Secure Crowdsourcing-based Cooperative Spectrum Sensing

Rui Zhang*, Jinxue Zhang*, Yanchao Zhang*, and Chi Zhang†
*Arizona State University, Tempe, AZ, USA
† University of Science and Technology of China
*{ruizhang,jxzhang,yczhang}@asu.edu, †chizhang@ustc.edu.cn

***Abstract*—Cooperative (spectrum) sensing is a key function for dynamic spectrum access and is essential for avoiding interference with licensed primary users and identifying spectrum holes. A promising approach for effective cooperative sensing over a large geographic region is to rely on special spectrum-sensing providers (SSPs), which outsource spectrum-sensing tasks to distributed mobile users. Its feasibility is deeply rooted in the ubiquitous penetration of mobile devices into everyday life. Crowdsourcing-based cooperative spectrum sensing is, however, vulnerable to malicious sensing data injection attack, in which a malicious CR users submit false sensing reports containing power measurements much larger (or smaller) than the true value to inflate (or deflate) the final average, in which case the SSP may falsely determine that the channel is busy (or vacant). In this paper, we propose a novel scheme to enable secure crowdsourcing-based cooperative spectrum sensing by jointly considering the instantaneous trustworthiness of mobile detectors in combination with their reputation scores during data fusion. Our scheme can enable robust cooperative sensing even if the malicious CR users are the majority. The efficacy and efficiency of our scheme have been confirmed by extensive simulation studies.**

I. Introduction

Cooperative spectrum sensing (CSS) is a key function for dynamic spectrum access and is essential for avoiding interference with licensed primary users and identifying spectrum holes [1]. It relies on spatially distributed cognitive radio (CR) users to jointly detect the occupancy of a licensed channel in a specific location and time range. In contrast to spectrum sensing by individual CR users, CSS could largely mitigate many factors such as multipath fading and shadowing [1] and thus has considerably better performance.

Centralized CSS involves a centralized fusion center (FC) which instructs selected CR users to sense a specific channel and then makes a global decision about channel occupancy by aggregating received local sensing results. Local spectrum sensing at cooperative CR users normally relies on energy detection, matched filter detection, or cyclostationary-feature detection. Data fusion can be in the form of either soft or hard combination, which requires the CR users to report raw sensing data or local decisions to the FC, respectively. As in [2]–[6], we consider soft combining in this paper.

A promising method for effective CSS over a large geographic region is to explore the emerging *crowdsourcing* paradigm, in which special *spectrum-sensing provider*s (SSPs) [6]–[9] outsource spectrum-sensing tasks to distributed mobile users called *mobile detector*s who themselves may also be secondary CR users. The feasibility of crowdsourcing-based CSS (CCSS for short) is deeply rooted in the ubiquitous penetration of mobile devices into everyday life. Specifically, according to a recent Cisco report [10], the number of mobile devices such as smartphones and tablets will exceed the world population in 2012 and hit 10 billion in 2016, which implies sufficient geographic coverage especially in highly populated regions such as metropolitan areas. Moreover, they can always accurately self-localize based on hybrid GPS, WiFi, and cellular positioning techniques. Since dynamic spectrum access is expected to be pervasive in future wireless systems, it is widely expected that future mobile devices can perform spectrum sensing via either internal spectrum sensors or external ones acquired from other parties like the SSP [1], [6], [8], [9], [11].

CCSS, though appealing, is vulnerable to false sensing reports, each containing a power measurement much larger (or smaller) than the true value to inflate (or deflate) the final average. A false sensing report can come from a normal mobile detector with a faulty spectrum sensor, a dishonest one wishing to save energy by faking data without actual sensing, or a malicious one aiming to prevent other users from using the channel by submitting an extremely high (or low) power measurement. Without sound defenses in place, the SSP may be misled by false sensing reports to falsely determine that the channel is busy (or vacant). It is thus critical to ensure secure soft combination such that the impact of possible false sensing reports can be minimized.

The prior work on secure CSS against false sensing reports can be generally classified into three categories. The first category such as [3]–[6], [9] uses various anomaly detection techniques to identify false sensing reports and would fail if they constitute the majority, as discussed in [8]. The second category such as [2], [3], [12] uses reputations to differentiate malicious mobile detectors from legitimate ones and is unable to handle sudden change in mobile detectors' behaviors. More recent work [8] relies on some trusted nodes to detect false sensing reports which requires real signal propagation data from primary users (PUs) that are often difficult to obtain. A sound soft combination scheme that can withstand a majority of malicious mobile detectors without too strong assumptions remains an open challenge.

As the first work of its kind, we propose a novel scheme to realize secure CCSS in the presence of malicious mobile detectors possibly being the majority without requiring real signal propagation data from PUs. Our scheme relies on using a few trusted *anchor* detectors to evaluate the instantaneous trustworthiness of mobile detectors in combination with their reputation scores. Our scheme can enable robust PU detection even when the majority of mobile detectors are malicious as

978-1-4673-5946-7/13/$31.00 ©2013 IEEE

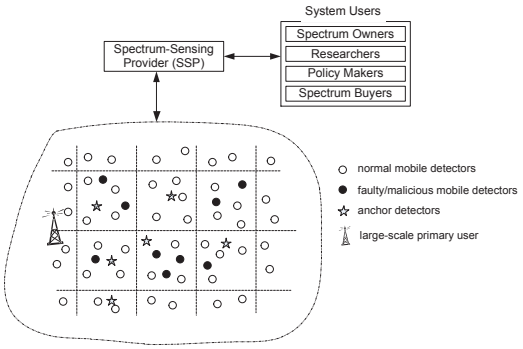

Fig. 1: A CCSS architecture.

long as there are enough trustworthy sensing reports submitted from legitimate mobile detectors. Our contribution in this paper can be summarized as follows.

- We propose a novel metric to measure the instantaneous trustworthiness of a sensing report based on trusted anchor detectors and the relationship between receiving power and distance.
- We design a novel secure soft combination scheme based on the prioritized weighted sequential probability ratio test, in which sensing reports are assigned different weights based on their reputation scores and prioritized according to their instantaneous trustworthiness.
- We confirm the high efficacy and efficiency of our scheme by extensive simulation studies.

The rest of the paper is organized as follows. Section II introduces the system and adversary models. Section III presents our proposed solution. Section IV reports the performance evaluation based on detailed simulation studies. Section V discusses the related work. Section VI concludes this paper.

II. System and Adversary Models

A. System Model

Fig. 1 shows the CCSS architecture under consideration. The SSP divides its service region into equally-sized cells and deploys some *anchor* detectors at strategic locations, e.g., the corners or center of each cell. Similar to the trusted nodes in [8], anchor detectors can be remotely attested by the SSP and excluded if they are detected as compromised. Due to cost constraints, the SSP cannot afford to deploy too many anchor detectors. As a result, although anchor detectors can provide the most trustworthy spectrum-sensing reports, the SSP still relies on the majority of mobile detectors to reach sufficiently high detection accuracy. Our subsequent discussion will focus on a cell with anchor detectors denoted by Θ_a and mobile detectors denoted by Θ, where $|\Theta_a| \ll |\Theta|$.

Mobile detectors correspond to humans using mobile devices such as smartphones and tablets to participate in CSS, and they can perform spectrum sensing via either spectrum sensors embedded into mobile devices or external ones which are provided by the SSP and can communicate with mobile devices. Finally, we assume that mobile detectors can accurately self-localize via hybrid GPS, cellular, and WiFi positioning techniques.

We consider large-scale PUs such as TV stations and cellular base stations (expected in the future [13], [14]) with a large transmission range and known fixed locations. Extending our work to support small-scale and/or mobile PUs such as wireless microphones is left as our future work.

B. Signal Propagation and Spectrum-sensing Models

We adopt the signal propagation model in [15], under which the received primary signal strength at mobile detector i can be expressed as

$$P_i = P_0(\frac{d_0}{d_i})^{\alpha} e^{X_i} e^{Y_i} \quad \text{(Watt)} \tag{1}$$

where d_0 is the reference distance, P_0 is the received primary signal strength at d_0, d_i is the distance from mobile detector i to the primary user, α is the pathloss exponent with typical value between 2 and 5, e^{X_i} and e^{Y_i} represent the effect of shadowing fading and multi-path fading, respectively, where $X_i \sim \mathcal{N}(0, \sigma^2)$.

Assuming that the channel bandwidth is much larger than the coherent bandwidth, the effect of multi-path fading is negligible, i.e., $Y_i = 0$ for all i. In addition, we assume that X_i and X_j are independent for all $i \neq j$, i.e., each mobile detector experiences i.i.d. Gaussian shadowing and fading, which holds when the distance between mobile detectors i and j exceeds decorrelation distance [16].

We assume energy detection for local spectrum sensing at mobile detectors, which is the most widely-used detection technique for its simplicity and efficiency. In particular, on receiving a sensing task from the SSP, each mobile detector collects m RSS (received signal strength) samples. The sensing report from detector i is denoted as $\mathbf{x}_i = (x_{i,1}, \cdots, x_{i,m})$. The test statistic of the energy detector is the average RSS (including the noise power), i.e., $S_i = \frac{1}{m}\sum_{k=1}^{m} x_{i,k}$, which can be approximated as a Gaussian random variable using the Central Limit Theorem (CLT) [17], [18] as

$$S_i \sim \begin{cases} \mathcal{N}(N_o, \frac{2N_o^2}{m}) & \mathcal{H}_0 : \text{Primary user is absent} \\ \mathcal{N}(N_o + \bar{P}_i, \frac{2(\bar{P}_i + N_o)^2}{m}) & \mathcal{H}_1 : \text{Primary user is present} \end{cases}, \tag{2}$$

where $\bar{P}_i = \mathsf{E}(P_i)$ is the average received power at detector i, and N_o is the noise power, e.g., -96 dBm for a 6MHz TV channel.

C. Adversary Model

We assume that the adversary is aware of our scheme and has full control over multiple malicious detectors who may launch the following attacks.

- A malicious mobile detector may report high RSS values when the primary signal is absent, aiming at increasing the probability of false alarm and preventing CR users from using the channel.
- A malicious mobile detector may also report low RSS values when the primary signal is present, aiming at increasing the probability of miss detection and causing increased interference to the primary user.

Malicious mobile detectors could be the majority in a cell. We, however, assume that there are enough normal detectors submitting faithful sensing reports. Otherwise, it is fundamentally difficult to realize robust PU detection with desired miss detection and false alarm probabilities.

It is beyond the scope of this paper to consider other possible attacks against cooperative sensing. For example, a powerful adversary may jam the channel to prevent mobile detectors from communicating with the SSP. These attacks are not unique to cooperative sensing and can be mitigated by spread-spectrum techniques [19], [20].

III. Secure Combination for CCSS

In this section, we first outline our secure combination scheme for CCSS and then detail its design.

A. Overview

Our scheme relies on using trusted anchor detectors to evaluate the *instantaneous trustworthiness* of mobile detectors in combination with their *reputation scores*. The key insight is that a mobile detector's reputation score and the instantaneous trustworthiness of his sensing report have different trust implications. On the one hand, the reputation score is to predict his future performance based on his past long-term behavior and is nevertheless incapable of handling sudden change in his current behavior. On the other hand, the instantaneous trustworthiness of his sensing report only reflects the level of fitting with the trusted reports from anchor detectors in the current sensing task while is unable to incorporate his long-term behavior. Although the reports from anchor detectors are trusted to have not undergone malicious modifications, they may be inaccurate due to possible multi-path fading/shadowing and other channel impairments. We thus propose to explore both the instantaneous trustworthiness and reputation scores of mobile detectors to realize robust PU detection.

Specifically, our scheme uses instantaneous trustworthiness and reputation scores of mobile detectors in different ways. To enable robust data fusion, we propose a prioritized weighted-probability-ratio test to combine sensing reports, in which the sensing reports are ordered according to their instantaneous trustworthiness and assigned different weights according to their reputation scores. The sensing reports are fed to the algorithm one at a time, and a decision is made when certain criterion is reached. By doing so, as long as there are sufficient normal mobile detectors, the final decision will not be misled even if malicious mobile detectors are the majority.

In what follows, we detail the design of our scheme, including *instantaneous trustworthiness measure*, *prioritized weighted sequential probability ratio test*, and *fine-grained reputation management*.

B. Instantaneous Trustworthiness Measure

We first introduce a novel metric to evaluate the instantaneous trustworthiness of any mobile detectors $i \in \Theta \cup \Theta_A$ (or equivalently, their reports). For convenience only, we abuse the notation by letting Θ and Θ_a denote the mobile and anchor detectors who all submitted a sensing report to the SSP, where the cardinality $|\Theta|$ is normally much larger than $|\Theta_a|$.

Our key insight can be explained as follows. According to Eqs. (1) and (2), we know that the receiving powers at two honest mobile detectors either are both close to noise if the primary user is absent, or satisfy certain condition with respect to their distances to the primary user if the primary user is present. Consider any two mobile detectors i and j with their distances to the primary user d_i and d_j, respectively. Their test statistics are denoted by S_i and S_j, respectively, which are assumed to be independent Gaussian random variables. We define the following random variable

$$Z_{i,j} = \rho(d_i^\alpha(S_i - N_o) - d_j^\alpha(S_j - N_o)) \ , \tag{3}$$

where $\rho = \sqrt{\frac{1}{2(d_i^{2\alpha}+d_j^{2\alpha})}}$.

When the primary user is absent, we have

$$\mathsf{E}(Z_{i,j}|\mathcal{H}_0) = \mathsf{E}(\rho(d_i^\alpha(S_i - N_o) - d_j^\alpha(S_j - N_o))) = 0 \ ,$$

and

$$\begin{aligned}
\mathsf{VAR}(Z_{i,j}|\mathcal{H}_0) &= \rho^2\mathsf{VAR}(d_i^\alpha(S_i - N_o) - d_j^\alpha(S_j - N_o)) \\
&= \rho^2(\mathsf{VAR}(d_i^\alpha S_i) + \mathsf{VAR}(d_j^\alpha S_j)) \\
&= \frac{2d_i^{2\alpha}N_o^2 + 2d_j^{2\alpha}N_o^2}{2m(d_i^{2\alpha}+d_j^{2\alpha})} \\
&= \frac{N_o^2}{m} \ .
\end{aligned}$$

Similarly, when the primary user is present, we have

$$\begin{aligned}
\mathsf{E}(Z_{i,j}|\mathcal{H}_1) &= \mathsf{E}(\rho d_i^\alpha(S_i - N_o) - d_j^\alpha(S_j - N_o)) \\
&= \mathsf{E}(d_i^\alpha \bar{P}_i - d_j^\alpha \bar{P}_j) \\
&= \mathsf{E}(d_i^\alpha P_0(\frac{d_0}{d_i})^\alpha e^{X_i}e^{Y_i} - d_j^\alpha P_0(\frac{d_0}{d_j})^\alpha e^{X_j}e^{Y_j}) \\
&= \mathsf{E}(P_0 d_0^\alpha e^{X_i} - P_0 d_0 e^{X_j}) \\
&= P_0 d_0^\alpha(\mathsf{E}(e^{X_i}) - \mathsf{E}(e^{X_j})) \\
&= 0 \ ,
\end{aligned}$$

where the third equality holds because $Y_i = 0$ (cf. Section II-B). Since FCC requires that unlicensed CR devices reliably detect incumbent signals at very low SNRs (e.g., as low as -22 dB in the IEEE 802.22 standard [21]), it is typically assumed that $N_o \gg P_i$ for all $i \in \Theta \cup \Theta_a$. It follows that

$$\begin{aligned}
\mathsf{VAR}(Z_{i,j}|\mathcal{H}_1) &= \rho^2\mathsf{VAR}(d_i^\alpha(S_i - N_o) - d_j^\alpha(S_j - N_o)) \\
&= \rho^2(\mathsf{VAR}(d_i^\alpha S_i) + \mathsf{VAR}(d_j^\alpha S_j)) \\
&= \frac{2d_i^{2\alpha}(\bar{P}_i + N_o)^2 + 2d_j^{2\alpha}(\bar{P}_j + N_o)^2}{2m(d_i^{2\alpha}+d_j^{2\alpha})} \\
&\approx \frac{N_o^2}{m} \ .
\end{aligned}$$

Therefore, no matter whether the primary user is present or not, $Z_{i,j}$ is approximately Gaussian distributed with zero mean and variance N_o^2/m if the reports S_i and S_j are highly correlated with the distance d_i and d_j. Otherwise, the distribution of $Z_{i,j}$ is unpredictable.

Assume that S_j is provided by a trustworthy anchor detector $j \in \Theta_a$. We can thus assess the trustworthiness of S_i with regard to S_j through the likelihood of $Z_{i,j}$ being generated from the Gaussian distribution $\mathcal{N}(0, N_o^2/m)$. In particular, assume that detectors i and j report s_i and s_j as

an observation of S_i and S_j, respectively, based on which the SSP constructs an observation $z_{i,j}$ of $Z_{i,j}$. The likelihood of $z_{i,j}$ being generated from $\mathcal{N}(0, N_o^2/m)$ is given by

$$\mathsf{L}(z_{i,j}|\mathcal{N}(0, N_o^2/m)) = \frac{1}{\sqrt{2\pi N_o^2/m}} e^{-\frac{m z_{i,j}^2}{N_o^2}} , \quad (4)$$

which monotonically decreases as $|z_{i,j}|$ increases. Therefore, we define the *relative instantaneous trustworthiness* of s_i with regard to s_j as $|z_{i,j}|$. The smaller $|z_{i,j}|$, the more trustworthy s_i with regard to s_j, and vice versa. In addition, we have $|z_{j,j}| = 0$ for any anchor detector $j \in \Theta_a$.

We then measure the overall instantaneous trustworthiness of s_i by combining all the relative instantaneous trustworthiness values $\{|z_{i,j}|\}_{j\in\Theta_a}$. In particular, we view detector s_i's $|\Theta_a|$ relative instantaneous trustworthiness values as a point in the $|\Theta_a|$-dimensional space $P_i = (|z_{i,1}|, \cdots, |z_{i,|\Theta_a|}|)$ and define the overall instantaneous trustworthiness of s_i as the Euclidean distance between P_i and the origin, which is given by

$$t_i = (\sum_{j\in\Theta_a} |z_{i,j}|^2)^{\frac{1}{2}} . \quad (5)$$

The smaller t_i, the more trustworthy of s_i, and vice versa.

We have a few remarks about the instantaneous trustworthiness measure t_i. First, when there is only one anchor detector, say j, we have $t_j = 0$ as $z_{j,j} = 0$, meaning that s_j is the most trustworthy sensing report. Second, it is possible that an anchor detector j generates a bad sensing report due to temporal channel impairments. In this case, a malicious mobile detector i with false sensing report may gain high relative instantaneous trustworthiness with regard to anchor detector j, i.e., low $|z_{i,j}|$. It is, however, impossible for him to simultaneously gain high instantaneous trustworthiness at the other anchor detectors. It is therefore necessary to have multiple anchor detectors. Finally, when the primary user is present, a malicious mobile detector may submit a false sensing report along with a falsified location aiming at cheating the SSP into computing a wrong but high instantaneous trustworthiness. Our instantaneous trustworthiness measure is resilient to this attack, as if the false sensing report and location could together lead to a lower t_i (i.e., high instantaneous trustworthiness), it is equivalent to a sensing report submitted by a good mobile detector i' at the reported location.

C. Prioritized Weighted Sequential Probability Ratio Test

Once the SSP evaluates the instantaneous trustworthiness of all anchor and mobile detectors in $\Theta \cup \Theta_a$, it applies the Weighted Sequential Probability Ratio Test (WSPRT) technique [2] to aggregate the sensing reports by prioritizing those with higher instantaneous trustworthiness and also assigning higher weights to those from detectors with higher reputation scores, which we call Prioritized Weighted Sequential Probability Ratio Test (PWSPRT).

To perform PWSPRT, the SSP first ranks all the sensing reports according to their instantaneous trustworthiness t_i in an ascending order. We then define the following decision variable

$$\mathbb{V} = \sum_{i\in\underline{\Theta}} \ln(\frac{\mathsf{P}(S_i|\mathcal{H}_1)}{\mathsf{P}(S_i|\mathcal{H}_0)})^{\mathsf{w}_i} , \quad (6)$$

where $\mathsf{P}(S|\mathcal{H}_k)$ refers to the probability density function of a random variable S under $\mathcal{H}_k$ ($k = 0$ or 1), $\underline{\Theta}$ denotes a subset of detectors in $\Theta \cup \Theta_a$ whose reports have been aggregated, and $\mathsf{w}_i \in [0, 1]$ is the normalized reputation score of detector i used as the weight here, which will be explained in Section III-D.

The SSP's decision is based on the following criterion:

- Accept $\mathcal{H}_1$ and terminate if $\mathbb{V} \geq A$;
- Accept $\mathcal{H}_0$ and terminate if $\mathbb{V} \leq B$;
- Aggregate an additional report and add the corresponding detector index to $\underline{\Theta}$ if $A < \mathbb{V} < B$,

where A and B are two decision thresholds derived from the desired miss detection and false alarm probabilities. In particular, let χ and ψ denote the desired miss detection and false alarm probabilities, respectively. The decision thresholds are given in [22] as

$$A = \ln(\frac{1-\chi}{\psi}) \quad \text{and} \quad B = \ln(\frac{\chi}{1-\psi}) . \quad (7)$$

In each iteration, the SSP chooses a sensing report with the lowest rank from the remaining reports, updates $\mathbb{V}$ according to Eq. (6), and checks if a final decision can be reached. In addition, in case a decision cannot be reached after aggregating all the sensing reports, the SSP permissively accepts $\mathcal{H}_0$ to avoid potential interference with the primary user. In the end, the SSP updates the reputation profile for each mobile detector (see Section III-D).

Our scheme obviously has greater resilience to false sensing reports. In particular, a sensing report from a less reputable mobile detector will be assigned a smaller weight and is thus less likely to drastically affect the final decision. In addition, a sensing report with low instantaneous trustworthiness will be counted only if a final decision cannot be reached after combining all the other sensing reports with higher instantaneous trustworthiness (i.e., smaller t_i). As long as there are sufficient mobile detectors in the cell, a robust decision can still be reached even if there are much more malicious mobile detectors.

D. Fine-grained Reputation Management

As discussed in Section III-C, the reputation scores of mobile detectors are used to combine their sensing reports in PWSPRT. Now we present a novel reputation system for the SSP to record the past sensing performance of mobile detectors.

Our reputation system will be built upon our previous work [23] which is firmly rooted in the classical Bayesian inference theory used to estimate one or more unknown quantities from the results of a sequence of multinomial trials. For clarity, we outline the adopted Dirichlet-Multinomial model as follows and refer to [24] for more details. A multinomial trial process is a sequence of independent, identically distributed (i.i.d.) random variables U_1, U_2, ..., each taking one of ϖ possible outcomes $\{o_i\}_{i=1}^{\varpi}$. We then denote the common probability density function (PDF) of the trial variables by $p_i = \mathsf{P}(\mathsf{U}_j = o_i)$ for $1 \leq i \leq \varpi$, where $p_i > 0$ and $\sum_{i=1}^{\varpi} p_i = 1$. Let $\mathbf{p} = (p_1, ..., p_\varpi)$ and $\mathbf{z} = (z_1, ..., z_\varpi)$ which is the vector of observation counts of each outcome after N multinomial trials,

namely, $\sum_{i=1}^{k} z_i = N$. The multinomial sampling distribution [24] states that

$$f(\mathbf{z}|\mathbf{p}) = \mathsf{Mult}(N|p_1, ..., p_\varpi) = \frac{N!}{\prod_{i=1}^{\varpi} z_i!} \prod_{i=1}^{\varpi} p_i^{z_i} \ .$$

It is commonly assumed in Bayesian inference that $\mathbf{p}$ has a conjugate prior distribution[1] known as the Dirichlet,

$$f(\mathbf{p}) = \mathsf{Dir}(\mathbf{p}|\alpha_1, ..., \alpha_\varpi) = \frac{\Gamma(\sum_{i=1}^{\varpi} \alpha_i)}{\prod_{i=1}^{\varpi} \Gamma(\alpha_i)} \prod_{i=1}^{\varpi} p_i^{\alpha_i - 1} \ ,$$

where $p_i \neq 0$ if $\alpha_i < 1$ and Γ is the gamma function[2]. The positive parameters α_i can be interpreted as "prior observation counts" for events governed by p_i. Then the posterior distribution is also Dirichlet [24],

$$\begin{aligned} f(\mathbf{p}|\mathbf{z}) &= \frac{f(\mathbf{z}|\mathbf{p}) \times f(\mathbf{p})}{f(\mathbf{z})} \\ &= \frac{\Gamma(\sum_{i=1}^{\varpi} (\alpha_i + z_i))}{\prod_{i=1}^{\varpi} \Gamma(\alpha_i + z_i)} \prod_{i=1}^{\varpi} p_i^{\alpha_i + z_i - 1} \\ &= \mathsf{Dir}(\mathbf{p}|\alpha_1 + z_1, ..., \alpha_\varpi + z_\varpi), \end{aligned} \tag{8}$$

which can be used to make statements about $\mathbf{p}$ considered as a set of random quantities. The posterior mean of p_i, which maybe be interpreted as the posterior probability of observing outcome o_i in a future multinomial trial, is

$$\mathsf{E}[p_i|\mathbf{z}] = \frac{\alpha_i + z_i}{\sum_{i=1}^{\varpi} (\alpha_i + z_i)} \ . \tag{9}$$

In what follows, we detail how to apply the Dirichlet-Multinomial model in our scheme.

Let $\varpi = 2(q+1)$ for some integer $q \geq 1$. The SSP first divides the range $(-\infty, \infty)$ into $2q+2$ intervals, denoted by $I_1, \cdots, I_{2q+2}$. Recall that A and B ($B < 0 < A$) are the decision thresholds used in PWSPRT, which correspond to $\mathcal{H}_1$ and $\mathcal{H}_0$, respectively (cf. Eq. (7)). The jth interval is given by

$$I_j = \begin{cases} (-\infty, B] & \text{if } j = 1, \\ (\frac{(k^{q+2-j}-1)B}{k^q-1}, \frac{(k^{q+1-j}-1)B}{k^q-1}] & \text{if } 2 \leq j \leq q+1, \\ (\frac{(k^{j-q-2}-1)A}{k^q-1}, \frac{(k^{j-q-1}-1)A}{k^q-1}] & \text{if } q+2 \leq j \leq 2q+1, \\ (A, \infty) & \text{if } j = 2q+2 \ , \end{cases} \tag{10}$$

where $k > 1$ is a system parameter. Let $|I_j|$ denote the length of the jth interval. It follows that $|I_j| = k|I_{j+1}|$ for all $2 \leq j \leq q$, and $|I_j| = k|I_{j-1}|$ for all $q+2 \leq j \leq 2q$. The reason to have the length of intervals form two geometric sequences is that most normal detectors will have a relative small negative or positive contribution in low SNR environment. By choosing small length for the intervals in the middle, we can better differentiate the performance levels among different detectors.

After each sensing task, the SSP maps the performance of each mobile detector into one of the ϖ levels. In particular, for each $i \in \Theta$, let $\mathbf{c}_i = \ln \mathsf{P}(S_i|\mathcal{H}_1) - \ln \mathsf{P}(S_i|\mathcal{H}_0)$ be the potential contribution of mobile detector i in PWSPRT, regardless of its weight $\mathbf{w}_i$. The SSP first maps $\mathbf{c}_i$ into one of the ϖ intervals, say I_{η_i}. The performance level of mobile detector i is then given by

$$l_i = \begin{cases} \eta_i & \text{if } \mathcal{H}_1 \text{ is accepted,} \\ \varpi + 1 - \eta_i & \text{if } \mathcal{H}_0 \text{ is accepted.} \end{cases} \tag{11}$$

In other words, if mobile detector $i \in \underline{\Theta}$ has a positive (or negative) contribution to the final decision, its sensing performance will be mapped into one of the higher (lower) $q+1$ levels.

The SSP maintains a reputation profile for every mobile detector $i \in \Theta \cup \Theta_a$, represented by ϖ counters $\{c_{i,s}\}_{s=1}^{\varpi}$. Each counter $c_{i,s}$ corresponds to the sth performance level and is initialized to c_0. After every sensing task, the SSP increases the corresponding counter of every mobile detector $\underline{\Theta}$ involved in PWSPRT according to his performance level.

The SSP then computes $w_{i,s} = \frac{c_{i,s}}{\sum_{s=1}^{\varpi} c_{i,s}}$ for all $s \in [1, \varpi]$, where $w_{i,s}$ refers to the expected probability that detector i will have level-s sensing performance (cf. Eq. (9)). If the SSP desires a performance level no less than $l \in [1, \varpi]$, it computes the reputation score for detector i as

$$w_i = \sum_{s=1}^{l} w_{i,s} \ .$$

Let $w_{\max}$ be maximum reputation score among all mobile detectors $\Theta \cup \Theta_a$. The normalized reputation score of detector i is then given by

$$\mathsf{w}_i = w_i / w_{\max} \ , \tag{12}$$

which will be used as the weight of detector i in PWSPRT.

The choice of l is important. In particular, the higher l is, the lower the weight w_i for each $i \in \Theta \cup \Theta_a$, the fewer mobile detectors with a non-zero weight, and vice versa. We will study the tradeoff between sensing quality and resilience to malicious mobile detectors using simulations in Section IV.

In addition, past performance may not always be relevant for determining the current performance of mobile detectors who may update their devices and/or vary their behaviors over time. To deal with this situation, the SSP could choose a *discount factor* ν between $[0, 1.0]$ to assign more weight to recency. At regular intervals, the SSP updates $\{c_{i,s}\}_{s=1}^{\varpi} := \{\nu c_{i,s}\}_{s=1}^{\varpi}$. Discounting the past not only helps identify mobile detectors who behave well initially and poorly afterwards, but also permits a disreputable mobile detector to reform by starting to have good performance.

IV. Performance Evaluation

In this section, we evaluate the proposed scheme using extensive simulation. As the only piece of prior work that targets malicious detectors being the majority, the solution in [8] relies on real signal propagation data which may be very difficult to obtain especially in urban environments. It is thus less meaningful to directly compare our work with [8] because our scheme does not require real signal propagation data. Instead, we compare our work with the techniques proposed in [2] (denoted by CPB) and [3] (denoted by KKB) that are under similar signal-propagation models and assumptions as well as the standard SPRT [25] that corresponds to no defense in place.

[1]The property that the posterior distribution follows the same parametric form as the prior distribution is called *conjugacy* [24].

[2]If x is an integer, $\Gamma(x) = (x-1)!$.

TABLE I: Default Simulation Setting

Para.	Value	Description
$\|\Theta\|$	100	Number of mobile detectors
M	50	Number of malicious mobile detectors
$\|\Theta_a\|$	5	Number of anchor detectors
d_0	1m	Reference distance
P_0	90 dBm	The received power at d_0
m	6×10^3 [4]	Number of samples
α	3.7	Path loss exponent
χ	0.01	Desired miss detection probability
ψ	0.1	Desired false alarm probability
σ	5.5 dB [17]	The standard deviation of shadow fading X_i
α_s	1	Initial value for each counter in reputation profile
ϖ	22	Total number of service levels
k	1.4	Ratio between adjacent performance intervals
l	12	Minimum desired service level

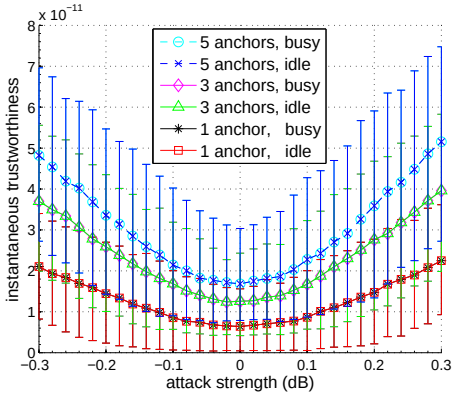

Fig. 2: Instantanoes trustworthiness vs. attack strength.

A. Simulation Setup

As in [4], we consider an IEEE 802.22 WRAN environment with a single DTV transmitter with 6MHz bandwidth and 150.3 km transmission range [17]. We simulate a rectangle cell of 5×5 km^2. The distance between the center of the cell to the primary user is 145 km. We set the minimum distance between any two detectors to be 200 m to decorrelate their shadow fading X_i [16]. In addition, we call a malicious mobile detector i has an attack strength T (dB) if it reports a $s_i + T$ where s_i is the true average of the RSSI values [4]. We assume that there are 100 mobile detectors in the cell, among which M are malicious.

Table I lists the default parameters used in our simulation unless stated otherwise. The simulation is done in Matlab, and each point is the average of 10000 runs, each with a random seed. In addition, since both CPB [2] and our scheme use reputation scores, meaning that the outcomes of later rounds are partially determined by those of previous rounds, we divide the total 10000 rounds into 100 groups, each containing 100 rounds, and the reputation score of each mobile detector is reset at the beginning of each group.

B. Simulation Results

1) Instantaneous trustworthiness: We first report the simulation result for the proposed instantaneous trustworthiness measure, which is one of the key components of our scheme.

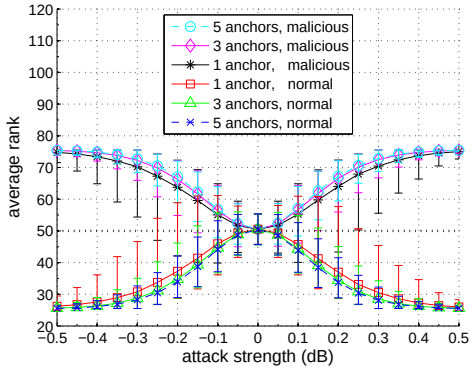

Fig. 3: The average rank of malicious mobile detectors vs. attack strength.

Fig. 2 shows the instantaneous trustworthiness of a malicious mobile detector with its attack strength T varying between -0.3 and 0.3 dB. We can see that the instantaneous trustworthiness increases as the attack strength $|T|$ increases. The reason is that the higher the attack strength, the larger deviation from the expected received power at its location, the larger $|z_{i,j}|$ with regard to each anchor node j, the larger t_i, and vice versa. In addition, instantaneous trustworthiness also increases as the number of anchor detectors increases, because each additional anchor detector corresponds to one relative instantaneous trustworthiness value that will be counted in the overall instantaneous trustworthiness. As a result, the more anchor detectors, the more sensitive the instantaneous trustworthiness measure to false sensing data attack.

Fig. 3 shows the average ranks of 50 malicious mobile detectors and 50 normal detectors varying with attack strength. We can see that the average rank of a malicious detector increases rapidly from 50 and converges to 75 as the attack strength increases, which means that the 50 malicious detectors constantly rank between 51 and 100, leading to an average rank of 75. In contrast, the average rank of 50 normal detectors decreases and converges to 25, meaning that the 50 normal detectors consistently rank between 1 and 50. These results are expected since malicious (or normal) detectors will have low (or high) instantaneous trustworthiness with high probability. In addition, we can see that the more anchor detectors, the smaller variance of the average rank for both malicious and normal mobile detectors. This means that by aggregating the relative instantaneous trustworthiness with regard to multiple anchor nodes, the rank based on instantaneous trustworthiness can effectively differentiate malicious detectors from normal detectors.

2) Reputation system: Fig. 4 shows the average normalized reputation scores of 50 normal detectors and 50 malicious detectors in each round with a different desired service level l. We can see that the average reputation score of normal mobile detectors increases slowly after each round, while that of malicious mobile detectors remains stable. The reason is that in each round, most detectors involved in PWSPRT will be normal detectors with high probability, so only the reputation counters of a subset of normal detectors will be updated, leading to a slow increase in their average reputation scores. For the same reason, the reputation counters of malicious

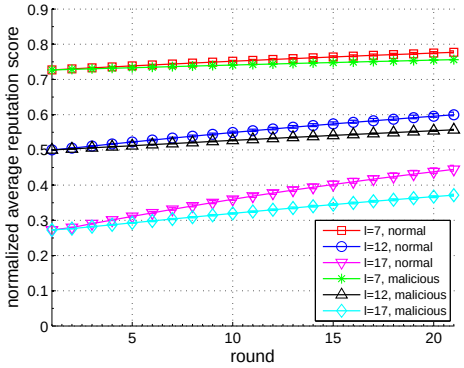

Fig. 4: The progressive average reputation scores of normal and malicious mobile detectors.

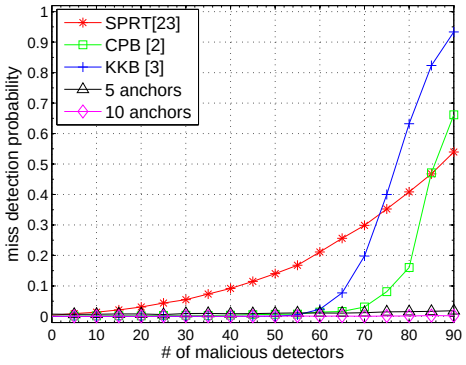

Fig. 5: Miss detection probability vs. # of malicious detectors.

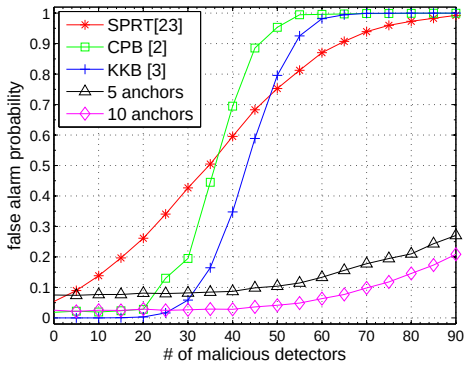

Fig. 6: False alarm probability vs. # of malicious detectors

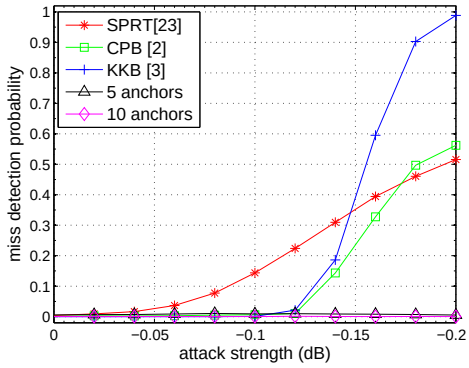

Fig. 7: Miss detection probability vs. attack strength.

detectors will not be updated, whose average reputation score will remain stable. Such updates can still guarantee good detectors having higher reputation scores than malicious ones. In addition, we can see that the higher l is, the smaller the initial reputation score for each detector, and the larger difference between the average reputation scores of normal detectors and malicious ones after sufficient rounds. This represents the tradeoff between the desired service level and convergence time as well as the final difference in the reputation scores of normal detectors and malicious ones.

3) Resilience to malicious mobile detectors: Fig. 5 shows the miss detection probabilities of our scheme, CPB, KKB, and SPRT varying with the number of malicious detectors, where the attack strength of malicious detectors is -0.1 dB. We can see that the miss detection probability of SPRT increases as the number of malicious detectors increases, which is expected. In addition, the miss detection probabilities of CPB and KKB are close to zero when the number of malicious detectors is below 60, meaning both of them are resilient to false sensing data attack when the malicious detectors do not constitute the majority. As the number of malicious detectors further increases, the miss detection probabilities of CPB increases and eventually exceeds that of SPRT. The reason is that once the malicious detectors dominate the cell, they will always determine the final decision and have their reputation scores increased, while the normal detectors will always make the "wrong" decision and have their reputation scores decreased. Similar trend can be observed about KKB, because normal detectors' sensing reports will be considered as outliers and filtered out once the malicious detectors constitute the majority. In contrast, the miss detection probability of our scheme is insensitive to the increase in the number of malicious detectors and remains below 0.05 even when the number of malicious detectors exceeds 90. The reason is that malicious detectors will be ranked after normal detectors with high probability using our instantaneous trustworthiness measure, so the SSP can make a correct decision as long as there are sufficient normal detectors.

Fig. 6 shows the false alarm probabilities of our scheme with CPB, KKB, and SPRT varying with the number of malicious detectors, where the attack strength of malicious detectors is 0.1 dB. Similar to Fig. 5, the false alarm probability of SPRT increases as the number of malicious detectors increases, which is of no surprise. The false alarm probabilities of CPB and KKB are both close to zero when the number of malicious detectors is smaller than 20 and increase as the number of malicious detectors further increases, which further demonstrate that they are effective against small fraction of malicious detectors but ineffective when the malicious detectors become the majority. In contrast, the false alarm probability of our scheme is much less sensitive to the increase in the number of malicious detectors. In addition, the more anchor detectors, the lower the false alarm probability, and vice versa.

Fig. 7 compares the miss detection probabilities of our scheme with CPB, KKB, and SPRT with the attack strength

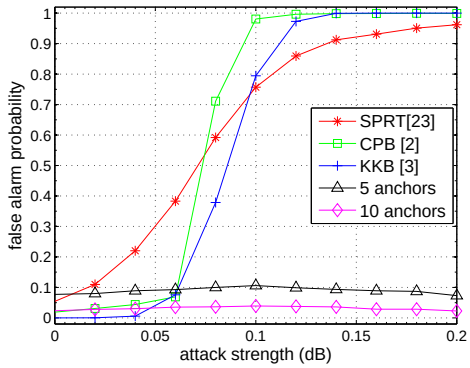

Fig. 8: False alarm probability vs. attack strength.

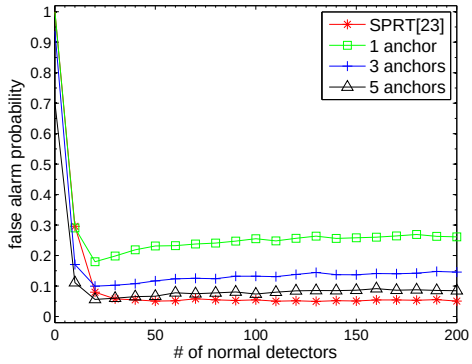

Fig. 9: False alarm probability vs. # of mobile detectors under no attack.

varying between 0 to -0.2 dB, where the number of malicious detectors is 50. We can see that the miss detection probabilities of CPB, KKB, and SPRT all increase as the attack strength increases. The reason is that neither CPB nor KKB can withstand the malicious mobile detectors being the majority, not to mention SPRT. In contrast, the miss detection probability of our scheme is relatively insensitive to the increase in attack strength as our instantaneous trustworthiness measure can effectively differentiate malicious detectors from the normal ones. As long as there are enough normal detectors, the SSP can make a correct decision under our scheme.

Fig. 8 compares the false alarm probabilities of our scheme with CPB, KKB, and SPRT. The result is very similar to that in Fig. 7 and is omitted here for space constraints.

4) Performance under no attack: Fig. 9 compares the false alarm probabilities of our scheme and SPRT varying with the number of mobile detectors where there is no malicious detectors. We can see that the false alarm probability of SPRT decreases from 1 to below 0.1 as the number of mobile detectors increases from 0 to 20 and remains stable as the number of mobile detectors further increases, which is expected for SPRT. In contrast, the false alarm probability of our scheme first decreases as the number of mobile detectors increases from 0 to 20 and then slightly increases as the number of mobile detectors further increases. The reason is that our scheme relies on the instantaneous trustworthiness measure to order all the sensing reports, which further relies on a few anchor detectors. The order for aggregating sensing reports in our scheme is thus different from the random order used in SPRT. Since an anchor detector may also report an inaccurate sensing report due to temporal channel impairment, a mobile detector with similar inaccurate sensing report will obtain high instantaneous trustworthiness (i.e., low t_i) if there are only a few anchor detectors, leading to the increase in the false alarm probability. In addition, we can see that using multiple anchor detectors can largely mitigate this limitation, because it is very unlikely for an inaccurate sensing report to simultaneously attain high relative instantaneous trustworthiness with regard to all the anchor detectors. We have also simulated the miss detection probability of our scheme under no attack. The result is very similar to that of Fig. 9 and is thus omitted here due to the space constraints.

C. Summary

We summarize the simulation results as follows.

- Our instantaneous trustworthiness metric can effectively differentiate normal detectors from malicious ones with the help of a small number of anchor detectors.
- Our scheme can enable robust PU detection even when the malicious detectors constitute the majority as long as there are sufficient number of normal detectors.
- When there are too few anchor detectors and too many mobile detectors, our scheme has a slightly worse performance than SPRT in case there is no attack. It is thus necessary to have multiple anchor detectors, say five, to achieve robust PU detection in practice.

The simulation results clearly demonstrate the significant advantage of our scheme over existing schemes under the similar models and assumptions.

V. Related Work

In this section, we briefly discuss some work in several areas which is most germane to our work in this paper.

As mentioned in Section I, previous works can be generally classified into three categories. The schemes proposed in [2]–[6], [9] use various anomaly detection techniques to identify false sensing reports, which would fail if false sensing reports constitute the majority. The second category such as [2], [3], [12] relies on reputation system to differentiate malicious CR users from legitimate users based on their past behaviors, but is unable to handle sudden change in mobile detectors' behaviors. The only piece of work that targets majority of false sensing reports appears in [8], which assumes that neighboring cells can help overturn the decision by the real signal propagation data from primary users. In contrast, our scheme does not rely on inter-cell crosscheck nor requires real signal propagation data from primary users. In addition, detecting false sensing reports in a distributed sensing architecture has been studied in [26], [27], which are orthogonal to our work in this paper.

Another line of work is to mitigate the Primary User Emulation attack, i.e., testing whether the legitimate primary user is using a licensed channel or whether an attacker is impersonating the primary user to use the channel. Proposed

solutions include primary user location estimation [28], authenticating primary user's signal via physically collocated helper node [29] or properly manipulating channel coding and modulation at the physical layer.

In addition, detecting possible spectrum misuse by arbitrary secondary users has been studied in [30], [31]. ALDO [30] uses statistical significance testing to detect illegitimate secondary users based on RSS measurements and the characteristics of radio propagation. The authors of [31] propose to let every legitimate channel user embed a cryptographic spectrum permit into its physical-layer cyclostationary features, which can be verified by mobile "police devices" dispatched by the spectrum owner. These works target different type of attack and are thus orthogonal to our work in this paper.

VI. Conclusion and Future Work

In this paper, we have presented a novel secure crowdsourcing-based cooperative spectrum sensing scheme. The key idea behind our scheme is to jointly consider the instantaneous trustworthiness of mobile detectors in combination with their reputation scores during data fusion. Our scheme can enable robust cooperative sensing even if the malicious CR users are the majority. Extensive simulation results have demonstrated the effectiveness of our proposed scheme. As our future work, we intend to investigate secure cooperative sensing for small-scale primary users.

Acknowledgement

This work was supported in part by the US National Science Foundation under grants CNS- 0716302 and CNS-0844972 (CAREER) and by the National Natural Science Foundation of China under grant 61202140. We would also like to thank anonymous reviewers for their constructive comments and helpful advice.

References

[1] I. Akyildiz, B. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 4, no. 1, pp. 40–62, Mar. 2011.

[2] R. Chen, J. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *INFOCOM'08*, April 2008, pp. 1876–1884.

[3] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *ICC'08*, may 2008, pp. 3406–3410.

[4] A. Min, K. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *ICNP'09*, Princeton, NJ, oct. 2009, pp. 294–303.

[5] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3554–3565, Nov. 2010.

[6] O. Fatemieh, R. Chandra, and C. Gunter, "Secure collaborative sensing for crowdsourcing spectrum data in white space networks," in *DySPAN'10*, Singapore, Apr. 2010.

[7] N. Shankar, C. Cordeiro, and K. Challapali, "Spectrum agile radios: utilization and sensing architectures," in *IEEE DySPAN'05*, Baltimore, MA, Nov. 2005.

[8] O. Fatemieh, M. LeMay, and C. Gunter, "Reliable telemetry in white spaces using remote attestation," in *ACSAC'11*, Orlando, FL, 2011, pp. 323–332.

[9] O. Fatemieh, A. Farhadi, R. Chandra, and C. Gunter, "Using classification to protect the integrity of spectrum measurements in white space networks," in *NDSS'11*, San Diego, CA, Feb. 2011.

[10] "Cisco visual networking index global mobile data traffic forecast update 2011-2016." [Online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf

[11] A. Min, X. Zhang, and K. Shin, "Detection of small-scale primary users in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 2, pp. 349 –361, Feb. 2011.

[12] K. Zeng, P. Paweczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 226 –228, march 2010.

[13] T. Kamakaris, M. Buddhikot, and R. Iyer, "A case for coordinated dynamic spectrum access in cellular networks," in *DySPAN'05*, Nov. 2005, pp. 289–298.

[14] H. Mutlu, M. Alanyali, and D. Starobinski, "Spot pricing of secondary spectrum usage in wireless cellular networks," in *INFOCOM'08*, April 2008, pp. 682 –690.

[15] M. Schwartz, *Mobile Wireless Communications*. Cambridge University Press, 2006.

[16] A. Algans, K. Pedersen, and P. Mogensen, "Experimental analysis of the joint statistical properties of azimuth spread, delay spread, and shadow fading," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 3, pp. 523–531, Apr. 2002.

[17] S. J. Shellhammer, S. S. N, R. Tandra, and J. Tomcik, "Performance of power detector sensors of DTV signals in IEEE 802.22 WRANs," in *TAPAS'06*, Boston, MA, 2006.

[18] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Sel. Topics Signal Process*, vol. 2, no. 1, pp. 4 –17, Feb. 2008.

[19] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications–a tutorial," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 855–884, May 1982.

[20] R. Zhang, Y. Liu, Y. Zhang, and X. Huang, "JR-SND: jamming-resilient secure neighbor discovery in mobile ad-hoc networks," in *IEEE ICDCS'11*, Minneapolis, Minnesota, June 2011.

[21] S. Shellhammer, "Numerical spectrum sensing requirements," IEEE Std. 802.22-06/0088r0, June 2006.

[22] A. Wald, *Sequential Analysis*. Dover Publications, 2004.

[23] Y. Zhang and Y. Fang, "A fine-grained reputation system for reliable service selection in peer-to-peer networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 8, pp. 1134–1145, Aug. 2007.

[24] A. Gelman, J. B. Carlin, H. S. Stern, and D. B. Rubin, *Bayesian Data Analysis*, 1st ed. Chapman & Hall/CRC, June 1995.

[25] Q. Zou, S. Zheng, and A. Sayed, "Cooperative sensing via sequential detection," *IEEE Transactions on Signal Processing*, vol. 58, no. 12, pp. 6266 –6283, Dec. 2010.

[26] F. Yu, H. Tang, M. Huang, Z. Li, and P. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *MILCOM'09*, oct. 2009.

[27] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. Hou, "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks," in *INFOCOM'12*, Orlando, FL, Mar. 2012, pp. 900–908.

[28] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communcations Special Issue on Cognitive Radio Theory and Applications*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[29] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *S&P'10*, Washington, DC, USA, 2010, pp. 286–301.

[30] S. Liu, L. Greenstein, Y. Chen, and W. Trappe, "ALDO: An anomaly detection framework for dynamic spectrum access networks," in *IEEE INFOCOM'09*, Rio de Janeiro, Brazil, Apr. 2009.

[31] L. Yang, Z. Zhang, B. Zhao, C. Kruegel, and H. Zheng, "Enforcing dynamic spectrum access with spectrum permits," in *ACM MobiHoc'12*, Hilton Head Island, SC, June 2012.