Trusted Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks

Shraboni Jana[+], Kai Zeng[*] and Prasant Mohapatra[+]
[+]University of California, Davis, CA 95616
[*]University of Michigan, Dearborn, MI 48128
sjana@ucdavis.edu, kzeng@umich.edu, pmohapatra@ucdavis.edu

***Abstract*—Collaborative spectrum sensing is a key technology in cognitive radio networks (CRNs). It is inaccurate if spectrum sensing nodes are malicious. Although mobility is an inherent property of wireless networks, there has been no prior work studying the detection of malicious users for collaborative spectrum sensing in mobile CRNs. Existing solutions based on user trust for secure collaborative spectrum sensing cannot be applied to mobile scenarios, since they do not consider the location diversity of the network, thus over penalize honest users who are at locations with severe pathloss. In this paper, we propose to use two trust parameters, Location Reliability and Malicious Intention (LRMI), to improve malicious and primary user detection in mobile CRNs under attacks. Location Reliability reflects pathloss characteristics of the wireless channel and Malicious Intention captures the true intention of secondary users, respectively. Simulations of our proposed detection mechanisms, LRMI, show that mobility helps train location reliability and detect malicious users. We show an improvement of malicious user detection rate by 3 times and primary user detection rate by 20% at false alarm rate of 5%, respectively.**

I. Introduction

With the ever-increasing wireless applications and traffic demand, spectrum shortage becomes a more severe and urgent problem. Cognitive radio technology [1] is considered as a promising solution to improve the spectrum utilization and alleviate the spectrum shortage. The basic idea of CRNs is that when the primary (licensed) users are absent, the secondary (unlicensed) cognitive users can opportunistically access the primary users' spectrum, but have to evacuate when the primary users emerge. Collaborative spectrum sensing is widely used for accommodating this dynamic and opportunistic spectrum access in CRNs [2]. In collaborative spectrum sensing, multiple secondary users sense the spectrum in a periodical or on-demand manner, and report their sensing results to a fusion center, which processes the reports and decides the presence or absence of a primary user. This collaborative spectrum sensing paradigm opens a hole to the attackers who can falsify the sensing results.

Existing solutions for detecting the sensing falsification attacks have focused on identifying the attackers as abnormal within a small area or for static secondary users [3], [4], [5], [6], [7]. Basically, when a user's report deviates from common readings beyond a certain threshold, its trust value is degraded. A dishonest attacker can thus be identified, and its negative impact on the spectrum sensing can be weakened or eliminated. However, these solutions have two major limitations. First, they assume the whole area has the same channel propagation characteristics, which is not practical. It has been found that the path-loss are different at different sensing regions [8]. Second, they assume the users are static and cannot be directly applied to mobile scenarios. To the best of our knowledge, no prior work has studied the impact of mobility on the collaborative spectrum sensing under attacks or provided applicable solutions.

In this paper, we propose to use two trust parameters, Location Reliability and Malicious Intention (LRMI), to improve malicious and hence primary user detection in mobile CRNs under attacks. Location Reliability (LR) reflects pathloss characteristics of the wireless channel and Malicious Intention (MI) captures the true intention of secondary users, respectively. We conduct extensive simulations to evaluate our proposed mechanisms and compare their performance with existing solutions. Our proposed detection mechanisms based on LRMI significantly outperforms existing solutions in terms of improving the malicious user detection rate by 3 times and primary user detection rate by 20% at false alarm rate of 5%, respectively. We find that with increase in number of users, mobility and system observation time, performance of our proposed scheme improves.

The paper is organized as follows. Section II discusses the related work. The system model is introduced in Section III followed by the problem formulation and our proposed solutions in Section IV. We evaluate our solutions and conclude this paper in Section V and Section VI, respectively.

II. Related Work

The performance gains, achieved by collaborative spectrum sensing in CRN is well established in literature. The centralized collaborative spectrum sensing has been included in the IEEE 802.22 standard draft [9]. The authors in [10], study impact of mobility on collaborative spectrum sensing. The authors show that because of mobility, the secondary user sensing results get uncorrelated faster thus giving better performance compared to spectrum sensing performed by static secondary users but does not consider the presence of malicious users.

To identify the malicious users in the CRN, the evaluation of trust for each secondary user under collaborative spectrum sensing has been addressed using different techniques in the literature. In the solution proposed by authors in [5], secondary users in close proximity are grouped into clusters and the system detects abnormal reports using shadow-fading correlation filters. The authors in [4] evaluates the secondary users trust, comparing deviation suffered by each secondary user's sensing measurement from the average measurement reported at the fusion center.

The Bayesian rule is applied in [6] to compute the a posteriori probability of being an attacker for each secondary user. When the posteriori probability of a certain secondary user exceeds the suspicious level threshold, it is claimed to be an attacker and is removed from the collaboration. For multiple attackers, the large number of combinations of attackers and honest users is removed by using an onion-peeling based approximation to reduce computational complexity. Abnormality detection algorithm based on proximity, which is widely used in the field of data mining has been introduced in [3], to solve the problem of malicious users in the system using history reports of each secondary user. The proposed architecture in [7], needs to collect spectrum sensing data from multiple sources or equipment on consumer premises. This process is known as crowdsourcing. The authors consider the area of interest is divided in cells and the credibility of these devices are kept in check by corroboration and merging among neighboring cells. The corroboration in a hierarchical structure is used to identify cells with significant number of malicious nodes.

To the best of our knowledge, none of the existing work studied malicious and primary user detection for mobile CRNs. Our proposed solutions are different from all the existing solutions that we separate the location reliability from the user trust, thus achieve better performance on malicious user detection.

III. System Model

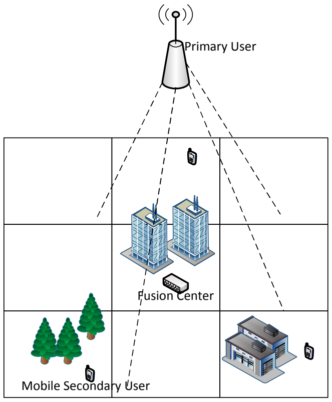

Fig. 1. System Model

We divide the area of interest into a grid (Figure 1) and each cell in a grid is assumed to experience path-loss exponent and shadowing characteristic of that cell. The assumption is reasonable since some areas will have deep fade caused by buildings, trees etc. compared to others. We use the term location and cell interchangeably in the rest of the document for cell in the grid. Our approach supports any number of cells with any shape and size depending on the required granularity. The primary user detection is modeled as a hypothesis test. At decision slot k, the null hypothesis H_0 indicates the primary user is idle, while the alternative hypothesis H_1 indicates the primary user is active. We further assume that the time the system is in either of the states H_0 and H_1 follow exponential distributions as commonly used in the literature, and that durations of successive active and inactive periods are independent of each other.

Let $U = \{u_1, u_2, ..., u_i, ..., u_N\}$ be set of N users in the system. Let $C = \{c_1, c_2, ..., c_j, ..., c_L\}$ be the set of cell identification numbers of L cells in the grid. If the bandwidth of the primary user signal is W, at each sensing slot, each user takes $2TW$ samples with the sample interval of T. Assuming the noise and primary signal to be uncorrelated, the distribution of the energy detector output for the k^{th} sensing slot for user u_i at location c_j [2] is,

$$Y^j_{i,k} \sim \begin{cases} \chi^2_{2TW} & H_0 \\ \chi^2_{2TW}(2\gamma^j_{i,k}) & H_1 \end{cases} \tag{1}$$

where $\gamma^j_{i,k} = \frac{|h^j_{i,k}|^2 P_t}{N_0 W} = \frac{Pr^j_{i,k}}{N_0 W}$ is referred as instantaneous signal-to-noise ratio experienced by a secondary user for transmit power P_t and channel gain $h^j_{i,k}$ at cell c_j. χ^2_{2TW} and $\chi^2_{2TW}(2\gamma^j_{i,k})$ denote central and non-central chi-square distributions with $2TW$ degrees of freedom, respectively.

Assuming channel bandwidth is much larger than the coherent bandwidth, effect of multi-path fading is negligible. The received primary user power at secondary user at a distance $d_{i,k}$ from primary user can be expressed as [11] in dB:

$$Pr^j_{i,k}(dB) = P_t(dB) - \{PL_0 + 10\alpha_j log_{10}(\frac{d_{i,k}}{d_0}) + \psi_j\} \tag{2}$$

where PL_0 is a path-loss at a reference distance d_0 in dB and is close to $20log10(\frac{4\pi d_0}{\lambda})$, where λ is wavelength. Path-loss exponent α_j ranges from 2 to 5 [8]. Empirical measurements support the log-normal distribution for ψ_j in dB.

The raw sensed signal power values are sent from secondary users to the fusion center, known as soft-combining whereas in hard-combining techniques a 0/1 decision from each secondary user is considered. We consider soft-combining in this paper because its performance is much better than hard-combining with only a slightly higher communication overhead [2]. At each sensing slot k, each user reports $Y^j_{i,k}$ along with their current cell c_j to the fusion center. In collaborative spectrum sensing, the fusion center will make a decision at each sensing slot whether primary user is active or not based on the reports received from the secondary users in the system.

The efficiency of such collaboration is reduced by the presence of malicious users. Each malicious user thwarts the system performance by-

- Reporting an increased observation $(Y^j_{i,k} + \Delta)$ when the primary user is inactive, thus increasing the false-alarm rate.
- Reporting a decreased observation $(Y^j_{i,k} - \Delta)$ when the primary user is active, thus increasing the missed-detection rate.
- Reporting incorrect cell number c_j.

We assume that each malicious user acts independently at each sensing slot. If the reliability of a user assigned by fusion center drops below a certain threshold (ξ), the user is considered malicious. Faulty nodes are not a part of the system. The number of malicious secondary users are always less than the number of honest users in the system.

IV. Malicious User(s) and Primary User Detection

We, propose to evaluate the reports at the fusion center based on two sources of evidence associated with each report - cell from which the report is generated (Location Reliability) and who has generated the report (Malicious Intention).

Location Reliability (LR)

Algorithm 1 Location Reliability (LR)

```
Initialize $K$
$S(c_j) = \{\phi\}, E(c_j) = 0 \forall c_j$ and $\beta_0(c_j) = \frac{1}{L} \forall c_j$
$tot_{rep}(c_j) = 0 \forall j$
For each $k$
for $c_j = 1 \rightarrow L$ do
    if $\mathcal{R}$ has $c_j$ then
        r = number of reports from cell $c_j$.
        $tot_{rep}(c_j) = tot_{rep}(c_j) + r$
        $S(c_j) = S(c_j) \bigcup \{Y^j_{i,k}\}$
        $E(c_j) = \frac{\sum S(c_j)}{tot_{rep}(c_j)}$
    end if
end for
$\beta_k(c_j) = \frac{E(c_j)}{\sum_j E(c_j)}$
```

Using Algorithm 1, the fusion center, evaluates the trust of each cell. At the beginning of the algorithm, all cells are given same trust values. We group the current reports, $\mathcal{R}$ with past reports based on the cell location informed by the secondary users. tot_{rep} represents number of reports received from the cell. At end of each sensing slot, we evaluate $\beta_k(c_j)$, the average sensing measurements reported from each cell, equivalent to the trust of a cell.

The malicious secondary users being mobile, their impact is distributed across the cells and is not concentrated in a particular cell(s). This user-diversity in a cell helps in convergence of $\beta_k(c_j)$ for cell c_j. Higher the user mobility, faster is the convergence of LR for the same system settings.

Malicious Intention (MI)

The true intention of a secondary user cannot be captured entirely by their respective sensing reports as honest users can be in bad locations experiencing deep path-loss and malicious users can be in good locations and vice versa. We use Dempster-Shafer (D-S) theory [12] to evaluate trustworthiness in collaborative spectrum sensing in mobile CRNs. In dynamic mobile CRNs, the D-S theory is well suited for two reasons - 1) it reflects uncertainty and the D-S theory rule of combination, 2) combines evidences from two or more sources to form inferences. The frame of discernment $\Theta_{u_i} = \{T, -T\}$ denotes a set of mutually exclusive and exhaustive hypotheses about the problem domain - if user u_i is trustworthy or malicious. The power set $2^{\Theta_{u_i}}$ is $\{\phi, T, -T, \{T, -T\}\}$. The Belief Mass Assignment (bma) for user u_i, represented by m_{u_i}, defines a mapping of the power set to the interval between 0 and 1. For each k,

$$m_{u_i} : 2^{\Theta_{u_i}} \rightarrow [0\ 1], m_{u_i}(\phi) = 0, \sum_{A_k \in 2^{\Theta_{u_i}}} m_{u_i}(A_k) = 1 \tag{3}$$

The bma function for k^{th} sensing, based on eqn. 3 and assuming the user trust to be exponential [13] -

$$m_{u_i}(A_k = T) = e^{-|D|} \tag{4}$$

$$m_{u_i}(A_k = -T) = 0 \tag{5}$$

$$m_{u_i}(A_k = \{T, -T\}) = 1 - m_{u_i}(A_k = T) \tag{6}$$

D, is the deviation in the user report. As the deviation D decreases, our belief in u_i increases and vice versa. The uncertainty due to the noise level experienced by the user is incorporated into $m_{u_i}(A_k = \{T, -T\})$. The deviation incurred by user u_i for any location c_j

$$D = (1 - \beta_k(c_j))\zeta_k(u_i), \zeta_k(u_i) = \frac{Y^j_{i,k} - avg\{Y^j_{i,k}\}^N_{i=1}}{std\{Y^j_{i,k}\}^N_{i=1}} \tag{7}$$

avg stands for average and std stands for standard deviation. Some users are more vulnerable to misreading due to their instantaneous location. The deviation in evidence received from a user in a cell is discounted based on location reliability $\beta_k(c_j)$ in eq. 7. For combination of subsequent bma evaluated at each step k, the D-S rule of combination gives [12] -

$$m_{u_i}(\{A = T\}) = \frac{\sum_{\bigcap A_r = A} \prod_{r=1}^{k} m_{u_i}(A_r)}{1 - \sum_{\bigcap A_r \neq A} \prod_{r=1}^{k} m_{u_i}(A_r)} \tag{8}$$

The confidence level of T for u_i is $T_k(u_i) = m_{u_i}(\{A = T\})$. For each k, we evaluate LRMI - $\beta_k(c_j)$ based on Algorithm 1 and eqn. 4 - 8 to capture malicious intention of the secondary users. We compare our solution LRMI, with the solution proposed in [4] (equation $7 - 12$ of [4]). We address the approach in [4] as Malicious Detection (MD) in our paper.

Secondary Users Reports Combining

The existing method used for soft combining is Equal Gain Combining (EGC) [2], which gives equal emphasis to all the individual measurements. For N users in collaborative spectrum sensing, with EGC rule at the fusion center

$$Y_k^{EGC} = \sum_{i=1}^{N} Y^j_{i,k}.w(j), w(j) = 1 \forall j. \tag{9}$$

For $Y_k^{EGC} > \eta$, the primary user status is H_1 otherwise H_0 for primary user detection threshold η. For users with trust values greater then ξ and applying the weight of each cell,

$$Y_k^{LRMI} = \sum_{i=1}^{N} Y^j_{i,k}.w(j), w(j) = \frac{\beta_k(c_j)}{\sum_j \beta_k(c_j)}, T_k(u_i) > \xi. \tag{10}$$

We need to normalize the location weights at each sensing slot as there may not be any report originated from a cell(s). There is no closed form solution for probability of primary user detection for log-normal fading [2] and therefore, we evaluate the system numerically. We analyze the performance of these solutions in terms of Receiver Operating Characteristics (ROC) for both malicious users detection and primary user detection. ROC is the plot of probability of detection vs. probability of false alarm rate.

V. Performance Evaluation

A. Simulation Settings

We consider the region of interest to be 1000 m away from primary user. The region is 1000 m x 1000 m and is divided into grid with L cells of equal area. We take average velocity $V = 20m/s$, cells $L = 9$ and system observation time $K = 120s$ for all simulation results unless otherwise mentioned. The secondary users send their location along with the sensing report during each sensing slot. The noise power is $-110dBm$ and primary user transmit power is $200mW$. The sensing duration of all secondary users is $1ms$ [9] and the users sense after every $1s$. We choose users to sense after every $1s$, as FCC requires secondary users to evacuate the spectrum in $2s$ when primary user becomes active. The time-bandwidth product for our simulation is 5. The path-loss exponent is selected randomly from 3 to 6 for each cell and shadowing between 2 to 20 dB. For simulation purpose, we assume the attack strength is $\Delta \sim \mathcal{N}(-10dBm, -5dBm)$ which fusion center is oblivious of. M is used to denote the number of malicious users in the system. We evaluate the system numerically. The malicious users detection threshold, ξ is taken from 0 to 1 with step-size 0.05 to evaluate ROC for malicious user(s) detection. $p_B = 0.5$ and $p_I = 0.5$ is the probability that primary user is busy and idle respectively.

Since the sensing duration ($\sim$ 1ms - 10ms) is so small, we assume the users locations remain unchanged during each sensing. We consider Smooth Random Mobility Model [14], which considers the two stochastic processes, speed and direction to have their values correlated to the previous one in order to avoid unrealistic patterns. We assume the users never pause. The acceleration of all secondary users are $\pm 4m/s^2$. The speed changes on an average after 25 seconds.

B. Simulation Results

a) Impact of secondary users: We vary number of secondary users in collaborative spectrum sensing. From Figure 2, it is obvious that as the total number of secondary users increases ($N = 5, 10, 20$) keeping percentage of malicious users constant (20% malicious nodes), the system performance improves. For $N = 10$, with decrease in number of malicious nodes in the system ($M = 4, M = 3, M = 2$), LRMI performance improves. MD gives a very high false alarm rate. It ignores the information that honest users can be at poor locations at times due to their mobility.

b) Impact of mobility: Due to mobility, the number of cell changes per unit time for mobile users increases with the speed for a fixed cell-area and cell-size [15], increasing user-diversity in a cell. To see the effect of user diversity in a cell with respect to ROC, we evaluate the performance of LRMI with malicious and non-malicious data for calculating LR in Figure 3. Note for MI, the data contains reports from malicious users. LR-H is for evaluation of LR with honest users in the system and LR-M is for the evaluation of LR with malicious data in the system. We find that the performance in both LR-H and LR-M cases differ only when the number of malicious nodes in the system is as high as 40%.

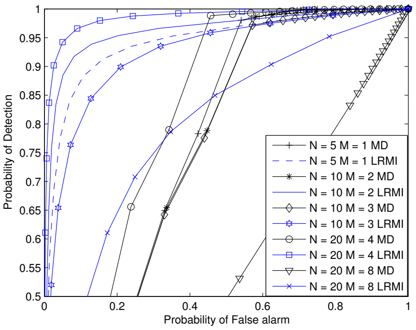

Fig. 2. Impact of secondary users - ROC for malicious user detection at $V = 20m/s$

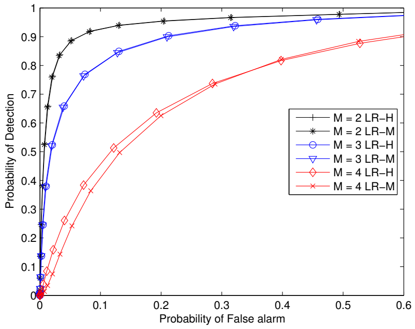

Fig. 3. Comparison of ROC curves for malicious user detection with LR evaluated both with honest data (LR-H) and malicious data (LR-M) for $N = 10$.

We study the performance of LRMI with different average velocity of secondary users. Figure 4 evaluates system performance for $V = 0m/s, V = 20m/s$ and $V = 40m/s$. As the average velocity of users is increased, performance of LRMI improves. MD performs better than LRMI at $V = 0m/s$ but for mobile secondary users, LRMI outperforms MD (Fig.4). Performance of LRMI further increases when the average speed of the mobile users is increased from $20m/s$ to $40m/s$. Thus mobility aids in malicious user detection.

c) Impact of number of sensings: We find that for a fixed setting of N, L, M and V, as the K is increased, the performance of malicious detection using LRMI increases. As expected, the performance ceases to exist after certain K. For $N = 10, M = 2, V = 20m/s, L = 9$, $K = 180sec$ performs better than $K = 120sec$ and $K = 60sec$. For the same settings with $M = 3$, with $K = 120sec$ and $K = 180sec$, there is almost no performance gain. Intuitively, as we take more sensings, the convergence of $\beta_k(c_j)\ \forall j$ converges to the actual weight of each cell but makes no difference after certain number of sensings. Figure 5 validates our argument.

d) Impact on primary user detection: We evaluate complementary ROC for primary user detection for LRMI and

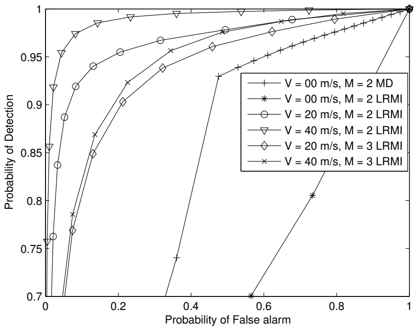

Fig. 4. Impact of velocity - ROC for malicious user detection with secondary users $N = 10$.

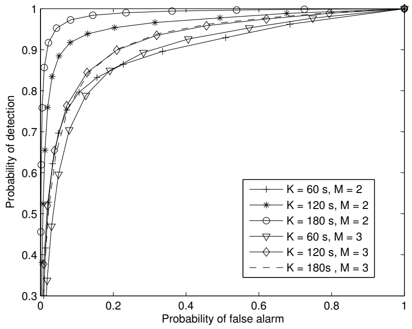

Fig. 5. Impact of LR sensings - ROC for malicious user detection. N = 10, L = 9, V = 20 m/s

MD approach with different number of malicious users in the system. We take $\eta = -120 : 0.5 : -20$ all in dBm and ξ = 0.5 for primary user ROC. The Figure 6 shows LRMI performs better than MD with 10% and 20% malicious nodes in the system. In Figure 7, keeping the percentage of malicious nodes constant in the system, we decrease the number of secondary users in the system. We observe, that MD performs poorly with respect to LRMI in such cases.

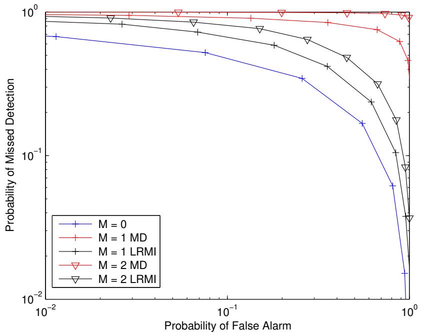

Fig. 6. Complementary ROC for primary user detection with $N = 10, V = 20m/s$.

VI. Conclusions & Future Work

We studied the performance of spectrum sensing under different path-loss and fading conditions and came up with a solution fitting for collaborative spectrum sensing in mobile CRNs with malicious user(s). The numerically simulated results showed that our approach (LRMI) greatly improves malicious and primary user detection in mobile CRNs. Mobility is also found to be an aiding factor in malicious users detection. The simulation results show that as the average velocity of the secondary users in the system increases, the ROC curves for the system improves. An interesting extension of the work will be to evaluate how malicious users can exploit mobility to their advantage and avoid getting detected.

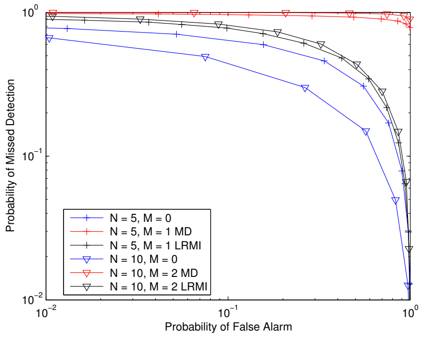

Fig. 7. Complementary ROC for primary user detection with 20% malicious nodes and $V = 40m/s$.

References

[1] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, pp. 2127–2159, Sep. 2006.

[2] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *IEEE DySPAN 2005*, Nov. 2005.

[3] H. Li and Z. Han, "Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: An abnormility detection approach," in *Proc. IEEE DySPAN*, Apr. 2010.

[4] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proc. ICC*, Sep. 2008.

[5] A. W. Min, K. G. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *Proc. ICNP*, Oct. 2009.

[6] W. Wang, H. Li, Y. Sun, and Z. Han, "Catch it: Detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE Globecom*, Apr. 2009.

[7] O. Fatemieh, R. Chandra, and C. A. Gunter, "Secure collaborative sensing for crowdsourcing spectrum data in white space networks," in *Proc. IEEE DySPAN*, Apr. 2010.

[8] S. M. Mishra, R. Tandra, and A. Sahai, "Coexistence with primary users of different scales," in *Proc. IEEE DySPAN*, Apr. 2007.

[9] www.ieee802.org/22. [Online]. Available: IEEE 802.22 WRAN WG on Broadband Wireless Access Standards.

[10] A. W. Min and K. G. Shin, "Impact of mobility on spectrum sensing in cognitive radio networks," in *Proc. of the 2009 ACM workshop on Cognitive radio networks*, 2009.

[11] A. Goldsmith, *Wireless Communication*. Cambridge University Press, 2006.

[12] K. Sentz, "Combination of evidence in dempster-shafer theory, ph.d." in *Systems Science and Industrial Engineering Department, Binghamton University*, Jan. 2002.

[13] T. Denoeux, "A k-nearest neighbor classification rule based on dempster-shafer theory," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 25, no. 5, pp. 804–813, May 1995.

[14] C. Bettstetter, "Smooth is better than sharp: A random mobility model for simulation of wireless networks," in *Proc. of the 4th ACM International Workshop on Modeling, Analysis, and Simulation of Wireless and Mobile Systems*, Jul. 2001.

[15] C. Bettsetetter, H. Hartenstein, and X. Perez-Costa, "Stochastic properties of the random waypoint mobility model," *Wireless Networks*, vol. 10, pp. 555–567, Sep. 2004.