This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

Believe Yourself: A User-centric Misbehavior Detection Scheme for Secure Collaborative Spectrum Sensing

Shuai Li, Haojin Zhu, Bo Yang, Cailian Chen, Xinping Guan
Shanghai Jiao Tong University, Shanghai, China
{shuailee, zhu-hj, bo.yang, cailianchen, xpguan}@sjtu.edu.cn

***Abstract*—Collaborative spectrum sensing has been proposed recently to facilitate precise detection of primary users in Cognitive Radio networks. However, it simultaneously introduces new security issue that the selfish or even misbehaving users could cheat a secondary user by depriving its access opportunity. To address this problem, we propose a novel User-centric Misbehavior Detection Scheme (UMDS) in this paper to detect malicious behaviors in collaborative spectrum sensing. The basic idea of UMDS is motivated by the fact that a mobile user tends to trust the sensing report generated by itself rather than the reports from other users. Therefore, a secondary user could independently determine if a sensing partner is malicious or not by calculating the correlation between the secondary user's own reports and those of secondary users. We also discuss how to further improve the performance of the UMDS by choosing an optimized threshold. The effectiveness and efficiency of the proposed scheme is demonstrated by extensive analysis and numerical results.**

Keywords – **Cognitive Radio Security, Collaborative Spectrum Sensing, Misbehavior Detection.**

I. Introduction

The ever increasing spectrum demand for emerging wireless applications has inspired the concept of Cognitive Radio (CR) [1], which is expected to improve the utilization of the precious natural resource, radio spectrum. Compared with the conventional spectrum management paradigms in which most of the spectrum is allocated to primary users for exclusive use, a CR system allows secondary users or lower-priority users to utilize the spectrum only if this spectrum is idle.

One of the major challenges in CR is how to detect available spectrum resources without introducing interference to the primary user. The performance of existing spectrum sensing schemes, (e.g., matched filter, energy detection, cyclostationary detection and wavelet detection [2]), degrades significantly when wireless channel experiences fading or shadowing. To address this issue, collaborative spectrum sensing, which combines sensing results of multiple users, is proposed as a promising approach to improve sensing performance [3]- [6].

In collaborative spectrum sensing, a secondary user is required to execute spectrum sensing to detect the Primary user's existence, then to exchange sensing reports with other proximate secondary users, and finally to judge whether primary user exists based on the collected reports. According to [3], the collaboration of secondary users could effectively improve the accuracy and reliability of spectrum sensing, and hence dramatically reduces the interference to primary user.

Most of the existing collaborative sensing schemes assume that the sensing participants are honest. This hypothesis, however, might be easily violated in the presence of selfish or even malicious secondary users, which may generate unauthenticated sensing report to cheat its neighbors with their access opportunities while maximizing its own benefits by enjoying a higher access chance. To address this issue, recently, several detection schemes have been proposed to achieve the secure collaborative sensing.

In [7], a detection scheme is developed to distinguish malicious Users from the honest ones. However, this scheme requires the prior knowledge about the channel usage habits of primary users (ON-OFF ratio), and the detection performance degrades when the ON-OFF ratio gets closer to 1. [8] proposed a reputation-based scheme, Weighted Sequential Probability Ratio Test (WSPRT). In this scheme, a Secondary user assigns a specific reputation to a neighbor user based on whether this neighbor's sensing report is consistent to the final decisions made by the majority. Such kind of voting based collaborative sensing schemes, which requires that the majority of the users are trustworthy, may not be applicable in a typical CR network which is characterized of dynamic network topology.

In this paper, we propose an User-centric Misbehavior Detection Scheme (UMDS) to thwart misbehaviors in collaborative spectrum sensing. UMDS is motivated by the old saying that *it is better to see for oneself rather than to hear for many times*. In other words, a mobile user tends to trust the sensing report generated by itself rather than the reports from other users. Therefore, in UMDS, a user chooses its own report as the trust base and evaluates other users' trust levels by comparing their sensing reports. By choosing an optimized system parameter, a user could detect the malicious users with a minimized false positive/negative rate.

Different from any existing schemes such as [7] and [8], UMDS is user-centric, ie. the secondary users are able to independently determine the credibility of the sensing reports from a specific user based on its own judgement. Therefore, UMDS is expected to achieve a higher robustness and can be implemented in the vicious environment where the number of dishonest users may exceed that of honest ones. In the meantime, UMDS needs no prior knowledge about malicious users. Further, considering that the threshold of the secondary

978-1-61284-233-2/11/$26.00 ©2011 IEEE

user executing UMDS may affect the final results of the detection, we will investigate how to derive an optimal threshold to improve the performance of UMDS.

The contribution of this paper is summarized as follows. Firstly, we develop a novel malicious user detection scheme in collaborative spectrum sensing, which has strong robustness and can be applied in challenging environment where the number of honest users may be less than that of malicious ones. In addition, this mechanism needs no prior knowledge about the environment or the malicious users.

This paper is organized as follows. System model is given in Section II. In Section III, UMDS and its optimization method would be introduced. Numerical analysis are shown in Section IV, and conclusion is drawn in Section V.

II. SYSTEM MODEL

In this section, we would briefly describe collaborative spectrum sensing which is based on energy detection as well as the attack models considered in this paper.

A. Collaborative Spectrum Sensing

The objective of collaborative spectrum sensing is to determine whether a certain primary user exists according to the fusion of cooperative secondary users' reports. In this paper, we assume that there are M primary users in a network, belonging to the set of $P = \{p_1, p_2, \cdots, p_M\}$. These primary users have the priority to use the fixed spectrum resources respectively. In the meantime, let $S = \{s_1, s_2, \cdots, s_N\}$ be the set of secondary users in this network and each of the secondary users $\{s_i, i \in N\}$ could access the spectrum when the primary user is absent. These secondary users also collaboratively detect the existence of the primary user. If one of them, say $\{s_\ell, \ell \in N\}$ detects the existence of $\{p_j, j \in M\}$, it would send report of " $p_j = 1$" to other secondary users. On the contrary, it would report "$p_j = -1$" for the non-detection of p_j's existence. We denote the report from s_ℓ as $\{R_\ell^j, \ell \in N, j \in M\}$. In the meantime, malicious users may send false reports to other secondary users in order to benefit itself, and we would use "$s_\ell = H$" and "$s_\ell = M$" to indicate s_ℓ is honest or malicious.

We also assume that a single secondary user uses energy detection method to detect the existence of primary users, and we don't consider the situation that the secondary user who is implementing UMDS stays in deep fading or shadowing. According to [9], the probability of false positive and detection in Rayleigh fading environment is as follows:

$$P_f = \Pr\{Y > \lambda | P_j = -1\} = \frac{\Gamma(m, \lambda_1/2)}{\Gamma(m)} \tag{1}$$

$$P_d = e^{-\frac{\lambda_1}{2}} \sum_{k=0}^{m-2} \frac{1}{k!} \left(\frac{\lambda_1}{2}\right)^k + \left(\frac{1+\bar{\gamma}}{\bar{\gamma}}\right)^{m-1} \times \left(e^{-\frac{\lambda_1}{2(1+\bar{\gamma})}} - e^{-\frac{\lambda_1}{2}} \sum_{k=0}^{m-2} \frac{1}{k!} \left(\frac{\lambda_1 \bar{\gamma}}{2(1+\bar{\gamma})}\right)^k\right) \tag{2}$$

where $\Gamma(\cdot)$ and $\Gamma(\cdot, \cdot)$ are complete and incomplete gamma functions respectively, $\bar{\gamma}$ is the average SNR as determined by path-loss and the transmitted power of the primary user, λ_1 is the threshold, and $m = TW$ is time-bandwidth product.

B. Attack Model

During collaborative spectrum sensing process, a malicious user may generate and distribute unreliable reports. In this paper we consider three kinds of attack models which are shown as follows:

- *Crude Data Falsification (CDF) Attack:* In each time slot, the attacker would always fabricate a report which is exactly opposite to its authentic sensing result. That is to say, if sensed energy is higher than the threshold, then the attacker would report the absence of the primary user. On the contrary, if the sensed energy is lower than the threshold, then attacker would report primary user's existence.
- *Smart Data Falsification (SDF) Attack:* In each time slot, the attacker chooses to attack or not with attack probability P_a in order to conceal its malicious behavior. That is to say, no matter primary user occupies the spectrum or not, the attacker has the probability of P_a to report an untrue result.
- *Sybil Attack:* In each time slot, the Sybil attacker may try to disseminate his forged CDF or SDF reports with multiple distinct identities to the users nearby, by which the attacker could win much more extra weights in cooperative decision or fusion and therefore make remarkable impacts on final decision with limited attack resources.

III. PROPOSED SCHEME

In this section, we would firstly propose the UMDS scheme which aims to robustly detect misbehaving users in the hostile environments by adopting a user-centric approach. We also discuss how to derive the optimal system parameters to further improve the UMDS performance.

A. *A* User-centric Misbehavior Detection Scheme

With respect to the mobility of CR networks, a single secondary user would frequently gets into unfamiliar environments, where the uncertainty of its spectrum sensing partners degrades the performance of collaborative sensing. What's more, selfish or malicious users could even enjoy an increased access opportunity by disseminate some misleading or untrue sensing reports, which pose a serious threat to the security of the honest secondary users.

To address this issue, we propose our User-centric Misbehavior Detection Scheme which is inspired by the old saying *it is better to see for oneself rather than to hear for many times*. Therefore, in UMDS, the secondary user's own reports are assigned a higher trustable level and are used for the foundation to distinguish the good users from malicious users. UMDS calculates the correlations among the honest users or between the honest and malicious ones. Because it is more likely for the honest users to have a consistent view on the

sensing report, the report correlation between honest users is supposed to be higher than that between honest and malicious users. By exploiting this, the secondary user could detect those malicious users whose reports have low correlation with it. Next, we will introduce our schemes in details.

We assume a secondary user $s_i, i \in N$ is the one who implements UMDS. It firstly collects the reports from other users. We suppose a typical collection period to be $T = nt, n = 1, 2, 3 \cdots$, where t is the time slot. In this collection period, the reports from User $s_\ell, \ell \in N$ about $p_j, j \in M$ are denoted as $R_\ell^j = [R_{\ell 1}^j, R_{\ell 2}^j, \cdots, R_{\ell n}^j]$, and R_ℓ^j is s_ℓ's decision matrix about p_j. Meanwhile, at some time slots $\bar{n}t, \bar{n} \in n$ when no report from s_ℓ is received due to failed sensing or transmission losses, we would set $R_{\ell\bar{n}}^j = 0$. In addition, in UMDS if the report $R_{\ell\bar{n}}^j \neq 0$ as well as $R_{i\bar{n}}^j \neq 0$, then $R_{\ell\bar{n}}^j$ would be considered to be a valid report. We use $R_{\ell\bar{n}}^j = e$ to denote $R_{\ell\bar{n}}^j$ as a valid report, and the number of effective reports in R_ℓ^j is y_ℓ^j. Furthermore, since there are M multiple primary users in the environment, s_i could obtain M decision matrixes from s_ℓ, which could be represented in the following set: $D_\ell = \{R_\ell^1, R_\ell^2, \cdots, R_\ell^M\}$.

Then, the secondary user s_i needs to patch the incomplete reports, which is marked as $p_j = 0$ in the report. The basic method is to eliminate the invalid reports' contribution to correlation calculation. The patch rule is presented as follows:

$$R_{l\bar{n}}^j = \begin{cases} 0 & if\ R_{i\bar{n}}^j = 0 \cap l \neq i \\ R_{i\bar{n}}^j & if\ R_{l\bar{n}}^j = 0 \cap l \neq i \end{cases} \tag{3}$$

After obtaining patched decision matrixes, the secondary user s_i will calculate the correlation value between his decision matrix R_i^j and R_ℓ^j, which could be described as follows:

$$W_\ell^j = \frac{1}{2} \sum_{\bar{n}=1}^{n} \left| R_{i\bar{n}}^j - R_{l\bar{n}}^j \right|, \quad l \in N\ j \in M \tag{4}$$

Then, a user having correlation value above a certain threshold would be identified to be malicious. And since there are M decision matrixes belonging to a single secondary user due to multiple primary users, we could get M detection results about the user according to M possibly unequal thresholds $\{\lambda_2^1, \lambda_2^2, \cdots, \lambda_2^M\}$. We then combine these results by OR-rule to further improve the preciseness of UMDS, and overall process of UMDS could be described in algorithm 1:

Algorithm 1: UMDS

```
Collect enough reports from other users
Perform patch rules
Determine thresholds {λ_2^1, λ_2^2, ··· , λ_2^M}
Set i = 1
for i < M + 1 do
    if W_i^1 > λ_2^1 ⋃ W_i^2 > λ_2^2 ⋃ ··· ⋃ W_i^M > λ_2^M then
        s_i = M
    else
        s_i = H
    end if                    //Perform OR-rule in fusion
    i=i+1
end for
```

B. Discussion on the probability of false positive/negative

In this section, we would further discuss the performance of UMDS in terms of its probability of false positive/negative.

Lemma 1: *(Probability of false positive) Given a detection threshold λ_2^j and specific primary user p_j, the probability G_f^j that a honest secondary user is wrongly identified as malicious user is:*

$$G_f^j = 1 - \Phi\left(\frac{\lambda_2^j - y_l^j Q_f^j}{\sqrt{y_l^j Q_f^j \left(1 - Q_f^j\right)}}\right) \tag{5}$$

,where Q_f is the probability that honest user's valid report is different from s_i's report in one time slot.

Proof: Let P_f^j and P_d^j denote s_i's probability of false positive and detection respectively when s_i detects the state of primary user P_j. Assume the required false positive rate and detection rate of qualified secondary users as P_f^H and aP_d^H. Then we could obtain:

$$\begin{aligned} Q_f^j &= \Pr\left\{ R_{l\bar{n}}^j \neq R_{i\bar{n}}^j \middle| s_l = H, R_{l\bar{n}}^j = e \right\} \\ &= \left[\left(1 - P_f^j\right) P_f^H + P_f^j \left(1 - P_f^H\right) \right] P_0^j \\ &+ \left[\left(1 - P_d^j\right) P_d^H + P_d^j \left(1 - P_d^H\right) \right] P_1^j \end{aligned} \tag{6}$$

,where P_1^j is the probability of p_j's existence, which could be obtained as follows:

$$P_1^j = \Pr\{p_j = 1\} = \frac{\sum_{\bar{n}=1}^{n} \left(\left| R_{i\bar{n}}^j \right| + R_{i\bar{n}}^j \right)}{2 \times \sum_{\bar{n}=1}^{n} \left| R_{i\bar{n}}^j \right|} \tag{7}$$

and P_0^j is p_j's absence rate:

$$P_0^j = \Pr\{p_j = 0\} = \frac{\sum_{\bar{n}=1}^{n} \left(\left| R_{i\bar{n}}^j \right| - R_{i\bar{n}}^j \right)}{2 \times \sum_{\bar{n}=1}^{n} \left| R_{i\bar{n}}^j \right|} \tag{8}$$

Therefore, $\frac{1}{2}\left|R_{i1}^j - R_{\ell 1}^j\right|, \frac{1}{2}\left|R_{i2}^j - R_{\ell 2}^j\right|, \cdots, \frac{1}{2}\left|R_{in}^j - R_{\ell n}^j\right|$ all follow Bernoulli distribution with identical success probability Q_f^j, and W_ℓ^j is the sum of them. we assume these variables are also independent, and the amount of them is large enough (more than 30). According to Central Limit Theorem (CLT), W_ℓ^j could be approximated to be Gaussian distribution as follows:

$$W_\ell^j \sim \mathcal{N}\left(y_l^j Q_f^j, y_l^j Q_f^j \left(1 - Q_f^j\right)\right)$$

Then given a threshold λ_1', we could get the probability of false positive when s_i detects malicious users:

$$G_f^j = 1 - \Phi\left(\frac{\lambda_2^j - y_l^j Q_f^j}{\sqrt{y_l^j Q_f^j \left(1 - Q_f^j\right)}}\right)$$

Lemma 2: *(Probability of false negative) Given a detection threshold λ_2^j and certain primary user p_j, the probability G_m that a malicious secondary user is wrongly identified as honest user is:*

$$G_m^j = \Phi(\frac{\lambda_2^j - y_l^j Q_d^j}{\sqrt{y_l^j Q_d^j \left(1 - Q_d^j\right)}}) \tag{9}$$

,where Q_d is the probability that malicious user's effective report is different from s_i's report in one time slot.

Proof: let the supposed false positive rate and detection rate of malicious secondary users to be P_f^M and P_d^M. Then we could obtain:

$$\begin{aligned} Q_d^j &= \Pr\left\{ R_{\ell\bar{n}}^j = R_{i\bar{n}}^j \middle| s_l = M, R_{\ell\bar{n}}^j = e \right\} \\ &= \left[\left(1 - P_f^j\right) P_f^M + P_f^j \left(1 - P_f^M\right)\right] P_0^j \\ &+ \left[\left(1 - P_d^j\right) P_d^M + P_d^j \left(1 - P_d^M\right)\right] P_1^j \end{aligned} \tag{10}$$

Similarly, W_ℓ^j also approximately follows Gaussian distribution:

$$W_l^j \sim \mathcal{N}\left(y_l^j Q_d^j, y_l^j Q_d^j \left(1 - Q_d^j\right)\right)$$

And the probability of false negative could be written as follows:

$$G_m^j = \Phi(\frac{\lambda_2^j - y_l^j Q_d^j}{\sqrt{y_l^j Q_d^j \left(1 - Q_d^j\right)}})$$

After fusion by OR-rule, the probability of false positive and negative may be written as follows:

$$T_f = 1 - \prod_{j=1}^{M} \left(1 - G_f^j\right) \tag{11}$$

$$T_m = \prod_{j=1}^{M} G_m^j \tag{12}$$

C. Optimization

From the above discussion, it is obvious that the thresholds $\{\lambda_1^1, \lambda_1^2, \cdots, \lambda_1^M\}$ and $\{\lambda_2^1, \lambda_2^2, \cdots, \lambda_2^M\}$ chosen by the secondary user have a direct affect on the performance of UMDS. Thus, in this section, we discuss how to choose the proper thresholds to further increase the performance of the proposed scheme. Here we adopt optimization technology to solve this problem, and the problem could be summarized as follows:

$$\min \quad f(\vec{\lambda}) = T_f + T_m$$

$$s.t. \quad \vec{\lambda} > 0$$

, where $\vec{\lambda} = [\lambda_1^1, \lambda_1^2, \cdots, \lambda_1^M, \lambda_2^1, \lambda_2^2, \cdots, \lambda_2^M]$. Here we implement Internal Penalty Function (IPF) method [10], and the optimization problem could be approximated as follows:

$$\min \quad f(\vec{\lambda}) = T_f + T_m + rB(\vec{\lambda})$$

$$s.t. \quad \vec{\lambda} > 0$$

, where r is a small positive number, $B(\vec{\lambda})$ is the barrier function, which could be defined as:

$$B(\vec{\lambda}) = \sum_{j=1}^{M} \left(\frac{1}{\lambda_1^j} + \frac{1}{\lambda_2^j}\right)$$

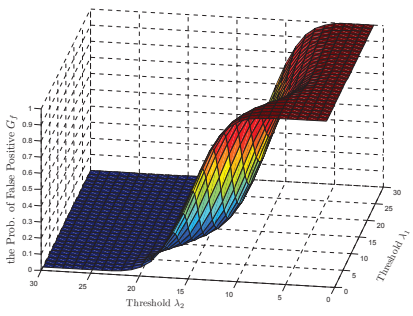
Then this problem could be solved as unconstrained optimization problem. We adopt Hooke-Jeeves (HJ) method [11] to solve it. The algorithm may be written in algorithm 2.

Algorithm 2: Optimization

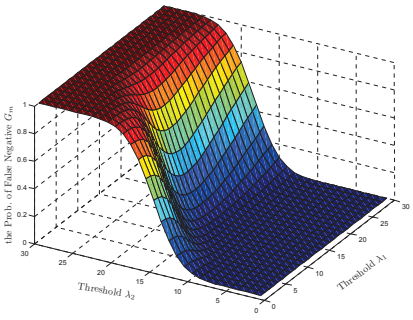
initialize $r > 0$, reduction coefficient $\varphi \in (0, 1)$, accuracy bound $\phi > 0$ // IPF parameters
initialize the step length δ, acceleration factor $\alpha \geq 1$, reduction factor $\beta \in (0 \cdot 1)$, accuracy bound $\varepsilon > 0, y^{(1)} = \gamma^{(1)} > 0$, $j = 1, k = 1$, and coordinate direction $\bar{e}_1, \bar{e}_2, \cdots, \bar{e}_{2M}$ // HJ parameters
for $rB(\vec{\lambda}^{(k)})/\varphi > \phi$ **do**
  for $\delta/\beta > \varepsilon \bigcup \vec{\lambda}^{(k)} \neq \vec{\lambda}^{(k-1)}$ **do**
    for $j < 2M$ **do**
      if $f\left(y^{(j)} + \delta e_j\right) < f\left(y^{(j)}\right)$ **then**
        $y^{(j+1)} = y^{(j)} + \delta e_j$
      else
        $y^{(j+1)} = y^{(j)}, j = j + 1;$
      end if
    end for // Detecting Motion
    if $f(y^{(2M+1)}) < f(\vec{\lambda}^{(k)})$ **then**
      $\vec{\lambda}^{(k+1)} = y^{(2M+1)}$ // Pattern Motion
      $y^{(1)} = \vec{\lambda}^{(k+1)} + \alpha(\vec{\lambda}^{(k+1)} - \vec{\lambda}^{(k)})$
    else
      $\delta = \beta\delta$, $y^{(1)} = \vec{\lambda}^{(k)}, \vec{\lambda}^{(k+1)} = \vec{\lambda}^{(k)}$
    end if
    k = k + 1,j = 1
  end for // HJ Process
  $r = \varphi r$
end for // IPF Process
return $\vec{\lambda}$

IV. NUMERICAL ANALYSIS

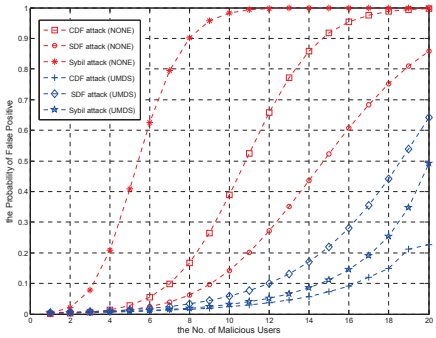
In this section, we would demonstrate the effectiveness of UMDS via numerical experiment. We assume that there are 3 primary users in the environment, and the time-bandwidth product is $m = 5$. We also assume there are another 20 secondary users which are of equality to access the idle spectrum. Here, we consider the Rayleigh Fading environment, and the average SNR $\bar{\gamma}$ is $10dB$. In a decision matrix, the number of effective samples $y_{\ell j}$ is set to be 30. we set $p_f^H = 0.2, p_m^H = 0.2, P_f^M = 0.8$ and $P_m^M = 0.8$. We also set $\lambda_1^i = 8, \lambda_2^i = 16, P_0^i = P_1^i = 0.5, i = 1 \sim 3$. In SDF and Sybil attacks, the attack probability P_a is set to 0.6 and an attacker would forge 2 identities to launch CDF attack.



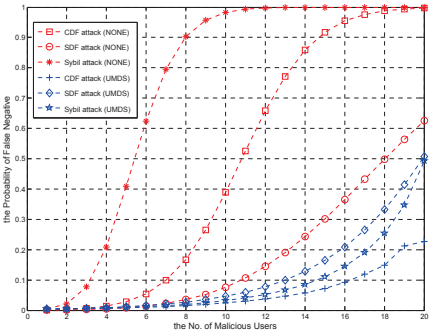
(a) Evaluation of UMDS by G_f



(b) Evaluation of UMDS by G_m



(c) None-proof vs. UMDS-aid by False Positive



(d) None-proof vs. UMDS-aid by False Negative

The evaluation of UMDS by G_f and G_m is given in figure (a) and (b), where we could see the probability of false positive/negative G_f and G_m are significantly affected by both λ_1 and λ_2^j chosen by the secondary user, and that there is a trade-off between G_m and G_f. We could also see that by choosing proper thresholds, G_f and G_m could be significantly reduced. We could reasonably infer that the performance of UMDS would be better after executing fusion in (11)(12) and optimization in algorithm 2. In figure (c) and (d), comparison has been made between none-proof and UMDS-aid collaborative spectrum sensing. We adopt Majority rule and from these figures, we could see false positive/negative of voting with UMDS is much lower than that of traditional voting under vicious environments, and UMDS has better robustness. We could also see that although SDF attack is much more moderate than the other two, this attack is much harder to be detected. In addition, in non-proof CR systems, Sybil attack is shown to be capable of doing a great harm to the system with fewer attackers, whereas in system adopting UMDS Sybil attack could be notably mitigated.

V. CONCLUSION

In this paper, we propose a novel scheme named UMDS to detect malicious behaviors for collaborative spectrum sensing in Cognitive Radio network. In UMDS, a secondary user distinguishes the misbehaving users from good users by calculating the correlation between his own reports and the reports from other users. Compared with existing researches, UMDS is expected to work well in the challenging environment where no prior knowledge about malicious users is required or the number of dishonest users may exceed that of hones ones. Our future work is to investigate the performance of UMDS under the condition of shadowing.

ACKNOWLEDGEMENT

This research was supported by National Natural Science Foundation of China (Grant No. 61003218 and No. 60934003) and Doctoral Fund of Ministry of Education of China (Grant No.20100073120065).

REFERENCES

[1] J, Mitola, G. Jr, "Cognitive Radio: making software radios more personal," *IEEE personal communications*, 1999.
[2] E. Hossain, D. Niyato, and Z. Han, "Dynamic Spectrum Access in Cognitive Radio Networks," Cambridge University Press, UK, 2008.
[3] A. Ghasemi, E. Sousa, "Collaborative Spectrum Sensing for Opportunistic access in fading environments," *in Proc. of DySPAN'05*, 2005.
[4] G. Ghurumuruhan and Y. Li, "Cooperative Spectrum Sensing in Cognitive Radio: PartI: Two User Networks," *IEEE Trans. on Wireless Communi., vol.6, no. 6, p.p. 2204-2213, Jun. 2007.*
[5] G. Ghurumuruhan and Y. Li, "Cooperative Spectrum Sensing in Cognitive Radio: PartII: Multiuser Networks," *IEEE Trans. on Wireless Communi., vol.6, no. 6, p.p. 2204-2213, Jun. 2007.*
[6] C. Lee, and W. wolf, "Energy Efficient Techniques for Cooperative Spectrum Sensing in Cognitive Radios," *in Proc. of IEEE Consumer Communications and Networking Conference*, Jan. 2008.
[7] W. Wang, H. Li, Y. Sun, Z. Han, "CatchIt: Detect Malicious Users in Collaborative Spectrum Sensing," *in Proc. of GLOBECOM'09*, 2009.
[8] R. Chen, J. Park, K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," Proc. *in Proc. of INFOCOM'08*.
[9] F. Digham, M. Alouini, M. Simon, "On the Energy Dectection of Unnown Signals Over Fading Channels" *in Proc. of ICC'03*, 2003.
[10] S. Rao, "Engineering Optimization: Theory and Practice," John Wiley and Sons Press, 2009.
[11] R. Hooke, T. Jeeves, ""Direct Search" Solution of Numerical and Statistical Problems," *Journal of the ACM (JACM)*, 1961.