EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

# A robust cooperative spectrum sensing scheme based on Dempster-Shafer theory and trustworthiness degree calculation in cognitive radio networks

Jinlong Wang, Shuo Feng*, Qihui Wu, Xueqiang Zheng, Yuhua Xu and Guoru Ding

**Abstract**

Cognitive radio (CR) is a promising technology that brings about remarkable improvement in spectrum utilization. To tackle the hidden terminal problem, cooperative spectrum sensing (CSS) which benefits from the spatial diversity has been studied extensively. Since CSS is vulnerable to the attacks initiated by malicious secondary users (SUs), several secure CSS schemes based on Dempster-Shafer theory have been proposed. However, the existing works only utilize the current difference of SUs, such as the difference in SNR or similarity degree, to evaluate the trustworthiness of each SU. As the current difference is only one-sided and sometimes inaccurate, the statistical information contained in each SU's historical behavior should not be overlooked. In this article, we propose a robust CSS scheme based on Dempster-Shafer theory and trustworthiness degree calculation. It is carried out in four successive steps, which are basic probability assignment (BPA), trustworthiness degree calculation, selection and adjustment of BPA, and combination by Dempster-Shafer rule, respectively. Our proposed scheme evaluates the trustworthiness degree of SUs from both current difference aspect and historical behavior aspect and exploits Dempster-Shafer theory's potential to establish a 'soft update' approach for the reputation value maintenance. It can not only differentiate malicious SUs from honest ones based on their historical behaviors but also reserve the current difference for each SU to achieve a better real-time performance. Abundant simulation results have validated that the proposed scheme outperforms the existing ones under the impact of different attack patterns and different number of malicious SUs.

**Keywords:** Cognitive radio networks; Cooperative spectrum sensing; Security; Dempster-Shafer theory; Trustworthiness degree calculation

## 1. Introduction

Due to the static licensing and allocation strategies, current spectrum regulation has resulted in extreme scarcity of available spectrum, while plenty of radio frequencies are actually unused temporally/geographically [1]. Motivated by the need for flexible management and efficient utilization of spectrum resources, cognitive radio (CR) is brought up and has been regarded as one of the most promising technologies [2]. CR enables secondary users (SUs) to access a spectrum band when it is not occupied by the primary user (PU). Different from traditional wireless networks, cognitive radio network (CRN) is able to (i) perceive and understand the surrounding environment, (ii) make intelligent decisions to optimize operating parameters (such as carrier frequency, transmission power, and network protocol), and (iii) reconfigure the network according to the environment situations [3,4]. Therefore, as a fundamental component in CR technology, reliable and efficient spectrum sensing is very important for the realization of CRN [5].

Among others, one crucial challenge in spectrum sensing is the hidden terminal problem [6], which occurs when SU is under deep shadowing or experiences multi-path fading. To deal with this problem, cooperative spectrum sensing (CSS) which makes benefit from the spatial diversity has been extensively studied [7-9]. In CSS, each SU performs the local spectrum sensing individually at first and forwards

* Correspondence: fengshuo1010@gmail.com
College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China

its measurements to the fusion center (FC). FC then fuses those measurements to make the global decision about PU's activity. There are rich literatures (see, e.g., [10-12] and the references therein) that have established the optimality of likelihood ratio test (LRT) in the detection problems. Quan et al. [13] have proposed an optimal linear CSS scheme, which makes the global decision over a linear combination of the local measurements. It has reduced the computational complexity and can reach performance comparable to LRT-based optimal fusion rules. Besides, several CSS schemes based on Dempster-Shafer theory have also been proposed in recent years [14-18]. In [14], Dempster-Shafer theory is firstly adopted in the data fusion of CSS. This scheme quantifies the channel condition between PU and SUs with a parameter called credibility and applies Dempster-Shafer theory to combine the local measurements with its associated credibility. Nhan and Insoo [15] propose an enhanced CSS scheme based on Dempster-Shafer theory and reliability source evaluation. Different from [14], it utilizes the signal-to-noise ratios (SNRs) to evaluate the degree of reliability for SUs. The reliability weight of each SU is then applied to adjust its measurements before making the final decision.

Unfortunately, CSS is vulnerable to the attacks initiated by malicious SUs. For example, malicious SUs may falsify their local measurements to mislead FC, which will degrade the performance of CSS significantly. Therefore, effective secure mechanisms are essentially required in a hostile wireless environment. Han et al. [16] propose an enhanced Dempster-Shafer theory-based CSS scheme that tackles the spectrum sensing data falsification (SSDF) attack. Based on the assumption that malicious SUs' evidences are different from honest SUs', this scheme uses the similarity degree to calculate the reliability of evidences and removes the evidences with low similarity degree from the combination. Nhan and Insoo [17] propose another Dempster-Shafer theory-based secure CSS scheme, which utilizes robust statistics to estimate the distribution parameters of PU's activity and evaluates the reliability of SUs with a simple counting method. Besides, several detection thresholds are adopted to eliminate different kinds of malicious SUs. In [18], a trusted CSS scheme for mobile CRNs is proposed. It utilizes the location reliability parameter to improve PU detection and improves malicious SU detection using both location reliability and Dempster-Shafer theory.

However, most of the existing Dempster-Shafer theory-based CSS schemes only utilize SUs' current difference, such as the difference in SNR or similarity degree, to evaluate the trustworthiness of each SU. Although this current difference can reflect SU's reliability to some extent, it is only one-sided and not always accurate, due to the dynamic character of wireless environment. Apart from the real-time information, the statistical information about SUs' historical behavior which reflects their past credibility should also be considered in the evaluation of trustworthiness. To the best of our knowledge, none of the existing works has studied the trustworthiness of SUs from both current difference and historical behavior at the same time. None of these works has exploited Dempster-Shafer theory's ability for reflecting uncertainty in the utilization of historical behavior, either.

Therefore, in this article, we propose a robust CSS scheme based on Dempster-Shafer theory and trustworthiness degree calculation. It is carried out in four successive steps, which are basic probability assignment (BPA), trustworthiness degree calculation, selection and adjustment of BPA, and combination by Dempster-Shafer rule, respectively. The main contributions of this article can be summarized as follows:

1. We propose to evaluate the trustworthiness degree of SUs from both current difference aspect and historical behavior aspect. Our proposed scheme not only differentiates malicious SUs from honest ones effectively based on their historical behaviors but also reserves the current difference for each SU to achieve a better real-time performance.
2. We establish a 'soft update' approach for each SU's reputation value maintenance by exploiting Dempster-Shafer theory's ability for reflecting uncertainty, based on each SU's historical reports. Besides, we consider a more general situation where the final decision is imperfect and thus adjust the relative status of decisions made by FC and SUs in the soft update process.
3. Our proposed scheme is easy for implementation. The reputation value maintenance can be performed in an iterative manner, which causes no additional computational complexity or storage cost. In addition, no prior knowledge such as the average SNR of each SU is needed at FC, which will reduce the communication overhead as well.

The rest of this article is organized as follows: Section 2 describes the system model. Section 3 proposes the robust CSS scheme based on Dempster-Shafer theory and trustworthiness degree calculation and discusses the four steps of this scheme in detail. In Section 4, numerical simulation results are presented. Finally, the conclusions are drawn in Section 5.

## 2. System model

In this section, we describe the scenario of CSS in CRNs and introduce two attack patterns considered in this article.

### 2.1 Cooperative spectrum sensing

As illustrated in Figure 1, we consider a CRN that consists of one PU, $n$ SUs, and one FC. At first, each SU

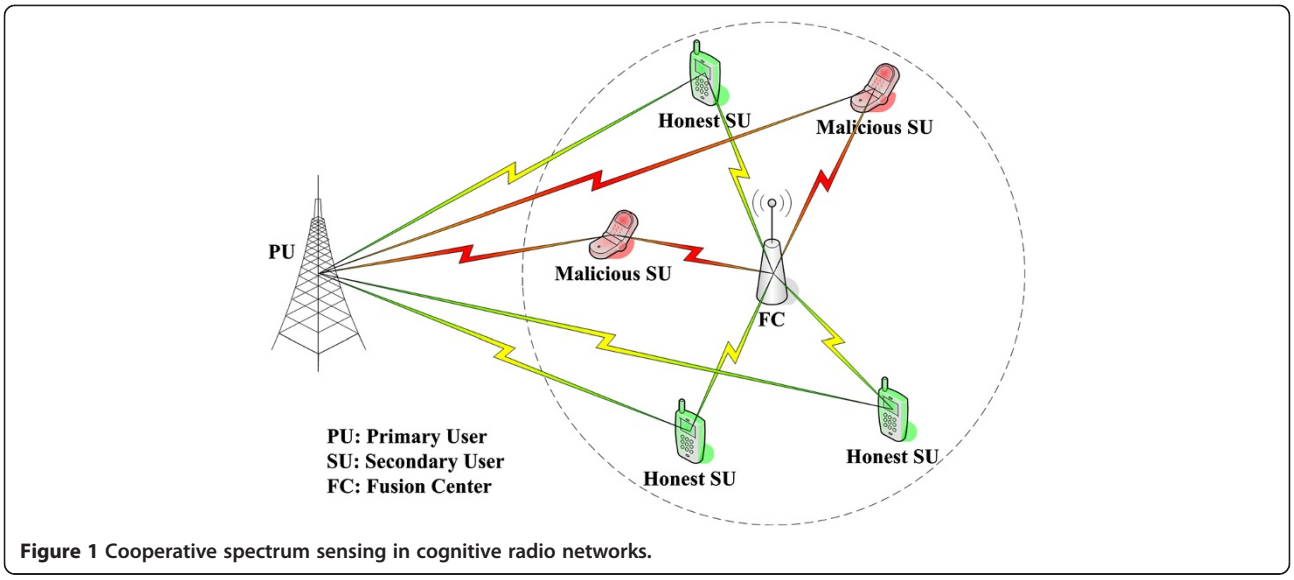


**Figure 1** Cooperative spectrum sensing in cognitive radio networks.

independently performs local spectrum sensing, which can be formulated as a binary hypothesis testing [6]:

$$x_i(t) = \begin{cases} n_i(t), & H_0 \\ h_i(t)s(t) + n_i(t), & H_1 \end{cases} \quad (1)$$

where $x_i(t)$ is the received signal at $SU_i$, $n_i(t)$ is the additive white Gaussian noise (AWGN), $h_i(t)$ is the amplitude gain of the sensing channel, and $s(t)$ is the signal transmitted by PU, respectively. $H_0$ represents that PU is inactive, and $H_1$ represents that PU is active. Without loss of generality, $s(t)$ and $n_i(t)$ are assumed to be independent.

We also make an assumption that energy detection method is employed by every SU in the local spectrum sensing phase. By applying a band-pass filter, the received energy at $SU_i$ can be measured by [19]

$$x_{E_i} = \sum_{j=1}^{N} |x_{ij}|^2 \quad (2)$$

where $x_{ij}$ is the $j$th sample of the received signal at $SU_i$. Besides, $N = 2TW$, and $TW$ is the time-bandwidth product. When $N$ is large enough (e.g., $N \geq 10$), $x_{E_i}$ can be approximated as a Gaussian random variable under both hypotheses $H_0$ and $H_1$ and denoted as [20]

$$\begin{cases} x_{E_i} \sim N(\mu_{0i}, \sigma_{0i}^2), & H_0 \\ x_{E_i} \sim N(\mu_{1i}, \sigma_{1i}^2), & H_1 \end{cases} \quad (3)$$

Here, $\mu_{0i}$, $\mu_{1i}$ and $\sigma_{0i}^2$, $\sigma_{1i}^2$ are the means and variances under hypotheses $H_0$ and $H_1$, respectively.

$$\begin{cases} \mu_{0i} = N, & \sigma_{0i}^2 = 2N \\ \mu_{1i} = N(\gamma_i + 1), & \sigma_{1i}^2 = 2N(2\gamma_i + 1) \end{cases} \quad (4)$$

where $\gamma_i$ is the average SNR at $SU_i$. To perform CSS, SUs will then send their reports of the local spectrum sensing to FC for further processing. These reports can either be the received energy $x_{E_i}$ or a function of it (such as 1-bit hard decision), depending on the specific fusion rule adopted by FC.

At the $L$th sensing slot, the report of $SU_i$ can be denoted as $u_i^L$. Then, all the reports received by FC can be denoted as

$$\vec{u}^{\,L} = [u_1^L, u_2^L, \ldots, u_n^L] \quad (5)$$

based on which the final decision $u_0^L$ about PU's activity is made.

### 2.2 Attack patterns

Figure 1 also indicates that among all the SUs, there may be several malicious ones (which are less than the honest ones generally). The malicious SUs send falsified reports to FC and hope incorrect final decision $u_0^L$ will be made under the misleading. There are many ways to falsify reports for malicious SUs. In this article, we consider that each malicious SU falsifies its received energy at first and then reports a function of the falsified energy to the FC.

Two attack patterns, false alarm (FA) attack and false alarm & miss detection (FAMD) attack [21], are adopted and generalized in this article. Both of them can be characterized by three parameters, which are the attack threshold, the attack strength factor, and the attack probability. Specifically, the FA and FAMD attack patterns can be modeled as follows:

1. FA attack: At the $L$th sensing slot, if the received energy $x_{E_i}$ of FA attacker $SU_i$ is higher than the attack threshold $\delta_1$, it will not initiate an attack and

hold $x_{E_i}$. Otherwise, it will choose whether to attack with the attack probability $p_{a1}$. Moreover, if it chooses to attack, the received energy $x_{E_i}$ will be multiplied by the attack strength factor $\eta_1$ ($\eta_1 > 1$). Therefore, the FA attack pattern can be denoted as

$$x'_{E_i} = \begin{cases} x_{E_i} \cdot \eta_1, & \text{if } x_{E_i} \le \delta_1 \text{ and } \mathrm{SU}_i \text{ chooses to attack } (p_{a1}) \\ x_{E_i}, & \text{otherwise} \end{cases} \tag{6}$$

This attack pattern will increase the false alarm probability and result in the underutilization of available spectrum or the exclusive usage of it by FA attackers.

2. FAMD attack: At the $L$th sensing slot, if the received energy $x_{E_i}$ of FAMD attacker $\mathrm{SU}_i$ is higher than the attack threshold $\delta_2$, it will choose whether to attack with the attack probability $p_{a2}$ and multiply $x_{E_i}$ by the attack strength factor $\eta_2$ ($\eta_2 < 1$) if it chooses to attack. On the contrary, if $x_{E_i}$ is lower than the attack threshold $\delta_2$, it will choose whether to attack with the attack probability $p_{a3}$ and multiply $x_{E_i}$ by the attack strength factor $\eta_3$ ($\eta_3 > 1$) if it chooses to attack. Therefore, the FAMD attack pattern can be denoted as

$$x'_{E_i} = \begin{cases} x_{E_i} \cdot \eta_2, & \text{if } x_{E_i} > \delta_2 \text{ and } \mathrm{SU}_i \text{ chooses to attack } (p_{a2}) \\ x_{E_i} \cdot \eta_3, & \text{if } x_{E_i} \le \delta_2 \text{ and } \mathrm{SU}_i \text{ chooses to attack } (p_{a3}) \\ x_{E_i}, & \text{otherwise} \end{cases} \tag{7}$$

This attack pattern will increase both the false alarm probability and the miss detection probability, which not only leads to the unfair utilization of available spectrum but also causes more harmful interferences to the PU.

Under each of the two attack patterns, the falsified energy $x'_{E_i}$ is used to create local reports, which are then forwarded to FC. For simplicity in representation, we denote the energy used by $\mathrm{SU}_i$ to create reports at the $L$th sensing slot as $x^L_{E_i}$, which is either the original $x_{E_i}$ (for honest SUs) or the falsified $x'_{E_i}$ (for malicious SUs). That is,

$$x^L_{E_i} = \begin{cases} x_{E_i}, & \text{if } \mathrm{SU}_i \text{ is honest} \\ x'_{E_i}, & \text{if } \mathrm{SU}_i \text{ is malicious} \end{cases} \tag{8}$$

## 3. Robust cooperative spectrum sensing scheme based on Dempster-Shafer theory and trustworthiness degree calculation

In this section, we propose a robust CSS scheme based on Dempster-Shafer theory and trustworthiness degree calculation in CRNs. Dempster-Shafer theory is a mathematical theory of evidence [22], which can be viewed as an effective method for reasoning and making decisions. Since Dempster-Shafer theory is capable of combining reports from different SUs under the influence of uncertainty, it is well-suited for the CSS in CRN.

As shown in Figure 2, the proposed robust CSS scheme is carried out in four successive steps, which are basic probability assignment (BPA), trustworthiness degree calculation, selection and adjustment of BPA, and combination by Dempster-Shafer rule, respectively. The detailed discussions are given as follows.

### 3.1 Basic probability assignment

Since the detection of PU's activity is a binary hypothesis testing essentially, the framework of discernment for Dempster-Shafer theory is defined as $\Omega = \{H_1, H_0\}$. The BPA refers to a function $m$, which maps the power set of $\Omega$ (i.e., $\mathfrak{R}(\Omega)$) to the interval of [0, 1] and can be denoted as [22]

$$m : \mathfrak{R}(\Omega) \rightarrow [0, 1] \tag{9}$$

such that

$$m(\varnothing) = 0 \tag{10}$$

$$\sum_{k=1}^{|\mathfrak{R}(\Omega)|} m(A_k) = 1 \tag{11}$$

where $A_k \in \mathfrak{R}(\Omega)$, $\mathfrak{R}(\Omega) = \{\varnothing, H_0, H_1, \Omega\}$, and $|\mathfrak{R}(\Omega)|$ is the cardinality of $\mathfrak{R}(\Omega)$.

For each $A_k$, the value $m(A_k)$ expresses the proportion to which all available and relevant evidence supports the claim that a particular element of $\Omega$ belongs to set $A_k$ [23]. In other words, $m(A_k)$ represents the belief that one is willing to commit exactly to set $A_k$, given a certain piece of evidence. Each set $A_k$ that satisfies $m(A_k) > 0$ is called a focal set. Besides, in Dempster-Shafer theory, the belief function Bel and the plausibility function Pl are defined as

$$\mathrm{Bel}(B) = \sum_{A_k | A_k \subseteq B} m(A_k) \tag{12}$$

$$\mathrm{Pl}(B) = \sum_{A_k | A_k \cap B \neq \varnothing} m(A_k) \tag{13}$$

where $B \in \mathfrak{R}(\Omega)$. Bel($B$) measures the minimum or necessary support for hypothesis $B$, while Pl($B$) measures the maximum or potential support that could be placed in hypothesis $B$ if more evidence became available.

Due to the fact that $\mathrm{Bel}(H_0) = m(H_0)$ and $\mathrm{Bel}(H_1) = m(H_1)$ in the binary detection problem of CSS, we consistently use BPA function $m$ to represent the belief of hypotheses $H_0$ and $H_1$ in the following discussion.

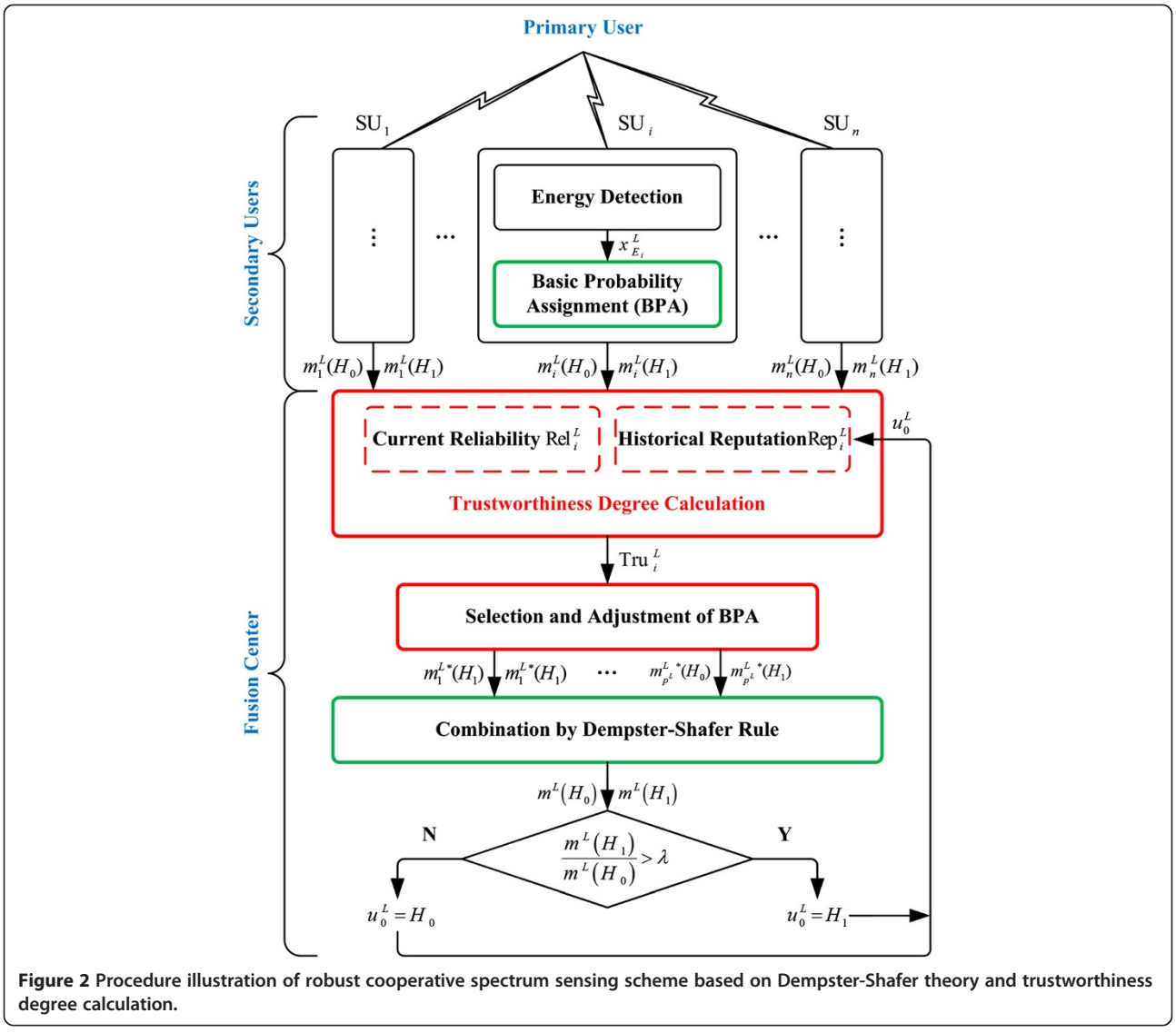


**Figure 2** Procedure illustration of robust cooperative spectrum sensing scheme based on Dempster-Shafer theory and trustworthiness degree calculation.

After the energy detection, $SU_i$ estimates its own BPAs based on $x_{E_i}^L$ according to the following formulation [19]:

$$m_i^L(H_0) = \int_{x_{E_i}^L}^{+\infty} \frac{1}{\sqrt{2\pi}\sigma_{0i}} \exp\left(-\frac{(x-\mu_{0i})^2}{2\sigma_{0i}^2}\right) dx \qquad (14)$$

$$m_i^L(H_1) = \int_{-\infty}^{x_{E_i}^L} \frac{1}{\sqrt{2\pi}\sigma_{1i}} \exp\left(-\frac{(x-\mu_{1i})^2}{2\sigma_{1i}^2}\right) dx \qquad (15)$$

and then sends the BPAs to FC. That is to say, the report of $SU_i$ at the $L$th sensing slot is $u_i^L = \left[m_i^L(H_0), m_i^L(H_1)\right]$.

### 3.2 Trustworthiness degree calculation

To eliminate or alleviate the performance deterioration caused by attack behaviors, the reports from different SUs should be treated discriminatingly. In the proposed scheme, the trustworthiness of each SU is evaluated by its trustworthiness degree, which involves two variables, i.e., the current reliability and the historical reputation. Specifically, the current reliability of $SU_i$ reflects the credibility of BPAs from $SU_i$ at the $L$th sensing slot, while the historical reputation of $SU_i$ reflects the credibility of previous reports from $SU_i$. By merging these two variables, both real-time and statistical information about the trustworthiness of $SU_i$ are well utilized.

#### 3.2.1 Current reliability

Since the reports from a malicious SU are falsified at some sensing slots, they are not always consistent with the reports from other SUs. Therefore, we can evaluate the current reliability of $SU_i$ based on its reports' similarity with other SUs at each sensing slot. Specifically, the

similarity degree of reported BPAs between $SU_i$ and $SU_j$ can be expressed by the following formulation [16]

$$\mathrm{sim}_{ij}^{L}=\frac{\sum_{k=1}^{|\mathfrak{R}(\Omega)|}\min\left(m_i^L(A_k),m_j^L(A_k)\right)}{\sum_{k=1}^{|\mathfrak{R}(\Omega)|}\max\left(m_i^L(A_k),m_j^L(A_k)\right)} \tag{16}$$

Note that $m_i^L(\Omega)$ within can be obtained by

$$m_i^L(\Omega)=1-m_i^L(H_0)-m_i^L(H_1) \tag{17}$$

according to (11). Then, the similarity degree matrix can be expressed as

$$\mathrm{Sim}^{L}=\begin{bmatrix}1 & \cdots & \mathrm{sim}_{1j}^{L} & \cdots & \mathrm{sim}_{1n}^{L}\\ \vdots & 1 & \vdots & \vdots & \vdots\\ \mathrm{sim}_{i1}^{L} & \cdots & 1 & \cdots & \mathrm{sim}_{in}^{L}\\ \vdots & \vdots & \vdots & 1 & \vdots\\ \mathrm{sim}_{n1}^{L} & \cdots & \mathrm{sim}_{nj}^{L} & \cdots & 1\end{bmatrix} \tag{18}$$

By adding up the total similarity degree of $SU_i$ with respect to other SUs, the support to the BPAs from $SU_i$ at the $L$th sensing slot is denoted as

$$\mathrm{Sup}_i^L=\sum_{j=1}^{n}\mathrm{sim}_{ij}^{L},\quad j\neq i,\quad i,j=1,2,\ldots,n \tag{19}$$

Thus, the current reliability of $SU_i$ can be obtained by normalizing the support and written as

$$\mathrm{Rel}_i^L=\frac{\mathrm{Sup}_i^L}{\max_i\left(\mathrm{Sup}_i^L\right)} \tag{20}$$

However, due to the open and dynamic character of wireless environment, there are many possibilities that can result in low current reliability. Apart from the attack behavior, the channel randomness (i.e., shadowing or fading effects, noise uncertainty) may also lead to inaccurate BPA estimation for SUs. Under such random influences, one honest SU may have poor sensing performance at some particular sensing slots. At that time, its reports will be inconsistent with the reports from other honest SUs or even have higher similarity degree with the reports from malicious SUs. Furthermore, if the number of malicious SUs increases in the network, these malicious SUs will support each other and distort the evaluation of current reliability significantly. In other words, we can neither conclude a SU to be honest or to be malicious precisely with the help of current reliability alone. To tackle this problem, the reputation mechanism is introduced into the proposed scheme.

#### 3.2.2 Historical reputation

Although historical reputation cannot evaluate which SUs are more trustworthy in real time, it can provide useful suggestions about the past credibility of SUs based on their previous reports. Besides, it is more stable and insusceptible to the random influences. Therefore, the historical reputation and the current reliability are complementary to each other and can both be utilized in the calculation of trustworthiness degree.

Most of the existing reputation mechanisms in CSS calculate historical reputation value of $SU_i$ by simply counting the times that the local decision of $SU_i$ is consistent with FC's final decision [24-26]. There are two main drawbacks in such approaches: First, these mechanisms assume that the final decision is faultless and thus use it as the benchmark, which can hardly be satisfied under the presence of attacks. Second, the counting method only cares about whether the local decision consists with the final decision or not. If they are consistent, the reputation value is updated by adding 1; otherwise, it is updated by subtracting 1. This method leaves the maintenance of reputation value with only two options and loses valuable information contained in the details of each past sensing slot.

In the proposed scheme, Dempster-Shafer theory is exploited to establish a soft update approach for historical reputation maintenance. This soft update approach takes the imperfectness of final decision into consideration and updates the reputation value of $SU_i$ at the $L$th sensing slot based on the BPAs of both $SU_i$ and FC at the $(L-1)$th sensing slot. Specifically, we define two parameters, the self-assessed confidence $c_i$ and the center-assessed confidence $c$, to differentiate particular cases in making final decisions. A higher $c_i$ (or $c$) represents that $SU_i$ (or FC) is more confirmative about its decision. Both self-assessed confidence and center-assessed confidence at the $(L-1)$th sensing slot are calculated by FC and can be written as

$$c_i^{L-1}=\left|m_i^{L-1}(H_1)-m_i^{L-1}(H_0)\right| \tag{21}$$

$$c^{L-1}=\left|m^{L-1}(H_1)-m^{L-1}(H_0)\right| \tag{22}$$

respectively. Here, $m^{L-1}(H_1)$ and $m^{L-1}(H_0)$ refer to the combined BPAs of FC at the $(L-1)$th sensing slot. Obviously, $c_i^{L-1}\in[0,1]$ and $c^{L-1}\in[0,1]$. Therefore, with the soft update approach, the reputation value of $SU_i$ at the $L$th sensing slot can be obtained as

$$r_i^L=r_i^{L-1}+(-1)^{u_0^{L-1}+v_i^{L-1}}\cdot c^{L-1}\cdot\frac{\left(c_i^{L-1}+\alpha\right)}{\alpha+1},\qquad \alpha\geq 0,\qquad L=2,3,\ldots \tag{23}$$

where $r_i^{L-1}$ is the reputation value of $SU_i$ at the $(L-1)$th sensing slot, $u_0^{L-1}$ is the 1-bit final decision, and $v_i^{L-1}$ is

the virtual 1-bit local decision of $SU_i$ inferred by FC. Note that $SU_i$ does not need to make or report its local hard decision (which would cause additional overhead), since this local decision can be reasoned from its reported BPAs by FC. That is,

$$v_i^{L-1} = \begin{cases} 0, & \dfrac{m_i^{L-1}(H_1)}{m_i^{L-1}(H_0)} \le \lambda \\ 1, & \dfrac{m_i^{L-1}(H_1)}{m_i^{L-1}(H_0)} > \lambda \end{cases} \tag{24}$$

where $\lambda$ is the decision threshold chosen by FC to meet different performance requirements.

The soft update approach for historical reputation maintenance can be explained with (23) basically. First, whether the reputation value $r_i^L$ is increased or decreased is determined by the 1-bit final decision $u_0^{L-1}$ and the virtual 1-bit local decision $v_i^{L-1}$. If $u_0^{L-1}$ and $v_i^{L-1}$ are consistent, $r_i^L$ increases; if not, $r_i^L$ decreases. This means the SUs whose local decisions are consistent with the final decision made by FC will gain a better reputation. Second, the variation of reputation value is determined by the self-assessed confidence $c^{L-1}$ and the center-assessed confidence $c^{L-1}$. If both $c_i^{L-1}$ and $c^{L-1}$ approach to 1 (meaning both $SU_i$ and FC are very confirmative about their own decisions), then the variation of reputation value will also approach to 1. If $SU_i$ (or FC) is not sure about the correctness of its decision, then $c_i^{L-1}$ (or $c^{L-1}$) decreases, and the variation of reputation value will decrease consequently. As a result, the reputation value is updated flexibly according to the particular cases in making final decisions of the last sensing slot (which is why it is called the soft update approach).

Besides, due to the fact that final decisions may be incorrect from time to time but are still more accurate than local decisions, parameter $\alpha$ is employed to adjust the relative status between FC and SUs in the soft update. In general, $\alpha$ should not be set too large; otherwise, the historical reputation will be updated with little contribution from the self-assessed confidence; on the other hand, effectively differentiating the BPAs from FC and SUs requires that $\alpha$ should not be set too small, either. In practice, the parameter $\alpha$ can be modified based on some previous experience or based on the experimental measurements when the number and attack patterns of malicious SUs are known.

Then, the historical reputation of $SU_i$ at the $L$th sensing slot can be normalized as

$$\mathrm{Rep}_i^L = \begin{cases} \dfrac{r_i^L}{\max_i\left(r_i^L\right)}, & r_i^L > 0 \\ 0, & r_i^L \le 0 \end{cases} \tag{25}$$

Initially, $r_i^1 = \Delta, \quad i = 1, 2, \ldots, n$. It should be pointed out that there are many feasible ways to merge the current reliability and the historical reputation. In this article, we adopt a simple way to obtain the trustworthiness degree by normalizing the sum of current reliability and historical reputation as the preliminary effort, which is

$$\mathrm{Tru}_i^L = \begin{cases} \dfrac{\mathrm{Rel}_i^L + \mathrm{Rep}_i^L}{\max_i\left(\mathrm{Rel}_i^L + \mathrm{Rep}_i^L\right)}, & \mathrm{Rep}_i^L > 0 \\ 0, & \mathrm{Rep}_i^L = 0 \end{cases} \tag{26}$$

As a result, the trustworthiness degree calculation of the proposed scheme can not only differentiate malicious SUs from honest ones based on their historical behaviors but also reserve the current difference for each SU to achieve a better real-time performance.

### 3.3 Selection and adjustment of BPA

According to the trustworthiness degree of each SU, the BPAs that are qualified to participate in the following combination can be selected and adjusted. For $SU_i$, if its trustworthiness degree is lower than a certain threshold, i.e., $\mathrm{Tru}_i^L \le \beta$, then it is regarded as a malicious SU and will be discarded from the following step at the $L$th sensing slot; otherwise, the BPAs of $SU_i$ are adjusted by FC with the corresponding trustworthiness degree

$$m_i^{L*}(H_0) = \mathrm{Tru}_i^L \cdot m_i^L(H_0) \tag{27}$$

$$m_i^{L*}(H_1) = \mathrm{Tru}_i^L \cdot m_i^L(H_1) \tag{28}$$

and

$$m_i^{L*}(\Omega) = 1 - m_i^{L*}(H_0) - m_i^{L*}(H_1) \tag{29}$$

### 3.4 Combination by Dempster-Shafer rule

To make the final decision $u_0^L$, all the adjusted BPAs are appropriately aggregated to obtain the combined BPAs according to the combination rule of Dempster-Shafer theory [22]

$$m^L(H_0) = m_1^{L*} \oplus m_2^{L*} \oplus \cdots \oplus m_{p^L}^{L*}(H_0) = \frac{\sum_{\cap A_i = H_0} \prod_{i=1}^{p^L} m_i^{L*}(A_i)}{1 - \sum_{\cap A_i = \varnothing} \prod_{i=1}^{p^L} m_i^{L*}(A_i)} \tag{30}$$

$$m^L(H_1) = m_1^{L*} \oplus m_2^{L*} \oplus \cdots \oplus m_{p^L}^{L*}(H_1) = \frac{\sum_{\cap A_i = H_1} \prod_{i=1}^{p^L} m_i^{L*}(A_i)}{1 - \sum_{\cap A_i = \varnothing} \prod_{i=1}^{p^L} m_i^{L*}(A_i)} \tag{31}$$

where $A_i \in \mathfrak{R}(\Omega)$, $i = 1, 2, \ldots, p^L$, and $p^L$ is the number of SUs whose BPAs are selected and adjusted to participate in the combination at the $L$th sensing slot.

At last, the combined BPAs $m^L(H_0)$ and $m^L(H_1)$ are used to make the final decision according to the following decision rule

$$u_0^L = \begin{cases} 0, & \text{Decide } H_0 \text{ if } \dfrac{m^L(H_1)}{m^L(H_0)} \le \lambda \\ 1, & \text{Decide } H_1 \text{ if } \dfrac{m^L(H_1)}{m^L(H_0)} > \lambda \end{cases} \quad (32)$$

where $\lambda$ is the same decision threshold as adopted in [24]. Once the final decision is made, the historical reputation can be updated according to [23] for the detection of the next sensing slot.

*Remark*. It is noted from [23] that the soft update approach for historical reputation maintenance can be implemented with low computational complexity and storage cost. The reputation value of each SU is updated in an iterative manner, which only needs its reputation value of the very last sensing slot. More importantly, the soft update approach takes advantage of Dempster-Shafer theory's ability of representing uncertainty by using BPAs to update the historical reputation, which is more suitable than traditional counting method.

## 4. Simulation results

In this section, abundant simulation results are presented to compare the performance of the proposed robust CSS scheme with several existing schemes, as shown from Figures 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14. Specifically, the curve of 'OPT LIN' shows the optimal linear CSS scheme proposed in [13], 'OPT LRT' shows the LRT-based optimal fusion rule presented in [11], and 'SINGLE' shows the situation of single SU spectrum sensing. Three CSS schemes based on Dempster-Shafer theory are presented here: 'RSE D-S' shows the enhanced scheme with reliability source evaluation proposed in [15], 'SIM D-S' shows another enhanced scheme with similarity degree calculation proposed in [16], and our proposed robust scheme is shown as 'TRU D-S.' The impact of both FA and FAMD attack patterns is investigated with different number of malicious SUs jointly. MATLAB is used to simulate the system.

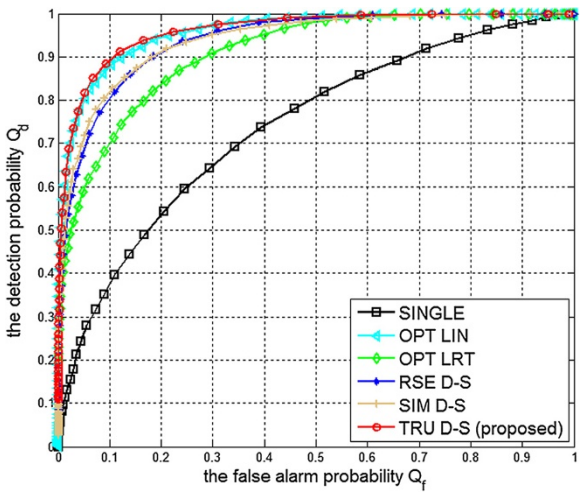


**Figure 4** Performance comparison of each scheme when $SU_6$ (with average SNR $\gamma_6 = -1$ dB) is a FA attacker.

### 4.1 Parameter setting

The simulations are performed in a CRN with one PU, $n = 6$ SU, and one FC. PU is assumed to be a digital television (DTV) base station. The probabilities of presence and absence of PU are both set to be 0.5. The time-bandwidth product $TW = 10$, the adjusting parameter $\alpha = 1$, the initial reputation value $\Delta$ of each SU is 5, and the trustworthiness degree threshold $\beta = 0.7$. Without

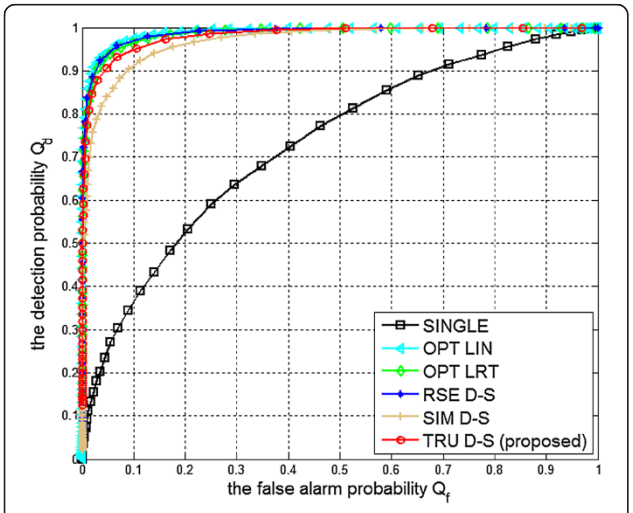


**Figure 3** Performance comparison of each scheme when there is no malicious SU.

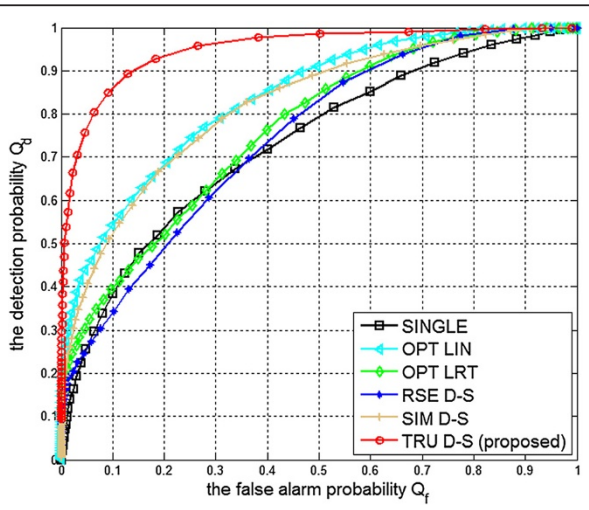


**Figure 5** Performance comparison of each scheme when $SU_6$ (with average SNR $\gamma_6 = -1$ dB) is a FAMD attacker.

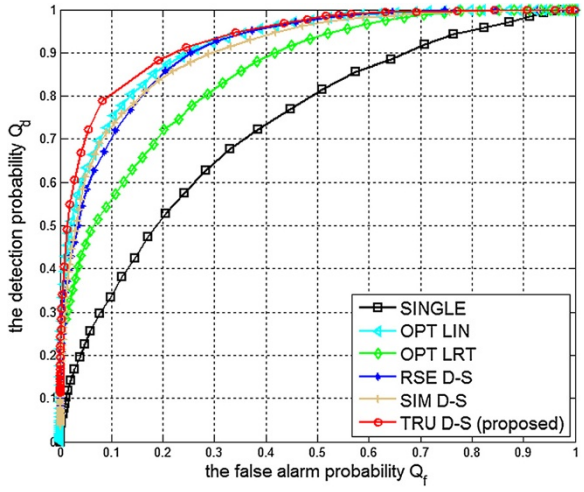


**Figure 6** Performance comparison of each scheme when both $SU_4$ ($\gamma_4 = -3$ dB) and $SU_6$ ($\gamma_6 = -1$ dB) are FA attackers.

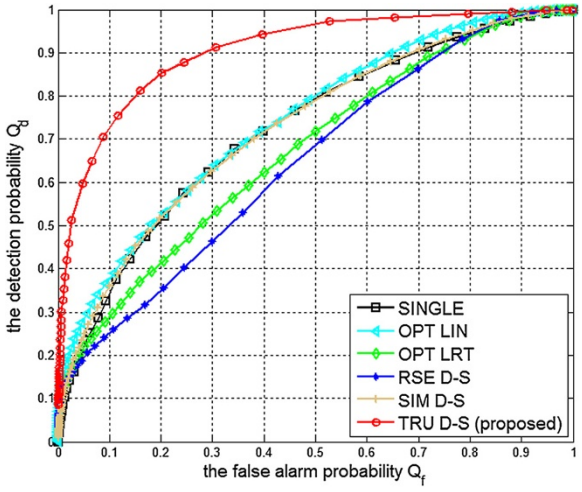


**Figure 8** Performance comparison of each scheme when $SU_4$ ($\gamma_4 = -3$ dB) is a FA attacker and $SU_6$ ($\gamma_6 = -1$ dB) is a FAMD attacker.

loss of generality, we choose some simple attack parameters in the simulation. Specifically, the attack strength factors $\eta_1 = \eta_3 = 2$, $\eta_2 = 0.5$, and the attack probabilities $p_{a1} = p_{a2} = p_{a3} = 1$. The attack thresholds $\delta_1$ and $\delta_2$ are both chosen as an energy level, which is the right intersection of two probability density functions (PDFs) under hypotheses $H_0$ and $H_1$ of each SU. Besides, the average SNR of six SUs are considered to be −6, −5, −4, −3, −2, and −1 dB, respectively. Simulations are run for 10,000 rounds.

### 4.2 Performance evaluation

Figure 3 shows the sensing performance of each CSS scheme through receiver operating characteristics (ROC) curve, under the condition that there is no malicious SU existing in the network. The curve of SINGLE which represents the sensing performance of $SU_2$ (i.e., the one with average SNR $\gamma_2 = -5$ dB) is shown as reference. As can be seen, every CSS scheme works quite well through cooperation in a non-hostile environment. It should be pointed out that, although our proposed TRU D-S scheme works better than SIM D-S scheme, it is slightly worse than OPT LIN, OPT LRT, and RSE D-S schemes. However, the limited advantage of OPT LIN, OPT LRT, and RSE D-S schemes is achieved by using the average SNR of each SU in the fusion. Since no such prior knowledge is required at FC for the proposed scheme, it is much easier to implement in practice.

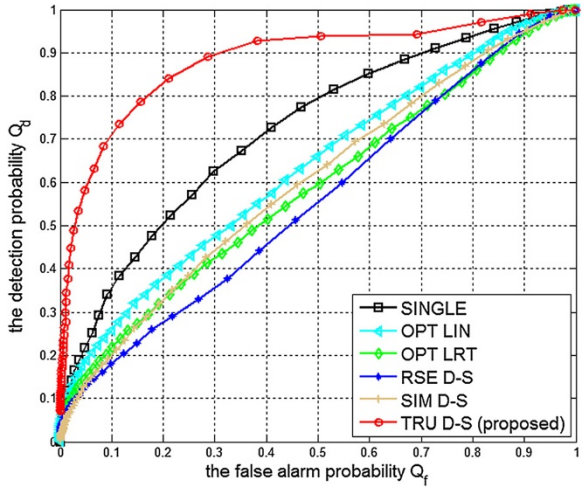


**Figure 7** Performance comparison of each scheme when both $SU_4$ ($\gamma_4 = -3$ dB) and $SU_6$ ($\gamma_6 = -1$ dB) are FAMD attackers.

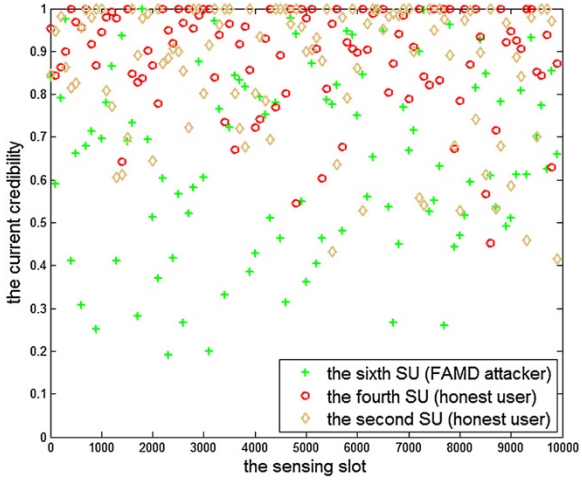


**Figure 9** The dynamic change of the current reliability when $SU_6$ is a FAMD attacker (same as Figure 5).

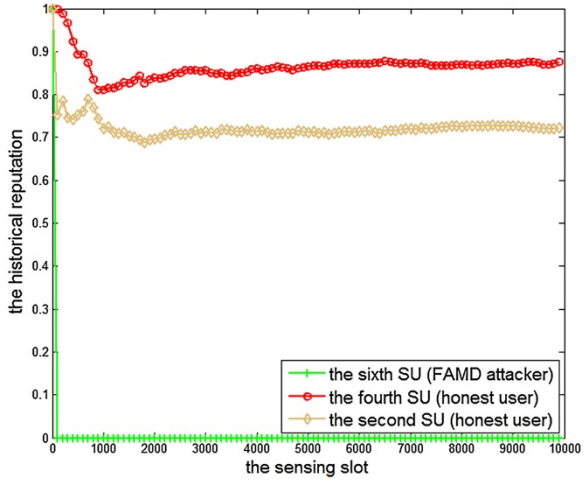


**Figure 10** The dynamic change of the historical reputation when $SU_6$ is a FAMD attacker (same as Figure 5).

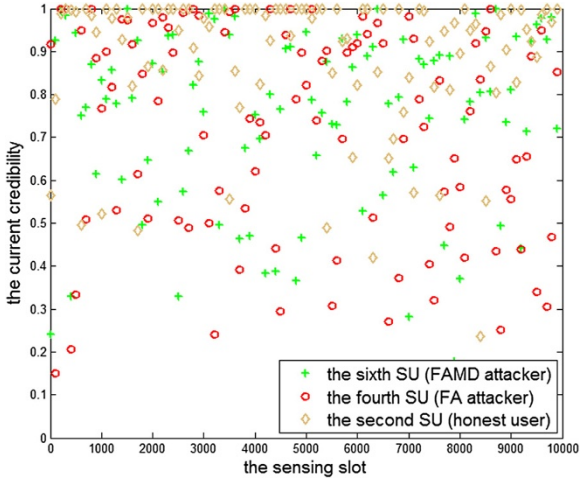


**Figure 12** The dynamic change of the current reliability when $SU_4$ is a FA attacker and $SU_6$ is a FAMD attacker (same as Figure 8).

The scenario of one malicious SU existing is presented in Figures 4 and 5. Specifically, Figure 4 shows the sensing performance of each scheme when the malicious SU adopts FA attack pattern, while Figure 5 shows that of each scheme when the malicious SU is a FAMD attacker. In both figures, the worst case where $SU_6$ (with the highest average SNR $\gamma_6 = -1$ dB) is the malicious SU is considered. As before, SINGLE shows the sensing performance of $SU_2$ as reference. From Figure 4, we can see that both proposed TRU D-S scheme and OPT LIN scheme can achieve a desirable performance and work better than other CSS schemes. Figure 5 has substantiated that among all the CSS schemes presented, the proposed scheme is most robust to FAMD attack. The performance gain is mainly achieved by calculating the trustworthiness degree to select and adjust BPAs for the combination, as discussed in Sections 3.2 and 3.3.

Figures 6,7,8 have shown the sensing performance of each CSS scheme when two malicious SUs appear. In Figure 6, two FA attackers are considered. Without loss of generality, we select $SU_4$ (i.e., the one with average SNR $\gamma_4 = -3$ dB) and $SU_6$ as attackers in the simulation. Similarly, $SU_4$ and $SU_6$ are chosen as FAMD attackers in Figure 7. In Figure 8, $SU_4$ and $SU_6$ are chosen as FA attacker and FAMD attacker, respectively. Comparing Figures 6,7,8 with Figures 4 and 5, we can see that the overall performance of all schemes would degrade if the

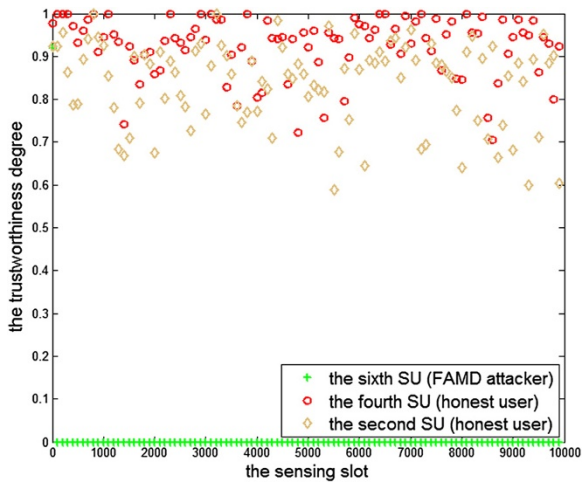


**Figure 11** The dynamic change of the trustworthiness degree when $SU_6$ is a FAMD attacker (same as Figure 5).

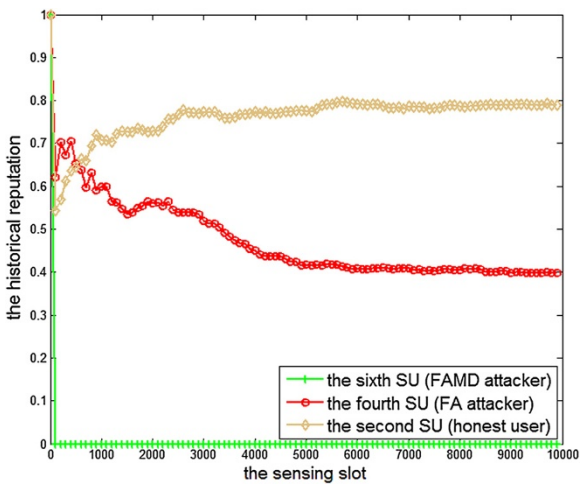


**Figure 13** The dynamic change of the historical reputation when $SU_4$ is a FA attacker and $SU_6$ is a FAMD attacker (same as Figure 8).

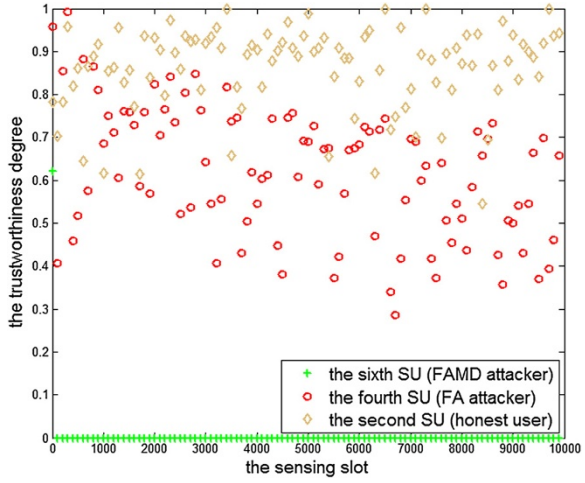


**Figure 14 The dynamic change of the trustworthiness degree when $SU_4$ is a FA attacker and $SU_6$ is a FAMD attacker (same as Figure 8).**

number of malicious SUs increases. Besides, Figure 6 has shown that OPT LRT scheme is vulnerable to two FA attackers, while OPT LIN, RSE D-S, SIM D-S, and the proposed scheme still remain robust. However, as illustrated in Figures 7 and 8, all CSS schemes except ours will suffer heavy degradation in performance when a FAMD attacker occurs. It is shown that the proposed TRU D-S scheme can detect the malicious behavior effectively and outperform other schemes significantly.

From Figures 9,10,11,12,13,14, the effectiveness of trustworthiness degree calculation in the proposed scheme is shown clearly. The dynamic change of the current reliability, the historical reputation, and the trustworthiness degree of SUs are shown under two different circumstances, respectively. The decision threshold here is chosen as $\lambda = 1$.

To be specific, Figures 9,10,11 show the dynamic change in a circumstance where $SU_6$ is a FAMD attacker, which is the same situation as in Figure 5. From Figure 9, we can see that although the current reliability of the FAMD attacker seems to be lower than that of honest SUs in average, it can still approach to 1 every now and then. Besides, it is hard to tell which of the two honest SUs has a better performance. Figure 10 shows that the historical reputation of the FAMD attacker drops to zero very quickly, which means its attack behavior has been effectively detected. The historical reputation of $SU_4$ is higher than $SU_2$ due to the fact that $SU_4$ has a higher average SNR. As a result, the FAMD attacker will have zero trustworthiness degree and be discarded from the combination, as illustrated in Figure 11. Moreover, the trustworthiness degree of $SU_4$ is obviously higher than that of $SU_2$, which means $SU_4$ will play a more important role in the final decision-making.

Figures 12,13,14 show the dynamic change in a circumstance where $SU_4$ is a FA attacker and $SU_6$ is a FAMD attacker, which is the same situation as in Figure 8. It is nearly impossible to differentiate malicious SUs in Figure 12, since the current reliability of every SU is similarly disordered. Fortunately, as shown in Figure 13, the FAMD attacker will be detected quickly and effectively considering its historical reputation. We should point out that although the historical reputation of the FAMD attacker drops very fast from the beginning, it still affects the final decision-making before it is discarded. Therefore, at the time the FAMD attacker's historical reputation comes to zero, the FA attacker will have higher historical reputation than honest $SU_2$. But after a while, the historical reputation of $SU_2$ will recover gradually, while that of the FA attacker falls to a relatively low level. As illustrated in Figure 14, the trustworthiness degree of FAMD attacker is zero, and the trustworthiness degree of FA attacker is much lower than that of the honest $SU_2$. It verifies that the trustworthiness degree calculation can not only differentiate malicious SUs from honest ones based on their historical behaviors but also reserve the current difference of each SU's sensing result caused by the uncertainty of wireless environment.

## 5. Conclusions

In this article, we have proposed a robust CSS scheme based on Dempster-Shafer theory and trustworthiness degree calculation. It is carried out in four successive steps, which are BPA, trustworthiness degree calculation, selection and adjustment of BPA, and combination by Dempster-Shafer rule, respectively. In the proposed scheme, the trustworthiness degree of each SU is evaluated from both current difference aspect and historical behavior aspect, and Dempster-Shafer theory's potential is exploited to establish a soft update approach for the reputation value maintenance. Our proposed scheme can not only differentiate malicious SUs from honest ones effectively based on their historical behaviors but also reserve the current difference for each SU to achieve a better real-time performance. Abundant simulation results have been conducted and validated that the proposed scheme outperforms the existing ones under the impact of different attack patterns and different number of malicious SUs. In the future work, more sophisticated attack patterns will be considered, and more effective methods for calculating the trustworthiness degree will be investigated.

**Competing interests**
The authors declare that they have no competing interests.

**Acknowledgements**
This work was supported by the National Basic Research Program of China under Grant No. 2009CB320400, the National Science Foundation of China under Grant Nos. 61172062, 61301160, and 60932002, and in part by the Jiangsu Province Natural Science Foundation under Grant No. BK2011116.

Received: 8 January 2014 Accepted: 6 March 2014
Published: 21 March 2014

**References**

1. S Haykin, Cognitive radio: brain-empowered wireless communications. IEEE J. Sel. Areas. Commun. **23**(2), 201–220 (2005)
2. KB Letaief, W Zhang, Cooperative communications for cognitive radio networks. Proc. IEEE **97**(5), 878–893 (2009)
3. J Mitola, Cognitive radio architecture evolution. Proc. IEEE **97**(4), 626–641 (2009)
4. YH Xu, A Anpalagan, QH Wu, L Shen, Z Gao, JL Wang, *Decision-theoretic distributed channel selection for opportunistic spectrum access: strategies, challenges and solutions* (IEEE Commun. Surv. Tutor.). doi:10.1109/SURV.2013.030713.00189
5. IF Akyildiz, W-Y Lee, MC Vuran, A survey on spectrum management in cognitive radio networks. IEEE Commun. Mag. **46**(4), 40–48 (2008)
6. A Ghasemi, ES Sousa, Opportunistic spectrum access in fading channels through collaborative sensing. J. Commun. **2**(2), 71–82 (2007)
7. W Zhang, KB Letaief, Cooperative spectrum sensing with transmit and relay diversity in cognitive radio networks. IEEE Trans. Wirel. Commun. **7**(12), 4761–4766 (2008)
8. J Unnikrishnan, VV Veeravalli, Cooperative sensing for primary detection in cognitive radio. IEEE J. Sel. Topics. Signal. Process. **2**(1), 18–27 (2008)
9. GR Ding, QH Wu, Y-D Yao, Kernel-based learning for statistical signal processing in cognitive radio networks. IEEE Signal Process. Mag. **30**(4), 126–136 (2013)
10. PK Varshney, *Distributed Detection and Data Fusion* (Springer, New York, 1997)
11. SM Kay, *Fundamentals of Statistical Signal Processing: Detection Theory* (Prentice-Hall, New Jersey, 1998)
12. B Chen, PK Willett, On the optimality of the likelihood-ratio test for local sensor decision rules in the presence of non-ideal channels. IEEE Trans. Inform. Theory. **51**(2), 693–699 (2005)
13. Z Quan, SG Cui, AH Sayed, Optimal linear cooperation for spectrum sensing in cognitive radio networks. IEEE J. Sel. Topics Signal. Process. **2**(1), 28–40 (2008)
14. QH Peng, K Zeng, J Wang, SQ Li, A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context, in *17th IEEE International Symposium on Personal*, in *Indoor and Mobile Radio Communications (IEEE PIMRC)* (IEEE, Piscataway, 2006), pp. 2511–2515
15. N-T Nhan, K Insoo, An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context. IEEE Commun. Lett. **13**(7), 492–494 (2009)
16. Y Han, Q Chen, J-X Wang, *An enhanced D-S theory cooperative spectrum sensing algorithm against SSDF attack, in 75th IEEE Vehicular Technology Conference (IEEE VTC Spring)* (Piscataway, IEEE, 2012), pp. 1–5
17. N-T Nhan, K Insoo, A robust secure cooperative spectrum sensing scheme based on evidence theory and robust statistics in cognitive radio. IEICE Trans. Commun. **92**(12), 3644–3652 (2009)
18. S Jana, K Zeng, W Cheng, P Mohapatra, Trusted collaborative spectrum sensing for mobile cognitive radio networks. IEEE Trans. Inf. Foren. Sec. **8**(9), 1497–1507 (2013)
19. N-T Nhan, K Insoo, Evidence-theory-based cooperative spectrum sensing with efficient quantization method in cognitive radio. IEEE Trans. Veh. Technol. **60**(1), 185–195 (2011)
20. H Urkowitz, Energy detection of unknown deterministic signals. Proc. IEEE **55**(4), 523–531 (1967)
21. WK Wang, HS Li, Y Sun, Z Han, Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks. EURASIP J. Adv. Signal Process. **2010**(4), 1–15 (2010)
22. G Shafer, *A Mathematical Theory of Evidence* (Princeton, New Jersey, 1976)
23. GJ Klir, *Uncertainty and Information: Foundations of Generalized Information Theory* (Wiley, New Jersey, 2006)
24. RL Chen, JM Park, K Bian, *Robust distributed spectrum sensing in cognitive radio networks, in 27th IEEE International Conference on Computer Communications* (Piscataway, IEEE INFOCOM) (IEEE, 2008). pp. 31–35
25. F Gao, W Yuan, W Liu, *WQ Cheng, S Wang, A robust and efficient cooperative spectrum sensing scheme in cognitive radio networks, in 58th IEEE International Conference on Computer Communications (IEEE ICC)* (Piscataway, IEEE, 2010), pp. 1–5
26. K Zeng, P Pawelczak, D Cabric, Reputation-based cooperative spectrum sensing with trusted nodes assistance. IEEE Commun. Lett. **14**(3), 226–228 (2010)

doi:10.1186/1687-6180-2014-35
**Cite this article as:** Wang *et al.*: **A robust cooperative spectrum sensing scheme based on Dempster-Shafer theory and trustworthiness degree calculation in cognitive radio networks.** *EURASIP Journal on Advances in Signal Processing* 2014 **2014**:35.