Ad Hoc Networks 10 (2012) 831–844

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

# Detecting anomalous spectrum usage in dynamic spectrum access networks

Song Liu [a], Larry J. Greenstein [a], Wade Trappe [a], Yingying Chen [b,*]

[a] WINLAB, Rutgers University, North Brunswick, NJ 08902, United States
[b] Stevens Institute of Technology, Hoboken, NJ 07030, United States

ARTICLE INFO

*Article history:*
Available online 17 April 2011

*Keywords:*
Cognitive radio
Ad hoc networks
Dynamic spectrum access
Anomaly detection
Energy detection
Channel fading
Significance test

ABSTRACT

Dynamic spectrum access has been proposed as a means to share scarce radio resources, and requires devices to follow protocols that access spectrum resources in a proper, disciplined manner. For a cognitive radio network to achieve this goal, spectrum policies and the ability to enforce them are necessary. Detection of an unauthorized (anomalous) usage is one of the critical issues in spectrum etiquette enforcement. In this paper, we present a network structure for dynamic spectrum access and formulate the anomalous usage detection problem using statistical significance testing. The detection problem investigated considers two cases, namely, the authorized (primary) transmitter is (i) mobile and (ii) fixed. We propose a detection scheme for each case by exploiting the spatial pattern of received signal energy across a network of sensors. Analytical models are formulated when the distribution of the energy measurements is given and, due to the intractability of the general problem, we present an algorithm using machine learning techniques to solve the general case when the statistics of the energy measurements are unknown. Our simulation results show that our approaches can effectively detect unauthorized spectrum usage with a detection probability above 0.9 while keeping the false alarm rate less than 0.1 when only one unauthorized radio is present, and the detection probability is even higher for more unauthorized radios.



## 1. Introduction

The openness of the lower-layer protocol stacks in cognitive radios (CR), and their subsequent ability to adapt their waveforms, make them an appealing solution to dynamic spectrum access (DSA). The open nature of their protocols facilitates the flexible spectrum utilization and promote spectrally-efficient communication. Nevertheless, due to the exposure of the protocol stacks to the public, CR platforms can become a tempting target for adversaries or irresponsible secondary users [1]. A misuse of a CR can significantly compromise the benefits of DSA and threaten the privileges of incumbent users. This problem is especially challenging when CR are organized as an ad hoc network whose topology can be varying dynamically without central coordination [2,3]. Therefore, having the ability to enforce spectrum etiquettes is critical to effectiveness and correctness of a DSA system.

Identification of a malicious or reckless spectrum usage is an essential component of etiquette enforcement functions. This is basically a problem of distinguishing bad (unauthorized) transmissions from good (authorized) ones. While sophisticated signal processing techniques have been designed for detecting a desired signal from interference [4,5], they are of little help in this new paradigm of spectrum access. In many DSA systems (e.g., spectrum leasing), there can be a heterogeneous collection of authorized users and it is impractical to enumerate all of their signal structures. Even if the authorized signal is known

* Corresponding author.
*E-mail addresses:* song@winlab.rutgers.edu (S. Liu), ljg@winlab.rutgers.edu (L.J. Greenstein), trappe@winlab.rutgers.edu (W. Trappe), yingying.chen@stevens.edu (Y. Chen).

1570-8705/$ - see front matter © 2011 Published by Elsevier B.V.
doi:10.1016/j.adhoc.2011.04.003

(e.g., TV signals in IEEE 802.22), unauthorized users can disguise themselves by emulating authorized signals [6]. Therefore, an effective detection mechanism should not rely on programmable features, such as signal patterns. Fortunately, there is one aspect of the problem that cannot be easily modified—the propagation channel. This motivates us to pursue a reliable detection approach by making use of the characteristics of radio propagation. Specifically, in this paper, our detection will be based on the measurement of received signal energy at a group of collaborating sensors. Anomaly (or attack) detection based on received signal strength in wireless networks has been addressed in several papers. However, most of the existing studies assume some constraints on unauthorized transmitters, such as location [7] and mobility [8], or assume a constant transmission power of the authorized transmitters [9]. Such assumptions limit the flexibility and robustness of the solutions, especially for DSA in ad hoc networks.

In this paper, we investigate the spectrum anomaly detection problem in a broader context, where we do not make any assumption about unauthorized users. Since it is impractical to find a comprehensive description about anomalous behaviors, our detection method is only based on energy measurements from authorized transmitters. As a result, we formulate the detection problem as a statistical significance test. Here, we define normal usage as being no more than one transmitter (static or mobile) operating in each portion (e.g., channel) of the spectrum. Based on this assumption, our work is motivated by two properties of the spatial distribution of the received signal strength (RSS):

- The RSS (or received power in dB) from a single transmitter[1] decays approximately linearly with the logarithmic distance from the source, but it is no longer the case when the RSS is a sum of multiple transmitters at different locations.
- Transmitters at different locations will lead to different spatial distributions of the RSS. This spatial map, or *signalprint*, is an effective characterization of a transmitter.

By making use of these properties, we propose two detection methods according to the mobility of the authorized transmitter. Specifically, when the authorized transmitter is mobile, we exploit the property that log-scale path loss tends to increase linearly with log-distance. Unauthorized transmitters can then be detected by a significance test of the linearity of measured dB energy vs. log-distance. For the case where the authorized transmitter is fixed, we use the notion of signalprints, i.e., the spatial pattern of RSS. Unauthorized transmitters can then be detected by a significance test by comparing the current pattern with a stored pattern of the authorized transmitter. In each case, we initially assume the sensor network knows the statistics of the detected energies, and so it can set its decision region to obtain a specified false alarm rate. We also describe a machine-learning approach that can be used in the more general scenario when the statistics of the detected energies are *not* known.

The rest of the paper is organized as follows. Section 2 reviews previous works in anomalous signal detection. Section 3 presents our detection system structure and an analytical model of the energy detector output. In Section 4, we present a general significance testing model for the anomalous spectrum usage detection. We propose analytical and empirical solutions in Section 5 and present simulation results in Section 6. Section 7 concludes our work.

## 2. Related work

Spectrum usage enforcement is an emerging issue coming with the development of cognitive radios. [1] presented a trusted radio infrastructure dedicated to spectrum regulation in a DSA environment. The work formalized the spectrum policies and proposed a sensing architecture which is the system basis of our study. An unauthorized user in a DSA network can either be a reckless radio or a malicious attacker. The attack by emulating a primary user, named PUE by Chen and Park [7], is in fact a spoofing attack specially launched in DSA networks for illegal occupation of the spectrum. Detection methods based on location verification were proposed in [7,10]. Given the location of the primary transmitter, dedicated sensors collaboratively verify the source location of a received signal by its path loss fading rate, time difference of arrival, and location of the maximum received signal strength, respectively. All these methods are non-interactive based which do not require to modify the incumbent system. However, they all assume the primary transmitter's location is known and far away from the sensing area where illegal users reside. Otherwise, these methods may not work well due to the low accuracy of their location estimations.

Although few research efforts are dedicated to anomaly detection in DSA networks, there is a rich body of works addressing the detection of spoofing attacks in generic wireless networks. RSS based detection is one of the extensively studied methods due to its low implementation complexity and inherent correspondence to the propagation environments. The most related work to ours was published in [11]. In that work, two transmitters at different locations are distinguished by comparing their signalprints, a vector of RSS measured at multiple receivers. The proposed method share the same principle as the fingerprint based localization [12]. Specifically, transmitters at different locations lead to different spatial distribution of RSS and thus an attacker can be detected by examining the difference between its signalprint and the authentic one. Without specifying the false alarm probability, the paper reported above 95% detection accuracy by a testbed experiment. However, since the method is not based on the statistic of RSS values, it is impossible to choose a detection threshold according to a desired false alarm probability.

On the other hand, model based detection methods are based on the stochastic characteristics of RSS, where the detection threshold can be analytically determined given the false alarm probability. In [9], the authors proposed a

[1] Since the measuring circuit we use is commonly called an energy detector, we will use 'RSS' and 'energy' interchangeably in subsequent discussions.

Gaussian Mixture Model (GMM) to characterize the distribution of RSS, given the fact that commercial 802.11 radio devices generally have multiple antennas. The RSS from an authentic transmitter is profiled in terms of its GMM model parameters and attackers are detected using a likelihood-ratio test based on this profile. The method demonstrated superior performance to the method in [11]. However, it requires a constant transmission power at the authentic transmitter during detection, which limits its application in a more general system. A frequency domain fingerprint method was proposed in [13], where a profile of the channel response is built between the authentic transmitter and a receiver. The method also assumed a constant transmission power of the authentic user in order to compare two measurements at different times.

We have addressed the above limitations previously [14] by proposing two detection schemes based on the characteristics of radio propagation. In this paper, we have extended this previous work and present rigorous formulations for analyzing the two schemes.

## 3. A system model of dynamic spectrum access

### 3.1. DSA network structure

We consider a DSA network as illustrated in Fig. 1, where licensed (i.e., primary) and unlicensed (i.e., secondary) transmitters are scattered in an area filled with auxiliary spectrum sensors. In the paradigm of DSA, secondary users make use of idle spectrum resources by opportunistically accessing the network in these idle bands, which will not result in interference to incumbent users. However, such a spectrum efficiency can be easily undermined by a reckless user or an attacker who disguises itself as the primary transmitter in an attempt to convince other secondary users that a primary users has returned to use that spectrum band. Thus, a spectrum access policy is necessary as such a policy explicitly states the conditions for when a secondary user can and cannot use spectrum. The policies are defined by spectrum policy makers and are broadcast by a management unit, which can be either a stand alone central processor or a part of the primary transmitter's functions. For spectrum agility, the policies can change dynamically and users should be able to interpret them without human intervention. Interpreted languages, such as XG Policy Language (XGPL), have been proposed to formalize the policies [1]. To enforce spectrum policies, a trusted spectrum sensor network is responsible for collecting spectrum usage data and reporting them to the spectrum management unit. Given the inherent correlation of the spectrum measurements over space and time, various source coding and data fusion strategies have been proposed to optimize the cost of data gathering. Interested users are referred to the related work in [15,16]. By utilizing the measurements over multiple sensors, the management unit applies appropriate detection rules to identify anomalous usage and further locate anomalous transmitters. A cooperative decision scheme is often preferred to combat the sensing uncertainties due to fading channels and other spectrum irregularities [17,18].

To minimize the interference, we assume there should be no more than one authorized transmitter in a certain spectrum band at any time. In addition, since an interference signal may use the same signal structure as a primary

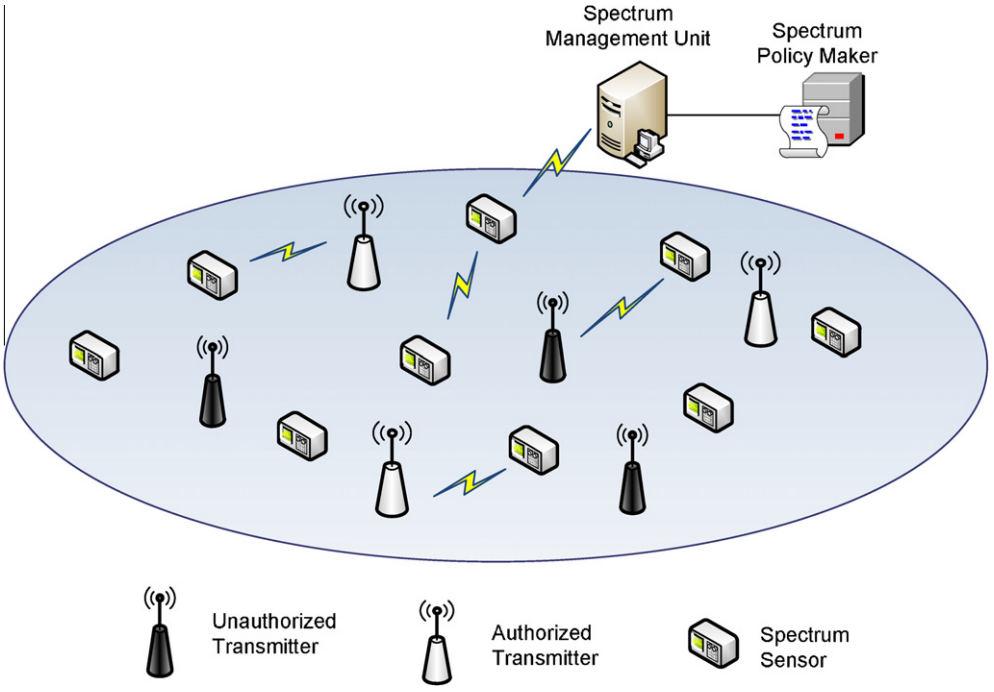


**Fig. 1.** A DSA environment, with primary and unauthorized transmitters within an area populated with spectrum sensors. Spectrum sensors cooperatively detect the presence of the unauthorized transmitters via the local exchange of energy measurements.

signal, the proposed detection algorithms will be based on received signal energy.

### 3.2. Energy detection model at one sensor

We consider a time-domain energy detector consisting of a band-pass filter (BPF), Nyquist sampling A/D converter, square-law device and integrator, as depicted in Fig. 2. At the $n$th sensor, the output of an energy detector can be expressed as

$$y_n = \sum_{l=1}^{L} |r_n(l) + w_n(l)|^2, \tag{1}$$

where $r_n(l)$ is the complex received signal at the $n$th sensor, and $w_n(l)$ is the complex Gaussian noise with zero mean and variance $\sigma_w^2$ at each phase. $w_n(l)$ is i.i.d. over the $L$ temporal energy samples. Previous work has shown that $y_n/\sigma_w^2$ has a noncentral chi square distribution [19]. In this section, we will show that its distribution can be approximated to lognormal for two extreme cases. The results here will be utilized to develop our detection algorithms.

Let $\mu_{r,n}(l)\cos\theta_n(l)$ and $\mu_{r,n}(l)\sin\theta_n(l)$ be the real and imaginary part of $r_n(l)$, respectively, where $\theta_n$ is an arbitrary phase value. Then the total received signal envelop $|r_n(l) + w_n(l)|$ is Ricean distributed with the $K$-factor

$$K_n(l) = \frac{\mu_{r,n}^2(l)}{2\sigma_w^2}. \tag{2}$$

It is easy to see that $K_n(l)$ is the instantaneous SNR at the $n$th sensor. By approximating a Ricean distribution as Nakagami [20, p. 79], $p_n = |r_n(l) + w_n(l)|^2$ has a gamma distribution with the PDF

$$f(p_n) = \frac{p_n^{m_{n,l}-1}}{\Gamma(m_{n,l})a_n^{m_{n,l}}} \exp\left(-\frac{p_n}{a_n}\right), \tag{3}$$

where

$$a_n = \frac{E[p_n]}{m_{n,l}}, \tag{4}$$

and

$$m_{n,l} = \frac{(K_n(l)+1)^2}{2K_n(l)+1}. \tag{5}$$

In the following two asymptotic cases, we show that the sum of $L$ energy samples are also gamma distributed.

#### 3.2.1. Asymptotic distribution of $y_n$ for very large-SNR

When $\mu_{r,n}^2(l) \gg 2\sigma_w^2, K_n(l) \gg 1$ and

$$a_n = \frac{E[p_n]}{m_{n,l}} = \frac{\mu_{r,n}^2(l) + 2\sigma_w^2}{m_{n,l}} = \frac{(2K_n(l)+1)2\sigma_w^2}{(K_n(l)+1)} \approx 4\sigma_w^2. \tag{6}$$

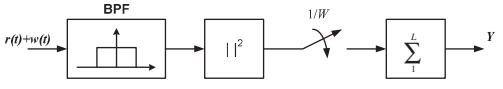


**Fig. 2.** The signal processing of the assumed energy detector. The square-law envelope detector produces the squared envelope of the BPF output, which is then sampled at uniform intervals. $W$ is the bandwidth of the BPF. The energy is estimated as the sum of $L$ such samples.

Then, the scale $a_n$ is a constant over the sample index $l$ and thus $y_n$ is also gamma distributed with the scale $a_n$ and the shape

$$m_n = \sum_{l=1}^{L} m_{n,l} = \sum_{l=1}^{L} \frac{(K_n(l)+1)^2}{2K_n(l)+1} \approx \frac{1}{2}\sum_{l=1}^{L}(K_n(l)+1) = \frac{L}{2} + \frac{1}{4\sigma_w^2}\sum_{l=1}^{L}\mu_{r,n}^2(l) = \frac{L}{2}(1+\bar{\beta}_n), \tag{7}$$

where

$$\bar{\beta}_n = \frac{\sum_{l=1}^{L}\mu_{r,n}^2(l)}{2\sigma_w^2 L}, \tag{8}$$

is the average received SNR within one measurement. When $\bar{\beta}_n$ is sufficiently large, $m_n$ in (7) can be further simplified by neglecting $L/2$. Following Appendix A, the dB quantity

$$Y_n = 10\log_{10}(y_n) \tag{9}$$

is approximately Gaussian-distributed.

#### 3.2.2. Asymptotic distribution of $y_n$ for very small-SNR

When $\mu_{r,n}^2(l) \ll 2\sigma_w^2$, $K_n(l) \approx 0$, $m_{n,l} \approx 1$, and

$$a_n = \frac{E[p_n]}{m_{n,l}} = \frac{(2K_n(l)+1)2\sigma_w^2}{(K_n(l)+1)} \approx 2\sigma_w^2. \tag{10}$$

Again, the scale $a_n$ is a constant over the sample index $l$ and thus $y_n$ is also gamma distributed with the scale $a_n$ and the shape

$$m_n = \sum_{l=1}^{L} m_{n,l} \approx L. \tag{11}$$

Similarly, $Y_n$ is Gaussian-distributed when $L$ is large. In addition, the signal power is negligible in this case and thus the energy measurement only includes the noise.

Therefore, for both of the above asymptotic distributions, $Y_n \sim \mathcal{N}\left(\mu_{Y,n}, \sigma_{W,n}^2\right)$ with the mean

$$\mu_{Y,n} = 10\log_{10}(a_n m_n), \tag{12}$$

and the variance

$$\sigma_{W,n}^2 = \left(\frac{10}{\ln 10}\right)^2 \psi'(m_n). \tag{13}$$

The parameters $a_n$ and $m_n$ are given by (6) and (7) or (10) and (11), depending on the approximations. A special treatment to $\mu_{Y,n}$ in the large-SNR approximation is that, we neglect the term, $L/2$, in (7), that is, $m_n = \bar{\beta}_n L/2$. The reason will be clear as follows.

In the detection analysis, we will approximate an energy measurement to either of these two asymptotic solutions, depending on the received SNR. It is then necessary to find an optimal SNR threshold to minimize the approximation error. From (7) we see that, when the average SNR $\bar{\beta}_n = 1$, two asymptotic approximations will give the same $\mu_{Y,n}$ and $\sigma_{W,n}^2$. Therefore, in the proposed analytical solutions, we will use the large-SNR approximation when the average SNR is greater than 0 dB, and use the small-SNR approximation otherwise.

### 3.3. Energy detection model over multiple sensors

In the case of a large-SNR, by neglecting the term $L/2$ in (7),

$$\mu_{Y,n} = 10\log_{10}\left(\sum_{l=1}^{L}\mu_{r,n}^2(l)\right). \tag{14}$$

Note that $Y_n$ is Gaussian-distributed conditional on the received signal energy $\sum_{l=1}^{L}\mu_{r,n}^2(l)$ within one measurement, we rewrite the energy detector output as

$$Y_n = Y_{0,n} + Y_{S,n} + Y_{W,n}, \tag{15}$$

where $Y_{0,n} + Y_{S,n} = \mu_{Y,n}$ and $Y_{W,n} \sim \mathcal{N}\left(0, \sigma_{W,n}^2\right)$ accounts for the randomness due to the noise.

We use $Y_{0,n}$ to quantify the measured energy due only to the deterministic path loss fading, and it is generally given by

$$Y_{0,n} = Y_0 - 10\gamma\log_{10}(d_n/d_0), \tag{16}$$

where $Y_0$ is the signal strength measured at the reference distance $d_0$, $d_n$ is the distance between the transmitter and the $n$th sensor, and $\gamma$ is the path loss exponent.[2]

Further, $Y_{S,n}$ accounts for the multipath and shadow fading at different locations, and we model $Y_{S,n}$ as a spatial Gaussian process,[3] $Y_{S,n} \sim \mathcal{N}\left(0, \sigma_{S,n}^2\right)$. Taking into account the spatial correlation of channel fading, we assume $\mathbf{Y}S = (Y_S,1, Y_{S,2}, \ldots, Y_{S,N})$ are jointly Gaussian, $Y_S \sim \mathcal{N}(0, \Sigma_S)$.

Since the randomness due to the noise (quantified by $Y_{W,n}$) and that due to the channel fading (quantified by $Y_{S,n}$) are independent, $Y_n$ is Gaussian-distributed over space, that is,

$$Y_n \sim \mathcal{N}\left(Y_{0,n}, \sigma_{S,n}^2 + \sigma_M^2 + \sigma_{W,n}^2\right). \tag{17}$$

In addition, the measurements from all the $N$ sensors, $\mathbf{Y} = (Y_1, Y_2, \ldots, Y_N)$, are also jointly Gaussian with the covariance matrix

$$\Sigma_Y = \Sigma_S + \Lambda_W, \tag{18}$$

where $\Lambda_W$ is a diagonal matrix and its $n$th diagonal element is $\sigma_{W,n}^2$.

In the case of very small-SNR, we virtually neglect the signal strength (see (10) and (11)) and thus the energy measurement $Y_n$ is i.i.d. Gaussian across sensors.

In the following, we devise detection algorithms based on the above models. Before proceeding, we note the summation over $l$ in (14) may itself vary from measurement to measurement, depending on the signal format. For example, for constant-envelope modulations, it will be fixed; and it will vary slightly for QPSK. For OFDM, the individual terms will be i.i.d. with a distribution close to exponential; thus, the summation over $l$ will be Gamma-distributed, with order $L$. Our detailed analysis of this case (not reported here) shows that the result is an added Gaussian term in $Y_n$, (15), which is totally correlated across $n$. For all practical values of $L$, the statistical variation is so small that its impact on the numerical results is negligible. We thus assert that our formulation is good for all signal formats.

[2] Here we do not specify the direction of a propagation link, as depicted in the model (16). Therefore, the authorized transmitter is assumed to use an omnidirectional antenna.

[3] The shadow fading is widely modeled as lognormal over space [21]. The multipath fading can be modeled as a Nakagami distribution and thus its gain (in the linear ratio) is also gamma distributed. Again by Appendix A, it approximates to lognormal. However, this approximation is not always accurate as the parameter $m$ in (39) can be small.

## 4. Modeling anomalous detection using significance testing

In general, we only have the information in the normal situation and thus the detection of anomalous usage can be formulated as a statistical significance testing problem. The received signal at each sensor is defined as:

$$\mathcal{H}_0 : r(t) + w(t), \quad \text{normal usage}, \tag{19a}$$
$$\mathcal{H}_1 : r(t) + u(t) + w(t), \quad \text{anomalous usage}, \tag{19b}$$

where $r(t)$ is the signal from an authorized transmitters complying with the spectrum policy, $u(t)$ is an unknown unauthorized signal, and $w(t)$ is noise that we assume to be additive and white Gaussian with zero mean. The normal spectrum usage is defined as the null hypothesis $\mathcal{H}_0$.

A significance testing problem consists of the following key components:

- Test statistic $\mathbf{v}$: a measure of the observed data.
- Acceptance region $\Omega$: if $\mathbf{v} \in \Omega$, we accept the null hypothesis $\mathcal{H}_0$.
- Significance level $\alpha$: the probability of incorrectly rejecting the null hypothesis, i.e., the probability of false alarm.

In our detection problem, the observed data is a series of energy measurements, $\mathbf{Y} = (Y_1, Y_2, \ldots, Y_N)$, where $Y_n$ is given by Sections 3.2 and 3.3. For different statistics of $\mathbf{Y}$ in what follows, we will define $\mathbf{v}$ and $\Omega$ so that, for a specified false alarm probability $\alpha$, $Prob(\mathbf{v} \notin \Omega|\mathcal{H}_0) \leqslant \alpha$, where $\mathbf{v}$ not in $\Omega$ declares the presence of the anomalous behaviors in the network.

## 5. Detecting unauthorized spectrum usage in DSA networks

Unlike the conventional energy detection problems where a signal is detected from noise based on the noise power level [19,22], it is generally impractical to apply a threshold based on the authorized signal strength to detect interference. The authorized signal strength can be time-variant because of several effects, such as power control and transmitter mobility. This power variation can render the energy estimation useless. In this section, we propose two detection algorithms, one for the case where the authorized transmitter is mobile and one that works better but only for the stationary case. Provided the distribution of the authorized signal energy is known, we present analytical solutions to determining detection thresholds. In the more general case where it is hard to obtain such information, we propose to utilize a machine learning technique to derive empirical thresholds.

### 5.1. Linearity check for a mobile authorized transmitter

Following the discussion in Section 3.1, there should be only one authorized transmitter at any time in the spectrum under surveillance. Thus, the detection problem becomes distinguishing between single and multiple transmissions in the same spectral resource. To do this, we need a decision statistic that captures the characteristics of the radiation power in the case of a single transmission. Provided a single radio source, we rewrite the energy detector output in (15) as

$$Y_n = Y_0 - 10\gamma \log_{10}(d_n/d_0) + Y_{R,n}, \tag{20}$$

where $Y_{R,n} = Y_{S,n} + Y_{W,n} \sim \mathcal{N}\left(0, \sigma_{S,n}^2 + \sigma_M^2 + \sigma_{W,n}^2\right)$. Eq. (20) shows that, when the received SNR is large, the energy measurement (in log-scale) is a linear function of the log-distance (i.e., $\log_{10}(d)$) plus a random Gaussian term, $Y_{R,n}$, across the sensors. On the other hand, this linearity breaks when the measurement consists of signals from multiple transmitters (as corresponds to anomalous spectrum activity). As depicted in Fig. 3, where we measure the received signal energy at 10 sensors for 10 independent trials, the energy from a single transmitter shows distinct linear decay with the log-distance, whereas the RSS from two transmitters does not present the similar pattern. Thus, by examining the linearity of the energy measurements with log-distance, we may distinguish the case of a single transmission (i.e., normal usage) from the case of multiple overlapped transmissions (i.e., anomalous usage). It is worth noting that, as shown in (15), this method relies on the linear property of the channel fading, and thus the detection is performed only based on the energy measurements where the received SNR is greater than 0 dB (i.e., the large-SNR approximation is acceptable). With a slight abuse of notations, $N$ in the following denotes the number of energy measurements we actually use, which is less or equal to the number of all the sensors.

Further, the distance $d_n$ between the transmitter and a sensor can be obtained in two ways: (a) the authorized transmitter periodically announces its location, using a signal format that is decodable at the sensors or (b) the sensors cooperatively estimate the transmitter location based on measured RSS. In either case, a sensor knows its own location.

Given the distance $d_n$, the remaining unknown parameters are the mean $Y_0$ and the path loss exponent $\gamma$. In general, it is hard to obtain their accurate values, so we use linear least squares to estimate them.

Suppose $\mathbf{Y} = (Y_1, \ldots, Y_N)^T$ is the vector of $N$ energy measurements, and

$$\mathbf{A} = \begin{bmatrix} 1 & -10\log_{10}(d_1/d_0) \\ \vdots & \vdots \\ 1 & -10\log_{10}(d_N/d_0) \end{bmatrix}. \tag{21}$$

Note that $\mathbf{A}$ has a rank of 2 as long as there are at least two sensors with difference distances from the transmitter. Then, the least square estimation of $Y_0$ and $\gamma$ gives

$$\begin{aligned} \begin{bmatrix} \hat{Y}_0 \\ \hat{\gamma} \end{bmatrix} &= \left(\mathbf{A}^T\mathbf{A}\right)^{-1}\mathbf{A}^T\mathbf{Y} = \left(\mathbf{A}^T\mathbf{A}\right)^{-1}\mathbf{A}^T\left(\mathbf{A}\begin{bmatrix} Y_0 \\ \gamma \end{bmatrix} + \mathbf{Y}_R\right) \\ &= \begin{bmatrix} Y_0 \\ \gamma \end{bmatrix} + \left(\mathbf{A}^T\mathbf{A}\right)^{-1}\mathbf{A}^T\mathbf{Y}_R, \end{aligned} \tag{22}$$

where $\mathbf{Y}_R = (Y_{R,1}, Y_{R,2}, \ldots, Y_{R,N})^T \sim \mathcal{N}(0, \Sigma_Y)$ as defined in (18). Further, we define the vector of the estimation error (residuals) $\hat{\mathbf{e}}$ as

$$\begin{aligned} \hat{\mathbf{e}} &= \mathbf{Y} - \hat{\mathbf{Y}} = \mathbf{A}\begin{bmatrix} Y_0 \\ \gamma \end{bmatrix} + \mathbf{Y}_R - \mathbf{A}\begin{bmatrix} \hat{Y}_0 \\ \hat{\gamma} \end{bmatrix} \\ &= \mathbf{Y}_R - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{Y}_R = (\mathbf{I} - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T)\mathbf{Y}_R. \end{aligned} \tag{23}$$

When the distance matrix $\mathbf{A}$ is exactly known, the residuals are independent of the transmission power. Based on the linearity of the propagation model, we infer that the distribution of the residuals in the normal usage case should differ from that of the anomalous case. Then, the residuals $\hat{\mathbf{e}}$ can be a measure of linearity. However, its

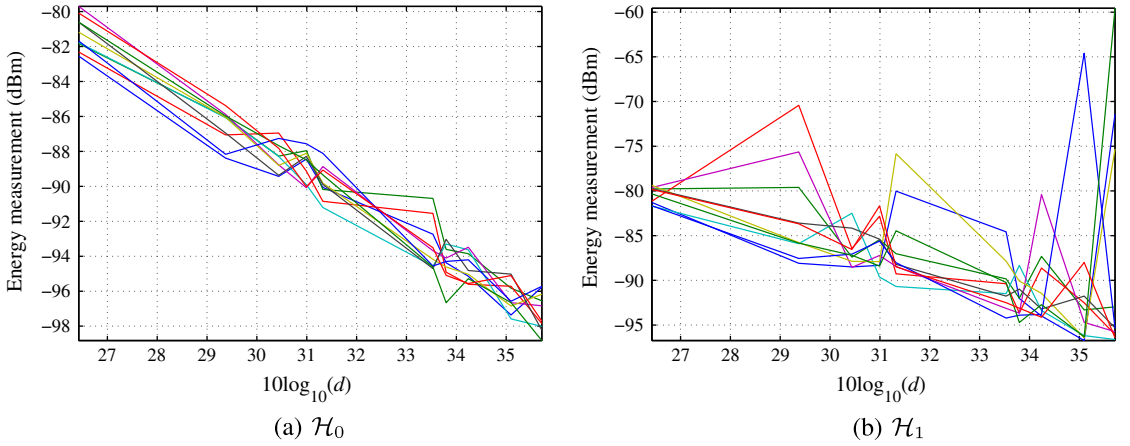


**Fig. 3.** Energy measurement vs. logarithmic distance between an authorized transmitter and $N = 10$ sensors. In an 100-m × 100-m area, the authorized transmitter is located at the center and the sensors are uniformly scattered. In the $\mathcal{H}_1$ case, one unauthorized transmitter is randomly located. Path loss exponent $\gamma = 3.5$ and $\sigma_{S,n} = 1$ dB in (15). The noise power is neglected. Detailed simulation settings are given in Section 6.1. Each curve denotes an independent trial with random shadow fading and random location of the unauthorized transmitter.

distribution is not always explicit. As Appendix B shows, the matrix $\mathbf{D} = (\mathbf{I} - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T)$ in (23) is singular, so $\hat{\mathbf{e}}$ is no longer a multivariate Gaussian even though $\mathbf{Y}_R$ is. To facilitate the analysis, we seek a new measure of the linearity, which not only has a known distribution but also retains as much information from $\hat{\mathbf{e}}$ as possible. Given that the $N \times N$ matrix $\mathbf{D}$ has two zero eigenvalues (see Appendix B), $\hat{\mathbf{e}}$ only has $N-2$ independent bases from $\mathbf{Y}_R$. Therefore, we can construct a new statistic $\hat{\mathbf{e}}_u$ whose distribution can be derived in the normal usage case, using the following theorem:

**Theorem 1.** *Given a multivariate Gaussian $\mathbf{Y}_R \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_Y)$ and a $N \times 2$ matrix $\mathbf{A}$ with rank of 2, we define $\hat{\mathbf{e}}_u = \mathbf{U}_2^T\hat{\mathbf{e}}$, where $\mathbf{U}_2$ is an $N \times (N-2)$ matrix consisting of $(N-2)$ eigenvectors of $\mathbf{A}\mathbf{A}^T$ that correspond to the $(N-2)$ zero eigenvalues. Then*

$$\hat{\mathbf{e}}_u \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_{\mathbf{e}}), \tag{24}$$

*where $\mathbf{\Sigma}_{\mathbf{e}} = \mathbf{U}_2^T\mathbf{\Sigma}_Y\mathbf{U}_2$.*

**Proof.** See Appendix B. □

Similar to the significance test in [23], we can define a likelihood-based acceptance region for $\hat{\mathbf{e}}_u$ as

$$\Omega = \{\hat{\mathbf{e}}_u : f(\hat{\mathbf{e}}_u) \geqslant f_T\}, \tag{25}$$

where the probability density function is

$$f(\hat{\mathbf{e}}_u) = (2\pi)^{-N/2}|\mathbf{\Sigma}_e|^{-1/2}\exp\left(-\frac{1}{2}\hat{\mathbf{e}}_u^T\mathbf{\Sigma}_e^{-1}\hat{\mathbf{e}}_u\right).$$

Then, $\Omega$ in (25) can also be expressed as

$$\Omega = \left\{\hat{\mathbf{e}}_u : \hat{\mathbf{e}}_u^T\mathbf{\Sigma}_e^{-1}\hat{\mathbf{e}}_u < T_e\right\}. \tag{26}$$

Therefore, we obtain the test statistic $\hat{\mathbf{e}}_{\mathrm{LCM}} = \hat{\mathbf{e}}_u^T\mathbf{\Sigma}_e^{-1}\hat{\mathbf{e}}_u$. It can be shown that $\hat{\mathbf{e}}_{\mathrm{LCM}}$ follows a chi-square distribution with $N-2$ degrees (e.g., see Section V-C in [23]). Thus, the false alarm probability is given by

$$P_F = \frac{\Gamma((N-2)/2, T_e/2)}{\Gamma((N-2)/2)}, \tag{27}$$

where $\Gamma(k, x)$ is the upper incomplete gamma function.

This probability is accurate only when the distance matrix $\mathbf{A}$ (or equivalently, the location of the authorized transmitter) is exactly known and the distribution of the energy measurements across sensors is lognormal. These two conditions are not often met in practice, which will result in an unknown distribution for the test statistic $\hat{\mathbf{e}}_{\mathrm{LCM}}$ and distort the target false alarm rate (i.e., $P_F$ in (27)), as we shall see in Section 6.2. To extend our algorithm to a more general scenario, we propose the application of One-class SVM (Support Vector Machines), proposed in [24], to find an acceptance region.

One-class SVM is a kernel based machine learning technique for data classification, which involves a training phase and a testing phase. Each data instance, either in the training set or in the testing set, is represented by one or multiple attributes. As the name of One-class SVM implies, all training data are from a class of interest and the goal is to empirically generate a model that can predict whether a data instance from the testing set belongs to this class. One-class SVM finds its use in the anomalous or outlier detection problems where the anomalous case cannot be accurately described using training data and thus the classification can only be formulated as a significance test (see Section 4). Therefore, the data attributes are the test statistics in our significance test model.

Since the SVM method can handle data with an unknown distribution, there can be many choices of data attributes in our anomalous detection problem. An obvious option is $\hat{\mathbf{e}}_{\mathrm{LCM}}$ derived in the analytical solution. However, it will result in a similar[4] detection performance to that of the analytical one in terms of the receiver operating characteristic (ROC). Since we are actually interested in the estimation residues $\hat{\mathbf{e}}$ given in (23), we use it directly in the SVM. $\hat{\mathbf{e}}$ is also more reliable compared to $\hat{\mathbf{e}}_{\mathrm{LCM}}$ as it involves less matrix manipulations, which are based on the assumption of the Gaussian distribution. Note that it is not necessary to assume the received SNR >0 dB in the SVM solution. Hence $\hat{\mathbf{e}}$ utilizes energy measurements from all the sensors regardless of the received SNR.

Provided the training data are sufficiently sampled from an underlying probability distribution (i.e., in the normal class), we apply One-class SVM to estimate a subset, $\Omega$ (i.e., a fraction of the training data), so that, any testing data from the same distribution will lie outside of $\Omega$ with a probability equal to a specified value, $v \in (0, 1)$. Apparently $v$ corresponds to the false alarm probability and $\Omega$ is the acceptance region in the significance test. In summary, given the energy measurements (thus $\hat{\mathbf{e}}$) that are well-sampled in the normal usage case, we use One-class SVM to find an empirical acceptance region corresponding to a specified false alarm probability, $P_F$. See Appendix C for the mathematical description of One-class SVM.

### 5.2. Signalprint check for a stationary authorized transmitter

Provided the authorized transmitter is stationary, we can further improve the performance of unauthorized signal detection by exploiting a more reliable metric, the signalprint. In this section, we present a fingerprint based method analogous to the fingerprint based localization [12]. Specifically, transmitters at different locations lead to different spatial distribution of RSS. Thus, an interference signal can be detected by examining the difference between its signalprint (i.e., the vector of energy measurements $\mathbf{Y}$) and the authorized one. The authorized signalprint can be obtained (i) if the authorized transmitter periodically broadcasts an "identity" signal that is decodable at the sensors or (ii) by using a previous measurement that is known from the authorized signal.

Denote the known authorized signal energy by $Y_n$ and the currently measured energy by $\widetilde{Y}_n$ at the $n$-th sensor. For measurements with large-SNR, since the channel is stationary, the shadowing and multipath fading $Y_{S,n}$ in (15) is constant over time. Thus,

[4] Note that the ROCs of the analytical solution and SVM are not necessarily the same even if they both use $\hat{\mathbf{e}}_{\mathrm{LCM}}$ as the test statistic, because they have different acceptance regions. Specifically, the analytical solution has a single-sided acceptance region as defined in (26) but the SVM has a double-sided acceptance region as given by (52).

$$\widetilde{Y}_n - Y_n = \widetilde{Y}_{0,n} - Y_{0,n} + \widetilde{Y}_{W,n} - Y_{W,n} = \widetilde{Y}_0 - Y_0 + \widetilde{Y}_{W,n} - Y_{W,n} = \widetilde{Y}_0 - Y_0 + dY_{W,n}. \quad (28)$$

Since $Y_{W,n}$ and $\widetilde{Y}_{W,n}$ are due to noise, they are independent of each other and $dY_{W,n} = \widetilde{Y}_{W,n} - Y_{W,n}$ is also Gaussian-distributed, that is, $dY_{W,n} \sim \mathcal{N}\left(0, \sigma^2_{\widetilde{W},n} + \sigma^2_{W,n}\right)$, where $\widetilde{Y}_{W,n} \sim \mathcal{N}\left(0, \sigma^2_{\widetilde{W},n}\right)$. The reference energy $Y_0$ can also be time-variant because (i) the authorized transmission power may change over time (e.g., by power control) and (ii) the signal strength $|r(t)|$ may change over time (e.g., an OFDM signal with many subcarriers). For measurements with small-SNR, we neglect the signal strength variation (see Section 3.2) comparing to $dY_{W,n}$. Combining the two approximations, we have[5]

$$\widetilde{Y}_n - Y_n = \begin{cases} C + dY_{W,n} & \text{if } \bar{\beta}_n \geqslant 0 \text{ dB}, \quad \text{(a)} \\ dY_{W,n} & \text{if } \bar{\beta}_n < 0 \text{ dB}, \quad \text{(b)} \end{cases} \quad (29)$$

where the signal strength shift $C = \widetilde{Y}_0 - Y_0$ is a constant across all the sensors. Denote $\mathbf{Y} = [Y_1, Y_2, \ldots, Y_N]^T$ and $\widetilde{\mathbf{Y}} = \left[\widetilde{Y}_1, \widetilde{Y}_2, \ldots, \widetilde{Y}_N\right]^T$. We estimate $C$ using a simple linear regression model,

$$\widehat{C} = \begin{cases} \widehat{C} = \frac{1}{N_r}\mathbf{e}_r^T\left(\widetilde{\mathbf{Y}} - Y\right) = \frac{1}{N_r}\sum_{n=1}^{N_r}\left(\widetilde{Y}_n - Y_n\right), & N_r > 0, \quad \text{(a)} \\ 0, & N_r = 0, \quad \text{(b)} \end{cases} \quad (30)$$

where $\mathbf{e}_r$ is a $N \times 1$ vector with the $n$th element

$$e_{r,n} = \begin{cases} 1 & \text{if } \bar{\beta}_n \geqslant 0 \text{ dB}, \quad \text{(a)} \\ 0 & \text{if } \bar{\beta}_n < 0 \text{ dB}. \quad \text{(b)} \end{cases} \quad (31)$$

$N_r$ is the number of 1's in $\mathbf{e}_r$. Without loss of generality, we assume the energy measurements from all the $N$ sensors are arranged so that the first $N_r$ measurements have SNR $\geqslant 0$ dB and thus the first $N_r$ elements of $\mathbf{e}_r$ are 1 and the rest of them are 0.

Then, the residue of the estimation is

$$\hat{\mathbf{e}} = \widetilde{\mathbf{Y}} - \mathbf{Y} - \widehat{C}\mathbf{e}_r = \widetilde{\mathbf{Y}} - \mathbf{Y} - \frac{1}{N_r}\mathbf{e}_r\mathbf{e}_r^T\left(\widetilde{\mathbf{Y}} - \mathbf{Y}\right), \quad \text{for } N_r > 0, \\ = (I - E_r)\left(\widetilde{\mathbf{Y}} - \mathbf{Y}\right), \quad (32)$$

where $E_r$ is a $N \times N$ matrix where all elements in the top left $N_r \times N_r$ block are $1/N_r$ and others are zeros.

The mean of the estimate residue is

$$\mathbb{E}[\hat{\mathbf{e}}] = (I - E_r)\mathbb{E}\left[\widetilde{\mathbf{Y}} - \mathbf{Y}\right]. \quad (33)$$

From (29), $\mathbb{E}\left[\widetilde{\mathbf{Y}} - \mathbf{Y}\right]$ gives a $N \times 1$ vector whose first $N_r$ elements are $C$ and the remaining elements are zeros. Then $\hat{\mathbf{e}}$ has zero mean.

[5] This method requires the same asymptotic approximation (either for large- or small-SNR) for both measurements $Y_n$ and $\widetilde{Y}_n$. For a good approximation in practice, we will only use the measurements where $Y_n$ and $\widetilde{Y}_n$ both have SNR greater or less than zero.

It is easy to show that $(I - E_r)$ is a singular matrix with rank of $(N-1)$. Thus the $N$ elements of $\hat{\mathbf{e}}$ is not jointly Gaussian-distributed. Similar to Theorem 1, we construct another vector (see Appendix D)

$$\hat{\mathbf{e}}_{sub} = Q_2^T\hat{\mathbf{e}} = Q_2^T\left(\widetilde{\mathbf{Y}} - \mathbf{Y}\right), \quad (34)$$

where $Q_2^T$ is a $(N-1) \times N$ matrix, consisting of $N-1$ eigenvectors of $E_r$ that correspond to $N-1$ zero eigenvalues. Then, the $N-1$ elements of $\hat{\mathbf{e}}_{sub}$ are jointly Gaussian-distributed with zero mean and variance (see Appendix D)

$$\Sigma_e = \mathbb{E}\left[\hat{\mathbf{e}}_{sub}\hat{\mathbf{e}}_{sub}^T\right] = Q_2^T\mathbb{E}\left[\left(\widetilde{\mathbf{Y}} - \mathbf{Y}\right)\left(\widetilde{\mathbf{Y}} - \mathbf{Y}\right)^T\right]Q_2 \\ = Q_2^T\left(\Lambda_{\widetilde{W}} + \Lambda_W\right)Q_2, \quad (35)$$

where $\Lambda_{\widetilde{Y}}$ and $\Lambda_W$ are covariance matrix for $\widetilde{Y}_W$ and $Y_W$, respectively, as defined in (18).

Similar to (26), the likelihood-based acceptance region for $\hat{\mathbf{e}}_{sub}$ is

$$\Omega = \left\{\hat{\mathbf{e}}_{sub} : \hat{\mathbf{e}}_{SCS} = \hat{\mathbf{e}}_{sub}^T\Sigma_e^{-1}\hat{\mathbf{e}}_{sub} < T_e\right\}. \quad (36)$$

The false alarm probability is

$$P_F = \frac{\Gamma((N-1)/2, T_e/2)}{\Gamma((N-1)/2)}. \quad (37)$$

Since this analytical solution is derived based on the asymptotic approximations in Section 3.2, we will see from Section 6.2 that, it is only accurate when the received SNR is either very large or very small. Therefore, for a general scenario where the approximations are no longer acceptable, we will apply the SVM method to obtain an empirical detection threshold. Similarly, we will use the residues, $\hat{\mathbf{e}}$, from (32) as the test statistics of the SVM.

## 6. Simulation evaluation

### 6.1. Simulation settings

In this section we evaluate the performance of our proposed methods, which we call LCM (Linearity-Check-for-Mobile-Transmitter, Section 5.1) and SCS (Signalprint-Check-for-Stationary-Transmitter, Section 5.2). Their performance were tested in a 100-m × 100-m square area, where $N$ sensors are randomly placed with a uniform probability distribution. Both authorized transmitter and unauthorized transmitters are randomly located in the area. Each result is an average over 20,000 independent trials (i.e., independent transmitter and sensor locations and independent random channel fadings). Unless otherwise noted, in these numerical studies we assume that, (a) there is only one unauthorized transmitter and it uses the same transmission power as the authorized user; (b) $N = 50$ for LCM and $N = 10$ for SCS; (c) the path loss, $\gamma = 3.5$, and the standard deviation of the fading, $\sigma_{S,n} = 4$ dB, which are typical values in an urban microcell environment with a very mild random fading; (d) the variation of the channel fading across all sensors is i.i.d., that is, $\Sigma_S$ in (18) is a diagonal matrix; (e) the number of samples in each energy measurement, $L = 16$.

### 6.2. Detection performance

Fig. 4 shows the complementary receiver operating characteristic (C-ROC) curves by LCM and SCS methods under various SNR conditions. The target false alarm probabilities are both from 0.002 to 0.2, set by (27) and (37), respectively. The ROC curves are shown for different SNR levels of energy measurements, represented by the median of received SNR among all the sensors, $\bar{\beta}_{med}$. For the SVM method in LCM where the location of the authorized transmitter is unknown (i.e., "SVM w/o location"), we estimate it by the weighted centroid as

$$[x, y] = \frac{\sum_{i=1}^{N_C} p_i [x_i, y_i]}{\sum_{i=1}^{N_C} p_i}, \tag{38}$$

where $p_i$ is the $i$th largest signal strength (in linear scale) from all the sensors and $(x_i, y_i)$ is the location of the corresponding sensor. It has been shown in [25] that an unbalanced distribution of sensors (with respect to the transmitter to be localized) can degrade the accuracy of a centroid based algorithm. To mitigate the impact due to the unbalanced network topology, we choose $N_C = 10$ sensors with the strongest energy measurement to perform the localization. An advantage of the SVM solutions seen from the results is that the actual $P_F$ is close to the designated one regardless of the SNR level. On the contrary, the analytical solution fails to predict the correct false alarm probability under certain SNR conditions. Specifically, in LCM, the actual and analytical false alarm probabilities match each other only for large $\bar{\beta}_{med}$ (e.g., >20 dB), because the analytical solution is based on the large-SNR approximation. In SCS, the analytical false alarm probability is accurate when the absolute dB value of $\bar{\beta}_{med}$ is large (e.g., ±20 dB), because the method makes use of data in both asymptotic conditions.

Regarding the detection performance, given a large-SNR (e.g., $\bar{\beta}_{med} = 20$ dB), both schemes achieve detection rate above 90% for a false alarm rate of 10%. Moreover, SCS achieves much higher detection probability using far fewer sensors than LCM, thanks to the more reliable metric based on signalprints. However, SCS can only be used in the case where the authorized transmitter is fixed while LCM does not have this constraint. In addition, the results show the effects of using the estimation residues, $\hat{\mathbf{e}}$, as the test statistics. In LCM, we observe that, given the location of the authorized transmitter, the analytical and SVM solutions have similar ROCs although they use different test statistics. In SCS, the detection rate by the SVM solution is more stable against SNR than that of the analytical solution. Particularly, the SVM solution is superior to the analytical one when the SNR of energy measurements is small (i.e., $\bar{\beta}_{med} \leqslant 0$ dB).

In the following results, we fix the false alarm rate at $P_F = 0.1$ and investigate the effects of different system parameters on the detection probability, $P_D$, of the proposed methods, where $P_D = 1 - P_M$.

The variation in energy measurements are mostly caused by the random channel fading and noise, as we have seen from (15). Their effects are illustrated in Fig. 5. From (20), we see that the variation of measurements mostly results from the random channel fading, $\sigma_{S,n}$. The noise, averaged by $L$ samples, has little impact on LCM. On the other hand, from (28), the variation of measurements is caused solely by the noise. Thus, with more samples in a measurement, the detection rate of SCS is higher.

Fig. 6 shows the detection probability for different values of interference-to-signal ratio (ISR), which is defined by the ratio of transmission power from unauthorized and authorized transmitter. For both methods, the detection rates monotonically increase with the interference power, except for the LCM's SVM solution where the unauthorized transmitter location is unknown (i.e., curves with triangle markers). For these cases, and when the noise power is negligible (e.g., $\bar{\beta}_{med} = 20$ dB), the machine learning based solution treats the signal strengths from both transmitters equally and it only tries to tell whether there are simultaneous transmissions. Thus, the detection probabilities appear approximately symmetric with respect to the ISR of 0 dB, where the highest accuracy is usually obtained. When the noise power is significant (e.g.,

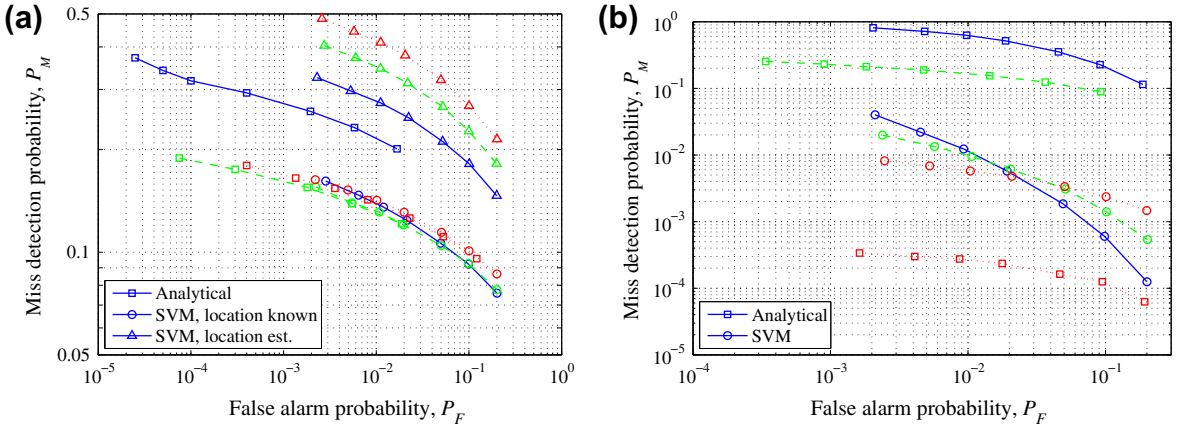


**Fig. 4.** Complementary ROC by (a) LCM and (b) SCS. The target false alarm probabilities are [0.002, 0.005, 0.01, 0.02, 0.05, 0.1, 0.2], highlighted by the markers. In LCM, the median of the received SNR among all the sensors is 0 dB (solid), 10 dB (dashed), and 20 dB (dotted). In SCS, the median of the received SNR among all the sensors is −20 dB (solid), 0 dB (dashed), and 20 dB (dotted).

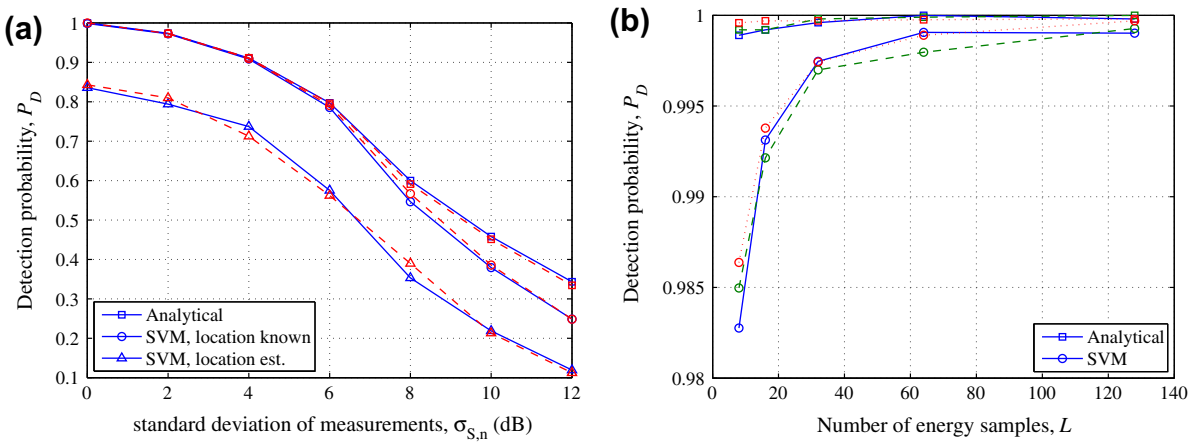


**Fig. 5.** The effects of energy measurement variation on the detection probability, $P_D = 1 - P_M$, for the actual false alarm rate of 0.1. $\bar{\beta}_{med} = 20$ dB. (a) $P_D$ vs. $\sigma_{S,n}$ for LCM. $L = 8$ (solid) and $L = 128$ (dashed); (b) $P_D$ vs. $L$ for SCS. $\sigma_{S,n} = 0$ dB (solid), 6 dB (dashed), and 12 dB (dotted).

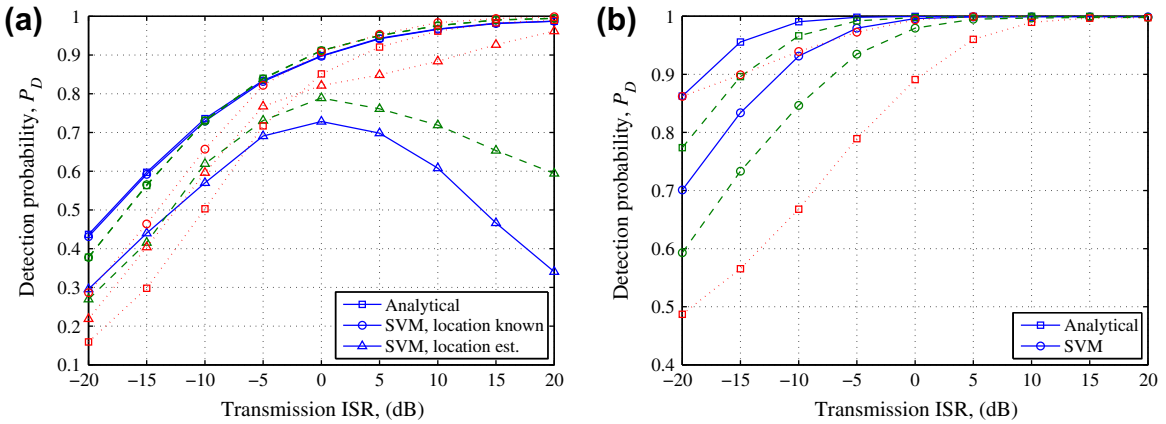


**Fig. 6.** Detection probability vs. transmission ISR by (a) LCM and (b) SCS, where $\bar{\beta}_{med}$ is 20 dB (solid), 10 dB (dashed) and 0 dB (dotted). The actual $P_F = 0.1$.

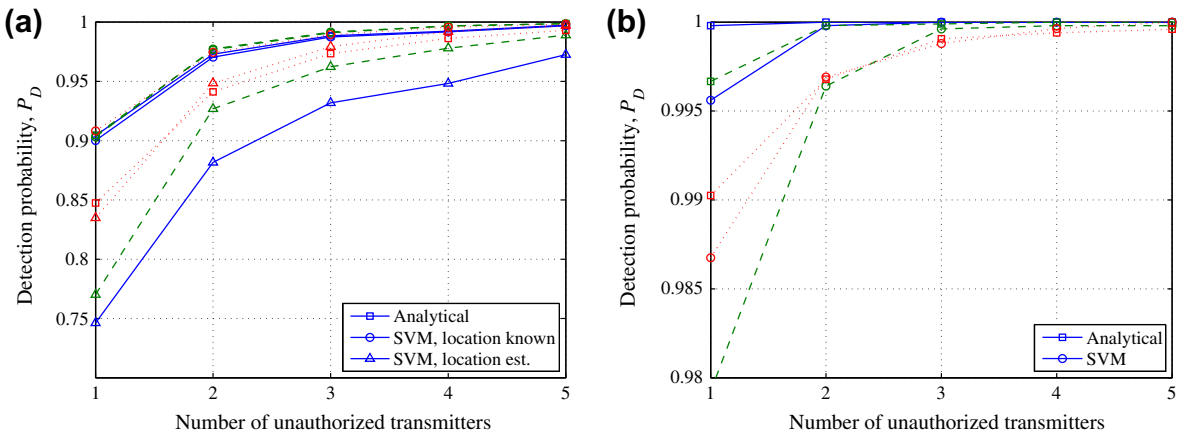


**Fig. 7.** Detection probability vs. the number of independent authorized transmitters, for (a) LCM and (b) SCS, where $\bar{\beta}_{med}$ is 20 dB (solid), 10 dB (dashed), and 5 dB (dotted). The total transmission power of the unauthorized radios equals the authorized transmission power (i.e., ISR = 0 dB). The actual $P_F = 0.1$.

$\bar{\beta}_{med} = 0$ dB), the estimation residues, $\hat{\mathbf{e}}$, are mostly contributed by noise in the normal case. When the interference power is significant (i.e., ISR > 0 dB), its impact on $\hat{\mathbf{e}}$ increases and it deviates the residues from those in the

normal (large noise) case. Therefore, when ISR > 0 dB, the detection probability increases as the SNR decreases.

We now consider the case of multiple unauthorized transmitters. The transmitters are assumed non-colluding and independent, so that their powers add noncoherently at each sensor. Intuitively, more unauthorized radios should lead to better detection because the total amount of transmitted power (and the resulting interference power at each sensor) increases. We thus address a more interesting scenario, where the total transmission powers from all unauthorized radios is fixed. Fig. 7 shows the detection probabilities of LCM and SCS schemes for different numbers of unauthorized transmitters. The unauthorized transmitters have equal transmission powers and are randomly located in the test area with a uniform distribution. In addition, the total transmission power from all the unauthorized radios is equal to the authorized one. We observe that more unauthorized radios leads to higher detection rates for both schemes, even if the aggregate interference power remains constant.

## 7. Conclusion

In this paper, we investigated the problem of detecting unauthorized spectrum usage in a dynamic spectrum access network. Assuming there is only one authorized user in each spectrum channel, we formulated the detection of anomalous spectrum usage as several statistical significance testing problems. With respect to the mobility of the authorized transmitter, we propose two detection algorithms. For the mobile case, we present a Linearity-Check-for-Mobile-Transmitter (LCM) method to examine the linear relation between log-scale RSS and logarithmic link distance. For the stationary case, we present a Signalprint-Check-for-Stationary-Transmitter (SCS) method to compare the current RSS pattern with a stored pattern of the authorized transmitter. Provided the distribution of the energy measurements is known, we derive analytical models for the significance test statistics. In the general case where the distribution is unknown, we introduce a machine-learning approach to provide empirical solutions.

The simulation results show that, the false alarm probabilities predicted by the analytical solutions are sensitive to the SNR of energy measurements across the sensor network. The accuracy of (27) increases with the SNR and the accuracy of (37) increases as the SNR changes away from 0 dB. Given the authorized transmitter location in LCM, the SVM based empirical solution and analytical solution have very similar detection probabilities. On the other hand, the empirical solution of SCS is more stable against noise than the analytical solution in terms of the detection performance. Furthermore, the random variation of measurements has different effects on the detection performance of two proposed schemes. Specifically, the random channel fading significantly deteriorates the detection rate of LCM but has little impact on SCS. In contrast, the number of samples in each measurement, indicating how well the noise can be averaged, is the only factor that determines the variance of measurements in SCS. Provided a large-SNR and a single unauthorized radio, both LCM and SCS schemes achieve a detection probability above 0.9 while keeping the false alarm rate less than 0.1. The detection probabilities are even higher when there are multiple unauthorized radios, for the same total interference power. Moreover, SCS is always superior to LCM in that it achieves much higher detection probability using far fewer sensors, thanks to the more reliable metric based on signalprints.

## Appendix A. Approximating a gamma distribution using a lognormal distribution

For a gamma distributed random variable $y$ whose PDF is given by

$$f(y) = \frac{y^{m-1}}{\Gamma(m)a^m}\exp\left(-\frac{y}{a}\right), \quad a = \frac{E[y]}{m}, \tag{39}$$

$Y = \ln(y)$ can be approximated by a normal distribution $\mathcal{N}(\mu_Y, \sigma_Y^2)$ given $m$ is large [26], where

$$\mu_Y = \ln(a) + \psi(m), \tag{40}$$

and

$$\sigma_Y = \sqrt{\psi'(m)}. \tag{41}$$

$\psi(m) = \frac{d}{dm}\ln\Gamma(m)$ is the digamma function and $\psi'(m) = \frac{d^2}{dm^2}\ln\Gamma(m)$ is the trigamma function. In addition, $\psi(m) \approx \ln(m)$ for a large $m$. We denote a lognormally distributed random variable $y \sim \text{Log}-\text{N}(\mu_Y, \sigma_Y^2)$.

## Appendix B. Proof of Theorem 1

**Proof.** Given that $\mathbf{A}$ in (21) is a $N \times 2$ matrix, using the singular value decomposition (SVD), we have

$$\mathbf{A} = \mathbf{U}\Lambda\mathbf{V}^T, \tag{42}$$

where $\mathbf{U}$ is a $N \times N$ orthogonal matrix, $\mathbf{V}$ is a $2 \times 2$ orthogonal matrix. $\Lambda$ is a $N \times 2$ diagonal matrix with two nonzero singular values (i.e., assuming there are at least two sensors that have different distances from the transmitter):

$$\Lambda_{N\times 2} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} \widetilde{\Lambda}_{2\times 2} \\ 0 \end{bmatrix}. \tag{43}$$

Then we have

$$\begin{aligned} \mathbf{A}\left(\mathbf{A}^T\mathbf{A}\right)^{-1}\mathbf{A}^T &= \mathbf{U}\Lambda\mathbf{V}^T\left(\mathbf{V}\Lambda^T\mathbf{U}^T\mathbf{U}\Lambda\mathbf{V}^T\right)^{-1}\mathbf{V}\Lambda^T\mathbf{U}^T \\ &= \mathbf{U}\Lambda\left(\Lambda^T\Lambda\right)^{-1}\Lambda^T\mathbf{U}^T = \mathbf{U}\begin{bmatrix}\widetilde{\Lambda} \\ 0\end{bmatrix}(\widetilde{\Lambda}\widetilde{\Lambda})^{-1}\begin{bmatrix}\widetilde{\Lambda} & 0\end{bmatrix}\mathbf{U}^T \\ &= \mathbf{U}\begin{bmatrix}\mathbf{I} \\ 0\end{bmatrix}\begin{bmatrix}\mathbf{I} & 0\end{bmatrix}\mathbf{U}^T = \mathbf{U}\begin{bmatrix}\mathbf{I}_{2\times 2} & 0 \\ 0 & 0\end{bmatrix}\mathbf{U}^T. \end{aligned} \tag{44}$$

Therefore,

$$\mathbf{D} = \mathbf{I} - \mathbf{A}\left(\mathbf{A}^T\mathbf{A}\right)^{-1}\mathbf{A}^T = \mathbf{U}\left(\mathbf{I}_{N\times N} - \begin{bmatrix}\mathbf{I}_{2\times 2} & 0\\ 0 & 0\end{bmatrix}\right)\mathbf{U}^T = \mathbf{U}\begin{bmatrix}0 & 0\\ 0 & \mathbf{I}_{(N-2)\times(N-2)}\end{bmatrix}\mathbf{U}^T. \tag{45}$$

There are 2 zero singular values in the matrix $\mathbf{D}$ and thus it is not invertible.

Now let $\mathbf{U} = [\mathbf{U}_1, \mathbf{U}_2]$, where $\mathbf{U}_1$ is $N \times 2$ and $\mathbf{U}_2$ is $N \times (N-2)$. Since

$$\mathbf{A}\mathbf{A}^T = \mathbf{U}\mathbf{\Lambda}\mathbf{\Lambda}^T\mathbf{U}^T = [\mathbf{U}_1, \mathbf{U}_2]\begin{bmatrix}\widetilde{\mathbf{\Lambda}}^2 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}\mathbf{U}_1^T\\ \mathbf{U}_2^T\end{bmatrix}, \tag{46}$$

$\mathbf{U}_2$ consists of $(N-2)$ eigenvectors of $\mathbf{A}\mathbf{A}^T$ corresponding to the $(N-2)$ zero eigenvalues.

Multiplying the residues $\hat{\mathbf{e}}$ by $\mathbf{U}_2^T$, we have

$$\hat{\mathbf{e}}_u = \mathbf{U}_2^T\hat{\mathbf{e}} = \mathbf{U}_2^T\mathbf{D}\mathbf{Y}_R = \mathbf{U}_2^T\mathbf{U}\begin{bmatrix}0 & 0\\ 0 & \mathbf{I}_{(N-2)\times(N-2)}\end{bmatrix}\mathbf{U}^T\mathbf{Y}_R = \mathbf{U}_2^T\mathbf{U}_2\mathbf{U}_2^T\mathbf{Y}_R = \mathbf{U}_2^T\mathbf{Y}_R. \tag{47}$$

Given $\mathbf{Y}_R \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_Y)$, it is known that $\hat{\mathbf{e}}_u \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_e)$, where

$$\mathbf{\Sigma}_{\mathbf{e}} = E\left[\hat{\mathbf{e}}_u\hat{\mathbf{e}}_u^T\right] = \mathbf{U}_2^T\mathbf{\Sigma}_Y\mathbf{U}_2. \qquad \square \tag{48}$$

## Appendix C. Mathematical model of One-class SVM

One-class SVM is defined by the following optimization problem [24],

$$\begin{aligned}\min_{\rho\in\mathbb{R},\xi\in\mathbb{R}^l}\quad & c\rho^2 + \frac{1}{\nu l}\sum_{i=1}^{l}\xi_i,\\ \text{s.t.}\quad & \|\Phi(\mathbf{v}_i) - c\|^2 \leqslant \rho^2 + \xi_i,\\ & \xi_i \geqslant 0, \quad i = 1,\ldots,l,\end{aligned} \tag{49}$$

where the data instance (i.e., the test statistics), $\mathbf{v}_i$, is the estimate residues in our anomaly detection work, given in (23) and (32), respectively. Hence $\mathbf{v}_i$ is a $N$-dimensional energy measurements. $k$ is the number of attributes in each data instance. Hence $k$ equals to $N$, the total number of spectrum sensors. $l$ is the number of data instances in the training set, that is, the number of trials in the training phase. $\xi = (\xi_1, \ldots, \xi_l)$ are slack variables, which allow a fraction of training data to be excluded from the hypersphere in the constraint. $\Phi(\mathbf{v}_i)$ is a mapping function that maps the measurements, $\mathbf{v}_i$, into a feature space where an inner product can be computed by a kernel function defined as $K_\Phi(\mathbf{v}_i, \mathbf{v}_j) = \Phi(\mathbf{v}_i)^T\Phi(\mathbf{v}_j)$. We use the radial basis function (RBF) as the kernel function in our study:

$$K_\Phi(\mathbf{v}_i, \mathbf{v}_j) = \exp\left(-\frac{1}{k}\|\mathbf{v}_i - \mathbf{v}_j\|^2\right), \quad k > 0. \tag{50}$$

The anomaly detection problem can be viewed as minimizing the radius $\rho$ of a hypersphere, centered at $c$, that encloses a subset of the training data (i.e., the acceptance region, $\Omega$).

The optimization problem (49) is solved by the dual problem,

$$\begin{aligned}\min_{\alpha}\quad & \sum_i\sum_j \alpha_i\alpha_j K_\Phi(\mathbf{v}_i, \mathbf{v}_j) - \sum_i \alpha_i K_\Phi(\mathbf{v}_i, \mathbf{v}_j),\\ \text{s.t.}\quad & 0 \leqslant \alpha_i \leqslant \frac{1}{\nu l}, \quad \sum_i \alpha_i = 1.\end{aligned} \tag{51}$$

Each data instance from the testing set, $\mathbf{u}$, is then classified using the decision function,

$$\begin{aligned}\mathcal{H}_0:\quad & \sum_i\sum_j \alpha_i\alpha_j K_\Phi(\mathbf{v}_i, \mathbf{v}_j) - 2\sum_i \alpha_i K_\Phi(\mathbf{v}_i, \mathbf{u})\\ & + K_\Phi(\mathbf{u}, \mathbf{u})\\ & \leqslant R^2.\end{aligned} \tag{52}$$

Note that we do not need to know the explicit form of $\Phi(\mathbf{v}_i)$ to solve the dual problem.

## Appendix D. Proof of Eq. (35)

From (29), we have

$$\mathbb{E}\left[\left(\widetilde{Y}_i - Y_i\right)\left(\widetilde{Y}_i - Y_i\right)\right] = \begin{cases} C^2 + \sigma^2_{\widetilde{W},i} + \sigma^2_{W,i}, & \text{if } \bar{\beta}_i \geqslant 0 \text{ dB}, \quad \text{(a)}\\ \sigma^2_{\widetilde{W},i} + \sigma^2_{W,i}, & \text{if } \bar{\beta}_i < 0 \text{ dB}, \quad \text{(b)}\end{cases} \tag{53}$$

and

$$\mathbb{E}\left[\left(\widetilde{Y}_i - Y_i\right)\left(\widetilde{Y}_j - Y_j\right)\right] = \begin{cases} C^2, & \text{if } \bar{\beta}_i \geqslant 0 \text{ dB and } \bar{\beta}_j \geqslant 0 \text{ dB}, \quad \text{(a)}\\ 0, & \text{if } \bar{\beta}_i < 0 \text{ dB and } \bar{\beta}_j < 0 \text{ dB}. \quad \text{(b)}\end{cases} \tag{54}$$

Then,

$$\mathbb{E}\left[\left(\widetilde{\mathbf{Y}} - \mathbf{Y}\right)\left(\widetilde{\mathbf{Y}} - \mathbf{Y}\right)^T\right] = \Lambda_{\widetilde{W}} + \Lambda_W + C^2 N_r E_r, \tag{55}$$

where $\Lambda_W$ is defined in (18) and $E_r$ is defined in (32). Since $E_r$ has the rank of 1, we construct a $N \times (N-1)$ matrix, $Q_2$, whose columns are the $N-1$ eigenvectors of $E_r$ corresponding to its $N-1$ zero eigenvalues. Then, we have $E_rQ_2 = 0$ and

$$\begin{aligned}\Sigma_e = \mathbb{E}\left[\hat{\mathbf{e}}_{sub}\hat{\mathbf{e}}_{sub}^T\right] &= Q_2^T\mathbb{E}\left[\left(\widetilde{\mathbf{Y}} - \mathbf{Y}\right)\left(\widetilde{\mathbf{Y}} - \mathbf{Y}\right)^T\right]Q_2\\ &= Q_2^T\left(\Lambda_{\widetilde{W}} + \Lambda_W\right)Q_2 + C^2N_rQ_2^TE_rQ_2\\ &= Q_2^T\left(\Lambda_{\widetilde{W}} + \Lambda_W\right)Q_2.\end{aligned} \tag{56}$$

## References

[1] W. Xu, P. Kamat, W. Trappe, TRIESTE: a trusted radio infrastructure for enforcing spectrum etiquettes, in: 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, 2006, SDR '06, 2006, pp. 101–109.
[2] I.F. Akyildiz, W.-Y. Lee, K.R. Chowdhury, CRAHNs: cognitive radio ad hoc networks, Ad Hoc Networks 7 (2009) 810–836.
[3] I. Akyildiz, W.-Y. Lee, K. Chowdhury, Spectrum management in cognitive radio ad hoc networks, Network, IEEE 23 (2009) 6–12.
[4] S. Verdú, Multiuser Detection, Cambridge University Press, New York, 1998.

[5] H.L.V. Trees, Detection, Estimation, and Modulation Theory, Wiley, New York, 2001.
[6] S. Haykin, Cognitive radio: brain-empowered wireless communications, IEEE Journal on Selected Areas in Communications 23 (2005) 201–220.
[7] R. Chen, J.-M. Park, Ensuring trustworthy spectrum sensing in cognitive radio networks, in: 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, 2006, SDR '06, 2006, pp. 110–119.
[8] J. Yang et al., Determining the number of attackers and localizing multiple adversaries in wireless spoofing attacks, in: Proceedings of INFOCOM 2009, The 28th IEEE International Conference on Computer Communications, Rio de Janeiro, Brazil, 2009.
[9] Y. Sheng et al., Detecting 802.11 mac layer spoofing using received signal strength, in: Proceedings of INFOCOM 2008, The 27th Conference on Computer Communications. IEEE, 2008, pp. 1768–1776.
[10] R. Chen, J.-M. Park, J.H. Reed, Defense against primary user emulation attacks in cognitive radio networks, IEEE Journal on Selected Areas in Communications 26 (2008) 25–37.
[11] D.B. Faria, D.R. Cheriton, Detecting identity-based attacks in wireless networks using signalprints, in: Proceedings of the 5th ACM workshop on Wireless security, Los Angeles, CA, 2006, pp. 43–52.
[12] P. Bahl, V.N. Padmanabhan, RADAR: an in-building RF-based user location and tracking system, in: Proceedings of INFOCOM 2000, 2000, pp. 775–784.
[13] L. Xiao et al., Using the physical layer for wireless authentication in time-variant channels, IEEE Transactions on Wireless Communications 7 (2008) 2571–2579.
[14] S. Liu et al., ALDO: an anomaly detection framework for dynamic spectrum access networks, in: Proceedings of INFOCOM 2009, IEEE, April 2009, pp. 675–683.
[15] R. Rajagopalan, P.K. Varshney, Data-aggregation techniques in sensor networks: a survey, IEEE Communications Surveys & Tutorials 8 (2006) 48–63.
[16] S. Ozdemir, Y. Xiao, Secure data aggregation in wireless sensor networks: a comprehensive overview, Computer Networks 53 (2009) 2022–2037.
[17] A. Ghasemi, E.S. Sousa, Spectrum sensing in cognitive radio networks: the cooperation-processing tradeoff, Wireless Communications and Mobile Computing 7 (2007) 1049–1060.
[18] E. Visotsky, S. Kuffner, R. Peterson, On collaborative detection of tv transmissions in support of dynamic spectrum sharing, in: First IEEE International Symposium on DySPAN 2005, 2005, pp. 338–345.
[19] H. Urkowitz, Energy detection of unknown deterministic signals, Proceedings of the IEEE 55 (1967) 523–531.
[20] A. Goldsmith, Wireless Communications, Cambridge University Press, New York, NY, 2005.
[21] M. Gudmundson, Correlation model for shadow fading in mobile radio systems, Electronics Letters 27 (1991) 2145–2146.
[22] F.F. Digham, M.S. Alouini, M.K. Simon, On the energy detection of unknown signals over fading channels, in: IEEE International Conference on Communications, 2003. ICC '03, 2003, pp. 3575–3579.
[23] Y. Chen, W. Trappe, R.P. Martin, Attack detection in wireless localization, in: 26th IEEE International Conference on Computer Communications, INFOCOM 2007, Anchorage, AK, 2007, pp. 1964–1972.
[24] B. Schölkopf et al., Estimating the support of a high-dimensional distribution, Neural Computation 13 (2001) 1443–1471.
[25] L. Xiao, L. Greenstein, N. Mandayam, Sensor-assisted localization in cellular systems, IEEE Transactions on Wireless Communications 6 (2007) 4244–4248.
[26] R.L. Prentice, A log gamma model and its maximum likelihood estimation, Biometrika 61 (1974) 539–544.

**Song Liu** (S'07–M'11) received the B.S. and M.S. degrees in electrical engineering from Tsinghua University, China, in 2000 and 2003, respectively, and the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, in 2010. He is currently a RF Engineer at Apple Inc., Cupertino, CA. His research interests include radio channel modeling, broadband power line systems, cognitive radio, and communication theory.

**Larry J. Greenstein** received the B.S., M.S. and Ph.D. degrees in electrical engineering from Illinois Institute of Technology in 1958, 1961 and 1967, respectively. From 1958 to 1970, he was at IIT Research Institute, where he worked on radio frequency interference and anti-clutter airborne radar. He joined Bell Laboratories in Holmdel, NJ in 1970. Over a 32-year career, he conducted research in digital satellites, point-to-point digital radio, optical transmission techniques and wireless communications. For 21 years during that period (1979–2000), he led a research department renowned for its contributions in these fields. Since 2002, he has been a research professor at Rutgers University's WINLAB, working on PHY-based security techniques, MIMO-based cellular systems, broadband power line systems, cognitive radio and channel modeling.
Dr. Greenstein is an IEEE Life Fellow, an AT&T Fellow, a recipient of the IEEE Communications Society's Edwin Howard Armstrong and Joseph LoCicero Awards, and co-author of several award-winning papers, including the IEEE Donald G. Fink Prize Paper Award. He has served on numerous editorial boards and technical program committees and was, and is now again, the IEEE Communications Society's Director of Journals.

**Wade Trappe** received his B.A. degree in Mathematics from The University of Texas at Austin in 1994, and the Ph.D. in Applied Mathematics and Scientific Computing from the University of Maryland in 2002. He is currently Associate Director at the Wireless Information Network Laboratory (WINLAB) and an associate professor in the Electrical and Computer Engineering Department at Rutgers University. His research interests include wireless security, wireless networking, multimedia security, and network security. He has led projects involving security and privacy for sensor networks, physical layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources, and new RFID technologies. Recently, his research group has developed several cross-layer security mechanisms for wireless networks, has developed jamming detection and jamming defense mechanisms for wireless networks, and has investigated privacy-enhancing routing methods for wireless networks. He has published over 100 papers,

including two best papers in media security, a best paper on the localization of cognitive radios, and several wireless security papers in premier conferences. His experience in network security and wireless systems spans 12 years, and he has co-authored a popular textbook in the field, Introduction to Cryptography with Coding Theory, as well as four other books on wireless systems and multimedia security. He is a member of the IEEE Signal Processing and Communications societies, and a member of the ACM.

**Yingying Chen** received her Ph.D. degree in Computer Science from Rutgers University. She is currently an assistant professor in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. Her research interests include wireless and systems security and privacy, wireless networking, and distributed systems. She has coauthored the book Securing Emerging Wireless Systems and published extensively in journal and conference papers. Prior to joining Stevens Institute of Technology, she was with Bell Laboratories and Optical Networking Group at Lucent Technologies. She received the IEEE Outstanding Contribution Award from IEEE New Jersey Coast Section each year 2005–2009. She is the recipient of the NSF CAREER award. She is also the recipient of the Best Technological Innovation Award from the International TinyOS Technology Exchange in 2006, as well as the Best Paper Award from the International Conference on Wireless On-demand Network Systems and Services (WONS) in 2009.