An Adaptive Deviation-tolerant Secure Scheme for Distributed Cooperative Spectrum Sensing

Sheng Liu*, Haojin Zhu*, Shuai Li*, Xu Li†, Cailian Chen*, Xinping Guan*
*Shanghai Jiao Tong University, Shanghai, China
{liusheng,zhu-hj,shuailee,cailianchen,xpguan}@sjtu.edu.cn
†Inria Lille - Nord Europe, France; xu.li@inria.fr

***Abstract*—Distributed collaborative spectrum sensing is a promising method to improve the precision and efficiency of primary user detection in cognitive radio networks. Despite its performance advantages, it introduces new security issues that malicious or selfish nodes may manipulate false sensing data to degrade or even covert the sensing result of the whole network. Existing research often utilizes a threshold to distinguish honest users and malicious ones. However, determining such a threshold is difficult due to the dynamic characteristic of cognitive radio networks, and it is likely to misjudge an honest node with a relatively large deviation to be malicious. In this paper, we propose an Adaptive Deviation-tolerant Secure Scheme (ADS) for distributed collaborative spectrum sensing, which aims to mitigate the misbehaviors of inside malicious nodes and, at the same time, tolerant the large deviation introduced by honest users. ADS achieves the trade off of sensing security and deviation tolerance by assigning a dynamic weight to each sensing node and utilizes an adaptive threshold to minimize the negative effect on honest users. We evaluate the performance of the scheme through both analytical and simulation based study.**

Keywords – **Distributed Collaborative Spectrum Sensing, Large Deviation-tolerant, Misbehavior Detection, Dynamic Weight, Adaptive Threshold**

I. Introduction

The ever increasing spectrum demand with the emerging wireless applications has inspired the concept of Cognitive Radio (CR) [1], which is proposed to optimize the utilization of the precious natural resource, the radio spectrum. Unlike the conventional spectrum management paradigm in which most of the spectrum is allocated to fixed licensed users (i.e. primary users (PUs)) for exclusive use, a CR system allows secondary users (SUs) to utilize the idle spectrum [2], as long as intolerable interference to PUs is not introduced.

One of the major challenges in CR networks is for SUs to detect the presence of PUs and thus decide which channel can be utilized without introducing inference to the licensed users. However, the detection performance of spectrum sensing by individual nodes degrades significantly when the communication channel suffers from multipath fading or shadowing [1]. To address this issue, cooperative spectrum sensing, which collects the observation of several SUs from different locations, has been proposed to increase the detection accuracy by exploiting the spatial diversity.

In general, collaborative spectrum sensing paradigms can be classified into two categories: centralized collaborative spectrum sensing and distributed cooperative spectrum sensing. Centralized collaborative spectrum sensing needs a fusion center (FC) to collect the sensing reports from all secondary users and make a final decision. However, the requirement for such a centralized infrastructure makes it less suitable for ad hoc networks. On the contrary, distributed cooperative sensing does not need any common receiver (FC) to perform data fusion; secondary users communicate with each other in a peer-to-peer manner and iteratively converge to a unified decision on the presence or absence of PUs. Recently, a bio-inspired consensus-based cooperative spectrum sensing scheme is introduced in [4] [5] for distributed measurement fusion and soft combination. Moreover, Zhang et al. [6] proposed a distributed weighted average consensus-based spectrum sensing according to the measured channel condition.

While holding the promise in significantly improving sensing performance, distributed collaborative spectrum sensing is also facing extra vulnerabilities that have not received sufficient attention yet. In particular, malicious nodes may transmit fake sensing reports to their neighboring nodes and thus subvert the consensus decision of SUs in the whole network, which is termed as data falsification attack [12]. Unlike centralized cooperative sensing in which FC receives the sensing reports from other SUs only once during each single decision making procedure, distributed sensing may require each user to transmit their state value many times until they reach a consensus and thus a vicious node can continuously inject forged data. Due to the distributed nature of collaborative spectrum sensing, any malicious behavior will propagate through the whole network, causing a long-term widespread impact that is likely to be severer than in a centralized sensing model.

Most of the existing work countering data falsification attack in ad hoc networks relies on a threshold for detecting malicious nodes [3] [7] [14]. A User-centric Misbehavior Detection Scheme (UMDS) is introduced in [14]. In UMDS, secondary users select their own sensing reports as the trust base and independently determine whether a sensing partner is malicous. Nevertheless, this scheme is not based on the distributed consensus-based cooperative spectrum sensing model. In [3] and [7], two different defense schemes against data falsification attack for distributed consensus-based sensing are proposed. In [3], the scheme eliminates the state value with the largest deviation from the local mean at each iteration step and

978-1-4673-0921-9/12/$31.00 ©2012 IEEE

thus it can only deal with the circumstance in which only one malicious node exists and would still exclude one state value even if there is no malicious node. In [7], the vulnerability of distributed consensus-based spectrum sensing is analyzed and an outlier detection algorithm with adaptive local threshold based on the Gaussian propagation fading model is proposed. However, due to the dynamic characteristic of cognitive radio networks (e.g. the mobility of SUs, and the fast changing wireless signal propagation fading environment because of the volatility of temperature and humidity), it is difficult and impractical to determine such a threshold accurately even with the prior knowledge about the channel usage habit of PUs, let alone the severe signal fading environment which may not have a suitable model. Using an inaccurate threshold to detect malicious nodes may result in undesirable consequence. For example, an innocent node that accidentally gets a real but large deviation would be mistakenly judged as malicious and thereafter be separated from the rest of the network, which is unfair for the misjudged one. What's worse, such an veracious node may identify its neighbor nodes as vicious because of its large deviation from others and probably obtain a wrong sensing result, which absolutely goes against the purpose of the cooperative sensing.

To address the above challenge, in this paper we propose an Adaptive Deviation-tolerant Secure Collaborative Spectrum Sensing Scheme (ADS) for distributed consensus-based spectrum sensing. This scheme mitigates the misbehavior of inside malicious nodes and meanwhile tolerates the occasional large deviation introduced by honest users. Unlike the existing solutions issued above, ADS achieves the trade off between sensing security and deviation tolerance by assigning a dynamic weight to each sensing node. On the one hand, in case of the existence of continuous malicious behaviors, it adaptively reduces the coefficient so that the misbehaviors will be eventually isolated from the network. On the other hand, in case of honest users with unusual large derivation in the sensing stage, it permits them to play a part in the final decision making process. Furthermore, ADS allows the dynamic threshold to be gradually tuned back to zero to further minimize the influence of the malicious users. We analyze the performance of ADS and demonstrate its efficacy through experiments and simulations.

The rest of the paper is organized as follows. Section II defines the system model; Section III elaborates ADS and analyzes its performance. Simulation results are reported in Section IV, followed by the closing remarks in Section V.

II. System Model

In this section, we define the network model utilized in this paper as well as the consensus-based distributed collaborative spectrum sensing and introduce our attack model.

A. Consensus-Based Distributed Collaborative Spectrum Sensing

The distributed spectrum sensing scheme usually contains two phases: sensing and fusion. At the sensing stage, each secondary user utilizes an appropriate sensing approach to obtain the channel usage condition. In this paper, we adopt the energy detection method and the value of a sensing report is the received power of primary users' signal. Next at the information fusion stage, each SU communicates with its neighbors to obtain their state values and employ the consensus iteration until the whole network reaches the global statistics. Finally, the SUs make their own decision about the presence of the primary users.

Assume that the network contains n SUs $\mathcal{I} = \{1, 2, ..., n\}$. To model the consensus algorithm, we represent the network of SUs by an undirected graph $\mathcal{G} = (\mathcal{E}, \mathcal{V})$, where $\mathcal{V} = \{v_i | i \in \mathcal{I}\}$ is the node set and $\mathcal{E} = \{e_{ij} = (v_i, v_j) | i, j \in \mathcal{I}\}$ the edge set. We use the i^{th} node to denote the ith SU. These two symbols will be used interchangeably. The ith SU's set of neighboring nodes are indicated by $\mathcal{N}_i = \{j | e_{ij} \in \mathcal{E}\}$. We define the number of elements in $\mathcal{N}_i$ as the degree of the node i and denote it by $|\mathcal{N}_i|$. A path in $\mathcal{G}$ consists of a sequence of nodes $(v_1, v_2, ..., v_l), l \geq 2$ satisfying $(e_{m,m+1}) \in \mathcal{E}, \forall 1 \leq m \leq l-1$. The graph $\mathcal{G}$ is connected if any two different nodes in $\mathcal{G}$ are connected by a path. Moreover, it is *strongly connected* if there exists a directed path from each node to any other node.

The Laplacian matrix $\mathcal{L} = (l_{ij})_{n \times n}$ of the graph $\mathcal{G}$ is defined as

$$l_{ij} = \begin{cases} |\mathcal{N}_i|, & \text{if } j = i \\ -1 & \text{if } j \neq i, \quad j \in \mathcal{N}_i \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

where $|\mathcal{N}_i|$ is the i^{th} node's degree. The consensus-based distributed spectrum sensing scheme can be stated using a discreted-time state equation:

$$x_i(k+1) = x_i(k) + \epsilon \sum_{j \in \mathcal{N}_i} (x_j(k) - x_i(k)) \tag{2}$$

where

$$0 < \epsilon < \left(\max_i |\mathcal{N}_i| \right)^{-1} = \frac{1}{\Delta} \tag{3}$$

Δ represents the maximum degree of the network. $x_i(0)$ is the i^{th} node original measurement in the sensing stage and $x_i(k)(k \geq 1)$ is the updated state value computed through the iterative formula mentioned above at time step k. As long as ϵ satisfies inequation (3) and $\mathcal{G}$ is connected, the whole network will asymptotically reach an average consensus with the limit $x^* = (1/n) \sum_{i=1}^{n} x_i(0)$ [4].

We can rewrite the formula in matrix form as follows:

$$\boldsymbol{x}(k+1) = \boldsymbol{P}\boldsymbol{x}(k), \tag{4}$$

where $\boldsymbol{P} = \boldsymbol{I} - \epsilon \boldsymbol{L}$. $\boldsymbol{P}$ is a doubly stochastic matrix because its elements are all nonnegative and all of the sum of its rows and columns is 1. Finally, after the whole network reaching a consensus, each secondary node will make its own decision about the usage condition of the channels using a predefined threshold λ_1.

$$\textit{Decision } \boldsymbol{H} = \begin{cases} 1, & x^* > \lambda_1 \\ 0, & x^* \leq \lambda_1 \end{cases} \tag{5}$$

where $\boldsymbol{H} = 1$ means the channel is occupied by the primary user at present while $\boldsymbol{H} = 0$ stands for the absence of the PU.

B. Attack Model

We consider inside attackers that are able to master all the keys used by SUs if there are any, fabricate fake reports and disseminate them to others. Specially, we take into account the following three types of attacks.

- *Sensing Data Falsification (SDF) Attack:* This attack only occurs in the sensing stage (i.e. the first stage). The attacker attempts to fabricate a false sensing report which has a large deviation from the authentic sensing data. However, in the iteration stage (i.e. the information fusion phase), malicious nodes correctly perform state update and send their state values to neighbor nodes. This kind of attack is difficult to distinguish from the behavior of an honest node with a true but large deviation value. To tolerate the large deviation from the honest node, our approach only decreases but not eliminates the negative effect of this attack.
- *Iterative State Falsification (ISF) Attack:* In this attack, the attacker not only manipulates a forged sensing data in the first stage, but also injects fake state value at each iteration step. This attack can cause a serious result due to its long-term impact. According to [7], in a connected graph, only one attacker that transmits a constant value at each step can make the whole network consensus asymptotically reach the fabricated value injected by the attacker.
- *Random Data Falsification (RDF) Attack:* The attacker randomly chooses to transmit either a forged state value or correctly execute the update procedure at each step. Due to its concealing feature, this attack is hard to detect.

We assume that the network is not dominated by the malicious nodes (i.e. the number of the honest nodes adjacent to each SU exceeds the number of attackers) and neglect the communication link failure which means our network topology is relatively fixed during the whole consensus process. In our paper, we only consider data falsification attack under the circumstance that the attackers do not know the global statistics of the whole network. Primary user emulation attack [15], location privacy related attacks [9], Dos attacks are not our focus. Blocking attack, covert adaptive data injection attack with global knowledge [7], Sybil attack [14] are also out of the scope of our work.

III. The Proposed Scheme

In this section, we present our ADS scheme, which aims to decrease the negative impact of the misbehavior by inside malicious nodes while allowing honest nodes to accidentally have large deviation measurements during the distributed cooperative sensing procedure. We demonstrate its effectiveness through analysis.

A. Adaptive Deviation-tolerant Scheme

Current research addressing the security issue of false data injection attack usually utilizes a threshold to distinguish honest nodes and malicious ones. However, as discussed previously, due to the dynamic characteristic of cognitive radio networks, it is difficult and impractical to obtain such a threshold accurately, especially in a severe signal fading environment or in a dynamic network with mobile SUs. Utilizing an inaccurate threshold, it is likely to mistakenly judge an honest node with a relatively large deviation guilty. Our ADS scheme aims to allow the veracious users with large deviation to participate in the iteration process while diminishing their negative impact by decreasing the corresponding coefficient. Moreover, malicious nodes that continuously inject forged data can be detected and their influence would be minimized. By utilizing an adaptive threshold, we further reduce the negative effect on the honest users.

We now elaborate our ADS scheme below. Firstly, in the first stage, similar to ordinary distributed spectrum sensing, each SU makes a measurement independently and transmits it to their neighbors. Then at every iteration step k in the fusion phase, each node counts the numbers of neighbors that have a deviation larger than a threshold λ_2 and not larger than λ_2, respectively. We denote them as $m_i(k)$ and $n_i(k)$ where the index i represents the i^{th} node. If $n_i(k) + 1 > m_i(k)$, the node can believe that its measurement is relatively correct and alter its state equation (2) as follows.

$$\begin{aligned} x_i(k+1) = x_i(k) &+ \epsilon \sum_{j \in \mathcal{N}_i^T} (x_j(k) - x_i(k)) \\ &+ \frac{\epsilon}{a} \sum_{j \in \mathcal{N}_i^F} (x_j(k) - x_i(k)) \end{aligned} \tag{6}$$

where $\mathcal{N}_i^F$ denotes the set of nodes satisfying $|x_j(k) - x_i(k)| > \lambda_2^i$ and $\mathcal{N}_i^T$ is the complement set of $\mathcal{N}_i^F$ in $\mathcal{N}_i$.

From the formula, we can see that the impact of the state value with a large deviation is reduced by decreasing its corresponding coefficient. Meanwhile, for those nodes likely to be incorrect (i.e. the nodes satisfying $n_i(k) + 1 < m_i(k)$), their state-update equation remain unchanged, which implies that they will normally update their state if they are not malicious nodes. However, if a malicious node continuously injects forged data at each step, the factor corresponding to it in the other nodes' iteration formula will keep declining to zero and finally the influence of them is excluded as a consequence.

To determine the ith node's threshold λ_2, we give the equation below without any prior knowledge.

$$\lambda_2^i(k) = \frac{1}{|\mathcal{N}_i|} \sum_{j^* \in \mathcal{N}_i} \left| x_{j^*}(k) - \frac{x_i(k) + \sum_{j \in \mathcal{N}_i} x_j(k)}{|\mathcal{N}_i| + 1} \right| \tag{7}$$

Considering that the false data injected by malicious nodes always have a large deviation from the authentic sensing results, we only get rid of the attacker by utilizing the threshold above. To say the least, even if all of the nodes' state values are closed to each other, the ith node merely obtain a result more

approximate to its own sensing report, which is believed to be correct. Furthermore, due to the convergence of the whole network, the threshold λ_2 converges to zero, which gives zero-tolerant to the attacker.

Absolutely, we can also use the method proposed in [7] to determine the initial value of λ_2 based on the signal propagation fading model and alter the threshold value through the equation.

$$\lambda_2^i(k+1) = \frac{\sum_{j\in\mathcal{N}_i} |x_j(k+1) - x_i(k+1)|}{\sum_{j\in\mathcal{N}_i} |x_j(k) - x_i(k)|}\lambda_2^i(k) \tag{8}$$

This formula can also lead λ_2 to zero. The overall procedure of ADS is described in Algorithm 1 below.

Algorithm 1: Adaptive Deviation-tolerant Scheme

```
set k = 0
for v_i ∈ V do
    set m_i = 0 and n_i = 0
end for
make the sensing measurement and obtain the initial x_i(0)
for the whole network consensus is not reached do
    for each node v_i ∈ V do
        for each node j ∈ N_i do
            if |x_i(k) − x_j(k)| > λ_2^i(k) then
                m_i = m_i + 1
            else
                n_i = n_i + 1
            end if
        end for
        if n_i + 1 > m_i then
            for each index j ∈ N_i^F do
                set l_ij = l_ij / a
            end for
        end if
        Update l_ii to make sure the ith row sum is 1
        set k = k + 1
        Update the state x_i(k)
    end for
end for
```

B. Performance Analysis of ADS

We now analyze the performance of our ADS scheme. For convenience of discussion, we only consider the situation with single user (malicious or not, i.e. SDF attack or honest node with large deviation) obtaining unusual report in the sensing stage. Note that, as long as the network is not dominated by the attacker, ADS can also be utilized in the circumstance that malicious nodes start to collude and is especially effective when dealing with the continuous vicious behavior. Without loss of generality, we consider the first node (i.e. v_1 and its neighbor nodes to be $v_2, ..., v_{1+|\mathcal{N}_1|}$) to be anomaly and define the state transform matrix $\mathcal{P}_t$ ($t \geq 0$) and the corresponding Lapacian Matrix $\mathcal{L}_t$ as follows:

$$p_{ij}^t = \begin{cases} 1-\epsilon|\mathcal{N}_i| & \text{if } i=j\notin\mathcal{N}_1 \\ \frac{\epsilon}{a^t} & \text{if } j=1 \text{ and } i\in\mathcal{N}_1 \\ \epsilon & \text{if } j\neq 1 \text{ and } j\in\mathcal{N}_i \\ 1-\epsilon|\mathcal{N}_i|+\epsilon-\frac{\epsilon}{a^t} & \text{if } i=j\neq 1 \text{ and } j\in\mathcal{N}_1 \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

$$l_{ij}^t = \begin{cases} -\frac{1}{a^t} & \text{if } j=1 \text{ and } i\in\mathcal{N}_1 \\ lij-1+\frac{1}{a^t} & \text{if } i=j\neq 1 \text{ and } j\in\mathcal{N}_1 \\ lij & \text{otherwise} \end{cases} \tag{10}$$

For data falsification attack detection, each time when the state value is found to have an unusual large deviation, the coefficient corresponding to $x_1(k)$ is immediately reduced and the state transform matrix $\mathcal{P}$ is changed. We suppose that $x_1(k)$ is finally at normal range when $\mathcal{P}$ is altered to $\mathcal{P}_{t_f}$. Thus we obtain the consensus result as:

$$x_f = \lim_{n_{t_f}\to\infty} \mathcal{P}_{t_f}^{n_{t_f}} \prod_{t=1}^{t_f-1} \mathcal{P}_t^{n_t} x(0) \tag{11}$$

where $n_j \geq 1$ for $j \geq 1$ and $x(0)$ is the initial state.

First, we prove the convergence of the system. This is equivalent to demonstrate the convergence of discrete system $x(k+1) = \mathcal{P}_t x(k)$. We consider the eigenvalue of corresponding matrix $\mathcal{L}_t$ at the first place. According to Gershgorin circle theorem [13], we have for every $j \in \mathcal{N}_1$

$$\left|\mu_z - |\mathcal{N}_j| + 1 - \frac{1}{a^t}\right| \leq |\mathcal{N}_j| - 1 + \frac{1}{a^t} \tag{12}$$

for $j \notin \mathcal{N}_1$

$$|\mu_z - |\mathcal{N}_j|| \leq |\mathcal{N}_j| \tag{13}$$

where $\mu_z (1 \leq z \leq n)$ is the eigenvalue of $\mathcal{L}_t$. Then we can conclude $0 \leq \mu_z \leq 2\Delta$, where Δ is the maximum degree. Because $0 < \epsilon < (\max_i |\mathcal{N}_i|)^{-1} = \frac{1}{\Delta}$ and $\mathcal{P}_t$'s eigenvalue is $\mu_z^* = 1 - \epsilon\mu_z$, we have $-1 < \mu_z^* \leq 1$. In addition, $\mathcal{G}$ is connected and $rank(\mathcal{G}) = n-1$ [4], so $\mathcal{L}_t$ has only one single zero eigenvalue, meaning that $\mathcal{P}_t$ has one single eigenvalue equal to one. As a result, we derive the system is convergent for any initial state.

Now we give the method to compute the $\lim_{n_{t_f}\to\infty} \mathcal{P}_{t_f}^{n_{t_f}}$. We provide a lemma as follows:

Lemma 1: *(Perron-Frobenius [11]) Let P be a primitive nonnegative matrix which has left eigenvector g satisfying $Pg = g$, and right eigenvector h^T satisfying $h^T P = h^T$. Then* $\lim_{k\to\infty} P^k = \frac{gh^T}{h^T g}$.

We assume the network graph is strongly connected, then $\mathcal{P}_{t_f}$ is primitive nonnegative matrix [11] and its left and right eigenvector is $g = \mathbf{1} = [1, ..., 1]^T$ and $h^T = [1, a^t, ..., a^t]$, respectively. Thus

$$\lim_{n_{t_f}\to\infty} \mathcal{P}_{t_f}^{n_{t_f}} = \frac{gh^T}{1 + a^t(n-1)} \tag{14}$$

With the result of $\lim_{n_{t_f}\to\infty}\mathcal{P}_{t_f}^{n_{t_f}}$, we have a theorem as below. We define the row vector v^T as follows:

$$v_i^T = \begin{cases} v_1 & \text{if } i = 1 \\ v_2 & \text{if } 2 \le i \le 1 + |N_1| \\ v_3 & \text{if } 2 + |N_1| \le i \le n \end{cases} \tag{15}$$

Note that for convenience of discussion, we just consider a two-hop network. A network of three-hop or more has the similar conclusion by merely extending $v^T = [v_1, v_2...v_2, v_3...v_3]$ and $v_3 \ge v_2 \ge a^t v_1$ to $v^T = [v_1, v_2...v_2, v_3...v_3, ..., v_n, ..., v_n]$ and $v_n \ge ... \ge v_3 \ge v_2 \ge a^t v_1$. Moreover, we define $|\mathcal{N}_b^B|$ and $|\mathcal{N}_c^A|$ as the number of elements in $\mathcal{N}_b^B = \{j \mid j \ne 1 \text{ and } j \notin \mathcal{N}_1 \text{ and } j \in \mathcal{N}_b\}$ for $\forall\ b \in \{b \mid 2 \le b \le 1 + |\mathcal{N}_1|\}$ and $\mathcal{N}_c^A = \{j \mid j \in \mathcal{N}_1 \text{ and } j \in \mathcal{N}_c\}$ for $\forall\ c \in \{\ c \mid 2 + |\mathcal{N}_1| \le c \le n\}$, respectively. We consider a network in which the number of two-hop nodes in one-hop's neighbor set is a constant and so does the number of one-hop nodes in two-hop's neighbor set (the node density is relatively uniform). This means $|\mathcal{N}_b^B| = |\mathcal{N}_2^B|$, $|\mathcal{N}_c^A| = |\mathcal{N}_3^A|$ as an invariable and $\mathcal{N}_b^B \ne \emptyset, \mathcal{N}_c^A \ne \emptyset$.

Theorem 1: *If $v_3 \ge v_2 \ge a^t v_1$ and $w^T = v^T\mathcal{P}_t$, then*

$$w_i^T = \begin{cases} w_1 & \textit{if } i = 1 \\ w_2 & \textit{if } 2 \le i \le 1 + |N_1| \\ w_3 & \textit{if } 2 + |N_1| \le i \le n \end{cases} \tag{16}$$

$v^T\mathbf{1} = w^T\mathbf{1}$ and $w_3 \ge w_2 \ge a^t w_1$, as long as $\epsilon \le \frac{1}{|\mathcal{N}_3^A|+|\mathcal{N}_2^B|}$ and $\epsilon \le \frac{1}{|\mathcal{N}_1|+1}$. $|\mathcal{N}_3^A|$ and $|\mathcal{N}_2^B|$ are definited as above.

Proof: From $w^T = v^T\mathcal{P}_t$, we could obtain:

$$w_1 = v_1 - \epsilon v_1|\mathcal{N}_1| + \frac{1}{a^t}\epsilon v_2|\mathcal{N}_1| \tag{17}$$

for $\forall\ b \in \{b \mid 2 \le b \le 1 + |\mathcal{N}_1|\}$:

$$w_b = w_2 = \epsilon v_1 + v_2 - \frac{1}{a^t}\epsilon v_2 + |\mathcal{N}_2^B|\epsilon(v_3 - v_2) \tag{18}$$

for $\forall\ c \in \{\ c \mid 2 + |\mathcal{N}_1| \le c \le n\}$:

$$w_c = w_3 = v_3 + |\mathcal{N}_3^A|\epsilon(v_2 - v_3) \tag{19}$$

Thus $w^T\mathbf{1} = w_1 + |\mathcal{N}_1|w_2 + (n - 1 - |\mathcal{N}_1|)w_3 = v_1 + |\mathcal{N}_1|v_2 + (n-1-|\mathcal{N}_1|)v_3 = v^T\mathbf{1}$. Note that here $|\mathcal{N}_1||\mathcal{N}_2^B| = (n-1-|\mathcal{N}_1|)|\mathcal{N}_3^A|$ because the state transform matrix $\mathcal{P}_t$ is a symmetric matrix by eliminating its first row and first column.

Now, we compare w_3, w_2 and $a^t w_1$.

$$w_2 - a^t w_1 = (v_2 - a^t v_1)[1 - \epsilon(\frac{1}{a^t} + |\mathcal{N}_1|)] + |\mathcal{N}_2^B|\epsilon(v_3 - v_2) \tag{20}$$

We have $\epsilon \le \frac{1}{|\mathcal{N}_1|+1}$, therefore $\epsilon \le \frac{1}{|\mathcal{N}_1|+a^{-t}}$. With $v_3 \ge v_2 \ge a^t v_1$, we can conclude $w_2 - a^t w_1 \ge 0$.

$$w_3 - w_2 = (v_3 - v_2)[1 - \epsilon(|\mathcal{N}_3^A| + |\mathcal{N}_2^B|)] + \epsilon(\frac{v_2}{a^t} - v_1) \tag{21}$$

Similarly, with $\epsilon \le \frac{1}{|\mathcal{N}_3^A|+|\mathcal{N}_2^B|}$ and $v_3 \ge v_2 \ge a^t v_1$, we can gain $w_3 - w_2 \ge 0$.

We denote the final consensus result as follows:

$$x_f = g\delta^T x(0) \tag{22}$$

where $g = [1, ..., 1]^T$ and $\delta^T = \frac{1}{1+a^t(n-1)}h^T\prod_{t=1}^{t_f-1}\mathcal{P}_t^{n_t} = [\delta_1, \delta_2, ..., \delta_n]$.

From Theorem 1 and $a \ge 1$, we deduce $\delta_n \ge ... \ge \delta_2 \ge a\delta_1$, $\delta_n + ... + \delta_2 + \delta_1 = 1$ and $\delta_1 \le \frac{1}{n}$, so the contribution of the state with large deviation(i.e. x_1) is reduced but not excluded by our scheme as long as the parameter ϵ can meet certain conditions, which means ADS allows veracious nodes with large deviation to participate in the iteration process while reducing the negative impact of SDF attack. Due to the fact $\delta_i \ge a\delta_1 : i \ge 2$, with the rise of parameter a, the effect of the large-deviation state on the final consensus result is further decreased.

IV. Performance Evaluation

A. Experiments Setup

We obtain our sensing report at the Building of Electronic Information and Electrical Engineering School located in Shanghai Jiao Tong University, Minhang Campus. By using Universal Software Radio Peripheral (USRP) with a TVRX daughterboard (50 MHz to 860 MHz Receiver) and a wide band antenna (70 MHz to 1000 MHz), we detect three channels of TV broadcasts in 13 sampling regions at the building. These sensing reports are significantly different, although some of the positions are adjacent to each other. We list the sensing reports from two pairs of neighbor regions $(9, 10)$ and $(11, 12)$ as below. From the table, we can see the tremendous diversity from their sensing results, thus conform that it is unreal and impractical to determine an accurate threshold in a wireless network to distinguish malicious nodes and honest ones. The exact positions of each regions can be found in [9].

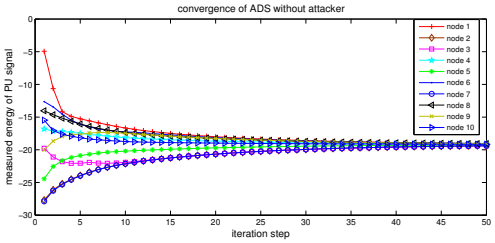
region	662-670MHz	750-758MHz	798-806MHz
9	-22.2938	-5.2868	-11.8057
10	-16.7460	-12.9037	-13.9781
11	-21.8713	-12.7158	-19.8206
12	-14.2647	-6.8082	-15.0492

B. Simulation Results

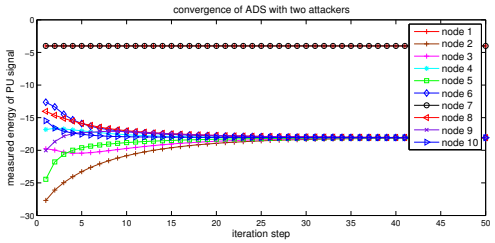
We utilize the average value of 550 sensing results at the frequency band 798-806MHz measured through USRP as our initial sensing data (i.e. $x_i(0)$). In our experiment, we select ten regions as our SUs to cooperate with each other to execute ADS. We choose the reducing factor $a = 5$ and $\epsilon = b = 1/10$.

In fig(a), we demonstrate the effectiveness of our scheme without attacker. From the figure, we could see the whole network reaches a final consensus though the initial state of each node vary significantly from each other. Moreover, the consensus result is -19.1897, better than the one -18.3698 of normal average distributed spectrum sensing scheme (i.e. $a = 1$).

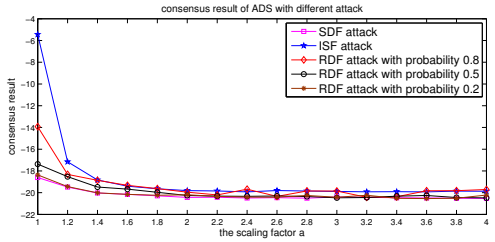
In fig(b), we consider the vicious environment with two attackers, node 1 and 7, executing ISF attack. For the normal distributed spectrum sensing, a consensus cannot be reached or the consensus result of the whole network will be asymptotically reduced to the value injected by the attacker [7]. However, our scheme can detect the continuous malicious behaviors



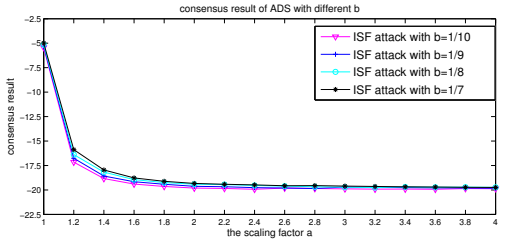
(a) Convergence without attacker



(b) Convergence with two attackers



(c) Consensus result under different attack



(d) Consensus result under different b

of attackers and exclude the compromised users, which makes the rest network of honest nodes reach a consensus.

Moreover, we evaluate the relationship between the consensus result and the reducing factor a under the circumstance malicious node 1 execute SDF attack, ISF attack and RDF attack, respectively. The result is averaged by 10000 simulation runs. As shown in fig(c), the scheme has a quite good resistance against different sorts of attack. Fig(d) displays the connection between the final consensus result and the factor a under different ϵ, which demonstrates that the influence of ϵ on the final convergence value is reduced by increasing the factor a.

V. Conclusion and Future Work

In this paper, we proposed a novel distributed spectrum sensing scheme named ADS to minimize the impact of attackers and at the same time avoid mistakenly judging an honest node to be malicious due to the inaccuracy of the threshold. In ADS, we adopt a dynamic weight and adaptive threshold to reduce the effect of malicious nodes while allowing honest user with a relatively large deviation to play a role in the consensus procedure. Moreover, we give the performance analysis of our scheme and demonstrate through experiments that ADS is secure, robust and effective. In the future, we will investigate the attack under random graph network topology due to the communication link failure.

Acknowledgment

The work was partially supported by National Basic Research Program of China under the grant no. 2010CB731803, NSF of China under 61003218, 60934003, 60974123, 61174127 and 70971086, Science and Technology Commission of Shanghai Municipality (STCSM), China under 11511501202, Doctoral Fund of Ministry of Education of China (Grant No.20100073120065) and "Chenguang Program under 09CG06.

References

[1] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "Next eneration/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks (Elsevier) Journal*, September 2006.

[2] I.F. Akyildiz, B.F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication (Elsevier) Journal*, Vol. 4, No. 1, pp. 40-62, Mar. 2011

[3] F. R. Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in Proc. of *MILCOM*, 2009. 2009.

[4] Z. Li, F. R. Yu, and M. Huang, "A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios", *IEEE Transaction on Vehicular Technology*, vol. 59, no. 1, pp. 383-393, 2010.

[5] F. R. Yu, M. Huang, and H. Tang, "Biologically inspired consensusbased spectrum sensing in mobile ad hoc networks with cognitive radios", *IEEE Networks*, vol. 24, no. 3, pp. 26-30, May 2010.

[6] W. Zhang, Z. Wang, Y. Guo, H. Liu, Y. Chen, and J. Mitola III, "Distributed cooperative spectrum sensing based on weighted average consensus," in *GLOBECOM*, 2011.

[7] Q.Yan, M.Li, T Jiang, W Lou, Y. Thomas Hou, "Vulnerability and Protection for Distributed Consensus-based Spectrum Sensing in Cognitive Radio Networks" in *INFOCOM*, 2012.

[8] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh,"White space networking with wi-fi like connectivity," in *SIGCOMM'09*.

[9] S. Li, H. Zhu, Z. Gao, X. Guan, and S. Shen, "Location Privacy Preservation in Collaborative Spectrum Sensing," in Proc. of *INFOCOM*, 2012.

[10] O. Fatemieh, A. Farhadi, R. Chandra, and C.A. Gunter, "Using classification to protect the integrity of spectrum measurements in white space networks" in Proc. of *NDSS*, 2011.

[11] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*. vol. 95, no. 1, pp. 215-233, 2007.

[12] A. W. Min, K.-H. Kim, and K. G. Shin, "Robust cooperative sensing via state estimation in cognitive radio networks,"in Proc. of *DySPAN*, 2011.

[13] R. A. Horn and C. R. Johnson, "Matrix Analysis," *Cambridge, U.K.: Cambridge Univ. Press*, 1987.

[14] S. Li, H. Zhu, B. Yang, C. Chen, and X. Guan,"Believe yourself: A user-centric misbehavior detection scheme for secure collaborative spectrum sensing", In Proc. of *ICC*, 2011.

[15] R. Chen, J.-M. Park, and J. H. Reed,"Defense against primary user emulation attacks in cognitive radio networks", *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25-37, Jan 2008.