

where the indicator function $J(A) = 1$ if A is true, and zero otherwise.

The calculation of the miss detection rate for spoofing attacks is much more complex and requires some degree of approximation. For each of the 992 Alice-Eve pairs (since Bob keeps in the same location), there are two groups of CIR data, each with $N = 3000$ vectors, received at different time. We compare the $(k-1)$-th CIR vector from Alice and k-th CIR from Eve, $k = 2, \cdots, N$, resulting in $N-1$ test statistics. When Alice and Eve stay in the l-th and j-th locations, respectively, the "snapshot" miss rate can be approximately given by

$$\beta(l, j) = \frac{1}{N-1} \sum_{k=2}^{N} J(L(\underline{\hat{H}}_l(k-1), \underline{\hat{H}}_j(k)) < \eta). \tag{4.62}$$

The two-board test has only one transmitter in the measurement. Hence $\underline{\hat{H}}_l(k)$ and $\underline{\hat{H}}_j(k)$ are measured at different time, if $l \neq j$. This time difference is at least several minutes. Similarly, the actual time difference between the measurements of $\underline{\hat{H}}_l(k-1)$ and $\underline{\hat{H}}_j(k)$ are much longer than that for a typical practical scenario. Thus the use of (4.62) for the miss rate calculation assumes that Bob can obtain the same CIR vector for any specified transmitter location, if the measurement postpones for that time difference. The assumption indeed increases the difference between $\underline{\hat{H}}_l(k-1)$ and $\underline{\hat{H}}_j(k)$, and thus (4.62) lower bounds β.

As mentioned, it is important to set an appropriate test threshold η: if η is too high,

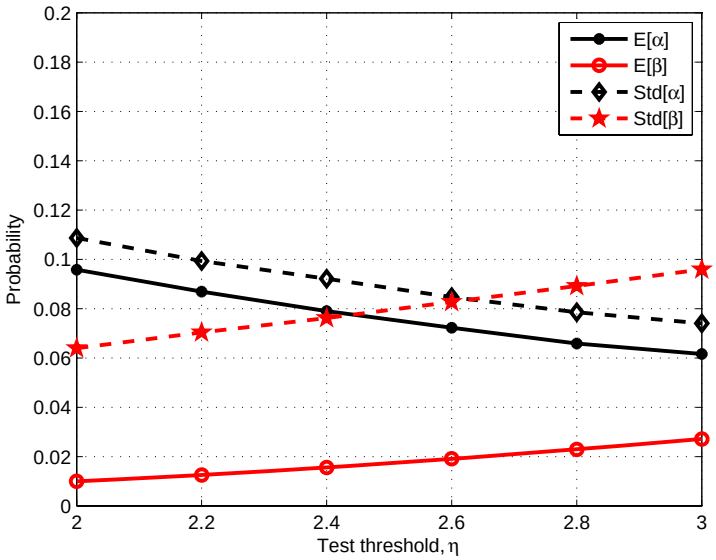
FP cannot detect any spoofing message. On the other hand, every message will be rejected if we choose a η that is too low. There are two strategies for the threshold selection:

- Pre-assigned threshold. A fixed threshold η is set according to the experiences or previous experiments. We choose the value corresponding to a good performance of FP averaged over most situations. This strategy does not provide an optimal η for each specific scenario. Moreover, this pre-assigned threshold requires large scale field tests that also cost efforts.

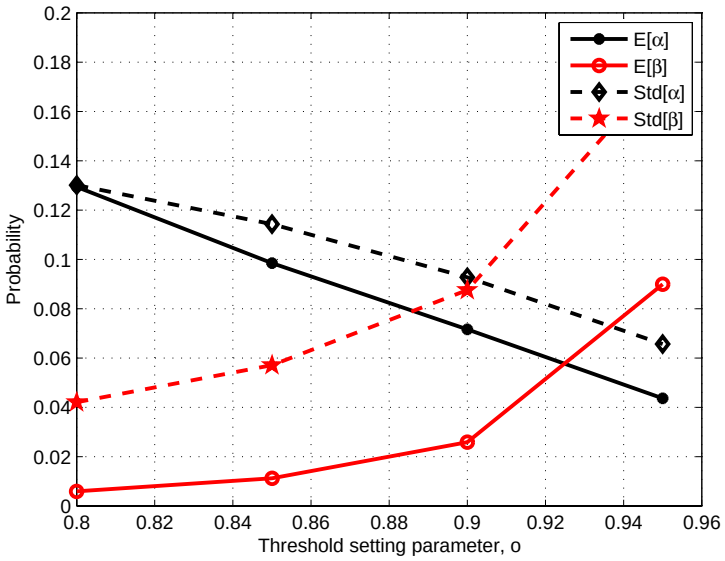
- Adaptive threshold. In this strategy, the legal user Alice is supposed to send $N_{tr}+1$ training messages in advance, in order to inform Bob about the range of her test statistics. In other words, when entering a new environment, Alice first continuously sends $N_{tr}+1$ messages to Bob. Based on these spoof-free messages, Bob calculates the corresponding test statistics $L(k)$, $k = 2, \cdots, N_{tr}+1$. Then he searches the o-th percentile value of these N_{tr} test statistics, and sets it as η in the FP test for the following $N - N_{tr} - 1$ CIR data. In this way, Bob adjusts the test threshold η according to the channel property of the specific environment. Ideally, this adaptive threshold policy enables a better balance between the false alarm rate and miss rate. However, the performance is very sensitive to o.

Figure 4.17 presents the average and standard deviation of $\alpha(l)$ over 32 Alice locations and $\beta(l,j)$ over 992 Alice-Eve pairs. It verifies the performance of FP for the fixed test threshold strategy. For example, given $\eta = 2.6$, the average $\alpha(l)$ and $\beta(l,j)$ are around 7% and 2%, respectively.

This figure also verifies the performance of the adaptive threshold strategy, with $N_{tr} = 400$ out of $N = 3000$ messages to train η. It is shown that the training-based η policy does



(a) Fixed test threshold η.



(b) Adaptive test threshold, with $N_{tr} = 400$ training messages.

Figure 4.17: The "snapshot" performance of FP, including the average and the standard deviation of the false alarm rate α, (4.61), and the miss rate β, (4.62). The test statistics, (4.20), are calculated using the CIR data obtained from the two-board experiment as shown in Fig. 4.16 and Table 4.1.

not evidently improve the performance of FP, unless the training is set to be even longer.

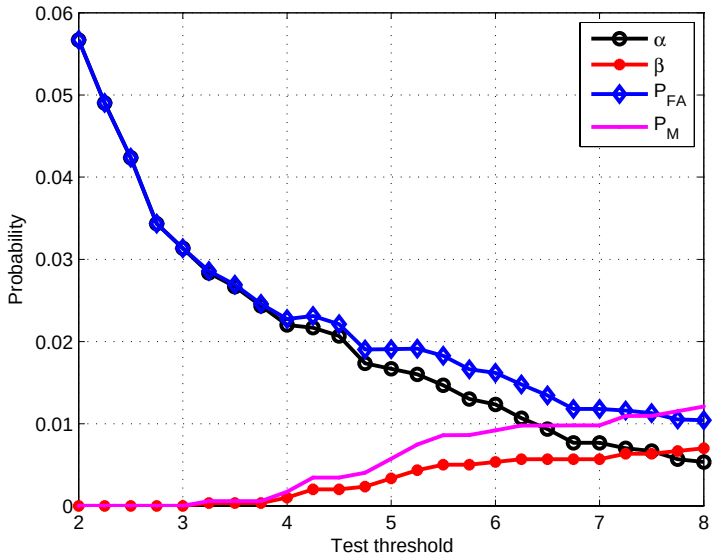
For both threshold strategies, the standard deviation of α and β are higher than the corresponding average value. This indicates that the FP test accurately discriminates most of the Alice and Eve pairs, while it fails in a few "bad" location pairs. This problem comes from the nature of the FP test, and cannot be addressed by simply improving the threshold policy. More specifically, a "bad" Alice-Eve pair does not happen frequently. Here, the time variation of the Alice-Bob channel is comparable to its difference with the Eve-Bob channel, or it changes so fast that the channel coherence time is smaller than most message intervals. In these rare cases, FP may fail to work, and a high-performance high-layer authentication process helps.

4.8.2 Three-Board Test

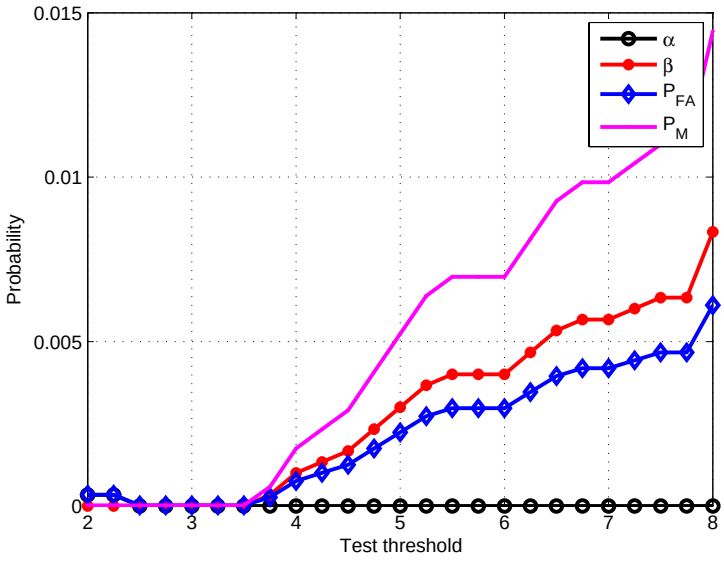
Now we evaluate the performance of FP using three boards that act as Alice, Bob and Eve, in the same building shown in Fig. 4.16. In the three-board experiment, Bob is still located in the place as denoted in Fig. 4.16, and continually sends probe messages to the other two boards, Alice and Eve. Alice and Eve estimate the Bob-Alice and Bob-Eve channel based on the probe messages. In this way, the Alice-Bob and Alice-Eve channel responses at the same time can be obtained using the channel reciprocity property.

Although the three-board experiment is more accurate than the two-board counterpart in the evaluation of the miss detection rate of Eve, it is hard to perform a large-scale field test that covers most of the possible Alice-Eve location pairs. Hence we only provide results for two specific terminal topologies.

In the first test scenario, Eve is located in the same room with Bob, while Alice is outside the room. Thus the Alice-Bob channel, $\underline{H}_A$, has larger time variations than $\underline{H}_E$. In the



(a) Case 1: Alice and Eve are located respectively near Location 15 and 23 in Fig. 4.16.



(b) Case 2: Same as Case 1, except the locations of Alice and Eve are reversed.

Figure 4.18: Performance of FP in two experiment scenarios with three boards, including both the snapshot performance, α and β, and the generalized performance, P_{FA} and P_M, calculated by (4.55) and (4.56), with $N_T = 2$ and $P_a = 70\%$ of the received messages coming from Alice. These two sub-figures use different scales in Y-axis.

second test, we exchanged the location of Alice and Eve, and thus $\underline{H}_E$ has larger channel variations.

As shown in Fig. 4.18, both α and β are mostly below 5% in both cases. The performance of FP criteria, P_{FA} and P_M, are in the same range, when $N_T = 2$ and 30% of the messages received by Bob are sent by Eve. As mentioned in Fig. 4.15, both P_{FA} and P_M decrease with P_a. Thus Fig. 4.18 verifies the performance of FP for spoofing messages no more than 30%.

Moreover, FP exibits significantly different performance, after the locations of Alice and Eve are reversed. The false alarm rate (either α or P_{FA}) in Case 1 is larger than the counterpart in Case 2, indicating that the performance of the FP test is more sensitive to the channel time variation of Alice than that of Eve.

Figure 4.18 also shows that unlike the snapshot counterpart α, P_{FA} does not always decrease with the test threshold η, since P_{FA} depends on both β and α. Hence a bad selection of η may lead to a large P_{FA}, as well as large P_M.

Finally, we have to address several issues if implementing the FP algorithm in a commercial 802.11 systems:

- The 16.6 MHz bandwidth in 802.11 systems is not always wide enough to provide very high resolution of the multipath phenomenon inside an office building. In some cases, the CIR is even presented as a single fading path, and thus the FP algorithm might experience performance degradation to a certain degree. Fortunately, the use of MIMO techniques improves the channel resolution and hence enhances the performance of FP in spoofing detection.

- The CIR data provided by an 802.11 mobile device, are scaled and corrupted by

factors, such as the thermal noise, and the receiver phase drift due to the drift of the local oscillator w.r.t. the transmitter's local oscillator.

- Realistically, many 802.11 testbench devices, such as IPLSVP, make timing or frequency errors in their channel estimation. As a consequence, the peaks of the CIRs shift in time, and the CIR data for the same channel may become very different to each other. To address this problem, we might use a technique called post-CIR-processing to reduce the timing error of the device.

- To the best of our knowledge, no commercial 802.11 provides estimation of the channel parameters, such as channel coherence time, and thus it is not possible to implement the high-performance FP test, such as GLRT L_g, (4.18).

4.9 Conclusion

We proposed a channel-based spoofing detection for wireless networks, utilizing channel estimation mechanism to detect spoofing messages. For this framework, we presented an optimized generalized likelihood ratio test, L_g, a practical test, L, which does not require the knowledge of channel parameters, and a RLS-based test, L_R. The efficacy of the scheme was first verified via numerical analysis using a frequency-selective Rayleigh channel model, independent of any specific network topology, building description, or channel emulation software.

More specifically, 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 optimal L_g test in many cases. For example, given path-loss exponent $\gamma = 4$, $M = 4$ independent channel samples in each message, SINR of the channel

estimation $\rho = 20$ dB, channel time variation, $b = 0.2$, the worst case performance of L_g and L are $\alpha = \beta = 4\%$ and $\alpha = \beta = 10\%$, respectively. The test statistic L also demonstrated excellent "average" results, over the variation of Alice-Eve locations.

The test L was also verified by using site-specific ray tracing. We considered typical in-building environments, where we used the ray-tracing tool WiSE to generate realistic average channel responses and used a multipath tapped delay line channel model for the temporal variation part of the channel response. Simulation results have confirmed the efficacy of the algorithm for realistic values of the measurement bandwidth (e.g., $W \sim 10$ MHz), number of response samples (e.g., $M \leq 10$) and transmit power (e.g., $P_T \sim 100$ mW). The miss rate is generally smaller than 0.01, for a specified false alarm rate of 0.01, in the static channel environment.

Simulation results show that the proposed scheme can detect spoofing attacks efficiently under slow terminal velocity. For instance, the detection rate is around 0.96, given a false alarm rate of 0.06, when the transmitter moves at a speed of 1.43 m/s and the frame duration equals to 3.5 ms.

One promising ongoing research direction is to integrate this scheme into a holistic cross-layer framework for wireless security. The aim would be to quantify the net benefit in thus augmenting traditional "higher-layer" network security mechanisms with physical layer methods.

Chapter 5

Channel-Based Sybil Detection

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 in hopes of depleting system resources. We propose an enhanced physical-layer authentication scheme to detect Sybil attacks, exploiting the spatial variability of radio channels in environments rich with 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 minimal 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 detecting Sybil attacks are usually below 0.01, with 3 tones, pilot power of 10 mW, and a system bandwidth of 20 MHz.

5.1 Introduction

Compared with wired networks, most wireless networks 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 IEEE WPA/ 802.11i/ 802.1X [37]. One serious consequence is that such networks are vulnerable to various identity-based attacks, such as Sybil attacks [7].

Sybil attacks were first introduced in the context of peer-to-peer networks [59] as a form of resource depletion attack, and then analyzed in the context of wireless networks [7, 60]. 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 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 (DoS) attack, Sybil attacks seriously endanger the availability of network services for wireless systems [60].

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 [38], the channel response decorrelates rapidly in space, in typical wireless scenarios rich with scatterers. Hence, two clients with similar channels 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

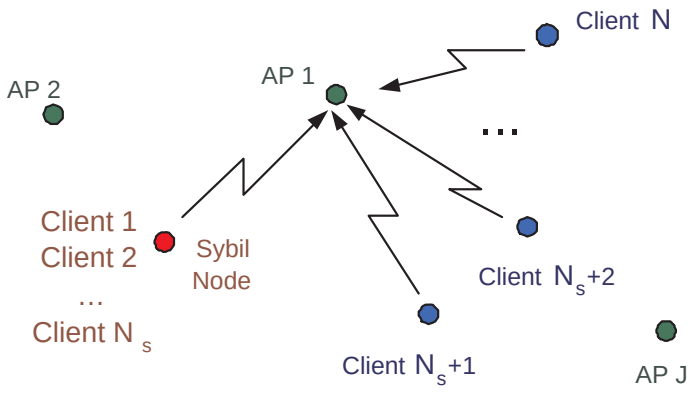


Figure 5.1: Sybil attack model with AP 1 receiving messages from N clients, where the first N_s clients are actually in the same terminal (i.e., Sybil node), while the remaining $N - N_s$ clients are legal users in distinct terminals. Sometimes, more than one (i.e., $J > 1$) AP cooperates to track channels from these clients.

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 described in Chapter 4.

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.

5.2 Sybil Attack Model

We present a generalized Sybil attack model in Fig. 5.1, where the serving access point (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. 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.

5.3 Single-AP Sybil Detection

5.3.1 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/preamble sequences to estimate channel frequency responses. Denote the true channel response at frequency f as $H_n(f)$, $1 \leq n \leq N$, 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 error: (1) the receiver thermal noise, which is modeled as white Gaussian noise; (2) the phase measurement rotation, due to the phase variation of the receiver local oscillator (LO) 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, $f \in (f_o - W/2, f_o + W/2]$, the AP obtains an M-dimension channel (row) vector $\hat{\mathbf{H}}_n$,

$$\hat{\mathbf{H}}_n = \mathbf{H}_n a_n e^{j\phi_n} + \mathbf{N}_n,\ 1 \leq n \leq N, \tag{5.1}$$

where the elements of arbitrary vector $\mathbf{A} = [A_1, \cdots, A_M]$ are samples from $A(f)$. More specifically, $A_m = A(f_o + W(m/M - 0.5))$; 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 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 $a_n \neq 1$.

5.3.2 Baseline Case: 2 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

$$\mathcal{H}_0 : \quad \mathbf{H}_1 \neq \mathbf{H}_2 \tag{5.2}$$

$$\mathcal{H}_1 : \quad \mathbf{H}_1 = \mathbf{H}_2. \tag{5.3}$$

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:

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

$$L(\hat{\mathbf{H}}_1, \hat{\mathbf{H}}_2) = \frac{1}{\sigma^2}||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 e^{j\phi}||^2, \tag{5.4}$$

where

$$\phi = \arg\min_x ||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 e^{jx}|| = Arg(\hat{\mathbf{H}}_1 \hat{\mathbf{H}}_2^H). \tag{5.5}$$

This test statistic is approximately a generalized likelihood ratio test. 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.

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, an approximate likelihood ratio test statistic becomes

$$L(\hat{\mathbf{H}}_1, \hat{\mathbf{H}}_2) = \frac{2||\hat{\mathbf{H}}_1 - w\hat{\mathbf{H}}_2||^2}{(1 + |w|^2)\sigma^2}, \tag{5.6}$$

where

$$w = \arg\min_x ||\hat{\mathbf{H}}_1 - x\hat{\mathbf{H}}_2|| = \hat{\mathbf{H}}_1 \hat{\mathbf{H}}_2^H / ||\hat{\mathbf{H}}_2||^2. \tag{5.7}$$

We 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 for a Sybil attack 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, given a 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

$$\alpha(k) = Pr(L \leq k|\mathcal{H}_0) \tag{5.8}$$

$$\beta(k) = Pr(L > k|\mathcal{H}_1). \tag{5.9}$$

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

Theorem 5.3.1 *In a Sybil detection scenario with two clients, given the miss rate β, the false alarm rate is*

$$\alpha(\beta) = F_{\chi^2_{2M,\mu}}(F^{-1}_{\chi^2_{2M,0}}(1-\beta)), \tag{5.10}$$

where

$$\mu = ||\boldsymbol{H}_1 - \boldsymbol{H}_2 e^{jArg(\boldsymbol{H}_1\boldsymbol{H}_2^H)}||^2/\sigma^2, \tag{5.11}$$

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

$$\mu = 2||\boldsymbol{H}_1 - w\boldsymbol{H}_2||^2/(1+|w|^2)\sigma^2, \tag{5.12}$$

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

Proof: 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 $\mathbf{H}_1 = \mathbf{H}_2$, (5.3). From (5.1), (5.5), and the assumption that $Arg(\hat{\mathbf{H}}_n) \approx Arg(\mathbf{H}_n e^{j\phi_n})$, which is reasonable for the high-SNR conditions where the

system must operate, we can obtain

$$\begin{aligned}
&\mathbf{H}_1 e^{j\phi_1} - \mathbf{H}_2 e^{j\phi_2} e^{j\phi} \\
=&\mathbf{H}_1 e^{j\phi_1}(1 - e^{j(\phi_2-\phi_1+Arg(\hat{\mathbf{H}}_1\hat{\mathbf{H}}_2^H))}) \\
\approx&\mathbf{H}_1 e^{j\phi_1}(1 - e^{j(\phi_2-\phi_1+Arg(\mathbf{H}_1)+\phi_1-Arg(\mathbf{H}_2)-\phi_2)}) \\
=&e^{j\phi_1}\mathbf{H}_1(1 - e^{j(Arg(\mathbf{H}_1)-Arg(\mathbf{H}_2))} = \mathbf{0}.
\end{aligned} \tag{5.13}$$

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 $\mathbf{N}_m = \mathbf{N}_{1,m} - e^{j\phi}\mathbf{N}_{2,m} \sim CN(0, 2\sigma^2)$, $m = 1, \cdots, M$. From (5.1), (5.4), and (5.13), the test statistic L under $\mathcal{H}_1$ can be written as

$$\begin{aligned}
&L = \frac{1}{\sigma^2}||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 e^{j\phi}||^2 \\
=&\frac{1}{\sigma^2}||\mathbf{H}_1 e^{j\phi_1} + \mathbf{N}_1 - \hat{\mathbf{H}}_2 e^{\phi_2+j\phi} - e^{j\phi}\mathbf{N}_2||^2 \\
=&\frac{||\mathbf{N}_1 - e^{j\phi}\mathbf{N}_2||^2}{\sigma^2} \\
=&\frac{1}{\sigma^2}\left(\sum_{m=1}^{M}(\mathrm{Re}(\mathbf{X}_m))^2 + \sum_{m=1}^{M}(\mathrm{Im}(\mathbf{X}_m))^2\right) \sim \chi^2_{2M},
\end{aligned} \tag{5.14}$$

which is a Chi-square random variable with $2M$ degrees of freedom [56].

Similarly, when $\mathcal{H}_0$ is true, we usually have $\mathbf{H}_1 \neq \mathbf{H}_2$. From (5.1) and (5.4), the test statistic L under $\mathcal{H}_0$ can be written as

$$\begin{aligned}
&L = \frac{1}{\sigma^2}||\hat{\mathbf{H}}_1 - \hat{\mathbf{H}}_2 e^{j\phi}||^2 \\
=&\frac{1}{\sigma^2}||\mathbf{H}_1 e^{j\phi_1} - \mathbf{H}_2 e^{j(\phi+\phi_2)} + \mathbf{N}_1 - e^{j\phi}\mathbf{N}_2||^2 \\
=&\frac{1}{\sigma^2}||\mathbf{H}_1 - \mathbf{H}_2 e^{j(\phi+\phi_2-\phi_1)} + e^{-j\phi_1}\mathbf{N}_1 - e^{j(\phi-\phi_1)}\mathbf{N}_2||^2 \\
\approx&\frac{1}{\sigma^2}||\mathbf{H}_1 - \mathbf{H}_2 e^{j(Arg(\mathbf{H}_1\mathbf{H}_2^H))} + e^{-j\phi_1}\mathbf{N}_1 \\
&\quad - e^{j(\phi_2+Arg(\mathbf{H}_1\mathbf{H}_2^H))}\mathbf{N}_2||^2 \sim \chi^2_{2M,\mu},
\end{aligned} \tag{5.15}$$

where $\mu = ||\mathbf{H}_1 - \mathbf{H}_2 e^{jArg(\mathbf{H}_1\mathbf{H}_2^H)}||^2/\sigma^2$, which is a non-central Chi-square variable with a non-centrality 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

$$\alpha = Pr(L \leq k|\mathcal{H}_0) = F_{\chi^2_{2M,\mu}}(k), \tag{5.16}$$

$$\beta = Pr(L > k|\mathcal{H}_1) = 1 - F_{\chi^2_{2M}}(k), \tag{5.17}$$

where $F_X(\cdot)$ is the CDF of the random variable X. From (5.16) and (5.17), the false alarm rate for a given miss rate can be written as

$$\alpha(\beta) = F_{\chi^2_{2M,\mu}}(F^{-1}_{\chi^2_{2M,0}}(1-\beta)), \tag{5.18}$$

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 (5.1), (5.3), (5.7), 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

$$\begin{aligned}\mathbf{H}_1 x_1 - w\mathbf{H}_2 x_2 &= \mathbf{H}_1 x_1 - x_2 \hat{\mathbf{H}}_1 \hat{\mathbf{H}}_2^H \mathbf{H}_2/||\hat{\mathbf{H}}_2||^2 \\ &\approx \mathbf{H}_1 x_1 - x_2 \mathbf{H}_1 x_1 \mathbf{H}_2^H x_2^* \mathbf{H}_2/||\mathbf{H}_1||^2 x_2 x_2^* = \mathbf{0}.\end{aligned} \tag{5.19}$$

From (5.6) and (5.19), we have

$$L_{\mathcal{H}_1} \approx \frac{2||\mathbf{N}_1 - w\mathbf{N}_2||^2}{(1+|w|^2)\sigma^2} \sim \chi^2_{2M}. \tag{5.20}$$

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

$$L = \frac{2||\mathbf{H}_1 - w\mathbf{H}_2 + \mathbf{N}_1 - w\mathbf{N}_2||^2}{(1+|w|^2)\sigma^2} \sim \chi^2_{2M,\mu}, \tag{5.21}$$

where

$$\mu = 2||\mathbf{H}_1 - w\mathbf{H}_2||^2/(1+|w|^2)\sigma^2. \tag{5.22}$$

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

5.3.3 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

$$I(m) = \begin{cases} 1, & \text{Client } m \text{ is a Sybil} \\ 0, & \text{Client } m \text{ is legal} \end{cases} . \tag{5.23}$$

If the AP claims the m-th 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., $\mathbf{H}_1 = \mathbf{H}_n$, $n \leq N_s$, an ideal error-free decision is

$$I(m) = \begin{cases} 1, & 1 \leq m \leq N_s \\ 0, & N_s < m \leq N \end{cases} . \tag{5.24}$$

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

$$\alpha(N, N_s) = \begin{cases} \frac{\sum_{m=N_s+1}^{N} E[I(m)]}{N - N_s}, & N > N_s \\ 0, & N = N_s \end{cases} , \tag{5.25}$$

$$\beta(N, N_s) = \begin{cases} 0, & N_s = 1 \\ 1 - \frac{\sum_{m=1}^{N_s} E[I(m)]}{N_s}, & N_s > 1 \end{cases} , \tag{5.26}$$

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 5.3.2. More specifically, α in (5.8) and β in (5.9), correspond to $\alpha(2, 0)$ in (5.25) and $\beta(2, 2)$ in (5.26), 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

$$I(m) = \begin{cases} 1, & \exists L(m,n) \leq k, 1 \leq n \leq N, n \neq m \\ 0, & \text{otherwise} \end{cases}. \tag{5.27}$$

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

$$L(m,n) = \begin{cases} \frac{||\hat{\mathbf{H}}_m - \hat{\mathbf{H}}_n e^{j\phi}||^2}{\sigma^2}, & \text{constant power} \\ \frac{2||\hat{\mathbf{H}}_m - w\hat{\mathbf{H}}_n||^2}{(1+|w|^2)\sigma^2}, & \text{adaptive power} \end{cases}, \tag{5.28}$$

where $\phi = Arg(\hat{\mathbf{H}}_m \hat{\mathbf{H}}_n^H)$, and $w = \hat{\mathbf{H}}_m \hat{\mathbf{H}}_n^H / ||\hat{\mathbf{H}}_n||^2$. It is actually based on (5.4) and (5.6).

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

Theorem 5.3.2 *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 respectively by*

$$\alpha(N, N_s) = 1 - \frac{\sum_{m=N_s+1}^{N} (1 - F_{\chi^2_{2M,\mu(m,1)}}(k))^{N_s} \prod_{N_s+1 \leq n \leq N, n \neq m} (1 - F_{\chi^2_{2M,\mu(m,n)}}(k))}{N - N_s} \tag{5.29}$$

$$\beta(N, N_s) = (1 - F_{\chi^2_{2M}}(k))^{N_s - 1} \cdot \prod_{N_s+1 \leq n \leq N} (1 - F_{\chi^2_{2M,\mu(1,n)}}(k)), \tag{5.30}$$

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

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

$$\begin{aligned}
\alpha(N, N_s) &= \frac{\sum_{m=N_s+1}^{N} E[I(m)]}{N - N_s} \\
&= \frac{1}{N - N_s} \sum_{m=N_s+1}^{N} Pr[I(m) = 1] \\
&= 1 - \frac{1}{N - N_s} \sum_{m=N_s+1}^{N} Pr[I(m) = 0] \\
&= 1 - \frac{1}{N - N_s} \sum_{m=N_s+1}^{N} Pr[L(m, n) > k, \ \forall n \neq m] \\
&= 1 - \frac{1}{N - N_s} \sum_{m=N_s+1}^{N} \prod_{1 \leq n \leq N, n \neq m} Pr[L(m, n) > k] \\
&= 1 - \frac{1}{N - N_s} \sum_{m=N_s+1}^{N} \prod_{1 \leq n \leq N, n \neq m} (1 - F_{\chi^2_{2M, \mu(m,n)}}(k)) \\
&= 1 - \frac{1}{N - N_s} \sum_{m=N_s+1}^{N} (1 - F_{\chi^2_{2M, \mu(m,1)}}(k))^{N_s} \\
&\quad \prod_{N_s+1 \leq n \leq N, n \neq m} (1 - F_{\chi^2_{2M, \mu(m,n)}}(k)),
\end{aligned} \tag{5.31}$$

where

$$\mu(m, n) = 2||\mathbf{H}_m - w\mathbf{H}_n||^2/(1 + |w|^2)\sigma^2. \tag{5.32}$$

Similarly, we get the miss rate for a given k,

$$\begin{aligned}
\beta(N, N_s) &= 1 - \frac{\sum_{m=1}^{N_s} E[I(m)]}{N_s} \\
&= 1 - \frac{\sum_{m=1}^{N_s} Pr[I(m) = 1]}{N_s} \\
&= Pr[I(1) = 0] = Pr[L(1, n) > k, \ \forall n = 2, \cdots, N] \\
&= (1 - F_{\chi^2_{2M}}(k))^{N_s - 1} \prod_{n = N_s+1, \cdots, N} (1 - F_{\chi^2_{2M, \mu(1,n)}}(k)).
\end{aligned} \tag{5.33}$$

■

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

$$\alpha(N,1) = 1 - \frac{\sum_{m=2}^{N} \prod_{n \neq m} (1 - F_{\chi^2_{2M,\mu(m,n)}}(k))}{N-1}. \tag{5.34}$$

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

$$\beta(N,N) = (1 - F_{\chi^2_{2M}}(k))^{N-1}. \tag{5.35}$$

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

5.4 Multiple-AP Sybil Detection

It is common practice that wireless networks are deployed with multiple APs (i.e., $J > 1$). If we have additional APs available, these APs 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 non-zero, and denote the estimated channel response between the n-th client and the j-th AP as $\hat{\mathbf{H}}_n(j)$, where $1 \leq n \leq N$, and $1 \leq j \leq J$.

Suppose the APs cooperate in the Sybil detection process, using (5.27) 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 rotation. 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.

5.4.1 Synchronous APs

The channel frequency responses from synchronous APs have the same phase shift and magnitude scaling factor. Hence, we can ignore which AP the channel vector comes from, and combine them into an extended channel vector, $\underline{\hat{\mathbf{H}}}_n = [\hat{\mathbf{H}}_n(1); \hat{\mathbf{H}}_n(2); \cdots; \hat{\mathbf{H}}_n(J)]$. 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 (5.6),

$$L(m,n,J) = 2\frac{||\underline{\hat{\mathbf{H}}}_m - w\underline{\hat{\mathbf{H}}}_n||^2}{(1+|w|^2)\sigma^2}, \tag{5.36}$$

$$w = \underline{\hat{\mathbf{H}}}_m \underline{\hat{\mathbf{H}}}_n^H / ||\underline{\hat{\mathbf{H}}}_n||^2. \tag{5.37}$$

5.4.2 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, (5.6), from the J APs, i.e.,

$$L(m,n,J) = 2\sum_{j=1}^{J} \frac{||\hat{\mathbf{H}}_m(j) - w(j)\hat{\mathbf{H}}_n(j)||^2}{(1+|w(j)|^2)\sigma^2}, \tag{5.38}$$

$$w(j) = \hat{\mathbf{H}}_m(j)\hat{\mathbf{H}}_n^H(j) / ||\hat{\mathbf{H}}_n(j)||^2. \tag{5.39}$$

Theorem 5.4.1 *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 respectively by*

$$\alpha(N,N_s,J) = 1 - \frac{1}{N-N_s}\sum_{m=N_s+1}^{N}(1-F_{\chi^2_{2JM,\mu(m,1)}}(k))^{N_s}\prod_{N_s+1\le n\le N, n\neq m}(1-F_{\chi^2_{2JM,\mu(m,n)}}(k)) \tag{5.40}$$

$$\beta(N,N_s,J) = (1-F_{\chi^2_{2JM}}(k))^{N_s-1}\prod_{N_s+1\le n\le N}(1-F_{\chi^2_{2JM,\mu(1,n)}}(k)), \tag{5.41}$$

where

$$\mu(m,n) = \frac{2||\underline{\boldsymbol{H}}_m - w\underline{\boldsymbol{H}}_n||^2}{(1+|w|^2)\sigma^2}, \tag{5.42}$$

when the APs are synchronous; otherwise, when using asynchronous APs,

$$\mu(m,n) = \sum_{j=1}^{J} \frac{2||\boldsymbol{H}_m(j) - w(j)\boldsymbol{H}_n(j)||^2}{(1+|w(j)|^2)\sigma^2}, \tag{5.43}$$

where w and $w(j)$ are given by (5.37) and (5.39), respectively.

Proof: 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 non-central Chi-square variable with a non-centrality parameter μ, i.e.,

$$L = 2\sum_{j=1}^{J} \frac{||\mathbf{H}_1(j) - w(j)\mathbf{H}_2(j) + \mathbf{N}_1(j) - w(j)\mathbf{N}_2(j)||^2}{(1+|w(j)|^2)\sigma^2} \sim \chi^2_{2JM,\mu}, \tag{5.44}$$

where

$$\mu = 2\sum_{j=1}^{J} ||\mathbf{H}_1(j) - w(j)\mathbf{H}_2(j)||^2/(1+|w(j)|^2)\sigma^2. \tag{5.45}$$

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.,

$$L = 2\sum_{j=1}^{J} \frac{||\mathbf{N}_1(j) - w(j)\mathbf{N}_2(j)||^2}{(1+|w(j)|^2)\sigma^2} \sim \chi^2_{2JM}. \tag{5.46}$$

Similar to the proof of Theorem 5.3.2, the false alarm rate α and the miss rate β, respectively, are given by,

$$\alpha(N,N_s,J) = 1 - \frac{\sum_{m=N_s+1}^{N}(1-F_{\chi^2_{2JM,\mu(m,1)}}(k))^{N_s}\prod_{N_s+1\le n\ne m\le N}(1-F_{\chi^2_{2JM,\mu(m,n)}}(k))}{N-N_s} \tag{5.47}$$

$$\beta(N,N_s,J) = (1-F_{\chi^2_{2JM}}(k))^{N_s-1}\prod_{n=N_s+1,\cdots,N}(1-F_{\chi^2_{2JM,\mu(1,n)}}(k)), \tag{5.48}$$

where

$$\mu(m,n) = 2\sum_{j=1}^{J} ||\mathbf{H}_m(j) - w(j)\mathbf{H}_n(j)||^2/(1+|w(j)|^2)\sigma^2, \tag{5.49}$$

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

5.5 Implementation Issues

5.5.1 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 pilot 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 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.

5.5.2 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.

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) [61, 62].

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 in 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, the CRC parity check result is utilized to catch Sybil nodes who change the pilot transmission patterns.

Single-Carrier-based Systems: The proposed scheme can also be implemented in the wideband single carrier systems, e.g., code division multiple access (CDMA) 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. We 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 $W = (1 + \mathcal{B})/T$ [63]. 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 $[1, 0, 0, \cdots, 0]$, and every T seconds 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, $\mathcal{B}$).

5.5.3 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 [64]. 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, (5.36).

5.5.4 Integration with Spoofing Detection

We can integrate the proposed Sybil detection scheme with a spoofing detector (see Chapter 4) 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 [39].

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 (5.4). The rejection region for a spoofing attack is defined as 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.

5.6 Simulation and Numerical Results

5.6.1 Simulation Model

We have done simulations for a typical office building, for which a top view of the first floor is shown in Fig. 5.2. This floor of the building is 120 meters long, 14 meters wide and 4 meters high. For our experiments, we placed the APs in the hallway (the filled-in circles) at a height of 3 meters, 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 m $\times$ 67 m area, (outlined with a dashed line), and placed the clients randomly on a uniform grid of points with 1.5-meter 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

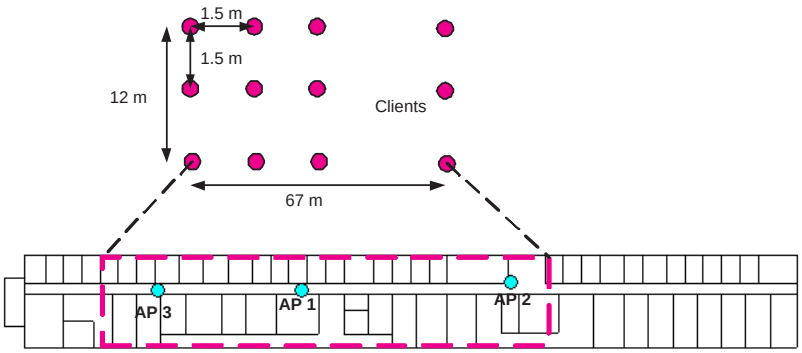


Figure 5.2: System topology assumed in the simulations. Three APs are located at [45.6, 6.2, 3.0] m, [77.0, 5.0, 3.0] m, and [24.0, 6.2, 3.0] m, respectively, in a 120 m × 14 m × 4 m office building. All clients, including both legal clients and Sybil, are located on dense grids at a height of 2 m. There are a total of 405 grid points.

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 mW. Noting that $P_N = \eta N_F b$, where η is the thermal noise density in mW/Hz, N_F is the receiver noise figure, and b is the measurement noise bandwidth per tone in Hz, we can write

$$\sigma^2 = \frac{\eta N_F b}{P_T/M}. \tag{5.50}$$

5.6.2 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, $M = 1, \cdots, 8$, 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 dB to 80 dB, with a median value of 35 dB, for $P_T = 10$ mW and $M = 1$.

Figure 5.3 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 Equation (5.50). 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. 5.4 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 mW and 1 mW pilot power, respectively, in order to make $\alpha < 0.01$ and $\beta = 0.01$. In addition, our scheme requires at least 2 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. 5.5 that the false alarm rate decreases with the system bandwidth in wideband systems, and remains within an acceptable range in narrowband systems with 2 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. 5.6 presents the performance with multiple clients (4 legal clients), including

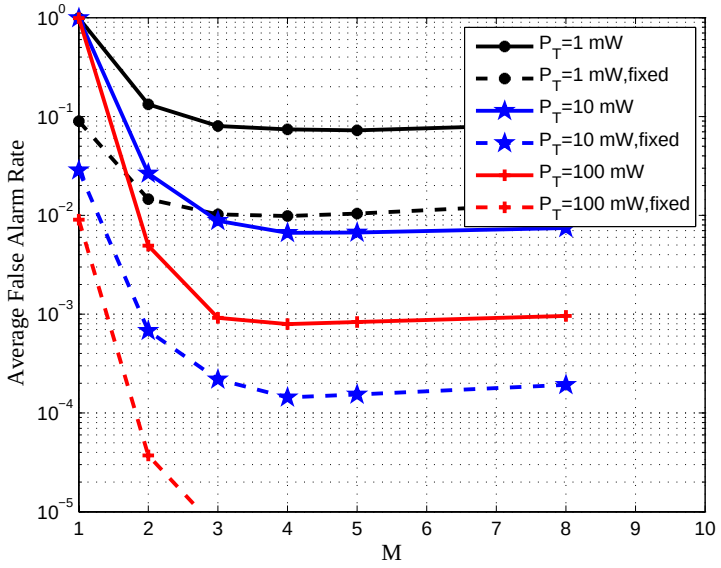


Figure 5.3: Average false alarm rate of Sybil detection in wideband systems, α, for a given miss rate $\beta = 0.01$, with two clients, one AP, $W = 20$ MHz, and $b = 0.25$ MHz. The curves with notation 'fixed' correspond to the cases where the receiver knows that the Sybil node uses constant power.

the receiver operating characteristic (ROC) curves. As indicated in (5.29) and (5.30), 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.

5.7 Experimental Verification

We verified the proposed scheme via field measurements in a different office building, for which a top view is shown in Fig. 5.7. The experimental settings were similar to those

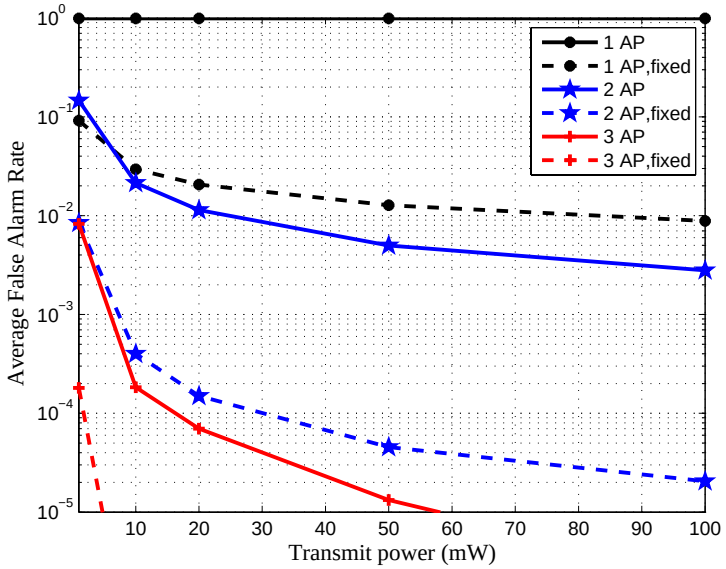


Figure 5.4: Average false alarm rate, α, for a given miss rate of $\beta = 0.01$, in narrowband systems, with 2 clients, $W = 300$ kHz, $M = 1$, and $b = 0.25$ MHz. The J APs are synchronous to each other. The curves with notation 'fixed' correspond to the cases where the receiver knows that the Sybil node uses constant power.

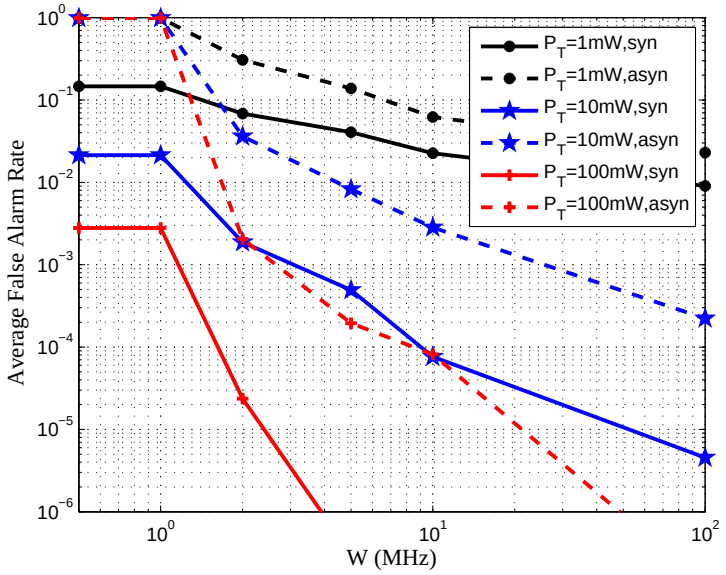
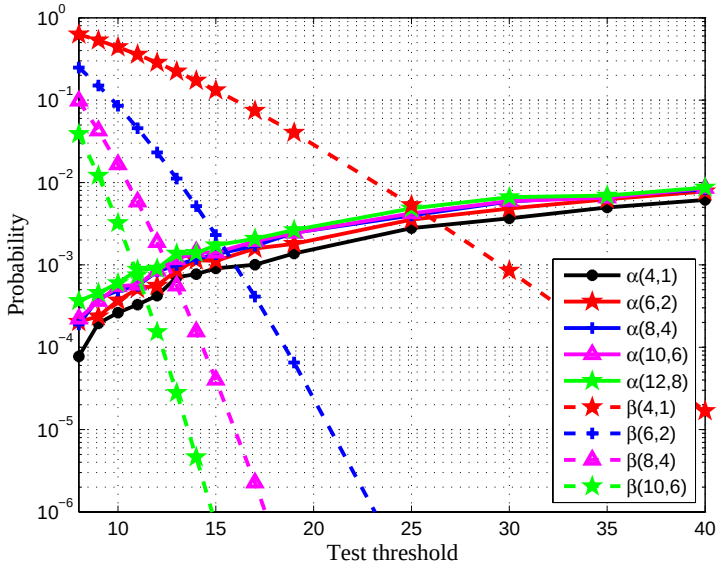
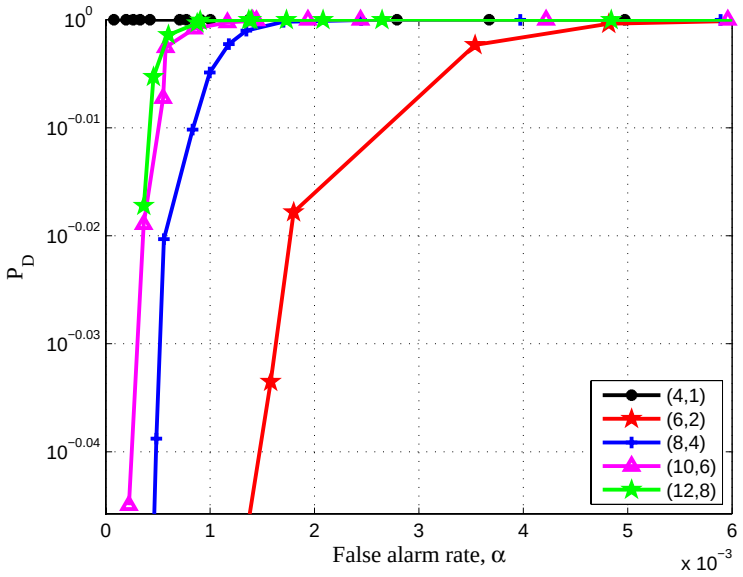


Figure 5.5: Impact of system bandwidth on Sybil detection, with 2 clients, 2 APs, $b = 0.25$ MHz, and $\beta = 0.01$. We set $M = 1$ when $W \leq 1$ MHz, $M = 2$ for $W = 2$ MHz, and $M = 3$ otherwise. The curves with notations 'syn' and 'asyn' correspond to synchronous APs and asynchronous APs, respectively.



(a) Performance probability



(b) Receiver operating characteristic

Figure 5.6: Performance of Sybil detection in the (N, N_s) systems, where there is one AP, 4 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.

using WiSE, except that the client grids were in a 4.55 m $\times$ 12.80 m area with 0.91-meter 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 previous section, 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 dB 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. 5.2.

Figure 5.8 presents the performance metrics as a function of test threshold k, given 4 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. 5.6.

5.8 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 [65–68]. Their performance was improved by exploiting the location information of sensor nodes [69]. The use of pairwise keys to prevent Sybil attacks was briefly discussed in [70]. These key management schemes, however, usually incur a large system overhead associated with key management,

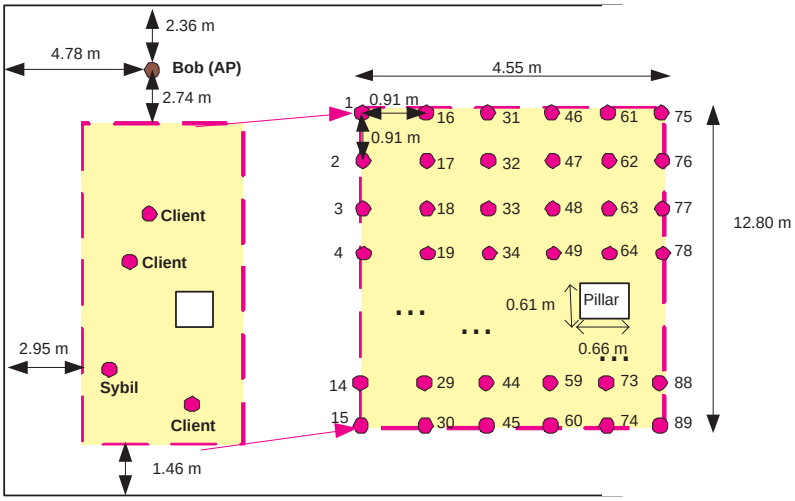


Figure 5.7: System topology assumed in the verifications. The serving AP is located at one corner in a large room. All clients, including both legal clients and Sybil, are located on 4.55 m $\times$ 12.80 m horizontal grids with 0.91-meter separations (with 89 grid points). Both AP and clients are at a height of 1.5 m.

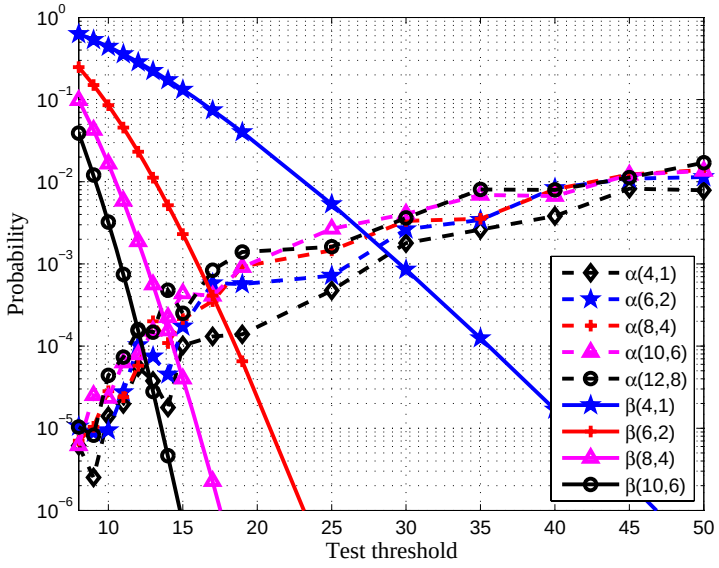


Figure 5.8: Performance of Sybil detection with one AP, in the (N, N_s) systems shown in Fig. 5.7, where there is one AP, 4 legal clients, and N_s ($= N - 4$) Sybil clients. We assume $M = 5$, $W = 20$ MHz, $P_T = 1$ μW, and $b = 0.25$ MHz.

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 among 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) [7, 36, 52]. 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 [53].

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 [71]. An authentication method to detect spoofing attacks using hypothesis testing was defined and further explored in [39–42]. Meanwhile, Patwari and Kasera propose the use of the channel impulse response to discriminate among the terminal locations in [53].

5.9 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 access points, 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 vector network analyzer. 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 3 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 receiver operating characteristic 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 access points can

overcome this limitation, and make channel-based authentication viable for narrowband systems.

Chapter 6

Conclusion

In this thesis, we have investigated the use of channel information to improve several higher-layer functions associated with wireless networks, based on the fact that the wireless medium contains location-specific information at various scales. This work consists of two parts: In the first part, sensor networks are deployed to measure the distribution of received signal strength, which is influenced by the large-scale channel gain variations, in order to estimate signal coverage (e.g., outage probability) and to locate mobiles. In the second part, a receiver (e.g., a WLAN access point) measures – from each received transmission – its current channel response, which is influenced by multipath (small-scale channel gain variations), in order to discriminate among transmitters and thus detect spoofing and Sybil attacks.

The first application we covered was the estimation of signal coverage, which is critical for the radio resource management and site planning of wireless systems, notably cellular systems, WLAN and DVB-H. The coverage measurements are performed using sensor networks in order to provide a round-the-clock, non-labor-intensive service that can facilitate slow adaptive changes in radio resources. In Chapter 2, we have demonstrated that accurate coverage outage estimation based on sensor networks is possible and moreover, that the required number of such measurements can be substantially reduced via importance sampling. We proposed a practical partial-cell sensor placement that does not require

channel parameter information, wherein the power-measuring sensors are distributed in a random and uniform way over base-mobile distances from 50% to 100% of the cell radius. Compared with the full-cell placement, the partial-cell placement reduces the number of sensors by ∼33%, while accurately estimating the cell outage probability.

As a future research direction, it would be interesting to perform field tests to verify the performance of the sensor placements in a multiple-cell environment, and to further analyze this issue from the viewpoint of measurement theory and data mining. Further, while we have focused in this thesis on sensor-based coverage estimation, a given operator may want to consider a wide range of approaches, including: (1) The traditional combining of site data with drive testing; (2) deploying a dedicated network of sensors (which is the case investigated here); (3) renting service from an existing multipurpose sensor network; (4) using a set of subscriber mobiles, equipped with GPS, to periodically measure and report power measurements; and so on. For those approaches based on sensor or mobile measurements, the rate of measurement-and-report (e.g., hourly, daily, etc) can be tailored to maintain acceptable levels of battery drain. Choosing among candidate approaches would require a cost/performance tradeoff analysis.

Another application of sensor networks is to mobile localization, which not only helps to improve many functions of wireless networks, such as radio resource management, mobility management and overall cellular system design, but also is critical for security purposes. In Chapter 3, we have investigated the application of sensor networks to locate mobiles, based on the received signal strength at the sensor receivers from a mobile's transmission. The investigation used a generic path-loss model incorporating distance effects and spatially correlated shadow fading. We have described four simple localization schemes and showed that they all meet E-911 requirements in most environments. Performance can be further

improved by implementing the MMSE algorithm, which ideally reaches the Cramer-Rao Bound. We have compared the MMSE algorithm and the four simple schemes when the model parameters are estimated via inter-sensor measurements.

Considering the sensor-based localization schemes described in Chapter 3, the following topics are promising future directions: (1) Investigate localization in the presence of interference, either from non-malicious users or from adversary radio sources, and devise alternative schemes, as appropriate; (2) Investigate the use of any such techniques in the context of cognitive radio (CR) networks [72]. We can envision embedding sensors within a CR environment, playing the role of "spectrum police". In such an application, the objective would be to use the police sensors to localize errant cognitive radios that are not properly transmitting, and then employ a second means to punish those errant cognitive radios, such as turning them off or adding their identities to a blacklist.

The second part of the thesis focused on the use of multipath information to improve wireless network security. Wireless systems are vulnerable to security threats, because of the broadcast nature of radio and the fact that users can easily change their MAC addresses, the basis for the receiver to identify senders. On the other hand, studies have shown that even advanced wireless security standards, such as 802.11i, have security flaws, such as the lack of mutual authentications and the protection of the control messages/management frames. Moreover, not every wireless system can afford these computationally expensive security mechanisms.

To address this problem, in Chapter 4 and 5, we have proposed a PHY-layer authentication scheme to detect spoofing attacks and Sybil attacks in wireless networks, based on the uniqueness of channel responses in rich-scattering environments. The scheme discriminates among transmitters with little additional system overhead, as it exploits pilots or preambles

that already exist in most wireless systems.

More specifically, we have built a generalized likelihood ratio test to detect attacks, considering environmental changes, terminal mobility, radio interference, receiver thermal noise and receiver phase drift. We have also proposed a simplified test with unknown parameters, and as a comparison, a test based on an adaptive filter of the channel estimation. We have verified the performance of the PHY-layer authentication scheme, using stochastic channel modeling, site-specific ray-tracing and field tests based on a network analyzer and an 802.11 testbench. Results have confirmed the efficacy of the scheme for realistic values of the measurement bandwidth (e.g., $W \sim 10$ MHz), number of response samples (e.g., $M \leq 10$) and transmit power (e.g., $P_T \sim 100$ mW). For example, the miss rate is generally smaller than 0.01, for a specified false alarm rate of 0.01, when the simplified test is used to detect spoofing attacks in a static channel environment.

We have also devised a double-layer authentication protocol to integrate our physical-layer authentication scheme into wireless systems, whereby the scheme either combines with higher-layer security mechanisms or works independently with performance degradation. Specifically, without the help of a higher-layer authentication process, the scheme has a much higher false alarm rate and miss rate in spoofing detection, due to its error propagation nature.

The channel-based authentication schemes described here suggest a number of research topics. To cite just a few: (1) Quantify all the benefits that the scheme brings to wireless security, e.g., the computation time that it saved for 802.11i when subjected to a series of spoofing attacks; (2) Perform some "online" authentication tests using an 802.11 test-bench in realistic communication scenarios; (3) Apply the channel-based scheme to improve authentication in a sensor-based cognitive radio network. In such a scenario, the police

sensors cited above might detect transmitters pretending to be primary users by exploiting the received channel information.

References

[1] T. Rappaport, *Wireless Communications Principles and Practice*, Prentice Hall, NJ, 1996.

[2] J. Caffery and G. Stuber, "Overview of radiolocation in CDMA cellular systems," *IEEE Commun. Mag.*, vol. 35, pp. 38–45, April 1998.

[3] FCC Docket No. 94-102, "Revision of the commission's rules to ensure compatibility with enhanced 911 emergency calling systems," RM-8143, July 1996.

[4] FCC NEWS, "FCC adjusts its rules to fasilitate the facilitate the development of nationwide enhanced wireless 911 systems," September 2000.

[5] H. Yang, F. Ricciato, S. Lu, and L. Zhang, "Securing a wireless world," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 442–454, February 2006.

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

[7] 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.

[8] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," in *MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking*, 2001, pp. 180–189.

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

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

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

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

[13] P. Bahl and V.N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *IEEE INFORCOM*, 2000.

[14] A. F. Molisch, *Wireless Communications*, John Wiley and Sons, 2005.

[15] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

[16] V. Erceg and et al, "An empirically based path loss model for wireless channels in suburban environments," *IEEE J. Select. Areas Commun.*, vol. 17, pp. 1205 – 1211, July 1999.

[17] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electron Lettrs.*, vol. 27, pp. 2145–2146, Nov 1991.

[18] P. Hahn and M. Jeruchim, "Developments in the theory and application of importance sampling," *IEEE Trans. Commun.*, vol. 35, pp. 706 – 714, July 1987.

[19] T. Kailath, A. H. Sayed, and B. Hassibi, *Linear Estimation*, Prentice-Hall, 2000.

[20] S. Kishore, L. J. Greenstein, H. V. Poor, and S. C. Schwartz, "Uplink capacity in a cdma macrocell with a hotspot microcell: exact and approximate analyses," *IEEE Trans. On Wireless Commun.*, vol. 2, pp. 364–374, March 2003.

[21] W. C. Jakes, *Microwave Mobile Communications*, chapter 7.2.1, IEEE Press, 1994.

[22] V. H. MacDonald, "The cellular concept," *Bell Sys. Tech. J.*, vol. 58, pp. 15–41, Jan. 1979.

[23] H. Holma and A. Toskala, *WCDMA for UMTS- Radio Access for Third Generation Mobile Communications*, John Wiley and Sons, New York, 2000.

[24] L. Xiao, L. Greenstein, N. Mandayam, and S. Periyalwar, "Sensor networks for estimating and updating the performance of cellular system," in *IEEE International Conference on Communications (ICC)*, Istanbul, Turkey, June 2006.

[25] L. Xiao, L. Greenstein, and N. Mandayam, "Distributed measurements for estimating and updating cellular system performance," *IEEE Trans. Commun.*, vol. 56, pp. 991–998, June 2008.

[26] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," *Computer Networks*, pp. 499–518, November 2003.

[27] L. Doherty, K. Pister, and L. Ghaoui, "Convex position estimation in wireless sensor networks," in *IEEE INFOCOM*, 2001.

[28] A. Savvides, H. Park, and M. Srivastava, "The bits and flops of the N-hop multilateration primitive for node localization problems," in *First ACM International Workshop on Wireless Sensor Networks and Application*, 2002.

[29] B. Parkinson and J. Spilker, *Global positioning system: theory and application*, American Institute of Astronautics and Aeronautics, 1996.

[30] D. Niculescu and B. Nath, "Ad-hoc positioning system," in *IEEE GLOBECOM*, Nov. 2001.

[31] D. Moore, J. Leonar, D. Rus, and S. Teller, "Robust distributed network localization with noisy range measurements," in *2nd ACM SenSys*, Maryland, USA, Nov. 2004.

[32] M.D Srinath, P.K. Rajasekaran, and R. Viswanathan, *Introduction to Statistical Signal Processing with Applications*, Prentice Hall, New Jersey, 1996.

[33] N. Patwari, J. Ash, S. Kyperountas, A. Hero, R. Moses, and N. Correal, "Locating the nodes, cooperative localization in wireless sensor networks," *IEEE Signal Processing Mag.*, pp. 54–69, July 2005.

[34] N. Patwari and A. Hero, "Using proximity and quantized RSS for sensor localization in wireless networks," in *ACM International Conference on Wireless Sensor Networks and Applications*, San Diego, CA, USA, 2003.

[35] L. Xiao, L. Greenstein, and N. Mandayam, "Sensor-assisted localization in cellular systems," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 4244–4248, December 2007.

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

[37] 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.

[38] W.C. Jakes Jr., *Microwave Mobile Communications*, Wiley, 1974.

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

[40] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. on Wireless Communications*, vol. 7, pp. 2571–2579, July 2008.

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

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

[43] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *IEEE Trans. on Wireless Communications*, in review.

[44] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics & Security*, in review.

[45] W. Trappe and L.C. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall, 2002.

[46] C. Corbett, R. Beyah, and J. Copeland, "A passive approach to wireless nic identication," in *IEEE International Conference on Communications*, 2006.

[47] J. Hall, M. Barbeau, and E. Kranakis, "Detection of transient in radio frequency fingerprinting using signal phase," in *Internet and Information Technology (CIIT)*, 2004.

[48] T. Kohno, A. Broido, and C. Claffy, "Remote physical device fingerprinting," in *IEEE Symposium on Security and Privacy*, 2005.

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

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

[51] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *The 14th Annual International Conference on Mobile Computing and Networking (ACM MobiCom)*, San Francisco, California,, USA, Sept. 2008.

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

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

[54] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*, Prentice Hall, Englewood Cliffs, 1993.

[55] S. Haykin, *Adaptive Filter Theory*, Prentice Hall, Englewood Cliffs, 1986.

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

[57] S. J. Fortune, D. H. Gay, B. W. Kernighan, O. Landron, M. H. Wright, and R. A. Valenzuela, "WiSE design of indoor wireless systems: Practical computation and optimization," *IEEE Computational Science and Engineering*, March 1995.

[58] IEEE Std 802.11 2007, "IEEE standard for information technology Telecommunications and information exchange between systems Local and metropolitan area networks specific requirements part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications," June 2007.

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

[60] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis and defenses," in *Proc. International Symposium on Information Processing in Sensor Networks (IPSN)*, April 2004, pp. 259 – 268.

[61] C. Snow, L. Lampe, and R. Schober, "Performance analysis and enhancement of multi-band OFDM for UWB commmunications," *IEEE Trans. Wireless Communications*, vol. 6, pp. 2182– 2192, June 2007.

[62] A. Ghosh, D. Wolter, J. Andrews, and R. Chen, "Broadband wireless access with WiMax/802.16: current performance benchmarks and future potential," *IEEE Communications Magzine*, vol. 43, pp. 129 – 136, February 2005.

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

[64] T.S. Rappaport, *Wireless Communications- Principles and Practice*, New Jersey: Prentice Hall, 2001.

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

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

[67] 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.

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

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

[70] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Elsevier Ad hoc networks journal*, vol. 1, pp. 293–315, Sept. 2003.

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

[72] I.F.Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "Next generation dynamic spectrum access cognitive radio wireless networks: A survey," *Computer Networks*, pp. 2127–2159, 2006.

Curriculum Vita

Liang Xiao

Education

2004-2009 Ph.D. in WINLAB, Electrical and Computer Engineering, Rutgers University

2000-2003 M.S. in Electrical Engineering, Tsinghua University, China

1996-2000 B.S. in Communication Engineering, Nanjing University of Posts & Telecommunications, China

Employment

2005-2009 Graduate Research Assistant, WINLAB, Electrical and Computer Engineering, Rutgers University

2008 Research Internship, InterDigital, King of Prussia, PA

2007 Research Internship, Bell Labs, Alcatel-Lucent, Whippany, NJ

2004-2005 Teaching Assistant, Electrical and Computer Engineering, Rutgers University

2003-2004 Teaching Assistant, Electrical and Computer Engineering, North Carolina State University

2000-2003 Research Assistant, Electrical Engineering, Tsinghua University, China

Publications

2008 L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. on Wireless Communications*, vol. 7, pp. 2571–2579, July 2008.

L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," *IEEE International Conference on Communications (ICC)*, pages 1520–1524, May 2008.

L. Xiao, L. Greenstein, and N. Mandayam, "Distributed measurements for estimating and updating cellular system performance," *IEEE Trans. Commun.*, vol. 56, pp.991–998, June 2008.

L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," *IEEE Conference on Information Sciences and Systems (CISS)*, March 2008, pp. 642–646.

L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *IEEE Trans. on Wireless Communications*, submitted.

L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," *IEEE Transactions on Information Forensics & Security*, submitted.

2007 L. Xiao, L. Greenstein, and N. Mandayam, "Sensor-assisted localization in cellular systems," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 4244–4248, December 2007.

L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," *IEEE International Conference on Communications (ICC)*, June 2007, pp. 4646–4651.

2006 L. Xiao, L. Greenstein, N. Mandayam, and S. Periyalwar. " Sensor networks for estimating and updating the performance of cellular system," *IEEE International Conference on Communications (ICC)*, pp. 2107-2111, Istanbul, Turkey, June 2006.

D. Samardzija, L. Xiao, and N. Mandayam, "Impact of pilot assisted channel state estimation on multiple antenna multiuser TDD systems with spatial filtering," *Conference on Information Sciences and Systems (CISS)*, pp. 381-385, Princeton, NJ, March 2006.

2004 L. Xiao and M. Xiao, "A new kind of MIMO-sensor networks M-SENMA," *IEEE Vehicular Technology Conference (VTC)*, vol. 4, pp. 2941-2945, Los Angeles, CA, Sept. 2004.

H. Dai, L. Xiao, and Q. Zhou, "Energy efficiency of MIMO transmission strategies in wireless sensor networks," *International Conference on Computing, Communications and Control Technologies (CCCT)*, Austin, TX, Aug. 2004.

2003 L. Xiao, S. Zhou, and Y. Yao, "QoS-oriented scheduling algorithm for 4G mobile multimedia OFDM communications," *IEEE International Symposium on Personal, Indoor and Mobile Radio (PIMRC)*, vol. 1, pp. 545-549, Sept. 2003, Beijing, China.

L. Xiao, A. Wang, S. Zhou, and Y. Yao, " A dynamic resource scheduling algorithm for OFDM system," *Asia-Pacific Conference on Communications (APCC)*, vol. 2, pp. 444-447, Malaysia, Sept. 2003.

L. Xiao, L. Dai, S. Zhou, and Y. Yao, "Information-theoretic capacity analysis in MIMO distributed antenna systems," *IEEE Vehicular Technology Conference (VTC)*, vol. 1, pp. 779-782, Jeju, Korea, April 2003.

A. Wang, L. Xiao, S. Zhou, X. Xu, and Y. Yao, " Dynamic Resource Management in the Fourth Generation Wireless Systems," *International Conference on Communication Technology (ICCT)*, Beijing, China, April 2003.

H. Zhuang, L. Dai, L. Xiao, and Y. Yao, "Spectral efficiency of distributed antenna system with random antenna layout," *Electronics Letter*, vol. 39, pp.495, March 2003.

2002 L. Xiao, L. Dai, H. Zhuang, S. Zhou, and Y. Yao, "A comparative study of MIMO capacity with different antenna topologies," *IEEE International Conference on Communication Systems (ICCS)*, vol. 1, pp. 431-435, Singapore, Nov. 2002.