Attack-Proof Cooperative Spectrum Sensing Based on Consensus Algorithm in Cognitive Radio Networks

Quan Liu, Jun Gao, Yunwei Guo and Siyang Liu
Department of Communication Engineering, Naval University of Engineering
Wuhan, 430033 - China
[e-mail: liuquan.hjgc@gmail.com; {alex-hjgc, sims_23, liusiyang514}@163.com]
*Corresponding author: Quan Liu

Received July 25, 2010; revised September 10, 2010; revised October 14; accepted October 17, 2010; published December 23, 2010

Abstract

Cooperative spectrum sensing (CSS) is an effective technology for alleviating the unreliability of local spectrum sensing due to fading/shadowing effects. Unlike most existing solutions, this paper considers the use of CSS technology in decentralized networks where a fusion center is not available. In such a decentralized network, some attackers may sneak into the ranks of cooperative users. On the basis of recent advances in bio-inspired consensus algorithms, an attack-proof, decentralized CSS scheme is proposed in which all secondary users can maintain cooperative sensing by exchanging information locally instead of requiring centralized control or data fusion. Users no longer need any prior knowledge of the network. To counter three potential categories of spectrum sensing data falsification (SSDF) attacks, some anti-attack strategies are applied to the iterative process of information exchange. This enables most authentic users to exclude potentially malicious users from their neighborhood. As represented by simulation results, the proposed scheme can generally ensure that most authentic users reach a consensus within the given number of iterations, and it also demonstrates much better robustness against different SSDF attacks than several existing schemes.

Keywords: Cognitive radio networks, cooperative spectrum sensing, consensus, spectrum sensing data falsification, metropolis weights

This research was supported by the National High-tech Research and Development Program of China [No.2009AAJ208, 2009AAJ116].

DOI: 10.3837/tiis.2010.12.004

1. Introduction

As evidenced by recent measurements [1], the increasingly severe problem of spectrum scarcity is largely due to inefficient static frequency allocation rather than to any physical shortage of spectrum. This has led regulatory agencies, such as the Federal Communications Commission (FCC), to reconsider the problem of spectrum management. With spectrum demands from emerging wireless applications rapidly increasing, spectrum policy reform is inevitable. Dynamic spectrum access (DSA) is the most explored idea for non-conventional spectrum management. Cognitive radio networks (CRNs), which are based on the hierarchical DSA model [2], seems to be a promising paradigm for thoroughly solving the spectrum scarcity problem, since unlicensed secondary users (SUs) in CRNs are allowed to share, opportunistically, any spectrum temporarily unused by licensed primary users (PUs).

To avoid any interference with the existing primary systems, the fundamental requirement for SUs is to periodically sense the presence of PUs. Among various possibilities, energy detection (ED) [3][4] is the optimal sensing algorithm and has been widely applied thanks to its relatively low complexity and lack of requirements for prior knowledge of the network. However, the performance of ED is very susceptible to multipath fading/shadowing and noise uncertainty, which necessitates cooperative spectrum sensing (CSS) among different SUs in the link layer of CRNs [5]. Consequently, many CSS schemes have been studied in recent literature. Most of them are fusion-based schemes, in which a base station (BS; in a centralized CRN) or a fusion center (FC; in a decentralized CRN) is always needed to perform data fusion [6][7][8] or decision combination [5][9][10]. Although such schemes can significantly improve sensing performance, they might be impractical in certain decentralized CRNs, in which a BS or FC may be not available to collect the local decisions or data from all cooperating users. Thus, some recent research has been conducted on CSS without fusion. In [11], assuming knowledge of the PU transmitter, Ganesan proposed a novel CSS scheme based on the relay and forwarding protocol without any centralized control. In [12], Z. Li and F.R. Yu were first to introduce the notion of bio-inspired consensus algorithms into decentralized CSS. These algorithms were initially related to certain complex natural phenomena, such as the flocking of birds, and are now widely used in wireless sensor networks [13]. The key feature of their scheme is that each SU can maintain coordination solely through local interactions with its neighbors, without any centralized control or combination. Such a fully distributed and scalable algorithm is feasible for decentralized CRNs, thus meriting further investigation.

Another fundamental issue in CSS is the security of the sensing procedure. Either centralized fusion or local information exchange could be attacked by malicious users, introducing some nontrivial security challenges. Thus, the security of these aspects should be addressed before the benefits of any CSS scheme may be fully reaped in practice. However, this area has yet to receive adequate attention. R. Chen classified the potential security threats to the sensing procedures into two categories: primary user emulation (PUE), in the physical layer, and spectrum sensing data falsification (SSDF), in the link layer [14]. In a PUE attack, a malicious user tries to gain priority over other SUs by transmitting signals that emulate the characteristics of a PU. To combat this, a transmitter verification scheme was proposed in [15]. In a SSDF attack, a malicious user sends false or confusing reports (decision or data) to the BS, FC, or its link neighbors, which could potentially disrupt CSS, thus causing interference with PUs or resulting in under-utilized, fallow licensed spectrum. To counter SSDF attacks against fusion-based CSS, the authors of [16] proposed some strategies based on a weighted sequential probability ratio test (WSPRT), and the authors of [17] placed the report history of each SU in high-dimensional space and detected possible abnormalities with the techniques used in data mining. Although [18] has done some initial work on the security issues of consensus-based CSS, to the best of our knowledge, no detailed discussion or further developments in this area are reported.

As a result, in this paper, we extend the study of consensus-based CSS, with the main focus on an unavoidable security problem: how to counter SSDF attacks on decentralized CRNs. The main contribution of our work is that we present an attack-proof CSS scheme utilizing a consensus algorithm without any central control or fusion. The proposed scheme is proactive in countering SSDF attacks, since each authentic SU can identify and reject false or confusing reports from malicious users during information exchange. If the time constraint for sensing permits, the states of authentic users will converge to a common value in most cases. Each SU then individually makes its own decision based on this final state. Extensive simulation results illustrate the improved robustness of the proposed scheme against all three potential SSDF attack models.

The remainder of this paper is organized as follows. In Section 2, the system model is described, together with a brief introduction to the notion of consensus, local energy detection, and SSDF attack models. In Section 3, based on the consensus algorithm, a CSS scheme is proposed to counter SSDF attacks. Section 4 provides the simulation results, and Section 5 presents the conclusions.

2. System Model

We consider a decentralized CRN composed of N cooperative SUs without any central control or fusion center. CSS is viewed as a typical multiagent coordination problem [19]. To solve this problem, we utilize a consensus algorithm as an iteration rule that specifies the information exchange between each SU and all of its neighbors. “Consensus” means reaching an agreement regarding a certain quantity of interest that depends on the states of all authentic, cooperating SUs.

Unlike traditional radios, SUs are inherently of lower priority on the network. Thus, each SU must be able to identify the spectrum before transmitting in order to avoid unacceptable interference with the PUs. While utilizing a spectrum hole, the SUs are also responsible for monitoring return PUs on the current channel so as to promptly vacate the channel if required. For simplicity, we assume that all SUs perform synchronous, periodic sensing with a generic time-fragment frame as shown in **Fig. 1**. This can be divided into four parts: local sensing, information exchange, final decision, and data transmission, each with the time duration of T_l, T_c, T_f and T_d, respectively. In a sensing period, each SU first individually performs local spectrum sensing and then establishes communication links with its neighbors to exchange its own states until the iteration exceeds the time limit T_c. With the last state of the iteration, each SU individually makes a final decision. Depending on whether the channel is identified as busy or idle, each user will keep silent or transmit during the data-transmission block. T_p denotes the sensing period, defined as the maximum time during which SUs may be unaware of a reappearing PU [20], and T_s is the total sensing overhead caused by all three steps of sensing (i.e., $T_s = T_l + T_c + T_f$). In this framework, both the sensing and transmission times should be fine-tuned to balance quality of service (QoS) with the avoidance of interference. This is often interpreted as maximizing the SUs’ spectrum efficiency as long as the requirement of PU protection can be satisfied [20]. Also, there exists another tradeoff between the overhead required for local processing and that required for cooperation, which can be solved by finding the optimal values of T_l and T_c to achieve a certain level of performance [21]. Both of these tradeoffs should be well balanced by means of some kind of sensing control in the MAC layer [22]. However, this is beyond the scope of this paper, so we assume that the values of T_l, T_c, and T_f have been regulated and that they are known by each SU.

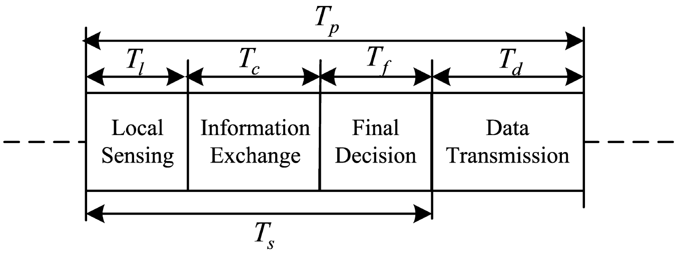


Fig. 1. Generic time-fragmentation frame

2.1 Local Spectrum Sensing

We choose energy detectors for local spectrum sensing without obscuring the analysis by employing sophisticated algorithms. The block diagram of the energy detector at the *i*-th SU ($i \in [1, N]$) is depicted in **Fig. 2** [3][4]. The received signal $x_i(t)$ is firstly sampled and filtered within the interested bandwidth W to remove out-of-band noise, and then the normalized accumulated energy in the observation interval T_l is computed as below [3]:

$$Y_i = \frac{1}{\delta_i^2}\sum_{n=1}^{2m} x_i^2(n) = \begin{cases} \frac{1}{\delta_i^2}\sum_{n=1}^{2m} w_i^2(n), & H_0 \\ \frac{1}{\delta_i^2}\sum_{n=1}^{2m}\left(h_i(n)s(n)+w_i(n)\right)^2, & H_1 \end{cases} \tag{1}$$

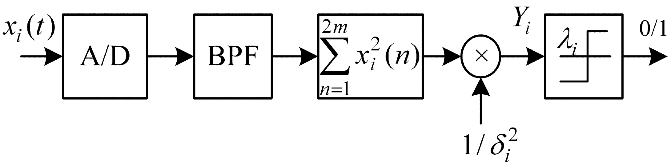


Fig. 2. Block diagram of the *i*-th energy detector

where m is the time-bandwidth product $m = WT_l$, $s(n)$ is the sampled primary signal, and $Y_i, h_i(n)$, and $w_i(n)$ represent the normalized test statistic, the sampled amplitude gain, and additive white Gaussian noise at the *i*-th SU, respectively. It has been derived in [3] that the test statistic Y_i has central and non-central chi-square distributions under H_0 and H_1, respectively:

$$Y_i \sim \begin{cases} \chi_{2m}^2, & H_0 \\ \chi_{2m}^2(2m\gamma_i), & H_1 \end{cases} \tag{2}$$

where $\gamma_i = P/(N_0 W)$ is the local sensing SNR, with P and N_0 being the power of the primary signal and the one-sided noise power spectral density, respectively. If a binary decision is needed locally, the normalized energy will be further compared to a local threshold λ_i to decide directly whether a PU signal is present or not [3].

2.2 SSDF Attack on Decentralized CSS

Decentralized CSS can be disrupted by SSDF attacks, since some hostile users may sneak into the ranks of cooperative SUs once they successfully cheat nearby authentic users into establishing data links with them. It is also possible for an honest SU to be compromised or controlled by adverse parties. Such hostile, compromised, or malicious SUs may launch SSDF attacks by sending false or confusing reports when exchanging information with their nearby neighbors, leading to some authentic SUs making wrong decisions or even leading to fatal sensing errors in the whole CRN. Such SSDF attacks can be categorized into three models [18]. The first model is a selfish SSDF attack, in which a malicious user always reports a presence decision or a relatively high energy value so that its neighbors are cheated out of the deserved spectrum opportunity. By contrast, in the second model, an interference SSDF attack, the malicious user always sends an absence decision or relatively little data, with the intention of causing interference with PUs. In the third model, a confusing SSDF attack, a malicious user sends out decisions or data at random, which confuses its neighbors or other SUs.

Admittedly, some intelligent malicious users might cooperate with each other to cheat the honest SUs more readily, and they might even adapt their own attack strategies to combat the authentic users' various anti-attack schemes. However, these are beyond the scope of the present paper and will be discussed in our further research.

3. Attack-Proof Cooperative Spectrum Sensing

In this section, an attack-proof CSS scheme based on the consensus algorithm is proposed, followed by a discussion of its convergence and sensing performance. We then provide a brief introduction to two existing consensus-based schemes. These will be used for comparison in the next section.

3.1 Proposed Scheme

It is assumed that each SU can establish reliable duplex communication links with its neighbors according to the MAC protocol. Thus, the decentralized CRN can be modeled as an undirected graph $G=(V,E)$, in which $V=\{1,2,\cdots N\}$ is the set of all SUs and E is the set of active links [19]. The potential attackers are included in the N cooperative SUs, and they can launch SSDF attacks with any, or any combination, of the attack models mentioned in Section 2.2.

Let $\mathbf{A}=\{a_{ij}\}$ be the adjacent matrix of the graph. The edge set can then be represented as $E=\{(i,j)\in V\times V, a_{ij}\neq 0\}$. Also, the neighbor set and the degree of the i-th SU are defined as $Ne_i=\{j\in V \mid a_{ij}\neq 0\}$ and $d_i=|Ne_i|=\sum_j a_{ij}$, respectively. The Laplacian of the graph is [19]:

$$\mathbf{L}=(l_{ij})_{N\times N}=\mathbf{D}-\mathbf{A} \tag{3}$$

where $\mathbf{D}=diag(d_1,d_2,\cdots d_N)$ is the degree matrix of the network. Then, the elements of $\mathbf{L}$ can be represented as:

$$l_{ij} = \begin{cases} -1, & if\ \ j \in Ne_i \\ d_i, & if\ \ j = i \\ 0, & otherwise \end{cases} \tag{4}$$

Based on the above assumptions, our proposed scheme can be represented with the following three steps:

Step 1. Local spectrum sensing. In this step, each SU individually performs local spectrum sensing with an energy detector, and the normalized accumulated energy within the observation time T_l is recorded as its initial state (i.e., $x_i(0) = Y_i$).

Step 2. Information exchange iteration. After synchronous local spectrum sensing, each SU tries to establish communication links with its nearby users. If the links are established successfully, all cooperative SUs will begin to exchange sensing states with their link neighbors. Because of the lack of any central authentication, malicious SUs could launch SSDF attacks secretly at any arbitrary moment by sending false or confusing reports to their neighboring users. Thus, in order to avoid the potential for wrong decisions, each authentic cooperating SU has to continually monitor the reports sent by its neighbors and reject misleading reports as soon as possible.

Given the above analysis, we introduce some special anti-attack techniques at each authentic SU during the information exchange. The detailed procedure is listed as follows.

1) For any authentic user $i \in [1, N]$, initialize the iteration with the state $x_i(0)$, $k = 0$.

2) At time instant k, update the SU's neighbor set $Ne_i(k)$ and degree $d_i(k)$. Then, register each neighbor's current report as: $R_{ij}(k) = x_j(k)$ for $\forall j \in Ne_i(k)$, and get the average value for the neighborhood:

$$u_i(k) = \frac{x_i(k) + \sum_{j \in Ne_i(k)} x_j(k)}{1 + d_i(k)} \tag{5}$$

3) Find the neighbor with the maximum deviation from $u_i(k)$, that is:

$$j_0 = \arg \max_{j \in Ne_i(k)} \left\{ x_j(k) - u_i(k) \right\} \tag{6}$$

and record that neighbor as a suspect selfish or interference attacker.

4) Calculate the average for the neighborhood without the suspect, that is:

$$u_i^{'}(k) = \frac{x_i(k) + \sum_{j \in Ne_i(k)} x_j(k) - x_{j_0}(k)}{d_i(k)} \tag{7}$$

5) Let λ_c be the predefined threshold for each user's final decision in Step 3. If $\left(u_i(k) - \lambda_c\right)\left(u_i^{'}(k) - \lambda_c\right) < 0$, then, because of its abnormality, the suspect j_0 is very likely an attacker of the first or second model. Thus, it should be excluded from the *i*-th SU's neighborhood, that is:

$$Ne_i(k) = Ne_i(k) / j_0 \tag{8}$$

6) If $k \geq 20$ and $\mathrm{mod}(k, 10) = 0$, then, for $\forall j \in Ne_i(k)$, calculate the standard deviations of its recent ten and the last ten reports to the *i*-th SU, respectively, and register them as:

$$a = std\left(R_{ij}(k-9), R_{ij}(k-8), \cdots, R_{ij}(k)\right), \tag{9}$$

$$b = std\left(R_{ij}(k-19), R_{ij}(k-18), \cdots, R_{ij}(k-10)\right) \tag{10}$$

7) If $a > b$ for some neighbor $j_1 \in Ne_i(k)$, then j_1 will be excluded from the neighborhood as a potential confusing attacker:

$$Ne_i(k) = Ne_i(k) / j_1 \tag{11}$$

8) Update each user's state with the following rule [23]:

$$x_i(k+1) = W_{ii}(k) x_i(k) + \sum\nolimits_{j \in Ne_i(k)} W_{ij}(k) x_j(k) \tag{12}$$

where $W_{ij}(k)$ is Metropolis weight, defined by [23] as:

$$W_{ij}(k) = \begin{cases} \dfrac{1}{1+\max\{d_i(k), d_j(k)\}}, & if \quad j \in Ne_i(k) \\ 1 - \sum\nolimits_{n \in Ne_i(k)} W_{in}(k), & if \quad i = j \\ 0, & otherwise \end{cases} \tag{13}$$

By this rule, the weight on each edge is one over one plus the larger degree at its two incident vertices, and the self-weights are chosen such that the sum of weights at each SU is 1. The corresponding vector form of the iteration rule can be represented as [23]:

$$\mathbf{X}(k+1) = \mathbf{W}(k)\mathbf{X}(k) \tag{14}$$

where $\mathbf{W}(k) = \{W_{ij}(k)\}$ denotes the Metropolis weight matrix, and

$$\mathbf{X}(k) = \{x_1(k), x_2(k), \cdots, x_N(k)\}$$

is the state vector of all cooperating SUs.

9) Update the discrete time instant: $k = k+1$.

10) If $k \geq T_c$ (T_c can be simply interpreted as the maximum iteration times), then break the iteration; else, continue from *2)*. That is, once the iteration time exceeds the given constraint, the information exchange must stop, whether or not a common value has been reached.

The motivation behind *6)* and *7)* in the above procedure can be explained as follows. According to the consensus notion [19][23], if the information exchange between the neighboring users is regularly carried out with the iteration rule (14), then, for any authentic neighbor $j \in Ne_i(k)$, its real state $x_j(k)$ will asymptotically converge to the average consensus [23] (also see (19) in subsection 3.2). As a result, the fluctuation of neighbor j's corresponding reports to the i-th SU will gradually decrease; thus, the standard deviation of the sequential piecewise reports assumes a non-increasing trend. For simplicity of implementation, every 10 reports are registered as one group; then, $a <= b$ for authentic neighbors. However, because of the randomness of its fabricated reports, this will not be the case should neighbor j be a confusing attacker who aims at deliberately disrupting cooperation. Therefore, we can use this characteristic to identify and reject the third type of attackers, at the cost of the extra memory required by each authentic SU to record the recent 20 reports from its neighbors.

Step 3. Final decision. Following the conclusion of information exchange, each user individually makes the final decision by comparing its final state with λ_c, that is:

$$D_i = \begin{cases} 1, & x_i(k) > \lambda_c \\ 0, & otherwise \end{cases} \tag{15}$$

3.2 Convergence Discussion

Undoubtedly, when there are no attackers, a simplified iteration procedure with only rule (14) suffices for carrying out the required information exchange. Without considering any anti-attack strategies, the network can be simply viewed as a fixed, undirected graph. In this case, the matrix $\mathbf{W}(k)$ from (13) is time-invariant (i.e., $\mathbf{W}(k)=\mathbf{W}$), symmetric, and doubly stochastic, with the following properties[23]:

$$\mathbf{1}^T\mathbf{W}=\mathbf{1}^T,\ \mathbf{W1}=\mathbf{1},\ \rho\left(\mathbf{W}-\mathbf{11}^T/N\right)<1 \tag{16}$$

where $\rho(\cdot)$ denotes the spectral radius [23] of the given matrix and $\mathbf{1}$ is the unit vector. That is, all of its row and column sums are equal to one, and all of the eigenvalues are real and ranged in $(-1,1]$. On the basis of (14), we define a *k*-step transition matrix as $\mathbf{\Psi}(k)=\mathbf{W}(k\text{-}1)\cdots\mathbf{W}(1)\mathbf{W}(0)$, and then we have:

$$\mathbf{X}(k)=\mathbf{\Psi}(k)\mathbf{X}(0) \tag{17}$$

Further, as derived in [23], we can obtain

$$\lim_{k\to\infty}\mathbf{\Psi}(k)=\lim_{k\to\infty}\mathbf{W}^k=\mathbf{11}^T/N \tag{18}$$

or, equivalently, all cooperative SUs will reach an average consensus asymptotically [19][23]

$$x_i(k)\to x^*=\frac{1}{N}\sum_{i=1}^{N}x_i(0)=\frac{1}{N}\sum_{i=1}^{N}Y_i,\ \ as\ \ k\to\infty,\ for\ \forall i\in[1,N] \tag{19}$$

with the convergence speed precisely $\rho\left(\mathbf{W}-\mathbf{11}^T/N\right)$ [23].

However, when several attackers are present, iteration with only rule (14) will lead to fatal sensing errors, since the average consensus will be disrupted. The whole network will move towards the false or random reports sent by attackers. In contrast, our proposed scheme applies some techniques to exclude potentially malicious users from the neighborhood of authentic SUs as soon as possible. This may result in unbalanced information exchange along certain edges of the initial graph. That is to say, although a potential attacker can still receive reports from neighboring authentic SUs, they may reject the attacker's own reports. With our iteration procedure, the neighborhood of each authentic user must be determined according to what it is receiving currently and has received in the past. As a result, the proposed scheme is essentially associated with a sequence of directed sub-graphs $G_a(k)=\left(V_a,E_a(k)\right)$, in which V_a and $E_a(k)$ denote the sets of authentic SUs and active edges, respectively. Enlightened by [24], we summarize the convergence of the proposed scheme with the following theorem.

Theorem: For dynamic sub-graphs $G_a(k)$, if there exists an infinite sequence of uniformly bounded, non-overlapping time intervals $[n,n+T)$, which can make the graph union $U_{k=n}^{n+T-1}G_a(k)=\left\{G_a(n),G_a(n+1),\cdots,G_a(n+T-1)\right\}$ strongly connected (or, equivalently, have a spanning tree), then a consensus can be asymptotically achieved through the proposed scheme.

Proof: Let $\mathbf{G_a}=\left\{G_{a1},G_{a2},\cdots G_{as}\right\}$ be the set of all possible directed sub-graphs $G_a(k)$ during the information exchange, and let $\overline{\mathbf{W}}_\mathbf{a}=\left\{\mathbf{W_{a1}},\mathbf{W_{a2}},\cdots\mathbf{W_{as}}\right\}$ be the corresponding set of all possible weight matrices $\mathbf{W_a}(k)$. Obviously, both $\mathbf{G_a}$ and $\overline{\mathbf{W}}_\mathbf{a}$ have finite elements.

Let the set $\left\{\mathbf{W}_a(n),\mathbf{W}_a(n+1),\cdots,\mathbf{W}_a(n+T\text{-}1)\right\}$ denote the weight matrices corresponding to the dynamic sub-graphs $G_a(k)$ at discrete times $k\in[n,n+T)$. By the definition in(13), we know that $\mathbf{W}_a(k)$ is a (row) stochastic matrix, with the diagonal entries $W_{aii}(k)$ always being strictly positive [23]. Thus, the matrix product

$$\Pi_{k=n}^{n+T-1}\mathbf{W}_a(k)=\mathbf{W}_a(n+T\text{-}1)\cdots\mathbf{W}_a(n+1)\mathbf{W}_a(n)$$

is a stochastic matrix with positive diagonal entries[24]. Also, from(13), $\mathbf{W}_a(k)$ is nonnegative, with all its entries $W_{aij} \geq 0$. Then, as proved by [25], we can get:

$$\Pi_{k=n}^{n+T-1}\mathbf{W}_a(k) \geq \mu \sum_{k=n}^{n+T-1}\mathbf{W}_a(k) \tag{20}$$

where $\mu > 0$ can be specified from matrices $\mathbf{W}_a(k)$ [25]. If the union $U_{k=n}^{n+T-1}G_a(k)$ has a spanning tree, then the directed graph corresponding to the matrix summation $\sum_{k=n}^{n+T-1}\mathbf{W}_a(k)$ also has a spanning tree, which in turn implies that the matrix product $\Pi_{k=n}^{n+T-1}\mathbf{W}_a(k)$ will also have a spanning tree [24].

As represented in [23], all eigenvalues of $\mathbf{W}_a(k)$ lie in the range of $(-1,1]$, with 1 being a trivial eigenvalue. According to lemmas 3.5 and 3.7 in [24], $\mathbf{W}_a(k)$ will be stochastic, indecomposable, and aperiodic (SIA). That is, $\lim_{n\to\infty}\mathbf{W}_a^n(k) = \mathbf{1}\mathbf{v}^T$, where $\mathbf{v}$ is some negative column vector satisfying $\mathbf{W}_a^T(k)\mathbf{v} = \mathbf{v}$ and $\mathbf{1}^T\mathbf{v} = 1$ [24]. Further, with the help of lemma 3.2 in [24], we can derive that the matrix product $\Pi_{k=n}^{n+T-1}\mathbf{W}_a(k)$ is also SIA. Then, there exists some column vector $\mathbf{y}$ such that:

$$\lim_{T\to\infty}\Pi_{k=n}^{n+T-1}\mathbf{W}_a(k) = 1\mathbf{y}^T \tag{21}$$

Therefore, a consensus can be asymptotically achieved through the proposed scheme with very weak long-term connectivity of the graph union required.

Intuitively, if the collection of authentic sub-graphs associated with the proposed scheme is strongly connected during information exchange, a consensus can be guaranteed at all authentic SUs. Essentially, such connectivity means that any two authentic SUs can directly or indirectly exchange their sensing results for sufficiently long duration [18]. Of course, in practice, even if the consensus-based scheme can reliably exclude attackers as soon as possible, some authentic users will inevitably be partially impacted by the malicious reports. In very rare cases, some might even be excluded as attackers by mistake due to the limitations of the anti-attack techniques. In addition, because of the sensing-time constraints, the iteration might be compelled to stop before reaching any acceptable consensus, which may also lead to a wrong decision at some SUs. However, allowing for these few exceptions, the proposed scheme generally still ensures that most authentic SUs converge to some common state with tolerable differences between them.

3.3 Sensing Performance Analysis

Because of the randomness of attacker's partial negative effects, it is very difficult to represent theoretically the exact cooperative sensing performance of the proposed scheme with closed forms. However, it can be approximated numerically by the average performance of all authentic SUs (see the simulation results in subsection 4.3).

It is obvious that the earlier real attackers are excluded, the less destruction authentic users will confront, thereby obtaining better sensing performance. Ideally, if the iteration time is sufficient, and if partial negative effects can be ignored, a common value will be reached as the final decision statistic by all authentic SUs:

$$x^* = \frac{1}{N_a}\sum_{j\in V_a} x_j(0) = \frac{1}{N_a}\sum_{j\in V_a} Y_j = \frac{1}{N_a}Y_0 \tag{22}$$

where N_a is the number of authentic SUs and $Y_0 = \sum_{j\in V_a} Y_j$ can be understood as the equal gain combination (EGC) test statistic of all authentic SUs [4]. It has been derived that the sum of N_a independent chi-square random variables is another chi-square variate [26], so, from (2):

$$Y_0 = \sum_{j\in V_a} Y_j \sim \begin{cases} \chi^2_{2mN_a}, & H_0 \\ \chi^2_{2mN_a}\left(2m\sum_{j\in V_a}\gamma_j\right), & H_1 \end{cases} \tag{23}$$

Thus, over an AWGN channel, the collective probabilities of false alarm and detection can be derived as [5]:

$$Q_f = P\left\{x^* > \lambda_c \mid H_0\right\} = P\left\{\sum_{j\in V_a} Y_j > N_a\lambda_c \mid H_0\right\} = 1-\Gamma\left(\frac{N_a\lambda_c}{2}, mN_a\right), \tag{24}$$

$$Q_d = P\left\{x^* > \lambda_c \mid H_1\right\} = P\left\{\sum_{j\in V_a} Y_j > N_a\lambda_c \mid H_1\right\} = Q\left(\sqrt{2m\sum_{j\in V_a}\gamma_j}, \sqrt{N_a\lambda_c}, mN_a\right) \tag{25}$$

where $Q(\cdot,\cdot,\cdot)$ and $\Gamma(\cdot,\cdot)$ denote the Marcum Q-function and the incomplete gamma function, respectively, with the definitions used in Matlab2009b [27]:

$$Q(a,b,m) = \int_b^\infty \frac{x^m}{a^{m-1}} \exp\left(-\frac{x^2+a^2}{2}\right) I_{m-1}(ax)\,dx\,, \tag{26}$$

$$\Gamma(x,a) = \frac{1}{\Gamma(a)}\int_0^x e^{-t}t^{a-1}dt\,, \tag{27}$$

and $\Gamma(a)$ is the gamma function $\Gamma(a) = \int_0^\infty e^{-t}t^{a-1}dt$.

Further, over fading channels, the corresponding average probability of detection is obtained by integrating (25) over the distribution of $\gamma_0 = \sum_{j\in V_a}\gamma_j$, that is:

$$\overline{Q}_d = \int_{\gamma_0} Q_d(x) f_{\gamma_0}(x)\,dx \tag{28}$$

where $f_{\gamma_0}(x)$ is the PDF of γ_0.

However, in practice, considering the unavoidable partial negative impacts from attackers and the sensing-time constraints, the variable matrix $\mathbf{W}(k)$ is, in general, not doubly stochastic. Thus, the final tolerable consensus of all authentic SUs is expected to deviate from the average value of their initial states to some extent. Moreover, in rare cases, some authentic users even might be mistaken as attackers, which will directly deteriorate the collective performance. Therefore, the expressions in (24)-(28) can only be regarded as the upper bounds for the proposed scheme's sensing performance in ideal cases.

3.4 Other Consensus-Based Schemes

Before continuing the simulation, we will introduce two existing consensus-based schemes, which we term for short the Basic scheme [12] and Yu scheme [18].

Basic scheme: This is the prototype of all consensus-based CSS schemes. All cooperative SUs are assumed to report honestly, and each updates the state only by the following iteration rule, without any anti-attack consideration [12]:

$$x_i(k+1) = x_i(k) + \varepsilon\sum_{j\in Ne_i(k)} a_{ij}\left(x_j(k) - x_i(k)\right) \tag{29}$$

where ε is the step size ranged in $0 < \varepsilon < 1/\Delta$, with Δ being the maximum degree of the graph.

Yu scheme: In this scheme, each authentic user directly excludes the link neighbor whose current report has the most deviation from the last mean value of the neighborhood and then iterates with the same rule as (29) [18].

Similarly, [19] has verified that rule (29) can guarantee a consensus by all cooperating users with an exponential rate of convergence. It is obvious that the Basic scheme can hardly counter any SSDF attacks. Although some initial attempts have been made in the Yu scheme [18], its effectiveness in countering these attacks is very limited, even sometimes resulting in unintentional fatal consequences, as we will show by simulation in Section 4. What should be especially noted is that, in practical implementation, it is difficult for each SU in both of these schemes to obtain prior knowledge of the network's maximum degree. Thus, we use an alternative rule based on Metropolis weights [23] as given in (14), by which each SU only needs to know the degrees of its neighbors to determine its next state. Besides that, the existing schemes never touch the sensing-time constraints, a problem that is addressed properly in the proposed scheme. Even if the time duration for local sensing or information exchange is insufficient, each authentic user can still obtain a final decision individually, though the collective sensing performance of the whole CRN might deteriorate to some extent. To minimize this deterioration, a novel MAC-layer sensing mechanism should be designed to optimize the sensing time before this scheme is implemented, though designing such a mechanism is outside the scope of this paper.

4. Simulation Results and Discussion

To evaluate its performance, this section will compare the proposed scheme with the two pre-existing schemes above. The simulations will concern the aspects of convergence and sensing performance.

4.1 Simulation Setup

We study a decentralized CRN, where the sensing channels of all SUs are modeled as quasi-static, flat, Suzuki fading channels [28] without any spatial correlation. Thus, the channel gains only vary from sensing period to sensing period, and the instantaneous SNR of any SU can be represented statistically as [28]:

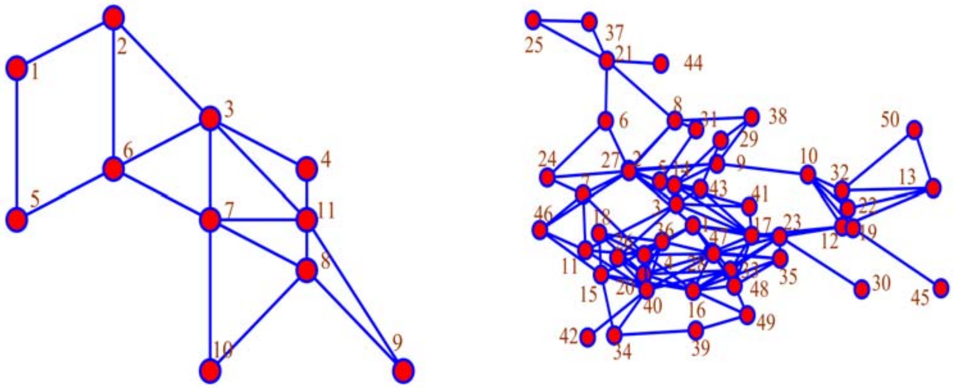
$$\gamma_{dB} = \overline{\gamma}_{dB} + Shadow_{dB} + Fading_{dB} \tag{30}$$

where the three terms in dB on the right denote the mean SNR, the shadowing (also called large-scale fading) effects, and the small-scale fading effects, respectively. In our simulations, the relative distances between any two SUs are assumed to be much smaller than their distances to the PU; thus, all SUs experience I.I.D channel effects, with the same $\overline{\gamma}_{dB} = 5\text{dB}$. Further, the shadowing effects are assumed to be log-normally distributed with the power-spread factor set as $\sigma_{dB} = 8\text{dB}$, and small-scale fading is modeled as Rayleigh fading for simplicity.

For each SU, energy detection is performed individually with the same time-bandwidth product $m = 5$, and we directly produce the output energy of each SU according to (2). The maximum number of iterations for local-information exchange in the second step is set to be 200, and the tolerance between the final states of any two SUs is set to be less than 0.1dB if consensus has been reached. For the simulations of the Basic and Yu schemes, all SUs are assumed to know the maximum degree of the network, and the step size is set to $\varepsilon = 0.99 / \Delta$.

4.2 Convergence Simulation

In the first part of our simulations, we consider two example topologies of CRNs to investigate the convergence of these three consensus-based schemes under different SSDF attacks. As shown in **Fig. 3 (a)** and **(b)**, both are modeled as connected graphs $G = (V, E)$. For simplicity, we assume that $a_{ij} = 0/1$ and that all edges have the same weight. The topology in **Fig. 3-(a)** denotes a CRN composed of 11 SUs and 18 links, while that in **Fig. 3-(b)** corresponds to a CRN with 50 SUs and 120 links. Four different scenarios are discussed: no attacker, one attacker, two attackers, and more than two attackers. For each scenario, 100,000 trials have been performed, and the threshold for making the final decision was set to $\lambda_c = 13.4$. Three indicators are defined to evaluate these three schemes. The failure ratio (FR) is the percentage of the cases in all trials in which more than 10% authentic SUs deviated from any one of the others by more than 0.1dB difference. This is used for assessing the extent of convergence failure. The time ratio (TR) is defined as the average proportion of the given iteration times that were required for more than 90% of authentic SUs to reach a tolerant consensus. Thus, TR well reflects the convergence speed. The third measurement is the attack-proof ratio (APR). It corresponds to the average percentage of the cases in all trials in which more than 90% of authentic SUs still made the right decisions when some attackers were present.



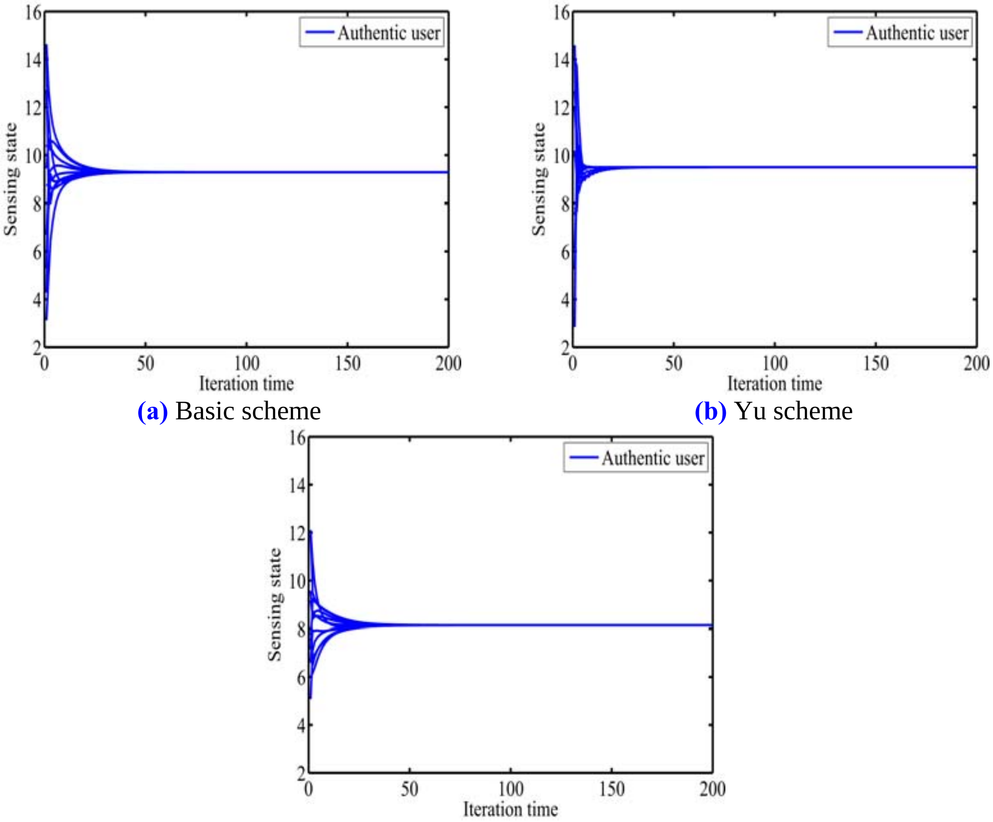
(a) 11 SUs and 18 links **(b)** 50 SUs and 120 links

Fig. 3. Two examples of the CRN topology

Table 1. Convergence comparison in the first topology when there are no attackers

Schemes	**Topology 1**		**Topology 2**	
	FR (%)	**TR (%)**	**FR (%)**	**TR (%)**
Basic	0	12.5	0	34.3
Yu	3.7	5.9	51.9	26.0
Proposed	2.1	10.5	7.4	36.2

We start with the simplest scenario, the one in which there are no attackers. As shown in the left part of **Table 1**, by 100,000 trials in the first topology, the Basic scheme can always guarantee an average consensus of the initial states, while both of the other schemes have some probability of convergence failure. In terms of convergence speed, the Yu scheme performs best, with only 11 iterations required on average before a tolerable consensus can be reached. The Basic and the proposed schemes need about 25 and 21 iteration times to reach consensus, respectively, or 12.5% and 10.5% of the given 200 iteration times. This is mainly because the Yu scheme directly excludes the neighbor with the maximum average deviation in any iteration, rapidly reducing the number of authentic links. For a random trial, **Fig. 4 (a)**, **(b)** and **(c)** depict the states of all 11 SUs in the first topology during the iteration process under H_0 in each of these three schemes, respectively. Similar results were obtained in the second topology. From the right part of **Table 1**, we can observe that all three schemes in the second topology required more iteration times to reach an acceptable consensus, and the failure ratio grew quickly in both the Yu scheme and the proposed scheme, since the probability that a single user will be mistaken as an attacker rises with the increasing scale of the network.



(a) Basic scheme

(b) Yu scheme

(c) The proposed scheme

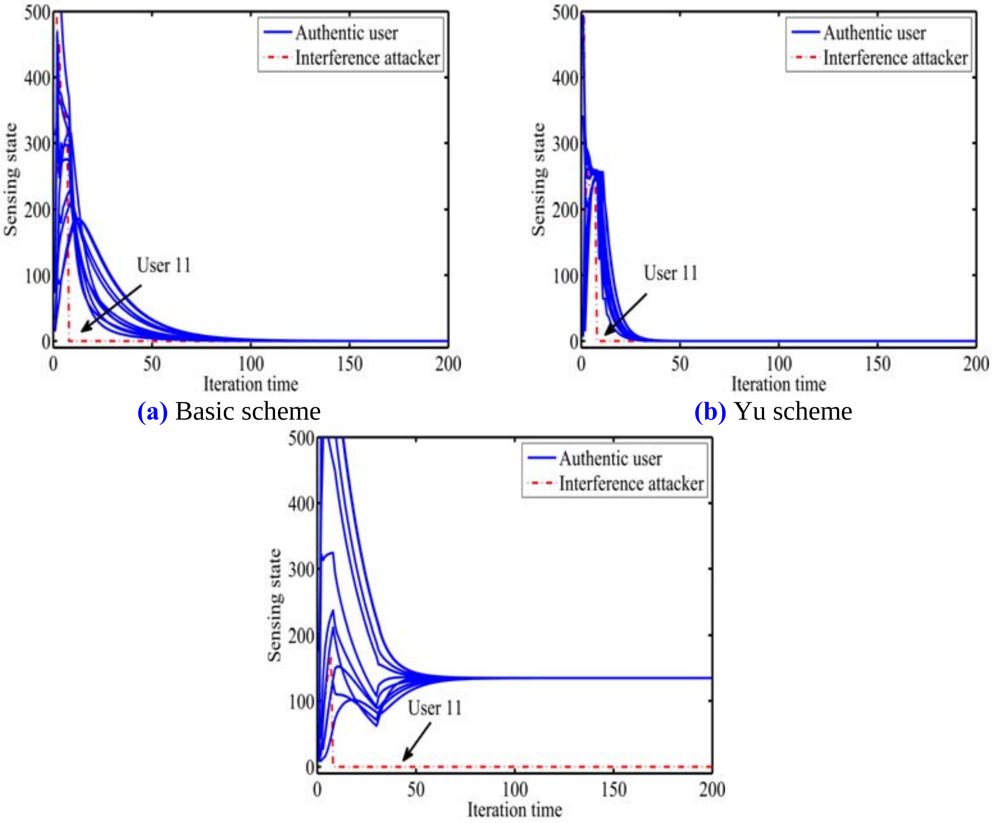
Fig. 4. Iteration process of all 11 SUs under H_0 by different consensus-based schemes when there are no any attackers in the CRN with the first topology

In the second scenario, one malicious user is assumed to be present in the CRN. Taking the first topology as an example, suppose the 11th SU is a malicious user who can launch SSDF attacks using the three models mentioned in Section 2. For a selfish attack, the 11th SU always reports '80' under H_0. Meanwhile, for an interference attack, it reports the invariable state '1' under H_1, and for a confusing attack, it sends a random report between [0, 10m] under H_0. All three attacks in this scenario are assumed to begin from the 8th iteration. **Table 2** lists the comparison between the three schemes in terms of the three indicators under different SSDF attack models, where time-ratio measurements greater than 100 % indicate that no tolerable convergence could be reached in any trial. It is clear that the proposed scheme can protect authentic users from all three types of SSDF attack, guaranteeing a consensus in most cases, while the other two schemes are very likely to confront fatal errors. In particular, under a confusing attack, both the Basic and Yu schemes hardly even converge over a very long time;

both have poor robustness against this model of attack. Such results are not surprising. The Basic scheme takes no consideration of sensing security, and the Yu scheme frequently fails to reject the real malicious user since the attacker-exclusion rule is too rough. This results in the whole network moving towards the false or confusing states generated by the attacker. To exemplify the proposed scheme's capability for excluding SSDF attacks, **Fig. 5** depicts the iteration process of all 11 SUs in a random trial of each of these three schemes when the 11th SU launches an interference attack.

Table 2. Convergence comparison in the first topology when there is one attacker

Schemes	Selfish attack			Interference attack			Confusing attack		
	FR (%)	TR (%)	APR (%)	FR (%)	TR (%)	APR (%)	FR (%)	TR (%)	APR (%)
Basic	0	41.5	0	0	85.5	0	100	100^+	0
Yu	4.5	27.0	2.5	3.8	61.0	1.1	100	100^+	0.5
Proposed	2.5	12.5	80.2	2.7	23.5	78.7	2.1	11.5	81.8



(a) Basic scheme

(b) Yu scheme

(c) The proposed scheme

Fig. 5. Iteration process of all 11 SUs under H_1 by different consensus-based schemes when there is one interference attacker in the CRN with the first topology

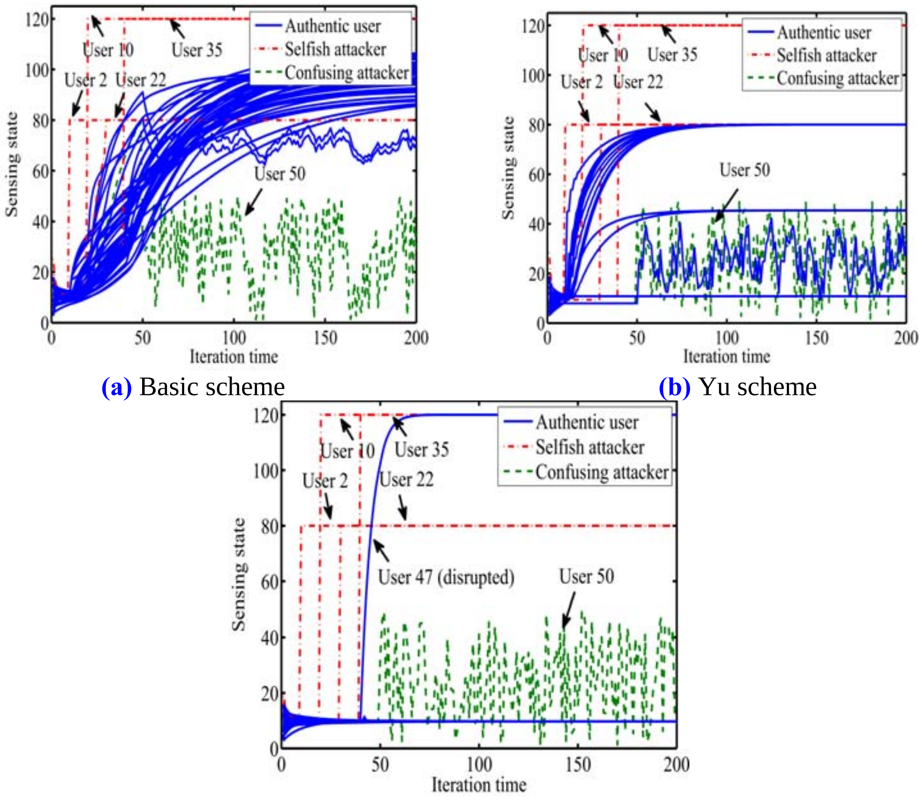
In the third scenario, we consider the case of two attackers. Within the first topology, the 5th and 11th SUs are assumed to launch SSDF attacks beginning with the 10th and 20th iterations, respectively. **Table 3** compares the indicators for each of the three schemes under different combinations of attack models used by these two malicious users. The condition '2 Selfish' means that users 5 and 11 always send ‘80’ and ‘120’ when attacking, respectively. ‘2 Interference’ represents the case that they always report ‘1’ and ‘3’, respectively, while ‘Selfish and Confusing’ denotes a combined attack in which user 5 always sends ‘80’ and user 11 sends random reports ranged in [0,10m]. From this table, the Basic and Yu schemes are proven to be more vulnerable than they are in the one-attacker scenario, while the proposed scheme has almost the same, powerful resistance to attack.

Table 3. Convergence comparison in the first topology when there are two attackers

Schemes	**2 Selfish**			**2 Interference**			**Selfish & Confusing**		
	FR (%)	**TR (%)**	**APR (%)**	**FR (%)**	**TR (%)**	**APR (%)**	**FR (%)**	**TR (%)**	**APR (%)**
Basic	100	100$^+$	0	100	100$^+$	0	100	100$^+$	0
Yu	100	100$^+$	0.5	100	100$^+$	0.1	100	100$^+$	0.1
Proposed	2.8	9.0	81.6	5.7	20.1	76.5	2.4	15.1	82.5

Table 4. Convergence comparison in the second topology when there are more than two attackers

Schemes	**FR (%)**	**TR (%)**	**APR (%)**
Basic	100	100$^+$	0
Yu	100	100$^+$	0
Proposed	11.1	38.0	77.2



(a) Basic scheme **(b)** Yu scheme

(c) The proposed scheme

Fig. 6. Iteration process of all 50 SUs under H_0 by different consensus-based schemes when there are more than two attackers in the CRN with the second topology

We have also done some simulations with more than two attackers in the second topology, in which the users with the numbers 2, 10, 22, and 35 launch selfish attacks beginning with the 10th, 20th, 30th and 40th iterations and with invariable malicious reports ‘80’, ‘120’, ‘80’, and ‘120’, respectively. In addition, user 50 begins its confusing attack from the 50th iteration, with a random report in the range [0, 10m]. Similarly, from **Table 4** and **Fig. 6**, we can observe that the proposed scheme can successfully exclude these attacks, too, from the network in most cases, while the other two schemes always fail to counter them.

4.3 Sensing-Performance Simulation

For the second part, we further studied the sensing performance of the proposed scheme. The scenarios of no attacker, one attacker, and two attackers were considered. In each scenario, 100,000 trials were performed in random topologies with 11 SUs and 18 links, each topology similar to that shown in **Fig. 3-(a)**.

Fig. 7 plots the curves of the complementary receiver operating characteristics (CROC) for the three consensus-based schemes when there are no attackers. The numerical result under perfect conditions calculated from (24) and (28) is also shown, which indeed provides a theoretical upper bound for these three schemes. Of note is that the performance of the Basic scheme is pretty close to the theoretical upper bound, since this scheme can always guarantee an average consensus for the initial states. The deviation of the other two schemes from the upper bound is mainly caused by the constraints of the anti-attack strategies. Both trade some performance for robustness against potential SSDF attacks. In addition, the CROC curves of the three typical, centralized-fusion schemes based on the OR [5][21], MAJOR [21], and AND rules [21] are plotted in this figure. Obviously, without any attackers, the proposed and the OR-rule-based schemes have similar sensing performance, and they both outperform all others except the Basic scheme.

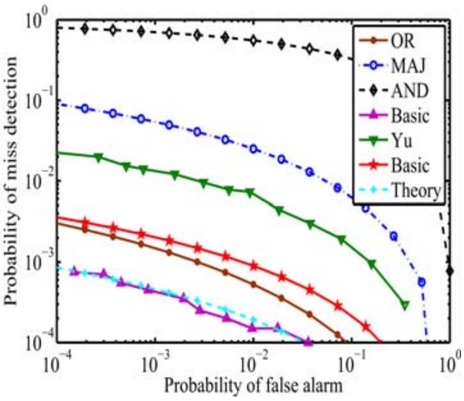
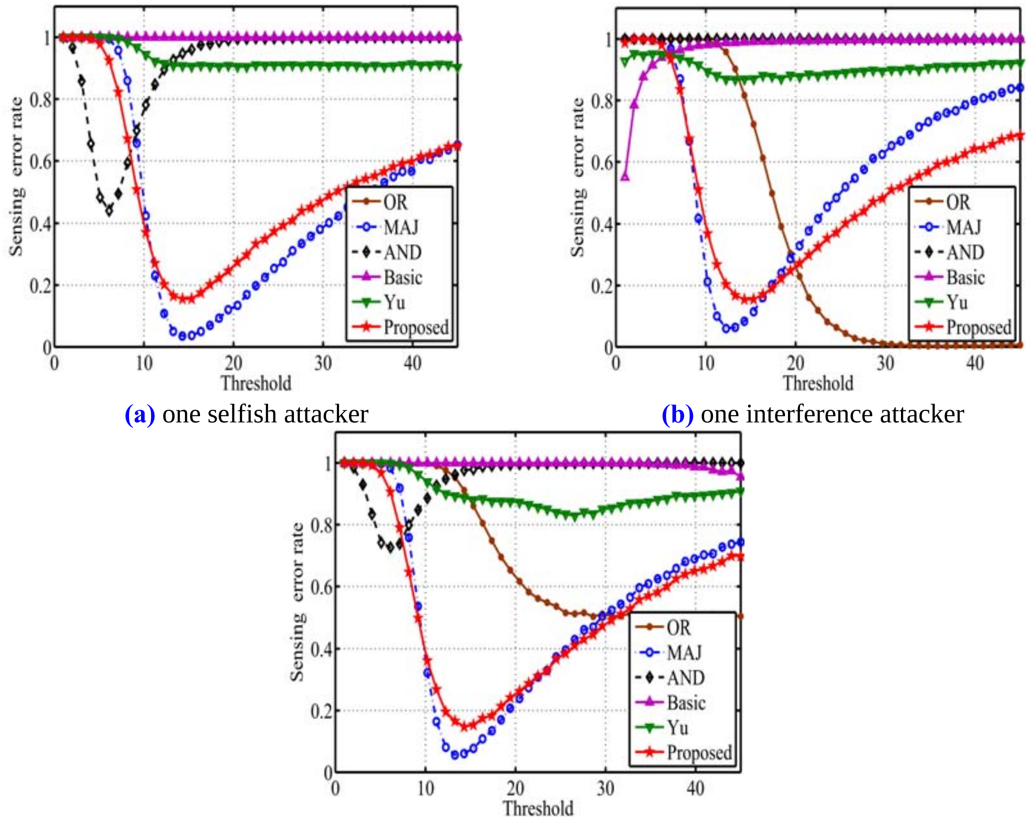


Fig. 7. CROC curves of three consensus-based schemes and three centralized fusion schemes based on typical *K* out of *N* fusion rule when there are no any attackers

If there are several attackers in the CRN, some of the above six schemes will confront fatal sensing errors. We thus use the total error rate (i.e., $Q_f + Q_m$) instead of the CROC curve to evaluate their robustness against SSDF attacks. In each trial, all malicious users are supposed to launch their attacks at a random iteration time ranged in [1, 50]. **Fig. 8** depicts the average error rates for all six schemes given different detection thresholds in 100,000 trials for which there is one attacker, with the subplots **(a)**, **(b)**, and **(c)** corresponding to the three different attack models. As indicated by this figure, among these schemes, only the proposed and the MAJOR-rule-based schemes can generally effectively defend CSS against all three attack models, while both the Basic and the Yu schemes are very vulnerable to any model of attack. It can be further observed that the OR-rule-based scheme is particularly sensitive to selfish attack, and the AND-rule-based scheme will be invalidated by interference attack.



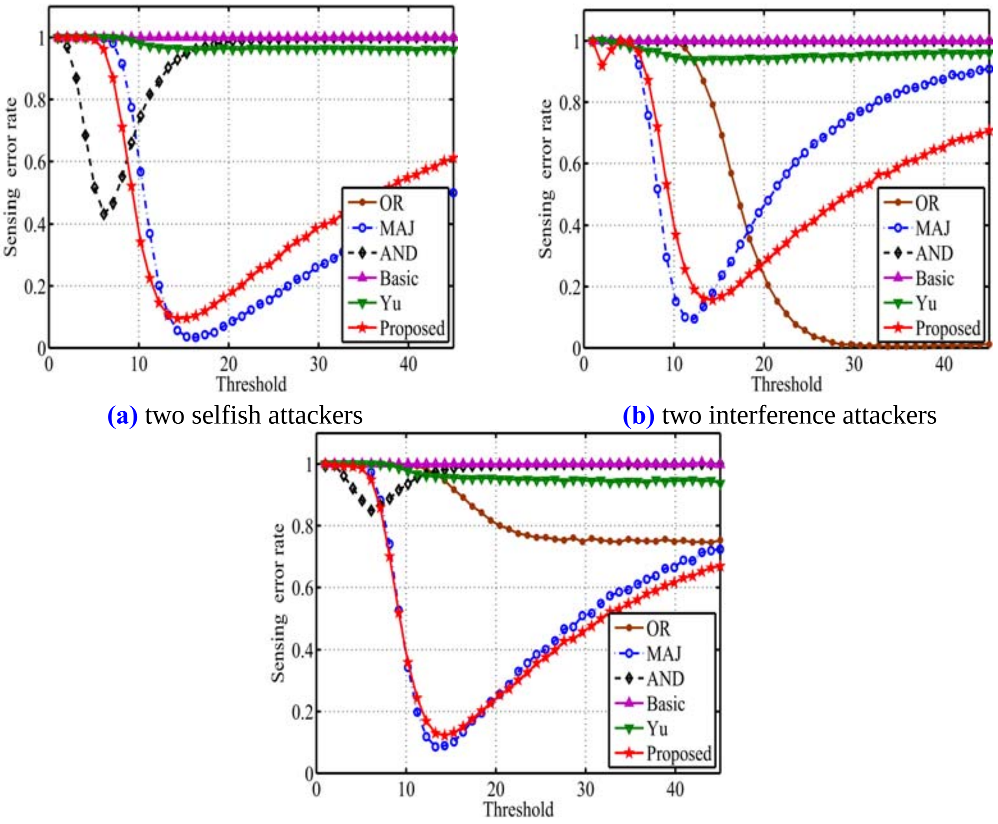
(a) one selfish attacker

(b) one interference attacker

(c) one confusing attacker

Fig. 8. The average error rates of all six schemes for different detection thresholds when there is one attacker

Similarly, corresponding results in the cases in which there are two selfish attackers, two interference attackers, or two confusing attackers are shown in **Fig. 9 (a)**, **(b)**, and **(c)**, respectively. Compared with the results in **Fig. 8**, as the number of malicious users increases, the robustness of the proposed scheme changes unremarkably in all three cases. The Basic scheme still has no resistance to attack, while the robustness of the other schemes may obviously deteriorate in certain cases. Furthermore, the sensing error rates of these schemes under different combined attacks are investigated. As expected, in all cases, the proposed and the MAJOR-rule-based schemes remain the best choices for defending the authentic SUs against attacks. With the Basic or Yu schemes, the whole network will face severe disruption. In particular, the OR-rule-based scheme is bound to end with sensing errors in the case of a ‘Selfish and Confusing’ attack, while the AND-rule-based scheme is invalidated by an ‘Interference and Confusing’ attack.



(a) two selfish attackers

(b) two interference attackers

(c) two confusing attackers

Fig. 9. The average error rates of all six schemes for different detection thresholds when there are two attackers

5. Conclusions and Future Work

In this paper, we have presented a secure, consensus-based CSS scheme to counter SSDF attacks in decentralized CRNs. Utilizing the notion of bio-inspired consensus, each cooperating user can individually make a final decision based solely on the local exchange of information within its neighborhood, rather than using any centralized control or fusion. To defend authentic users against three potential models of SSDF attack, we have introduced some attacker-exclusion techniques in the proposed scheme to proactively identify and reject any false or confusing reports given by malicious users during information exchange. Considering the practical implementation, we have replaced the traditional consensus iteration rule with another strategy based on Metropolis weights, so that each user no longer requires any prior knowledge of the whole network. Extensive simulation results have shown that the proposed scheme outperforms several existing solutions in terms of robustness against different SSDF attacks.

Some interesting issues on this topic for further research include MAC-layer sensing mechanisms, detailed protocols for information exchange, and more robust schemes for countering SSDF attacks when link failure occasionally occurs in the network because of mobility, fading, or power constraints.

References

[1] FCC, "ET Docket No. 03-222, Notice of proposed rulemaking and order," Federal Communications Commission, Washington, D.C., 2003.

[2] Q. Liu, J. Gao, J. Guan and Y. Guo, "A survey on linker layer key technologies in cognitive radio networks (in Chinese)," *Telecommunication Engineering*, vol. 50, no. 3, pp. 90-98, 2010.

[3] H. Urkowitz, "Energy detection of unknown deterministic signals," in *Proc. of IEEE*, vol. 55, no. 4, pp. 523-531, 1967. Article (CrossRef Link)

[4] F. F. Digham, M. Alouini and M. K. Simon, "On the energy detection of unknown signals over fading channels," in *Proc. of IEEE International Conf. on Communications*, Alaska, USA, pp. 3575-3579, 2003. Article (CrossRef Link)

[5] A. Ghasemi and E. S. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," *Journal of Communications (JCM)*, vol. 2, no. 2, pp. 71-82, 2007. Article (CrossRef Link)

[6] B. Shen, S. Ullah and K. Kwak, "Deflection coefficient maximization criterion based optimal cooperative spectrum sensing," *AEU - International Journal of Electronics and Communications*, vol. 64, no. 9, pp. 819-827, 2010. Article (CrossRef Link)

[7] B. Shen and K. S. Kwak, "Soft combination schemes for cooperative spectrum sensing in cognitive radio networks," *ETRI Journal*, vol. 31, no. 3, pp. 263-270, 2009. Article (CrossRef Link)

[8] J. Ma and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," in *Proc. of IEEE Global Telecommunications Conf., GLOBECOM*, Washington, DC, USA, pp. 3139-3143, 2007. Article (CrossRef Link)

[9] J. Shen, S. Liu, L. Zeng, G. Xie, J. Gao and Y. Liu, "Optimisation of cooperative spectrum sensing in cognitive radio network," *IET Communications*, vol. 3, no. 7, pp. 1170-1178, 2009. Article (CrossRef Link)

[10] D. Oh and Y. Lee, "Cooperative spectrum sensing with imperfect feedback channel in the cognitive radio systems," *International Journal of Communication Systems*, vol. 23, no. 3, pp. 763-779, 2010. Article (CrossRef Link)

[11] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, Part II: multiuser networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2214-2222, 2007. Article (CrossRef Link)

[12] Z. Li, F. R. Yu and M. Huang, "A cooperative spectrum sensing consensus scheme in cognitive radios," in *Proc. of IEEE Communications Society Conference on Computer Communications*, Leblon, Brazil, pp. 2546-2550, 2009. Article (CrossRef Link)

[13] F. R. Yu, M. Huang and H. Tang, "Biologically inspired consensus-based spectrum sensing in mobile ad Hoc networks with cognitive radios," *IEEE Networks*, no. May/June, pp. 26-30, 2010. Article (CrossRef Link)

[14] R. Chen, J. Park, Y. T. Hou and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 50-55, 2008. Article (CrossRef Link)

[15] R. Chen, J. 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, 2008. Article (CrossRef Link)

[16] R. Chen, J. Park and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. of IEEE Communications Society Conf. on Computer Communications*, Phoenix, AZ, USA, pp. 31-35, 2008. Article (CrossRef Link)

[17] H. Li and Z. Han, "Catching attacker(s): for collaborative spectrum sensing in cognitive radio systems: an abnormality detection approach," in *Proc. of IEEE Symposium on New Frontiers in Dynamic Spectrum*, Singapore, pp. 1-12, 2010. Article (CrossRef Link)

[18] 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 IEEE Military Communications Conf., MILCOM*, Boston, MA, USA, pp. 1-7, 2009. Article (CrossRef Link)

[19] R. Olfati-Saber, J. A. Fax and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," in Proc. *Proc. of the IEEE*, vol. 95, no. 1, pp. 215-233, 2007. Article (CrossRef Link)

[20] A. Ghasemi and E. S. Sousa, "Optimization of spectrum sensing for opportunistic spectrum access in cognitive radio networks," in *Proc. of 4th Annual IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, USA, pp. 1022-1026, 2007. Article (CrossRef Link)

[21] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: requirements, challenges and design trade-offs," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 32-39, 2008. Article (CrossRef Link)

[22] H. Kim and K. G. Shin, "Efficient discovery of spectrum opportunities with MAC-layer sensing in cognitive radio networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 5, pp. 533-545, 2008. Article (CrossRef Link)

[23] X. Lin, S. Boyd and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in *Proc. of 4th International Symposium on Information Processing in Sensor Networks, IPSN*, Los Angeles, USA, pp. 63-70, 2005. Article (CrossRef Link)

[24] W. Ren and R. W. Beard, "Consensus seeking in multiagent systems under dynamically changing interaction topologies," *IEEE Transactions on Automatic Control*, pp. 655-661, 2005. Article (CrossRef Link)

[25] A. Jadbabaie, J. Lin and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Transactions on Automatic Control*, vol. 48, no. 6, pp. 988-1001, 2003. Article (CrossRef Link)

[26] J. G. Proakis, "Digital Communications (Fourth Edition)," New York: MCGraw-Hill, 2001.

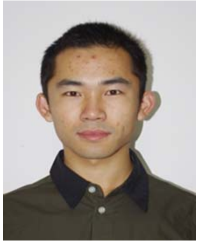
[27] M. Abramowitz and I. A. Stegun, "Handbook of Mathematical Functions, National Bureau of Standards, Applied Math. Series #55," New York: Dover Publications, 1965. Article (CrossRef Link)

[28] S. Kyperountas, N. Correal, Q. Shi and Z. Ye, "Performance analysis of cooperative spectrum sensing in suzuki fading channels," in *Proc. of 2nd International Conf. on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom*, Orlando, USA, pp. 428-432, 2007. Article (CrossRef Link)

Quan Liu, Student Member, IEEE, received the B.S. degree in Communication Engineering from Naval University of Engineering, Wuhan, China, in 2006. Since 2008, he has been with the Software Radio Lab, Naval University of Engineering, where he is a Ph.D. candidate. His current interests include the key technologies in the Link Layer of cognitive radio network and multirate signal processing.

Jun Gao received the B.S. degree in Communication Engineering from Naval Electronic College of Engineering, in 1982, and the Ph.D. degree in Electronic Engineering from Beijing Institute of Technology in 1989. Since 1996, he has been a professor at Naval University of Engineering, and his research interests are digital communications and software radio systems.

Yunwei Guo received the B.S. degree in Communication Engineering from Naval University of Engineering, Wuhan, China, in 2004. Since 2008, he has been with the Software Radio Lab, Naval University of Engineering, where he is a Postgraduate. His current interest is spectrum sensing technology in cognitive radio network.



Siyang Liu received the B.S. degree in Underwater Acoustic Engineering from Harbin Engineering University, Heilongjiang, China, in 2009. Since 2009, he has been with the Software Radio Lab, Naval University of Engineering, as a Postgraduate. His current interest is dynamic spectrum allocation in cognitive radio network.