A Secure Cooperative Spectrum Sensing Scheme in Mobile Cognitive Radio Networks

Jun Du, 1 Daoxing Guo, 1 Bangning Zhang, 1 and Ligang Shang 2

1 College of Communications Engineering, PLA University of Science & Technology, Nanjing, Jiangsu 210007, China
2 Units 72959 PLA, Jinan, Shandong 250031, China

Correspondence should be addressed to Daoxing Guo; xyzgfg@163.com

Received 26 January 2014; Revised 13 May 2014; Accepted 19 May 2014; Published 5 June 2014

The reliability of cooperative spectrum sensing (CSS) can be severely degraded by the falsified spectrum sensing reports provided by malicious secondary users (SUs). However, in existing works, the problem of secure CSS in mobile cognitive radio networks (CRNs) has not been well considered yet. The detection of abnormal sensing reports in existing works does not evaluate both sensing reports and locations of SUs simultaneously. And the mobility pattern of all SUs is assumed to be similar, which is impractical in real mobile CRNs. In this paper, spatial correlation of the received signal strength among SUs is exploited to get the evidence whether the received signal strength is consistent with the location from where it is generated. And Dempster-Shafer theory is used to filter out abnormal reports by combining the evidence collected from the spatial correlation algorithm in each sensing period. To mitigate the adverse effects caused by the SUs’ mobility pattern, a fusion scheme based on SUs’ reputation is proposed. In comparison to the existing schemes, simulation results demonstrate that the proposed secure CSS scheme improves the primary user detection rate by 10% at false alarm rate of 0.1 when the mobility pattern of the SUs is different.

1. Introduction
Cognitive radio networks (CRNs) are expected to bring evolution to the spectrum scarcity problem through intelligent use of the underutilized or the free spectrum bands [1]. Being capable of utilizing the spectrum in an opportunistic manner, cognitive radio enables secondary users (SUs) to sense the portion of the spectrum that is available, select the appropriate channel for access, and vacate from the channel when the primary users (PUs) return.

Spectrum sensing is a vital phase in CRNs [2]. The goal of spectrum sensing is to detect accurately and reliably, in real time, the presence or absence of primary signals on a spectrum band. In a shadowed or fading environment, the received signal strengths (RSSs) at a SU may vary significantly at different locations. Spectrum sensing is hampered by the uncertainty resulting from channel randomness. To combat these impacts, cooperative spectrum sensing (CSS) schemes have been proposed to obtain the spatial diversity in CRNs [3, 4]. In CSS, information from different SUs is combined to make a decision on the presence or absence of the primary user.

CSS requires each SU has the ability to negotiate with another spectrum and network utilization. This negotiation process may be undertaken with the support of networks or simply by proceeding in an ad hoc manner [5]. However, the negotiation process can be manipulated by attackers in various ways, such as spectrum sensing data falsification (SSDF) attack [6]. Beside faulty nodes, according to the motivations, Chen et al. [7] classify the attackers into two types: selfish attacker and malicious attacker. Selfish attacker may report the presence of the primary user when its transmission demands cannot be met. The goal of selfish attacker is to monopolize the specific band sneakily by forcing all other SUs to evacuate it; malicious attacker may report absence or presence of the primary user opposite to its actual spectrum sensing results. The goal of this type of attacker is to prevent other SUs from using the spectrum and causing
a denial of service (DoS) or harmful interference to the PUs. Because of the possible existence of the attackers and the uncertainties in the primary signal from factors such as shadowing, the design of secure CSS is a challenging problem.

According to the cooperative interaction among attackers, there are generally two types of SSDF attacks existing in CRNs, that is, independent attack and collaborate attack [8]. In independent attacks, all the actions of attackers are based on their own observations of the PU’s status and there is no information exchanged between the attackers. For example, in [9], the authors model spectrum state transitions using a Markovian model and propose a conditional frequency check (CFC) to counter independent attack in CRNs. In collaborate attacks, a SSDF attacker acts according to local decisions of the honest users or the other attackers. To prevent collaborate attacks, the authors in [10] proposed a prevention mechanisms, which discourage selfish attackers from launching attacks by designing attack detection and punishment strategies. But the proposed prevention mechanisms are ineffective for malicious attackers. Although collaboration among attackers can improve the effectiveness of the damage, it has its own drawbacks. Collaborate attacks require additional infrastructure to coordinate the attackers and increase communication overhead among attackers, which can deplete the resources of the attackers or reduce the concealment of attack. In this paper, we assume that only independent attack exists in CRNs.

Contrary to the conventional CSS, the SUs are not assumed to be trusted a priori in secure CSS. Many secure CSS schemes have been proposed to resist the SSDF attack in literature, where these schemes usually consist of two-stage process: identify malicious SU and filter out contaminated sensing reports and combine the reports that are filtered by the first stage. When the locations of PUs and SUs are unknown a priori, nonlocation based schemes have been developed. For example, an enhanced weighted sequential probability ratio test (EWSPRT) [11] based on Bayesian detection is proposed for secure CSS. However, EWSPRT requires that the knowledge of a priori probability of SU’s sensing results reported by neighboring SUs at each sensing period. By using Geary’s C [19] is used to characterize the degree of correlation between sensing results reported by neighboring SUs at each sensing period. We proposed the Location-Reports Consistency (LRC) test to filter out inconsistent sensing reports (abnormal sensing value or incorrect location information) caused by the uncertainty of the noise or the attacker’s malicious behaviors. In the proposed scheme, the Geary’s C requires that the knowledge of a priori probability of SU’s sensing reports under hypothesis zero and one, such data may be unavailable in practice. A scheme [6] based on abnormality detection techniques is proposed to identify malicious SU. In [12], another scheme based on maximum a posterior estimation is proposed to calculate suspicious level of all SUs. When the suspicious level of a SU is beyond certain threshold, its reports will be temporarily removed from decision making. In [13], robust statistics was used to approximate the distributions for both hypotheses of all nodes, discriminatingly, based on their past data reports. An SU with abnormal estimated parameters will be detected as malicious SU, and its reports will be filtered out. The authors in [14] propose applying the Dixon’s test on the SUs’ energy data to suppress a malicious secondary user (SU) in centralised fusion based CRNs. When the fusion center (FC) can obtain the location information of the SUs, another type of location based schemes has also been developed. In [15], the authors view the area of interest as a grid of square cells and assumed that the FC can get reliable coordinate of each SU. The proposed mechanism is based on identifying outlier measurements inside each cell, as well as corroboration among neighboring cells in a hierarchical structure to identify cells with significant number of malicious SUs. In [16], spatial correlation among neighboring SUs is exploited to discard the abnormal sensing reports. The reports of an SU may be unreliable due to it moving to a bad location by chance or it submitting manipulated sensing reports. The author in [17] takes into consideration both location-diversity and mobility of SUs, and Dempster-Shafer theory is used to combine the credibility of each SU’s current and past reports, and the evaluation of trust for current report from each SU is given.

However, existing schemes have two limitations for its application in mobile scenario. Firstly, these schemes either assume the SUs are static or assume that all of the SUs have similar mobility pattern; that is, the average velocity of malicious SUs and honest SUs are the same, and their activity areas are also the same, which is impractical in real cognitive radio networks and may lead to incorrect conclusions. For example, existing schemes assume the number of attackers is always less than honest SUs; however, when the range of attackers’ activity area is smaller than the honest SUs, the attackers will dominate these areas, and such assumption will be invalid there. Secondly, existing works do not evaluate both sensing reports and locations of SUs simultaneously [18], or in other words the detection of abnormal sensing reports only based on the deviation from its neighbor’s reports, which is not accurate and may mistake the honest SUs located far away from the PU for malicious SUs or neglect the malicious SUs located near to the PU.

Considering the practical problems and limitations discussed above, we focus on the issue of secure CSS scheme for mobile CRNs. We proposed the Location-Reports Consistency (LRC) test to filter out inconsistent sensing reports (abnormal sensing value or incorrect location information) caused by the uncertainty of the noise or the attacker’s malicious behaviors. In the proposed scheme, the Geary’s C is used to characterize the degree of correlation between sensing results reported by neighboring SUs at each sensing period. By using Geary’s C, the credibility of each SU’s reports is collected. Being in mobile scenario, the neighbors of an SU may be different at each sensing period. Therefore, we propose using Dempster-Shafer theory to update the credibility of SUs’ reports at each sensing period, and those inconsistent sensing reports are filtered out. To mitigate the adverse effects caused by the diversity of SUs’ mobility pattern, we propose a Reputation based Data Fusion (RDF) scheme, which can efficiently mitigate attackers’ negative impact on the final decision while utilizing the benefits it will bring. The SUs’ reputations are built up based on Bayesian reputation model. The SU’s sensing reports are weighted at the FC, and hence the SU with bad reputation will have less effect on the final decision.

The main contributions of this paper can be summarized as follows.

(i) Propose the LRC test to filter out unreliable reports, which take into consideration both the SU’s sensing reports and locations simultaneously.
(ii) Propose the RDF scheme to weigh each SU’s sensing reports based on their reputation value, the proposed scheme updating each SU’s reputation value according to its behavior in the areas of different fading.

(iii) In-depth simulation in mobile CRNs shows our proposed secure CSS schemes outperforming existing scheme regardless of the attackers’ mobility pattern.

The remainder of this paper is organized as follows. In Section 2, we explained the system model in detail. In Section 3, we give the problem formulation and propose the solution. In Section 4, we evaluate the performance of our solution. Finally, we concluded this paper in Section 5.

2. System Model

The system is illustrated in Figure 1. We consider a primary transmitter, which is located far away from the CRNs. Thus the entire CRNs lie within the detection range of the primary signal. The CRNs, we considered, mainly urban areas, where trees, building, and so forth, will cause deep fading. Consider 𝑁 SUs collaborating for spectrum sensing. After each sensing period, SUs send their reports, based on their local observations, to a FC. We assume that there exist at most 𝑀 malice SUs and the remaining 𝑁 − 𝑀 SUs are honest. It is reasonable to assume that 𝑀 < 𝑁. The SUs are mobile and may be present at different locations at different times. And the mobile pattern of honest SUs and malicious SUs are different. The areas of CRNs can be divided into a grid, and each cell in a grid is assumed to have the same path-loss exponent and shadowing parameters of its own [17]. The total number of cells is 𝐿. In practice, the size or shape of a cell may be chosen differently which depends on the signal propagation environment and shadowing caused by obstacles between PU and SU.

2.1. Cooperative Spectrum Sensing Models. As a key technology for realizing opportunistic spectrum access, spectrum sensing aims to detect the presence of PUs accurately and quickly. Due to its applicability to a wide range of signals and mathematical amenity compared to other detectors, an energy detection spectrum sensing method [20] is used.

Each SU is having an energy detector as shown in Figure 2. The SUs sense the spectrum periodically slot by slot using energy detection. Assume that the bandwidth of the primary user signal is 𝑊 and sample interval is 𝑇. At each sensing period, each user senses the local spectrum and takes 𝑁 𝑡 = 2𝑇𝑊 samples of the signal measurements.

The sample 𝑥𝑖(𝑛) taken at time 𝑛 by the secondary user can then be written as follows:

\[ x_i(n) = \begin{cases} v_i(n) & H_0 \\ h_i(n) \cdot s(n) + v_i(n) & H_1, \end{cases} \]

where 𝐻₀ and 𝐻₁ are hypotheses to determine the absence and presence of the PU signal, respectively. 𝑠(𝑛) is the signal transmitted from the primary user and 𝑡𝑖(𝑛) denotes the gain of the channel between the PU and SU 𝑢𝑖. And 𝑣𝑖(𝑛) is the sample of the zero-mean additive white Gaussian noise (AWGN) with variance 𝜎².

As shown in Figure 2, the output of the energy detector for SU 𝑢𝑖, at 𝑘th sensing period, is

\[ Y_i(k) = \frac{1}{N} \sum_{n=1}^{N} |x_i(n)|^2. \]

As the number of samples 𝑁 𝑖 taken becomes sufficiently large, the distribution 𝑓𝑌𝑖(𝑘)(𝑦) of the test statistic 𝑌𝑖(𝑘) can be approximated using the central limit theorem as follows [21, 22]:

\[ f_{Y_i(k)}(y) \sim \begin{cases} \mathcal{N}\left(\sigma^2, \frac{2}{N} \sigma^4\right), & H_0 \\ \mathcal{N}\left(Pr_i + \sigma^2, \frac{2}{N} \left(Pr_i + \sigma^2\right)^2\right), & H_1, \end{cases} \]

where 𝑃𝑟𝑖 is the received power of a primary signal at the SU 𝑢𝑖.

At each sensing period, each SU 𝑢𝑖 sends 𝑌𝑖 along with its coordinates to the FC. SUs can find their current coordinates, based on localization techniques [23].

Based on the test statistic 𝑌𝑖(𝑘), the SU 𝑢𝑖 then makes a decision of the presence of the PU. The probability of making wrong decisions (false alarm and missed detection) can be defined and calculated as follows:

\[ P_{PA} = \text{Prob}(Y_i(k) \geq \eta | H_0) = Q \left( \frac{\eta - \sigma^2}{\sqrt{2/N} \sigma^2} \right), \]

\[ P_{MD} = \text{Prob}(Y_i(k) < \eta | H_1) = 1 - Q \left( \frac{\eta - (Pr_i + \sigma^2)}{\sqrt{2/N} \sigma^2} \right), \]

where the 𝑄(·) function is the complementary CDF of the standard Gaussian distribution. And 𝜂 is detection threshold at the FC.
By cooperation, SUs can share their sensing information for making a combined decision more accurate than the individual decisions [24]. In the CSS, multiple SUs observe the signal from the PU, and the observed signals at the SUs are combined at the FC. Hard and soft combinations are the typical combination strategies. The original sensing information is combined in the soft combination, whereas two-level quantized information is combined in the hard combination. In this paper, we use weighted soft combination to mitigate attackers’ negative impact on the final decision.

Let $Y(k)$ be the summation of the weighted reports from SUs at $k$th sensing period. The decision statistic of CSS is, thus,

$$Y(k) = \sum_{i=1}^{N} w_{ui}(k) Y_{ui}(k), \quad (5)$$

where $w_{ui}(k)$ denote the weighting coefficient for the report of the SU $u_i$.

Thus, the probability of detection and the probability of false alarm for CSS at $k$th sensing period are given by [21]

$$Q_f(k) = \Pr(Y(k) > \eta | H_0(k))$$

$$= Q \left( \frac{\eta - \sum_{i=1}^{N} w_{ui}(k) \sigma^2}{\sqrt{(2/N_i) \sum_{i=1}^{N} w_{ui}(k)^2 \sigma^2}} \right), \quad (6)$$

$$Q_d(k) = \Pr(Y(k) > \eta | H_1(k))$$

$$= 1 - Q \left( \frac{\eta - \sum_{i=1}^{N} w_{ui}(k) (P_{tr} + \sigma^2)}{\sqrt{(2/N_i) \sum_{i=1}^{N} w_{ui}(k)^2 (P_{tr} + \sigma^2)}} \right).$$

In Section 3.1, we will give the method to calculate $w_{ui}(k)$ in detail.

2.2. Signal Propagation Models. The received primary signal strength at SU $u_i$ at $k$th sensing period can be expressed as the propagation model [25]

$$P_{tr}(k) = P_t K_c \left( \frac{d_0}{d_i^\alpha} \right) Z_i(k) Ray_i(k), \quad (7)$$

where $P_t$ is the signal strength at the primary transmitter, $K_c$ a unitless constant which depends on the antenna characteristics and the average channel attenuation $K_c(dB) = -20 \log_{10}(4\pi d_0/\lambda)$, $\lambda$ the wavelength, $\alpha$ the path-loss exponent, $d_0$ the reference distance, and $d_i^\alpha$ the distance from the PU’s transmitter to the SU $u_i$ at $k$th sensing. And $Z_i(k)$ is the log-normal shadowing from the PU to the SU $u_i$ at $k$th sensing and $Ray_i(k)$ is the Rayleigh fading from the PU to the SU $u_i$ at $k$th sensing. It is reasonable to assume that the channel bandwidth is much larger than the coherent bandwidth. Therefore, the effect of Rayleigh fading is negligible [16].

2.3. Attack Model. A malicious SU may alter local spectrum sensing reports on purpose, misleading the fusion center to make the wrong decision. To make his attack action steady, the attacker may also reports incorrect location information. Here, we consider an independent attack where all the actions of malicious SUs are based on their own observations of the PU's status and there is no information exchanged between the malicious SUs. The fusion center is unaware of the number of attackers and the strategy of attack they employed.

We define two types of SSDF attacks [26] with three parameters: the attack threshold ($\delta$), the attack strength ($\Delta$) and the attack probability ($P_a$).

Selfish Attack. At each sensing period $k$, if attacker’s the local observation $Y_i(k)$ is lower than $\delta$, the attacker sends $Y_i(k) + \Delta$ with the probability $P_a$, instead of $Y_i(k)$; otherwise, it reports $Y_i(k)$. The attacker chooses $\delta$ in order to conceal its malicious behavior. And $P_a$ represent the probability that the attacker has communication demands. Obviously, the attacker launching selfish attack aims to get exclusive spectrum access or making the channel available for other unauthorized users.

Vandalism Attack. At each sensing period $k$, if the attacker’s local observation $Y_i(k)$ is lower than $\delta$, the attacker sends $Y_i(k) + \Delta$ with the probability $P_a$, instead of $Y_i(k)$; if the attacker’s local observation $Y_i(k)$ is higher than $\delta$, the attacker sends $Y_i(k) - \Delta$ with the probability $P_a$. The intention of the vandalism attacker is to both cause interference to PU and inhibit the communication of other SUs.

3. Secure Cooperative Spectrum Sensing Scheme

In this section we first propose the Location-Reports Consistency (LRC) test to filter out abnormal sensing reports based on spatial data analysis. Due to the difference of fading and shadowing characteristics in different locations of CRNs, the average received signal strength varies with locations [27]. Then according to this characteristic, we propose our algorithms for evaluating the quality of each cell, which is used to construct SUs’ reputation value. And finally, to mitigate the adverse effects caused by SUs mobility pattern, a fusion scheme based on SU’s reputation is proposed.
3.1. Location-Reports Consistency (LRC) Test. In shadow fading environment, the sensing reports made at the same time but different locations may not be independent [28]. For example, the sensing reports made at nearby locations may be closer in value than the sensing reports made at locations farther apart. Due to the fact that the correlation between two SUs’ reports at the same time is weaker with locations farther apart. Due to the fact that the correlation between two SUs’ reports at the same time is weaker with locations farther apart, SUs dominate the cell, the Geary’s C statistic is used to evaluate the credibility in CSS can be characterized by the following reasons. The motivation for selecting DST to evaluate credibility in CSS can be characterized by the following reasons.

The SU $u_i$’s sensing report to the fusion center at $k$th sensing can be expressed as

$$Y_i(k) = \text{Pr}_i(k) + N_i + E_i,$$

where $N_i$ is the noise power added to the SU $u_i$’s sensing result and $E_i \sim \mathcal{N}(0, \sigma^2/N)$ is the measurement error of the SU $u_i$.

According to (7), the shadowing component can be calculated by

$$Z_i(k) = C \text{Pr}_i(k) (d_i^k)\alpha,$$

where $C = 1/P_K(d_i^0)^\alpha$ is the constant value at given $\alpha$.

The correlation of the shadowing component can be expressed as

$$\text{Corr} \left( Z_i(k), Z_j(k) \right)
= C \left\{ \text{Corr} \left( Y_i(k) (d_i^k)^\alpha, Y_j(k) (d_j^k)^\alpha \right)
- \text{Corr} (N_i(k) (d_i^k)^\alpha, N_j(k) (d_j^k)^\alpha)
- \text{Corr} (E_i(k) (d_i^k)^\alpha, E_j(k) (d_j^k)^\alpha) \right\}.$$

At different location, the noise power of SU $u_i$ and $u_j$ are uncorrelated, and their measurement errors are also uncorrelated [16]; (10) can simplified as

$$\text{Corr} \left( Z_i(k), Z_j(k) \right)
= C \left\{ \text{Corr} \left( Y_i(k) (d_i^k)^\alpha, Y_j(k) (d_j^k)^\alpha \right) \right\}.$$

In our system model, SUs in the same cell have same path-loss exponent of that cell. From (11), the correlation in the product of sensing reports and the distance from the PU to the SU $\{Y_i(k)d_i^k\}$ preserves the correlation of the shadow fading. So we define a metric $z_i(k) = Y_i(k)d_i^k$ and use Geary’s $C$ statistic to evaluate both the sensing value and location which SUs have reported simultaneously.

Geary’s $C$ statistic is based on the deviations in responses of each observation with one another, and the definition is given by [19]

$$C = \frac{(n-1)\sum_{i=1}^{n} \sum_{j=1}^{n} W_{i,j} (z_i(k) - z_j(k))^2}{2 \left( \sum_{i=1}^{n} \sum_{j=1}^{n} W_{i,j} \left( z_i(k) - \bar{z} \right)^2 \right)},$$

where $n$ is the number of reports received from the cell $c_j$ at $k$th sensing period and $W_{i,j}$ is a weight indicating something about the spatial relationship of SU $u_i$ and $u_j$. Usually, the weight equals the reciprocal of the distance between two SUs, that is, $W_{i,j} = 1/d(u_i, u_j)$. And $\bar{z}$ is the mean of $z_i(k)$, that is, $\bar{z} = (1/n) \sum_{i=1}^{n} z_i(k)$. Geary’s $C$ measures the global spatial autocorrelation of SUs’ report in the same cell. It varies from 0 to 2, value 0 indicates strong negative correlation, and value 2 indicates strong positive correlation, and 1 means in the absence of autocorrelation. In order to find out abnormal SUs, we focused on one pair of SUs’ reports each time. In this special case, $n = 2$, $W_{i,j} = W_{j,i} = 0$; that is, at $k$th sensing period both the SU $u_i$ and $u_j$ visit the same cell $c_j$; the Geary’s $C$ between SU $u_i$ and $u_j$ is simplified as

$$C_{i,j}(k) = \frac{\left[ z_i(k) - z_j(k) \right]^2}{2 \left[ (z_i(k) - \bar{z})^2 + (z_j(k) - \bar{z})^2 \right]}.$$

The average Geary’s $C$ of the SU $u_i$ at $k$th sensing can be evaluated as

$$C_i(k) = \frac{1}{n} \sum_{j=1}^{n} C_{i,j}(k),$$

where $C_{i,j}(k)$ is the Geary’s $C$ between SU $u_i$ and $u_j$.

The expectation and the variance of Geary’s $C$ of the cell $c_j$ at $k$th sensing are $E[C_i(k)]$ and $\text{Var}[C_i(k)]$, respectively. The details of the expression are given in the Appendix.

Heuristically, when the SU $u_i$ in the cell $c_j$ at $k$th sensing period, the more deviating of $C_i(k)$ from $E[C_i(k)]$, the more suspiciousness of the SU $u_i$’s report. However, if malicious SUs dominate the cell, the Geary’s $C$ of a honest SU also deviates significantly from $E[C_i(k)]$. An accurate credibility of a SU cannot be got only by its sensing report at a single sensing period. The FC may accumulate a certain number of reports from an SU to get its credibility.

To quantify the uncertainty of an SUs’ reports’ credibility, the Dempster-Shafer theory (DST) is used to combine the uncertainty deriving from its sequential sensing reports to determine the overall uncertainty in redevelopment decision-making. Traditional probability theory has strict separation of aleatory and epistemic uncertainty. Aleatory uncertainty results from the fact that a system can behave in random ways, while epistemic uncertainty results from the lack of knowledge about a system [30]. Evidence theory can correctly represent epistemic uncertainties from intervals, degrees of belief, and probabilistic information [31]. The motivation for selecting DST to evaluate credibility in CSS can be characterized by the following reasons.
(1) DST allows for the direct representation of uncertainty of system responses to the SU’s report where an imprecise system input can be characterized by a set or an interval and the resulting output is a set or an interval.

(2) The evidence gets from one sensing period is imperfect or imprecise; DST can combine evidences from two or more sensing period to form a relatively perfect or precise references.

A SU's sensing report is either consistent with or inconsistent with its locations, so we have a set of hypothesis, that is, frame of discernment, \( \Theta = \{H, -H\} \), which represent the SU’s reports honest with or dishonest with its locations.

The power set \( 2^\Theta \), that is, including all possible subsets of the frame of discernment, is \( \{\phi, H, -H, \{H, -H\}\} \). A mapping function assigns a number in the range \([0, 1]\) to every singleton of \( 2^\Theta \) such that the numbers sum to 1. There is a mapping function \( m : 2^\Theta \rightarrow [0, 1] \) satisfying \( m(\phi) = 0 \), and \( \sum_{\sigma \in 2^\Theta} m(\sigma) = 1 \), and \( m(\sigma) \) is called Basic Probability Assignment (BPA) of \( s \).

According to previous analysis, if the average Geary’s C of the SU \( u_i \) deviates more from the Geary’s C of cell \( c_j \), which the SU \( u_i \) is in, the SU’s honesty BPA should be lesser. We designed a BPA and limited honesty BPA in the range \([0, 1]\):

\[
m_{u_i}(s_k = H) = e^{\left| C_{u_i}(k) - E[C(k)] \right| / \sqrt{\text{Var}[C(k)]}}.
\]

\[
m_{u_i}(s_k = -H) = 0,
\]

\[
m_{u_i}(s_k = \{H, -H\}) = 1 - m_{u_i}(s_k = H) - m_{u_i}(s_k = -H),
\]

where \( C_{u_i}(k) \) is the average Geary’s C of SU \( u_i \) at kth sensing period. \( E[C(k)] \) and \( \text{Var}[C(k)] \) represent the expectation and the variance of the Geary’s C of the cell \( c_j \) at kth sensing period, respectively.

The credibility of the SU \( u_i \)'s report can be deduced from its current and past reports. We use DST's combination scheme for updating the SU's bma at each sensing period:

\[
m_{u_i}(s_{k+1} = H) = \frac{\sum_{u_i = H} \prod_{1 \leq k \leq K} m_{u_i}(s_k)}{1 - \sum_{u_i = \phi} \prod_{1 \leq k \leq K} m_{u_i}(s_k)},
\]

The statistic of location-reports consistency test can be denoted by

\[
T_k(u_i) = m_{u_i}(s_{k+1} = H).
\]

Therefore, if \( T_k(u_i) \) is smaller than a threshold \( \varepsilon \), the report from the SU \( u_i \) at kth sensing period is incredible, and this report will be discarded.

3.2. Evaluate the Average of the Signal Strength Received from Each Cell. In the mobile cognitive radio networks, an SU may visit different cells over a period of time. Different cells may have different path-loss and shadowing characteristics, and the distance from the PU may also be different. Thus, the average of receiving signal strength of the PU may be different significantly at different cells. We can classify the cells according to the average of receiving signal strength of the PU from each cell. The reports from a low quality cell will be unreliable. However, it is unrealistic to have prior knowledge of fading and shadowing characteristics of all the cells, and many data-mining approaches cannot be applied without training data. In this section, we will evaluate the quality of each cell. We evaluate the quality of each cell for two reasons: (1) to give low weight to the reports come from the low quality cells and (2) to use these results to check the SUs intention and construct SUs’ reputation value. We will detail this reason in Section 3.3.

Let \( Y_{u_i} \) be the report of SU \( u_i \) at kth sensing and \( p_{u_i}^{c_j} \), be the probability of SU \( u_i \) in cell \( c_j \) at kth sensing. Then after \( K \) times sensing, the expected total number of reports generated by the SU \( u_i \) from cell \( c_j \) is \( \sum_{k=1}^{K} Y_{u_i} p_{u_i}^{c_j} \), and the expected sum of reports generated by the SU \( u_i \) from cell \( c_j \) is \( \sum_{k=1}^{K} Y_{u_i} p_{u_i}^{c_j} \).

Then, the average sensing reports of the SU \( u_i \) from the cell \( c_j \), denoted as \( T_{u_i}^{c_j} \), is

\[
T_{u_i}^{c_j} = \frac{\sum_{k=1}^{K} Y_{u_i} p_{u_i}^{c_j}}{\sum_{k=1}^{K} p_{u_i}^{c_j}}.
\]

**Proposition 1.** For a honest SU \( u_i \), the expected value of \( T_{u_i}^{c_j} \) is proportional to the average signal strength received from the cell \( c_j \). And the variance of \( T_{u_i}^{c_j} \) decreases with the number of sensing increasing.

**Proof.** From (3), we can express a SU \( u_i \)'s report as

\[
Y_{u_i} \mid \mathcal{H}_0 \sim \mathcal{N}\left( \sigma^2, \frac{2}{N_s} \sigma^2 \right),
\]

\[
Y_{u_i} \mid \mathcal{H}_1 \sim \mathcal{N}\left( \text{Pr}_i + \sigma^2, \frac{2}{N_s} (\text{Pr}_i + \sigma^2)^2 \right).
\]

We denote by \( Pr_i \) and \( P_i \) the probabilities that the PU is busy or idle, respectively.
Then
\[ Y_{u_i,k} = P_l \ast \left( Y_{u_i} \mid \mathcal{H}_0 \right) + P_B \ast \left( Y_{u_i} \mid \mathcal{H}_1 \right). \]  
(20)

After some algebra, the expectation of \( T_{u_i}^c \) can be expressed as
\[ E \left( T_{u_i}^c \right) = P_l \ast \sigma^2 + P_B \ast \left( P_{r_j} + \sigma^2 \right). \]  
(21)

It means that \( E(T_{u_i}^c) \) can be used to evaluate the quality of the average signal strength received from the cell \( c_j \).

The variance of \( T_{u_i}^c \) can be expressed as
\[
D \left( T_{u_i}^c \right) = \left[ \frac{P_l^2 \ast \sigma^4}{N_s} + \frac{P_B^2 \ast \left( P_{r_j} + \sigma^2 \right)^2}{N_s} \right] \frac{\sum_{k=1}^{K} \left( P_{u_i,k}^c \right)^2}{\left( \sum_{k=1}^{K} P_{u_i,k}^c \right)^2}.
\]  
(22)

Notice that \( 0 \leq P_{u_i,k}^c \leq 1, 1/K \leq \sum_{k=1}^{K} \left( P_{u_i,k}^c \right)^2 / \left( \sum_{k=1}^{K} P_{u_i,k}^c \right)^2 \leq 1 \) and \( \sum_{k=1}^{K} \left( P_{u_i,k}^c \right)^2 / \left( \sum_{k=1}^{K} P_{u_i,k}^c \right)^2 \) decreases monotonically as \( K \) increases.

Therefore \( D(T_{u_i}^c) \) decreases monotonically as \( K \) increases, and
\[
\frac{1}{K} \left[ \frac{P_l^2 \ast \sigma^4}{N_s} + \frac{P_B^2 \ast \left( P_{r_j} + \sigma^2 \right)^2}{N_s} \right] \leq D \left( T_{u_i}^c \right) \leq \left[ \frac{P_l^2 \ast \sigma^4}{N_s} + \frac{P_B^2 \ast \left( P_{r_j} + \sigma^2 \right)^2}{N_s} \right].
\]  
(23)

According to Proposition 1, \( E(T_{u_i}^c) \) can be interpreted as the evaluation of the average signal strength received from the cell \( c_j \) given by SU \( u_i \). And the accuracy of this evaluation improves as the number of sensing periods increases. For convenience of exposition, \( E(T_{u_i}^c) \) will be referred to as the evaluation of the quality of the cell \( c_j \) given by SU \( u_i \). Considering \( K \) sensing periods of observations, using empirical distribution function [32], \( E(T_{u_i}^c) \) can be estimated as

\[
E \left\{ T_{u_i}^c \right\} = \frac{\sum_{k=1}^{K} Y_{u_i,j}(k) \delta_{u_i}(k)}{\sum_{k=1}^{K} \delta_{u_i}(k)},
\]  
(24)

where \( \delta_{u_i}(k) = 1 \) for SU \( u_i \) in cell \( c_j \) at \( k \)th sensing, otherwise is 0.

We denote \( \text{Avg}_{u_i}(c_j) = E(T_{u_i}^c); \) let \( \text{Avg}(c_j) = \{ \text{Avg}_{u_1}(c_j), \text{Avg}_{u_2}(c_j), \ldots, \text{Avg}_{u_N}(c_j) \} \) be the set of evaluations for the quality of the cell \( c_j \) given by each SU. The quality of the cell \( c_j \) can be simply computed by averaging all the values in the set \( \text{Avg}(c_j) \). However, this method is not robust and can be easily manipulated by malicious SUs. Therefore, we use the \( \alpha \)-trimming method [33] to filter out abnormal evaluation values. The \( \alpha \)-trimmed mean, \( \mu_{c_j} \), is the robust evaluation of the cell \( c_j \). The values in the set \( \text{Avg}(c_j) \) are first sorted, and then an \( \alpha \) proportion of the smallest values and an \( \alpha \) proportion of the largest values are omitted in the calculation of the mean \( \mu_{c_j} \). If \( y_{1,N}, \ldots, y_{N,N} \) represent the order statistics, the \( \alpha \)-trimmed mean \( \mu_{c_j} \) is
\[
\mu_{c_j} = \frac{1}{N - 2 \left\lfloor N \alpha \right\rfloor} \sum_{j=1}^{N - \left\lfloor N \alpha \right\rfloor} y_{i,N}, \quad j = 1, 2, \ldots, L.
\]  
(25)

Therefore, the proposed algorithm for evaluating the quality of a cell is summarized in Procedure 1.

### 3.3. The Reputation Based Data Fusion (RDF) Scheme

The LRC test can detect whether an SU has reported manipulated sensing value or location information, but it did not consider the reliability of the reports of neighbors; that is, although an SU’s report shows high spatial correlation among its neighbors’ reports in the same cell, its neighbors’ reports are not always reliable. Because the average strength of sensing value reported from different quality cells is different. If the strength of a sensing value reported from low quality cell is higher than the average strength of sensing reports that the FC has received at \( k \)th sensing period, this sensing report may be unreliable. Likewise, if the strength of a sensing value reported from high quality cell is lower than the average strength of sensing reports that the FC has received at \( k \)th sensing period, this sensing report may also be unreliable.

We exploit this characteristic to construct SUs’ reputation value. Therefore, to mitigate the adverse effects caused by SUs...
mobility pattern, we proposed a new reputation based data fusion (RDF) scheme to provide a better fusion performance. The idea is to assign different weights based on SUs’ reputation value to their sensing reports. The FC then forms a weighted sum, which is compared to a threshold to decide whether the PU is active or not.

In this paper, we apply the Bayesian reputation model [34] for the SUs’ reputation value update and assign weight dynamically according to the reputation of each SU. The advantage of Bayesian reputation model is that they provide a sound mathematics basis for computing each SU’s reputation value. Let us denote $p_{ui}$ to be the probability where the SU $u_i$ acts honestly, and the parameter $r_{ui,k}$ represents the amount of positive feedback provided by the FC when the SU $u_i$ sends its top $k$ sensing reports to the FC. And the parameter $s_{ui,k}$ represents the amount of negative feedback provided by the FC when the SU $u_i$ sends its top $k$ sensing reports to the FC. Then the probability density function of $p_{ui}$, which is called the SU $u_i$’s reputation function, can be expressed using gamma function $\Gamma$ as

$$f(p_{ui} \mid r_{ui,k}, s_{ui,k}) = \frac{\Gamma(r_{ui,k} + s_{ui,k} + 2)}{\Gamma(r_{ui,k} + 1) \Gamma(s_{ui,k} + 1)} p_{ui}^{r_{ui,k}} (1 - p_{ui})^{s_{ui,k}},$$

where $0 \leq p_{ui} \leq 1, r_{ui,k} \geq 0, s_{ui,k} \geq 0$.

The probability expectation value of the SU $u_i$’s reputation function can be written as

$$\phi_i(k) = E(p_{ui}) = \frac{r_{ui,k} + 1}{r_{ui,k} + s_{ui,k} + 2},$$

where $\phi_i(k)$ is called the SU $u_i$’s reputation value at $k$th sensing period. $\phi_i(k)$ can be interpreted as the probability that the SU $u_i$ is expected to behave in future action.

The weights in soft combination scheme are assigned based on each SU’s reputation value. And the weighting coefficient for the report of the SU $u_i$ is defined as

$$w_{ui}(k) = \frac{\phi_i(k)}{\sum_{j=1}^{N} \phi_j(k)}.$$  

In the following, we give the derivation of $r_{ui,k}$ and $s_{ui,k}$ and consequently get the SU $u_i$’s reputation value $\phi_i(k)$.

At $k$th sensing period, an SU $u_i$ sends its sensing report to the FC, and the impact on building up its reputation can be represented as

$$\rho_i(k) = \begin{cases} 
0, & R_i^j (k) > \overline{R}_i (k), \quad q(C_j) < \overline{q} \\
0, & R_i^j (k) < \overline{R}_i (k), \quad q(C_j) > \overline{q} \\
1, & \text{others}
\end{cases}$$

$$\overline{R}_i (k) = \frac{\sum_{j=1}^{L} \sum_{i=1}^{N} R_i^j (k) \delta_i^j (k) \mathcal{J}(T_k (u_i) \geq \varepsilon)}{\sum_{j=1}^{L} \sum_{i=1}^{N} \delta_i^j (k) \mathcal{J}(T_k (u_i) \geq \varepsilon)}$$

where $\rho_i(k)$ denote the SU $u_i$ reputation value gained at $k$th sensing period, $R_i^j (k)$ denote the strength of the SU $u_i$’s sensing report from the cell $C_j$ at $k$th sensing period, $\overline{R}_i (k)$, defined in (30), is the average strength of sensing reports which are survived from LRC test, $\mathcal{J}()$ is the indicator function returning 1 when the statement in the parenthesis holds true and 0 otherwise, $\varepsilon$ is the threshold which is used in LRC test, $q(C_j)$ is the quality of the cell $C_j$, $\overline{q}$ is the median of the cell’s quality among all cells, and $\overline{q} = \text{median}_{1 \leq j \leq L} q(C_j)$.

If $R_i^j (k)$ which comes from low quality cell $C_j$ is higher than $\overline{R}_i (k)$, the SU $u_i$’s reputation value will be decreased. Likewise, if $R_i^j (k)$ which comes from high quality cell $C_j$ is lower than $\overline{R}_i (k)$, the SU $u_i$’s reputation value will also be decreased. In other cases, the SU $u_i$’s reputation value will be increased.

The SU $u_i$ may change its behavior over time, and, due to sensing error or other random factors, the SU $u_i$’s early reports may not always accurately reflect its true intention. We introduced the forgetting factor $\lambda$ to give less weight to old feedback than recent feedback.

Then $r_{ui,k}$ and $s_{ui,k}$ can be updated as

$$r_{ui,k} = \sum_{t=1}^{k} \rho_{ui} (t) \lambda^{k-t},$$

$$s_{ui,k} = \sum_{t=1}^{k} (1 - \rho_{ui} (t)) \lambda^{k-t}.$$  

According to (6) and (27)–(31), the probability of detection $Q_d$ and false alarm $Q_f$ for CSS system based on proposed scheme over $K$ sensing period can be calculated [17]:

$$Q_d = \frac{\sum_{k=1}^{K} Q_d (k) \delta_{H_k} (k)}{\sum_{k=1}^{K} \delta_{H_k} (k)},$$

$$Q_f = \frac{\sum_{k=1}^{K} Q_f (k) \delta_{H_k} (k)}{\sum_{k=1}^{K} \delta_{H_k} (k)}.$$  

$\delta_{H_k} (k) = 1$ denote the PU is active at $k$th sensing, and $\delta_{H_k} (k) = 1$ denote the PU is inactive at $k$th sensing.

## 4. Performance Evaluations and Discussions

In this section, we will evaluate our CSS scheme by comparing it with LRMI [17]. We first describe the simulation setup and then we will set up a simulation for two types of attacks and statistically compare the performance between our proposed scheme and LRMI.

### 4.1 Simulation Setup

In the simulations, the cognitive radio (CR) network is located within a 1000 m $\times$ 1000 m square area and the area is divided into $L = 9$ cells of equal size. $N = 20$ SUs moves according to the random waypoint mobility model [35]. Each SU moves with average velocity $V$ and a maximum idle time of 30 s. Honest and malicious SUs have different mobility pattern, that is, the average velocity of honest and
malicious SUs are $V$ and $V'$, respectively. And the number of activity cells for honest and malicious SUs are $AC$ and $AC'$, respectively. The path-loss exponent for each cell is randomly selected from 3 to 6. In the log-normal shadowing model, the standard deviation for each cell is randomly selected from 2 to 20 dB. The PU is located 1000 m away from the center of the area. The probability of presence and absence PU signal are both 0.5. The PU transmit power is 200 mW. For the local spectrum sensing, the bandwidth-time product is $TW = 5$ [36]. The local sensing time is 1 ms. The SU sense every 1 s, and in the simulation we take the sensing time, is $K = 120$ s. The SUs send their sensing result and their location coordinates to the FC during each sensing period. The noise power is $-110$ dBm. Among the $N = 20$ SUs, there are $M = 2, 4, 6, 8$ SSDF attackers. In the simulation, we assume attackers launch vandalism attack with the attack probability $P_a = 0.8$, and the attack threshold $\delta$, and the attack strength is $-109$ dBm and $\Delta \sim N(-10$ dBm, $-5$ dBm), respectively. The threshold used in LRC test is 0.5, and the forgetting factor in RDF is 0.9.

4.2. Comparison of Detection Performance. Without attackers, SU’s mobility increases spatiotemporal diversity in received primary signal strengths and thus improves the sensing performance [37]. If the malicious SUs are in the minority and the mobility models are the same for all SUs, as the average velocity of SU is increased, the performance of CSS improves [17]. To evaluate the influence of different mobility pattern of honest and malicious SUs on the performance of PU detection, we first study the performance of LDMI [17] and the proposed LRC-RDF with different average velocity of honest and malicious SU.

Impact of Mobility. Figure 3 shows that there is litter difference between the performance of LDMI and LRC-RDF for PU detection when honest and malicious SUs have the same average velocity. When the average velocity of malicious SU is different from the average velocity of honest SU, LRC-RDF performs better than LDMI. When the average velocity of malicious SU is slower than the average velocity of honest SU, the performance of PU detection is lower than that when the average velocity of malicious SU is faster than the average velocity of honest SU. Thus the velocity of malicious SU can affect the performance of PU detection.

Figure 4 shows the performance of PU detection when there are $M = 4$ malicious attackers, and the number of malicious attackers’ activity cells is smaller than the number of honest SUs’ activity cells. And we consider a worse case when the 4 malicious attackers selected same activity cells. We find that LRC-RDF outperforms LDMI on the performance of PU detection when the number of malicious attackers’ activity cells is smaller than the number of honest SUs’ activity cells. For example, when malicious attackers are moving around in the same 6 cells, the improvement of the detection rates by 10% at the false alarm rate of 10%. The smaller the number of malicious attackers’ activity cells, the greater the impact on the performance for PU detection. When all of malicious attackers stay in a cell, the performance of PU detection will be severely damaged.

Impact of SU. We study the performance of LRC-RDF for PU detection in mobile CRNs when the honest SUs and attackers have the same mobility pattern. Figure 5 shows when the
honest SUs and attackers have the same mobility pattern, as the average velocity of SUs increases and, keeping the number of attackers constant, the system performance improves. Keep the average velocity of SUs constant, as the number of attackers increases, the system performance decreases. Thus when honest SUs and attackers have similar models and mobility patterns, increasing in SUs’ average velocity helps to improve the system performance.

Impact of Number of Sensing. The probability of detection verse sensing time $K$ under malicious attacks is plotted in Figure 6, parameterized by the number of attackers. It is shown that as the sensing time increases, the performance of PU detection using LRC-RDF increases. When sensing time reaches up to some degree, increasing the sensing time will no longer help to increase the performance of PU detection.

The Performance of RDF. The SUs’ reputation weights are shown in Figure 7, in the presence of one attacker. The attacker launches vandalism attack during 1200–1500 sensing rounds, and in other sensing rounds it does not launch attack. From Figure 7, we observe that the average weights for honest SUs almost maintain a relatively high level while the attacker has been assigned a low weight. The proposed RDF scheme can effectively identify attackers and mitigate attackers’ impact on the final decision.

5. Conclusions

The design of a secure CSS scheme is a challenge task in mobile CRNs. In this paper, we have studied the performance of CSS when the areas of the CRNs have different path-loss and fading parameters. Our proposed secure CSS scheme requires no prior knowledge of the attackers’ or honest SUs’ mobility pattern, which is more practical in considering the dynamic attacking behaviors. The LRC test is proposed to filter out the SUs’ abnormal sensing reports according to their spatial locations. To mitigate the adverse effects caused by SUs mobility pattern, a fusion scheme based on SU’s reputation value is proposed, which can efficiently mitigate attackers’ negative impact on the final decision while utilizing the benefits it can bring. The mobility pattern found can be exploited by malicious SUs to increase the damage to the CSS. The simulation results have shown the robustness of the
proposed LRC-RDF scheme against malicious SU attack in mobile CRNs.

Appendix

The expect value and variance of Geary’s C are given in [38],

\[
E(C) = 1
\]

\[
\text{Var}(C) = \frac{1}{n(n-1)(n-3)} S_0^2 
\]

\[
\times \left\{ S_0^2 \left[ (n^2 - 3) - b(n-1)^2 \right] + S_1 (n-1) \left[ n^2 - 3n + 3 - b(n-1) \right] + \frac{1}{4} S_2 (n-1) \left[ b \left( n^2 - n + 2 \right) - \left( n^2 + 3n - 6 \right) \right] \right\},
\]

\[
S_0 = \sum_{i=1}^{n} \sum_{j=1}^{n} W_{i,j}, \quad S_1 = 2S_0, \quad S_2 = \sum_{i} \left( W_{i,0} + W_{0,i} \right)^2,
\]

\[
W_{i,0} = \sum_{j} W_{i,j}, \quad W_{0,j} = \sum_{j} W_{j,i},
\]

\[
b = \frac{n \sum (z_i(k) - \bar{z})^4}{\left( \sum (z_i(k) - \bar{z})^2 \right)^2}.
\]

(1)

where \(n\) is the number of reports received from the cell and \(\bar{z}\) is the mean of \(z_i(k)\), that is, \(\bar{z} = (1/n) \sum_{i=1}^{n} z_i(k)\).

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The authors would like to thank the National High-Tech Research & Development Program of China (863 Program) under Grant 2012AA01A508 for the project support.

References

[1] X. Chen, H. Chen, and W. Meng, "Cooperative communications for cognitive radio networks—from theory to applications,” IEEE Communications Surveys & Tutorials, 2014.

[2] B. Zhao and S. Sasaki, “Spectrum sensing for cognitive coexistent heterogeneous networks,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID 141480, 9 pages, 2013.

[3] Y. Wang, Y. Li, J. Yang, P. Wan, and Q. Wang, "An improved optimal linear weighted cooperative spectrum sensing algorithm for cognitive radio sensor networks," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 951205, 9 pages, 2013.

[4] D. Xue, E. Ekici, and M. C. Vuran, “Cooperative spectrum sensing in cognitive radio networks using multidimensional correlations,” IEEE Transactions on Wireless Communications, vol. 13, pp. 1832–1843, 2014.

[5] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, “Cognitive radio network security: a survey,” Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1691–1708, 2012.

[6] W. Mingchen, L. Bin, and Z. Chi, "Detection of collaborative SSDF attacks using abnormality detection algorithm in cognitive radio networks," in Proceedings of the IEEE International Conference on Communications Workshops (ICC '13), pp. 342–346, 2013.

[7] R. Chen, J.-M. J. Park, and K. Bian, "Robustness against Byzantine failures in distributed spectrum sensing," Computer Communications, vol. 35, no. 17, pp. 2115–2124, 2012.

[8] W. Jinlong, Y. Junnan, and W. Qihui, "Stealthy-attacker detection with a multidimensional feature vector for collaborative spectrum sensing," IEEE Transactions on Vehicular Technology, vol. 62, pp. 3996–4009, 2013.

[9] X. He, H. Dai, and P. Ning, "A byzantine attack defender in cognitive radio networks: the conditional frequency check," IEEE Transactions on Wireless Communications, vol. 12, no. 5, pp. 2512–2523, 2013.

[10] L. Duan, A. W. Min, J. Huang, and K. G. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 30, no. 9, pp. 1658–1665, 2012.

[11] F. Zhu and S.-W. Seo, "Enhanced robust cooperative spectrum sensing in cognitive radio," Journal of Communications and Networks, vol. 11, no. 2, pp. 122–133, 2009.

[12] W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: detect malicious nodes in cooperative spectrum sensing," in Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '09), M. Ulema, Ed., vol. 1-8, pp. 5071–5076, New York, NY, USA, December 2009.

[13] N. T. Nhan and I. Koo, “A secure distributed spectrum sensing scheme in cognitive radio,” in Proceedings of the Emerging Intelligent Computing Technology and Applications: With Aspects of Artificial Intelligence, Berlin, Germany, 2009.

[14] S. Shrivastava, A. Rajesh, and P. K. Bora, "Sliding window Dixon’s tests for malicious users’ suppression in a cooperative spectrum sensing system,” IET Communications, vol. 8, pp. 1065–1071, 2014.

[15] O. Fatemieh, R. Chandra, and C. A. Gunter, “Secure collaborative sensing for crowdsourcing spectrum data in white space networks,” in Proceedings of the IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN ‘10), pp. 1–12, April 2010.

[16] A. W. Min, K. G. Shin, and X. Hu, "Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation," IEEE Transactions on Mobile Computing, vol. 10, no. 10, pp. 1434–1447, 2011.

[17] S. Jana, K. Zeng, W. Cheng, and P. Mohapatra, “Trusted collaborative spectrum sensing for mobile cognitive radio networks,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 9, pp. 1497–1507, 2013.

[18] S. Yadav and M. J. Nene, “RSS based detection and expulsion of malicious users from cooperative sensing in Cognitive Radios,” in Proceedings of the 3rd IEEE International Advance Computing Conference (IACC ‘13), pp. 181–184, February 2013.
[19] A. Getis and J. K. Ord, "The analysis of spatial association by use of distance statistics," Geographical Analysis, vol. 24, pp. 189–206, 1992.

[20] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," IEEE Transactions on Wireless Communications, vol. 7, no. 4, pp. 1326–1337, 2008.

[21] R. Tandra and A. Sahai, "SNR walls for signal detection," IEEE Journal on Selected Topics in Signal Processing, vol. 2, no. 1, pp. 4–17, 2008.

[22] A. Sonnenschein and P. M. Fishman, "Radiometric detection of spread-spectrum signals in noise of uncertain power," IEEE Transactions on Aerospace and Electronic Systems, vol. 28, pp. 654–660, 1992.

[23] Y. Zhang, Y. Zhu, M. Lu, and A. Chen, "Using compressive sensing to reduce fingerprint collection for indoor localization," in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’13), pp. 4540–4545, Shanghai, China, April 2013.

[24] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in Proceedings of the 38th Asilomar Conference on Signals, Systems and Computers, M. B. Matthews, Ed., vol. 1-2, pp. 772–776, November 2004.

[25] A. Goldsmith, Wireless Communications, Cambridge University, 2005.

[26] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in Proceedings of the 43rd Annual Conference on Information Sciences and Systems (CISS ’09), pp. 130–134, IEEE, New York, NY, USA, March 2009.

[27] A. Chen, S. Kumar, and T. H. Lai, "Local barrier coverage in wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 9, no. 4, pp. 491–504, 2010.

[28] A. W. Min, K. G. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in Proceedings of the 17th IEEE International Conference on Network Protocols (ICNP ’09), pp. 294–303, New York, NY, USA, October 2009.

[29] G. Caso, L. D. Nardis, O. Holland, and M. G. D. Benedetto, "Impact of spatio-temporal correlation in cooperative spectrum sensing for mobile cognitive radio networks," in Proceedings of the 10th International Symposium on Wireless Communication Systems (ISWCS ’13), pp. 1–5, 2013.

[30] K. Sentz and S. Ferson, Combination of Evidence in Dempster-Shafer Theory, vol. 4015, Citeseer, 2002.

[31] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, Princeton, NJ, USA, 1976.

[32] B. M. Jedynak and S. Khudanpur, "Maximum likelihood set for estimating a probability mass function," Neural Computation, vol. 17, no. 7, pp. 1508–1530, 2005.

[33] P. Rousseuw and A. Leroy, Robust Regression and Outlier Detection, John Wiley & Sons, New York, NY, USA, 1987.

[34] A. Whitby, A. Jøsang, and J. Indulska, "Filtering out unfair ratings in bayesian reputation systems," in Proceedings of the 7th International Workshop on Trust in Agent Societies, 2004.

[35] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," IEEE Transactions on Mobile Computing, vol. 2, no. 3, pp. 257–269, 2003.

[36] A. Ghasemi and E. S. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," Journal of Communications, vol. 2, no. 2, pp. 71–82, 2007.
