symmetry

MDPI

Article

Faithworthy Collaborative Spectrum Sensing Based on Credibility and Evidence Theory for Cognitive Radio Networks

Fang Ye [1], Xun Zhang [1], Yibing Li [1,*] and Chunrui Tang [2]

[1] College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China; yefang0923@126.com (F.Y.); zhangxun0611@gmail.com (X.Z.)
[2] Dalian Airforce Communication NCO Academy, Dalian 116000, China; hljlxzx@163.com
* Correspondence: liyibing0920@126.com; Tel.: +86-133-0460-5678

Academic Editor: Angel Garrido
Received: 10 February 2017; Accepted: 1 March 2017; Published: 4 March 2017

Abstract: Cognitive radio (CR) has become a tempting technology that achieves significant improvement in spectrum utilization. To resolve the hidden terminal problem, collaborative spectrum sensing (CSS), which profits from spatial diversity, has been studied intensively in recent years. As CSS is vulnerable to the attacks launched by malicious secondary users (SUs), certain CSS security schemes based on the Dempster–Shafer theory of evidence have been proposed. Nevertheless, the available works only focus on the real-time difference of SUs, like the difference in similarity degree or SNR, to evaluate the credibility of each SU. Since the real-time difference is unilateral and sometimes inexact, the statistical information comprised in SUs' historical behaviors should not be ignored. In this paper, we propose a robust CSS method based on evidence theory and credibility calculation. It is executed in four consecutive procedures, which are basic probability assignment (BPA), holistic credibility calculation, option and amelioration of BPA and evidence combination via the Dempster–Shafer rule, respectively. Our scheme evaluates the holistic credibility of SUs from both the real-time difference and statistical sensing behavior of SUs. Moreover, considering that the transmitted data increase with the number of SUs increasing, we introduce the projection approximation approach to adjust the evidence theory to the binary hypothesis test in CSS; on this account, both the data volume to be transmitted and the workload at the data fusion center have been reduced. Malicious SUs can be distinguished from genuine ones based on their historical sensing behaviors, and SUs' real-time difference can be reserved to acquire a superior current performance. Abounding simulation results have proven that the proposed method outperforms the existing ones under the effect of different attack modes and different numbers of malicious SUs.

Keywords: cognitive radio (CR)networks; collaborative spectrum sensing (CSS); Dempster–Shafer theory of evidence; malicious secondary users' detection

1. Introduction

The frequency spectrum is treated as a valuable resource in the wireless communication field and is rendered inadequate for the increasing number of wireless services. In terms of the spectrum task report from the Federal Communication Commission (FCC), the usage of authorized spectrum alters according to geographic and temporal circumstances [1]. Cognitive radio (CR) arises as a tempting solution to the spectrum congestion problem by enabling opportunistic access to underutilized licensed bands that are lightly occupied by a licensed user (LU). CR is characterized by the fact that it adapts to the actual environment by transforming its transmitting parameters, such as frequency, modulation, frame format, etc. [2,3]. A precondition of secondary access is the absence of interference for the primary system. Spectrum sensing thereby plays an essential role in cognitive radio networks (CRNs).

Among fundamental spectrum sensing techniques, energy detection is predominant due to its simple implementation, as well as low computational complexity [4,5]. However, spectrum sensing conducted by a single node is hindered by uncertainty originating from channel randomness, such as multipath fading and shadow effect [6]. To combat these adverse impacts, collaborative spectrum sensing (CSS) schemes have been proposed to achieve spatial diversity in CRNs [7–9]. In CSS, messages reported from different SUs are combined at the data fusion center (DFC); DFC subsequently makes a global decision on the absence/presence of the LU.

There exists abundant literature that has established the optimality of likelihood ratio test (LRT) concerning detection issues, such as [10–12] and the references therein; yet, the computation complexity of LRT is quite high, and the closed form expressions of detection probability and false alarm probability cannot be derived. Quan et al. [13] have put forward an optimal linear CSS method, which makes the final decision over a linear weighted combination of the local measurements. The computational complexity has been reduced, and the performance compared favorably with LRT-based optimal fusion rules, which can be achieved, as well; but the DFC requires specific report channels to acquire and update a priori information. In recent years, plenty of algorithms have been proposed owing to the unique advantages of the Dempster–Shafer (D-S) theory of evidence in terms of uncertainty representation [14–19]. In [14], Dempster–Shafer theory is first applied in the data fusion of CSS. This method quantifies the channel condition between LU and SUs with credibility parameter and adopts D-S theory to fuse the local measurements with relevant credibility. Nhan and Insoo [15] came up with an enhanced CSS scheme based on D-S theory and reliability source evaluation. It exploits the signal-to-noise ratios (SNRs) to assess the reliability degree for SUs. The reliability weight of SUs is then applied to adjust their observational information before making the global decision. However, it uses much bandwidth to transmit the sensing data with the number of SUs increasing.

Although the participation of multiple SUs in CSS contributes to the improvement of detection accuracy, the global decision making may be misguided when SUs intentionally or unintentionally send falsified sensing information to the DFC during cooperation. This sort of attack in CSS, called the spectrum sensing data falsification (SSDF) attack, has significantly degraded collaborative detection correctness. Hence, effective security mechanisms are fundamentally demanded in an opponent wireless environment. Han et al. [16] propose an enhanced evidence theory-based CSS method to resist the SSDF attack. This scheme uses the similarity degree to evaluate the credibility of evidence and removes the evidence with low similarity degree from the combination. Facing the problem of faulty nodes in CRN, the CSS method in [17] adopts a mutually supportive degree among different sensor nodes to support adapted decision. Another evidence theory-based secure CSS scheme is proposed in [18], which employs robust statistics to calculate the distribution parameters of LU's activity and estimates the SUs' credibility with a simple counting technique. In addition, several detection approaches are adopted to counter distinct sorts of malicious SUs. In [19], a trusted CSS method for mobile CRNs is proposed, which improves malicious SU detection utilizing both location reliability and D-S theory. Wang et al. [20] take advantage of the "soft update" approach and evaluate the trustworthiness degree of SUs for enhancing the robustness of the CSS system.

However, these existing evidence theory-based CSS methods are not specifically suited for CRNs communications. This is basically because they are generally designed without considering challenges posed by the framework of resource-constrained nodes of CRNs; such as hardware limitations and low power budget. In addition, the majority of these CSS methods only consider SUs' current difference, for instance the SNR difference or similarity degree diversity, to estimate the credibility of each SU. Although this current difference tends to reflect SUs' reliability to some extent, it is unilateral and sometimes inexact, by virtue of the dynamic characteristic of wireless channels. Apart from real-time information, the statistical information about SUs' historical sensing behavior reflecting their past credibility should also be taken into account in the evaluation of sensing credibility.

Therefore, in this paper, we propose a robust CSS scheme based on D-S evidence theory and credibility calculation. It is executed in four consecutive procedures, which are basic probability assignment (BPA), holistic credibility calculation, option and amelioration of BPA and evidence combination via the Dempster–Shafer rule, respectively. The major contributions of this paper can be summarized as follows:

A. Considering transmitted data rises with the increase of the number of nodes and the power restriction of SUs, we introduce projection approximation approach to half decrease the amount of required transmitted data from SUs to the DFC. This is achieved by adapting the D-S evidence theory to the binary hypothesis test of the cognitive radio context.

B. Instead of evaluating the SUs only with their current measurements, we propose to evaluate the credibility of each SU from both statistical reputation and the real-time difference. The proposed method can not only effectively distinguish malicious SUs from genuine ones based on their past sensing behaviors, but also hold the current sensing difference for SUs to realize superior real-time performance.

C. No prior knowledge such as the average SNR of each SU is demanded at DFC, which reduces the communication cost. Moreover, our proposed method is simple to implement. The reputation value maintenance can be conducted in an iterative manner, which requires no additional computational complexity or storage overhead.

The remainder of the paper is organized as follows. In Section 2, we describe the system model with the energy detection and D-S theory; the attack models are introduced, as well. The robust Dempster–Shafer theory collaborative spectrum sensing method is proposed in Section 3, which elaborates the holistic credibility calculation in detail. Simulations and conclusions are respectively presented in Sections 4 and 5. Section 4 presents numerical simulation results. Finally, the conclusions are drawn in Section 5.

2. System Description

As a key technology for achieving opportunistic spectrum access, spectrum sensing aims to detect the presence of PUs accurately and quickly. In this article, we consider two processes for spectrum sensing, which the local spectrum sensing at each SU and the data fusion at the DFC. The CSS scenario in CRNs and two patterns of attack are described in this section.

2.1. Collaborative Spectrum Sensing

The network architecture we consider is a centralized network entity, such as a base-station in infrastructure-based networks, as showed in Figure 1. Assume that the CR network consists of one licensed user base station, which may be active with probability P_{H_1} or idle with probability P_{H_0} in a sensing time slot, n secondary users and one data fusion center. Firstly, the individual SU conducts local spectrum sensing independently, the process of which can be formulated as a binary hypothesis testing problem [6]:

$$\begin{aligned} H_0: &\quad y_i(t) = n_i(t) \\ H_1: &\quad y_i(t) = h_i s(t) + n_i(t) \end{aligned} \tag{1}$$

where $s(t)$ represents the signal transmitted by LU and $y_i(t)$ denotes the received signal at the i-th SU. The signal $s(t)$ is distorted by the channel gain $h_i(t)$, which is assumed to be constant during the sensing interval, and is further corrupted by the zero-mean additive white Gaussian noise (AWGN) $n_i(t)$, i.e., $n_i(t) \sim \mathcal{N}(0, \sigma_i^2)$. Hypothesis H_0 indicates that the spectrum is currently occupied by PU, and hypothesis H_1 indicates that spectrum is available for SUs; and t represents time. Without loss of generality, $n_i(t)$ and $s(t)$ are assumed to be independent of each other.

Due to its applicability to a wide range of signals and mathematical amenity compared to other detectors, energy detection is adopted by each SU in the local spectrum sensing stage; the input signal energy is measured by the energy detector within a specific time interval. By applying a band-pass filter, the received energy at SU$_i$ can be expressed as [4]:

$$y_{Ei} = \sum_{j=1}^{N} |y_{ij}|^2 \tag{2}$$

where y_{ij} is the j-th sample of the received signal at SU$_i$ and $N = 2TW$ with T and W being detection time and channel bandwidth, respectively. Naturally, TW is the time-bandwidth product. When N is relatively large (e.g., $N > 10$), y_{Ei} can be approximated as a Gaussian random variable under both hypotheses and denoted as [20]:

$$y_{Ei} \sim \begin{cases} \mathcal{N}(\mu_{0i}, \sigma_{0i}^2), & H_0 \\ \mathcal{N}(\mu_{1i}, \sigma_{1i}^2), & H_1 \end{cases} \tag{3}$$

where μ_{0i}, σ_{0i}^2, μ_{1i} and σ_{1i}^2 are the means and variances under hypotheses H_0 and H_1, respectively.

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

Here, γ_i is the average signal-to-noise ratio (SNR) at SU$_i$. In the CSS scheme, SUs send their local measurements to DFC, which is in charge of further information processing. These measurements can either be the received energy y_{Ei} or its function (like a one-bit hard decision or a double threshold decision), depending on the specific fusion rule utilized by DFC.

At the H-th sensing slot, the report of SU$_i$ can be denoted as u_i^H. Then, all of the reports received by DFC can be denoted as $u^H = [u_1^H, \ldots, u_i^H, \ldots, u_n^H]$, and the DFC makes a final global decision u_0^H about LU's activity.

2.2. SSDF Attack Models

As illustrated in Figure 1, certain compromised SUs exist among all SUs in CRNs. They report falsified results to DFC and expect DFC to make an incorrect global decision u_0^H under their misguidance. The means to tamper reports of malicious SUs can be multifold. This paper considers that malicious users (MUs) first distort their received energy accumulation and send the distorted energy to the DFC afterwards.

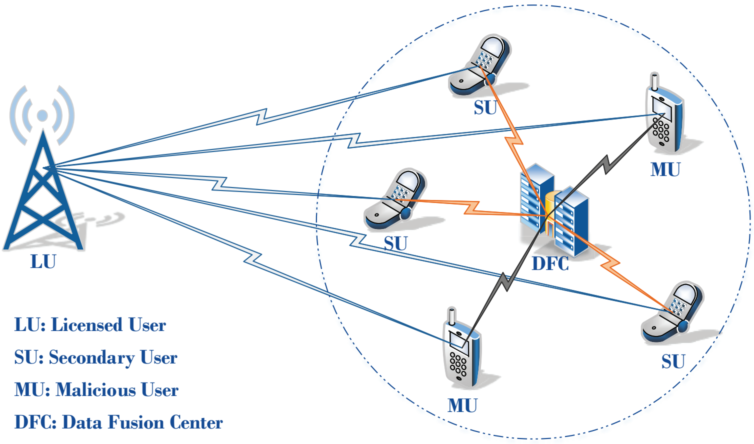

Figure 1. Collaborative spectrum sensing in CRNs.

We investigate two SSDF attack models, the false alarm and miss detection (FAMD) attack and the false alarm (FA) attack, as presented in [21]. Both can be described by three parameters, including the attack threshold (η), the attack intensity factor (ξ) and the attack probability (P_a). Specifically, these two attacks can be modeled as follows:

A. FAMD attack: For sensing slot H, the FAMD attacker launches an attack with probability P_a. If it intends to attack during this round, it will compare y_{Ei} with η. If the sensed energy y_{Ei} exceeds the attack threshold η, it will report $y_{Ei} + \xi$; otherwise, the attacker reports $y_{Ei} - \xi$. If the attacker chooses not to attack, it will just report y_{Ei}. This attack model tends to increase the misdetection and false alarm probability, which results in both the inequitable utility of the available spectrum and more damaging disturbances to the LU.

B. FA attack: For sensing slot H, if sensed energy y_{Ei} exceeds the attack threshold η, the attack will not be launched, and the energy will hold at y_{Ei}. On the contrary, it will attack with probability P_a by reporting $y_{Ei} + \xi$. This attack model is inclined to cause false alarm probability increase and the available spectrum underutilization or the exclusive usage of it by FA attackers.

Under each of the two attack models, the distorted energy y'_{Ei} is utilized to produce local measurements, which are subsequently delivered to DFC. In this paper, the energy used by SU$_i$ to create reports at the H-th sensing slot is expressed as y^L_{Ei}, which is either the original y_{Ei} for genuine SUs or the distorted y'_{Ei} for malicious SUs.

3. Faithworthy Collaborative Spectrum Sensing Based on Credibility and Evidence Theory for Cognitive Radio Networks

In this article, we propose a faithworthy CSS method based on credibility and evidence theory for CR networks. As first introduced by Dempster and later extended by Shafer, Dempster–Shafer (D-S) theory allows one to combine evidence from different sources and evaluate the credibility of the system state [22], which is regarded as an effective approach for decision making, as well. Due to its capability of merging results reported by SUs under the effect of uncertainty, D-S theory is quite suitable for collaborative spectrum sensing in CRNs.

Figure 2 shows that the proposed faithworthy CSS method is executed in four consecutive procedures, which are basic probability assignment with the PA approach, holistic credibility calculation, option and amelioration for BPA and evidence combination via the Dempster–Shafer rule, respectively. We give the specific discussions in detail as follows.

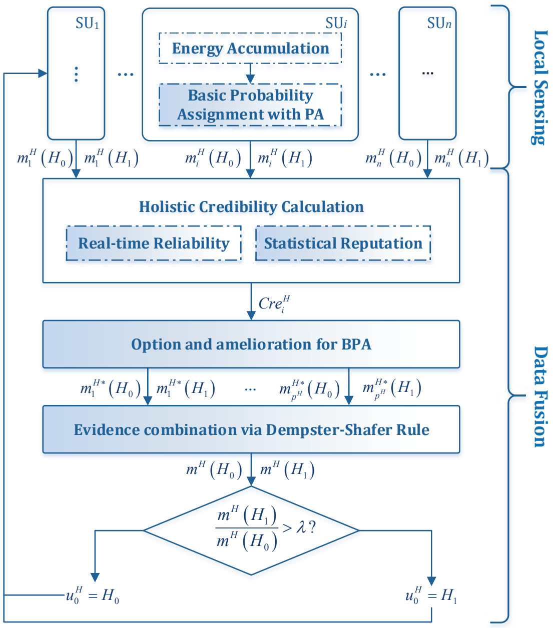
SU1
SUi
SUn
Energy Accumulation
Basic Probability Assignment with PA
Local Sensing
$m_1^H(H_0)$ $m_1^H(H_1)$
$m_i^H(H_0)$ $m_i^H(H_1)$
$m_n^H(H_0)$ $m_n^H(H_1)$
Holistic Credibility Calculation
Real-time Reliability
Statistical Reputation
Cre_i^H
Option and amelioration for BPA
$m_1^{H*}(H_0)$ $m_1^{H*}(H_1)$ ··· $m_{p^H}^{H*}(H_0)$ $m_{p^H}^{H*}(H_1)$
Evidence combination via Dempster-Shafer Rule
$m^H(H_0)$ $m^H(H_1)$
$\frac{m^H(H_1)}{m^H(H_0)} > \lambda?$
$u_0^H = H_0$
$u_0^H = H_1$
Data Fusion

Figure 2. Process description of the faithworthy collaborative spectrum sensing (CSS) scheme based on credibility and evidence theory in cognitive radio networks.

3.1. Basic Probability Assignment with the PA Approach

Detecting LU's state is a binary hypothesis testing problem in the context of spectrum sensing, and the recognition framework is $\Omega = \{H_1, H_0\}$. Naturally, 2^{Ω} is the set of all subsets of Ω, including the empty set $\varnothing$. SUs act as the information source and provide a set of elementary evidences. For SU_i, the evidence theory under the form of elementary masses assigns a belief mass to each element of the set 2^{Ω}. These masses are defined as function m, which maps the power set of Ω (i.e., $\Re(\Omega)$) to the interval of $[0, 1]$ and satisfies the following conditions: $m(\varnothing) = 0$ and $\sum_{k=1}^{|\Re(\Omega)|} m(A_k) = 1$, $A_k \in m(A_k)$, $2^{\Omega} = \{\varnothing, H_0, H_1, \Omega\}$ in the framework, and $|\Re(\Omega)|$ is the cardinality of $\Re(\Omega)$ [19]. For A_k, $m(A_k)$ represents that one believes to pledge exactly to set A_k, when a certain piece of evidence is given [23]. The set A_k satisfying $m(A_k) > 0$ is called the focal set, and in the D-S theory of evidence, the plausibility and belief function are expressed as follows:

$$\text{Pl}(B) = \sum_{A_k | A_k \bigcap B \neq \varnothing} m(A_k) \tag{5}$$

$$\text{Bel}(B) = \sum_{A_k | A_k \subseteq B} m(A_k) \tag{6}$$

where $B \in \Re(\Omega)$. $\text{Bel}(B)$ evaluates the minimum or definitive support for hypothesis B, whereas $\text{Pl}(B)$ evaluates the maximum or possible support that could be put in hypothesis B if more evidence became available. In the binary hypothesis test problem of CSS, in fact, $\text{Bel}(H_0) = m(H_0)$ and $\text{Bel}(H_1) = m(H_1)$. Therefore, in the following discussion, BPA function m is constantly utilized to denote the belief of hypotheses H_0 and H_1.

After the process of energy accumulation, the BPA function for each sensing node SU_i can be acquired according to the following equations [19]:

$$m_i^H(H_0) = \int_{y_{Ei}^H}^{+\infty} \frac{1}{\sqrt{2\pi}\sigma_{0i}} exp(-\frac{(x-\mu_{0i})^2}{2\sigma_{0i}^2})dx \tag{7}$$

$$m_i^H(H_1) = \int_{-\infty}^{y_{Ei}^H} \frac{1}{\sqrt{2\pi}\sigma_{1i}} exp(-\frac{(x-\mu_{1i})^2}{2\sigma_{1i}^2})dx \tag{8}$$

$$m_i^H(X) = 1 - m_i^H(H_0) - m_i^H(H_1) \tag{9}$$

where $i \in \{1, 2, \ldots, n\}$; SUs then send the BPAs to DFC. That is to say, the report of SU_i at the H-th sensing slot is $u_i^H = [m_i^H(H_0), m_i^H(H_1)]$.

Considering the power limitation of sensor nodes, the transmitting data from each SU to DFC need to be reduced. Under this circumstance, we propose to adjust BPA functions $m_i^H(X), m_i^H(H_0), m_i^H(H_1)$ into modified BPA functions $\hat{m}_i^H(H_0), \hat{m}_i^H(H_1)$ by utilizing a projection approximation (PA) technique.

On the basis of the fact that only hypotheses H_0 and H_1 are related to spectrum sensing, for the sake of ensuring that the modified BPA function is suitable for the D-S theory and has no impact on the performance of combination, we introduce the projection approximation approach to improve local BPA masses. At first, orthogonal decomposition is employed to project $m_i^H(X)$ onto the coordinate axes of hypotheses H_0 and H_1, then the projection of $m_i^H(X)$ can be denoted as:

$$\rho_{H_0}^H = \frac{m_i^H(H_0) \cdot m_i^H(X)}{\sqrt{m_i^H(H_0)^2 + m_i^H(H_1)^2}} \tag{10}$$

$$\rho_{H_0}^H = \frac{m_i^H(H_0) \cdot m_i^H(X)}{\sqrt{m_i^H(H_0)^2 + m_i^H(H_1)^2}} \tag{11}$$

Afterwards, adding the original BPAs under two hypotheses to their projections on the corresponding coordinate axis and carrying out normalization, the modified BPA function $\hat{m}_i^H(H_0)$, $\hat{m}_i^H(H_1)$ can thereby be obtained:

$$\hat{m}_i^H(H_1) = \frac{\rho_{H_1}^H + m_i^H(H_0)}{(m_i^H(H_0) + \rho_{H_0}^H) + (m_i^H(H_1) + \rho_{H_1}^H)} \tag{12}$$

$$\hat{m}_i^H(H_0) = \frac{\rho_{H_0}^H + m_i^H(H_0)}{(m_i^H(H_0) + \rho_{H_0}^H) + (m_i^H(H_1) + \rho_{H_1}^H)} \tag{13}$$

Due to $\hat{m}_i^H(H_0) + \hat{m}_i^H(H_1) = 1$, rendering $m_i^H(X) = 0$, consequently, in accordance with the PA approach in (14) and (15), not only the transmitting data from SU$_i$ to the DFC are half reduced, but also the bandwidth cost is deceased. This can be attributed to the fact that SU$_i$ only requires transmitting $\hat{m}_i^H(H_0)$, while other existing methods need to report both $m_i^H(H_1)$ and $m_i^H(H_0)$. The PA approach enables one to almost half reduce the transmission data for *n* SUs. This means a great advantage if there exists a high number of SUs, especially when the transmitting and the receiving accounting for the most power consuming part of the SUs are obliged to be considered; this PA approach is capable of achieving a long operational life span of sensor battery. In addition, the situation of the limited spectrum resources is quite urgent in wireless communication; in this case, the PA method also possesses an extremely high benefit of bandwidth owing to the reduction in transmitting data.

3.2. Holistic Credibility Calculation

In order to remove or mitigate the harmful effect on the performance caused by the attack behaviors of MUs, the reports from distinct nodes are supposed to be treated with dissimilarity. In the proposed scheme, the credibility of each SU is evaluated by its holistic credibility, which contains two factors, i.e., the real-time reliability and the statistical reputation. Specifically, the real-time reliability of SU$_i$ represents the credibility of BPAs from SU$_i$ at the H-th sensing round, whilst the statistical reputation of SU$_i$ represents the credibility of historical reports from SU$_i$. Through combining these two factors, both current and historical information about the credibility of each SU can be well exploited.

3.2.1. Real-Time Reliability

Since the local sensing results from the malicious SU will be distorted at some sensing slots, its evidence is not consistent with others' all of the time. In other words, if the evidence of one SU is similar to other SUs, this SU acquires a higher supportive degree from other SUs. Otherwise, if single SU's evidence is obviously different from others, it gets a less supportive degree from others. Then, it will be considered as untrustworthy and removed before fusing evidence at the DFC. Therefore, we can evaluate the real-time reliability of SU$_i$ based on its reports' similarity with other SUs at each sensing round. Specifically, the similarity degree of reported BPAs between SU$_i$ and SU$_j$ can be represented by the following formulation [16]:

$$sim_{ij}^H = \frac{\sum_{k=1}^{|\Re(\Omega)|} \min(\hat{m}_i^H(A_k), \hat{m}_j^H(A_k))}{\frac{1}{2}\sum_{k=1}^{|\Re(\Omega)|}(\hat{m}_i^H(A_k) + \hat{m}_j^H(A_k))} \tag{14}$$

Afterwards, the similarity degree matrix can be shown as:

$$Sim^H = \begin{pmatrix} 1 & \cdots & sim_{1j}^H & \cdots & sim_{1n}^H \\ \vdots & 1 & \vdots & \vdots & \vdots \\ sim_{i1}^H & \cdots & 1 & \cdots & sim_{in}^H \\ \vdots & \vdots & \vdots & 1 & \vdots \\ sim_{n1}^H & \cdots & sim_{nj}^H & \cdots & 1 \end{pmatrix} \tag{15}$$

The diagonal entries of the similarity degree matrix are all equal to one, and according to Equation (14), the value of each similarity degree is less than or equal to one. Consequently, the similarity degree matrix evidently possesses a convergence property, which ensures the effectiveness and validity of the proposed sensing method under the harmful attack behavior launched by malicious SUs. Through adding up the general similarity degree of SU$_i$ with regard to other SUs, the support to the BPAs from SU$_i$ at the H-th sensing slot is written as:

$$Sup_i^H = \sum_{j=1}^{n} sim_{ij}^H, \quad j \neq i, \quad i, j = 1, 2, \ldots, n \tag{16}$$

As a consequence, the real-time reliability of SU$_i$ can be acquired by normalizing the support and denoted as:

$$Rel_i^H = \frac{Sup_i^H}{\max(Sup_i^H)} \tag{17}$$

Nevertheless, CR networks have open and dynamic characteristics; there exist numerous possible factors that cause relatively low real-time reliability. Besides, the randomness of wireless channels (i.e., shadowing, fading effects and noise uncertainty) results in inaccurate BPA acquired by SUs at local sensing. Under the impact of all sorts of randomness, the performance of an honest SU can deteriorate severely at certain sensing slots. At that moment, its reported results have a great difference from others' reports or even have high similarity with the reports from MUs. In addition, if the number of malicious SUs in the network increases, the malicious SUs will support mutually and falsify the evaluation of real-time reliability remarkably. Therefore, only with the assistance of real-time reliability, we can neither arrive at a conclusion that an SU is genuine or malicious precisely. To resolve this issue, we introduce a reputation mechanism into the proposed scheme.

3.2.2. Statistical Reputation

Although statistical reputation cannot evaluate SU's credibility in a real-time manner, it is capable of obtaining the deduction concerning the historical reliability of SUs in line with their reported local results previously. Moreover, the statistical reputation is more stable due to its statistic characteristics; it is less likely to be affected by random interference. Therefore, statistical reputation and real-time reliability become mutually complementary; both factors should be jointly utilized to calculate the holistic credibility of cognitive users.

In most existing reputation-based CSS mechanisms [24–26], the reputation values of SUs are computed by simple counting rules. If the transmitted result of one SU is consistent with the global result made by DFC, then the reputation of this node is increased by one; otherwise, reducing the reputation by one. Two main drawbacks exist in this method: Firstly, this way of reputation updating is based on the global decision made by DFC and updating via the strategy of "same increase and decrease". When the correctness of the final decision cannot be guaranteed under the attack behavior of malicious SUs, the reference value of SU's reputation acquired by this approach declines to some degree. Secondly, the computing mode of the counting rule only cares about the consistency between local reports and the global decision. However, the BPA forwarded by SUs are dissimilar at each sensing round, which contains different messages with regard to the operating state of the LU. The process mode "black or white" leads to unnecessary losses of useful information.

In order to overcome the above shortcomings, we consider the imperfection of the global decision made by DFC and utilize the BPA reported from SU$_i$ and the BPA merged by DFC at the $(H-1)$-th slot to update the statistical reputation of SU$_i$ at the H-th slot. Specifically, for the sake of distinguishing with different situations when DFC makes final decisions, two parameters are defined: the self-evaluated faith f_i and the center-evaluated faith f, respectively. The higher self-evaluated faith f_i is, the more convinced that SU$_i$ is of its reported BPA. Similarly, higher center-evaluated faith f means a higher degree of conviction that the DFC feels about its combined BPA. Both the self-evaluated faith f_i and the center-evaluated faith f are calculated by the DFC.

At the $(H-1)$-th sensing round, the center-evaluated faith and the self-evaluated faith can be respectively expressed as:

$$f^{H-1} = |m^{H-1}(H_0) - m^{H-1}(H_1)| = |2 \cdot m^{H-1}(H_0) - 1| \tag{18}$$

$$f_i^{H-1} = |\hat{m}_i^{H-1}(H_0) - \hat{m}_i^{H-1}(H_1)| = |2 \cdot \hat{m}_i^{H-1}(H_0) - 1| \tag{19}$$

where $m^{H-1}(H_0)$ and $m^{H-1}(H_1)$ represent the combined BPAs calculated by the DFC at the $(H-1)$-th slot (the computational formula is given in Section 3.4). Obviously, $f^{H-1} \in [0,1]$ and $f_i^{H-1} \in [0,1]$. Hence, the statistical reputation of SU$_i$ can be calculated as follows:

$$r_i^H = l \cdot r_i^{H-1} + (-1)^{u_0^{H-1} + w_i^{H-1}} \cdot \frac{f_i^{H-1} + \alpha}{\alpha + 1} \cdot \frac{f^{H-1} + \beta}{\beta + 1}, \quad H = 2, 3, \ldots \tag{20}$$

where r_i^H represents the statistical reputation of SU$_i$ at the $(H-1)$-th sensing slot, u_0^{H-1} denotes the one-bit global decision made by the DFC, w_i^{H-1} denotes the suppositional local decision of SU$_i$ inferred by the DFC and l is the decay factor. It is worth noting that there is no need for SU$_i$ to make a decision or transmit its local decision result (in order to reduce network overhead). The DFC can deduce the local judgment that will be made by SU$_i$ from its forwarded BPA (i.e., the reported BPA from SU$_i$ contains this information). The suppositional local decision of SU$_i$ inferred by the DFC can be denoted as:

$$w_i^{H-1} = \begin{cases} 1, & \text{if } \frac{m_i^{H-1}(H_1)}{m_i^{H-1}(H_0)} > \lambda \\ 0, & \text{if } \frac{m_i^{H-1}(H_1)}{m_i^{H-1}(H_0)} \leq \lambda \end{cases} \tag{21}$$

where the decision threshold is determined by the DFC in terms of the different performance requirements of the spectrum sensing system.

The fundamental principle of the update mode of statistical reputation can be explained by Formula (24). In the first place, the variation tendency of statistical reputation r_i^H depends on the one-bit global decision u_0^{H-1} of DFC and the suppositional local decision w_i^{H-1}. If u_0^{H-1} is equal to w_i^{H-1}, statistical reputation r_i^H increases; otherwise, it decreases. This signifies that the cognitive user who makes the same decision result as DFC will obtain a higher statistical reputation. In the next place, the amplitude of variation of statistical reputation is decided by the center-evaluated faith f^{H-1} and the self-evaluated faith f_i^{H-1} jointly. If f^{H-1} and f_i^{H-1} are both close to one (here, SU$_i$ and DFC are both convinced of their BPAs), the change size of statistical reputation is also close to one. If the DFC (or SU$_i$) lacks faith in its BPA, then f^{H-1} (or f_i^{H-1}) will decrease, which leads to the changed size of r_i^H diminishing correspondingly. Therefore, statistical reputation is capable of performing updating with a flexible increase/decrease and changeable size according to the transmitted BPAs from SUs and the combined BPA made by DFC in the last sensing round.

Furthermore, although the global decision made by DFC may have errors at some sensing round, it is still more reliable than the reported decision of a single node (due to diversity gain). In view of this fact, we introduce amendatory parameters α, β to adjust the relative position between DFC and a single node. Generally speaking, $\beta > \alpha > 0$ is set to ensure the center-evaluated faith f^{H-1} plays an important role in the update of r_i^H; otherwise, the updating amplitude is basically decided by the self-evaluated faith f_i^{H-1} of SU$_i$; hence, the changeable size of r_i^H of each SU will become consistent basically, and the reputation assessment mechanism loses its function, as well. $\beta > \alpha$ also reflects the difference in credibility degree between DFC and the single node. In practical application, parameters α and β can be adjusted by empirical data in the CSS system or be determined by experimental results when the number of malicious SUs and attack patterns are known.

The single SU may possess distinct sensing performance at different sensing rounds due to human factors or objective factors; the reference value of the reported results a long time ago is relatively low and cannot reasonably reflect the current performance of SU. Therefore, the decay factor l is introduced to make the quality of the results reported recently accounting for a larger proportion. l should not be set too small, otherwise the historical behavior information cannot be brought into sufficient usage; on the other hand, remaining sensitive to the potential behavior change of SUs requires that l should not be set too large, either.

Different SUs have different reported history; generally, only part of SUs' statistical reputation values exceeds zero. We normalize the statistical reputations of these SUs, and r_i^H of SU$_i$ at the H-th sensing slot can be denoted as:

$$Rep_i^H = \begin{cases} \frac{r_i^H}{\max(r_i^H)}, & r_i^H > 0 \\ 0, & r_i^H \leq 0 \end{cases} \tag{22}$$

In the initial stage, $r_i^1 = \Delta, i = 1, 2, \ldots, n$. Apparently, manifold feasible modes can be utilized to combine the real-time reliability and statistical reputation effectively. Here, an easy and practicable mode is taken to acquire the holistic credibility by normalizing the sum of these two factors:

$$Cre_i^H = \begin{cases} \frac{Rel_i^H + Rep_i^H}{\max(Rel_i^H + Rep_i^H)}, & Rep_i^H > 0 \\ 0, & Rep_i^H = 0 \end{cases} \tag{23}$$

Consequently, the holistic credibility calculation can differentiate malicious SUs from genuine ones on account of their historical behaviors; besides, it can hold the current difference for SUs to realize better real-time performance, as well.

3.3. Option and Amelioration for BPA

In terms of the holistic credibility of SUs, the DFC is able to choose competent SUs to take part in the subsequent procedure of evidence combination. Concretely, we compare the holistic credibility Cre_i^H of SU$_i$ with a determined credibility threshold ς. If $Cre_i^H < \varsigma$, then it will be treated as a malicious user and abandoned at time slot H; conversely, if Cre_i^H exceeds threshold ς, the BPAs of SU$_i$ will be ameliorated by the DFC with the homologous holistic credibility:

$$m_i^{H*}(H_0) = Cre_i^H \cdot \hat{m}_i^H(H_0) \tag{24}$$

$$m_i^{H*}(H_1) = Cre_i^H \cdot \hat{m}_i^H(H_1) \tag{25}$$

3.4. Evidence Combination via the Dempster–Shafer Rule

All of the adjusted BPAs are appropriately merged to obtain the combined BPAs in accordance with the D-S evidence theory [22]:

$$m^H(H_0) = \frac{\sum\limits_{\bigcap A_i = H_0} \prod\limits_{i=1}^{p^H} m_i^{H*}(A_i)}{1 - \sum\limits_{\bigcap A_i = \varnothing} \prod\limits_{i=1}^{p^H} m_i^{H*}(A_i)} \tag{26}$$

$$m^H(H_1) = \frac{\sum\limits_{\bigcap A_i = H_1} \prod\limits_{i=1}^{p^H} m_i^{H*}(A_i)}{1 - \sum\limits_{\bigcap A_i = \varnothing} \prod\limits_{i=1}^{p^H} m_i^{H*}(A_i)} \tag{27}$$

where $A_i \in \Re(\Omega), i = 1, 2, \ldots, p^H$ and p^H represents the number of sensing nodes whose BPAs are opted and ameliorated to take part in the center data fusion at time round H.

Finally, in accordance with the following decision rule, the combined BPAs $m^H(H_1)$ and $m^H(H_0)$ are utilized to make the final global decision. The DFC compares $\frac{m^H(H_1)}{m^H(H_0)}$ with the decision threshold λ. If $\frac{m^H(H_1)}{m^H(H_0)} \leq \lambda$, the global decision u_0^H is H_0; if $\frac{m^H(H_1)}{m^H(H_0)} > \lambda$, the global decision u_0^H is H_1. λ is the same decision threshold as utilized in Equation (25). Once the DFC make the global decision, the statistical reputation can be updated for the detection of the next round of collaborative spectrum sensing.

4. Simulation Results

Numerous simulation experiments are provided in this section to evaluate the performance of the proposed faithworthy CSS scheme and compare it with several existing schemes, which are presented in Figures 3–8. Here, we presented four CSS schemes based on D-S evidence theory: 'D-S Cre' (Cre is the abbreviation for Credibility) represents our proposed faithworthy CSS scheme; the curve of 'D-S Men' (Men represents the author in [17]) shows the robust CSS method with mutually supportive degree presented in [17]; another enhanced scheme with similarity degree calculation proposed in [16] is shown as 'D-S Han'; and 'D-S Nhan' represents the enhanced scheme with reliability source evaluation proposed in [15]. Besides, 'OPT LIN' shows the optimal linear CSS scheme proposed in [13], and 'SINGLE' shows the spectrum sensing scenario of single SU. The effect of both FAMD and FA attack models is explored with different numbers of malicious SUs.

4.1. Simulation Parameter Setting

The simulation experiments are conducted in a CRN with one LU, $n = 6$ SUs and one DFC, which are considered to run for 10,000 rounds. We assume the LU signal is the Digital Television (DTV) signal as in [14], and the probabilities of the presence and absence of LU are $P_{H_1} = P_{H_0} = 0.5$. The time-bandwidth product TW is set to be 20. The initial reputation value Δ of each SU is six, and the credibility threshold ς is 0.75. In the statistical reputation, the decay factor l is set to be 0.9; the amendatory parameters $\alpha = 1$, $\beta = 3$. As for attack parameters, the attack with probabilities $P_a = 0.8$, and the attack intensity factors $\xi = 0.6$. We select the attack thresholds η as an right intersection point of two probability density functions (PDFs) under hypotheses H_1 and H_0. In addition, the average received SNR values of six nodes are set to be −5, −4, −3, −2, −1 and 0 dB, respectively.

4.2. Performance Evaluation

Under the situation that no malicious SUs exist in the CR network, Figure 3 illustrates the sensing performance of the aforementioned six CSS schemes through receiver operating characteristics (ROC) curves. We take the sensing performance of single node (the second SU with average SNR $\gamma_2 = -4$ dB) as a reference curve, which is presented in the rest of the simulations, as well. As can be seen from the figure, each of the sensing schemes achieves superior performance under the absence of SSDF attackers in the network. It should be admitted that although our proposed scheme obviously outperforms the D-S Han and D-S Men schemes, it is slightly inferior to the OPT LIN and D-S Nhan algorithms. However, these two schemes need a priori information that the DFC is required to possess the average SNR of each SU in order to achieve limited performance advantage. Contrarily, in our proposed D-S Cre algorithm, only cognitive nodes need to utilize their own average SNR information in the phase of local evidence extraction, while the DFC does not need such a priori information. Accordingly, the implementation requirements for the proposed D-S Cre scheme are lower; meanwhile, it is easier to realize in actual CRNs. Furthermore, owing to the aid of the PA approach, half of the transmitted data volume has been reduced, which greatly saves the valuable resources of the control channel.

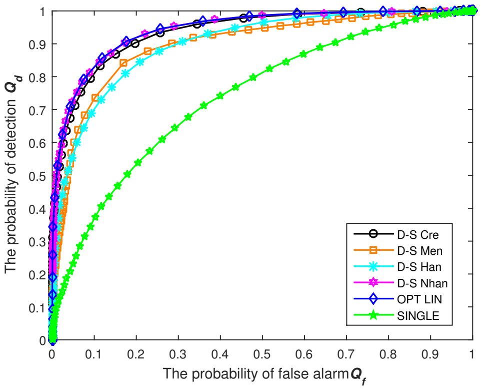

Figure 3. Detection performance comparison of each scheme without MUs . D-S, Dempster-Shafer; OPT LIN, optimal linear.

Figures 4 and 5 show the sensing performance when there is only one malicious SU in the network; among which, Figure 4 illustrates the sensing performance when the MU adopts the FAMD attack model, and Figure 5 shows the detection performance when the FA attack model is employed by the malicious SU. In both cases, the worst network circumstance has been considered, i.e., the cognitive node with the highest average SNR SU$_6$ ($\gamma_6 = -0$ dB) is the only MU. The performance of a single node is considered the same as above.

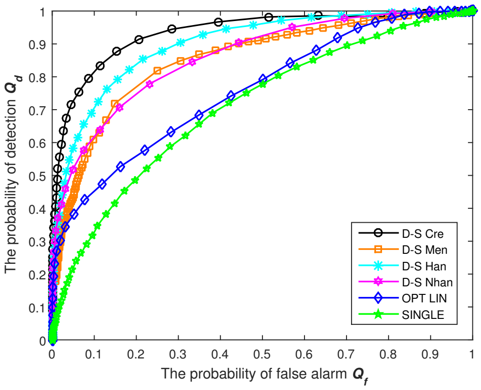

Figure 4. Detection performance comparison of each scheme when there is one false alarm and miss detection (FAMD) attacker in the network.

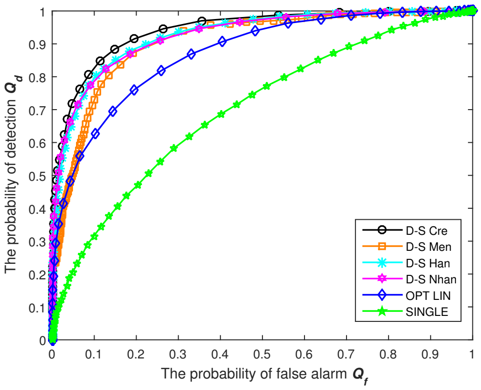

Figure 5. Detection performance comparison of each scheme when there is one FA attacker in the network.

We can see from Figure 4 that, under the impact of one FAMD attacker, the sensing performance of our proposed faithworthy CSS scheme performs spectrum sensing in a robust manner, and it is obviously superior to all o the algorithms that have been taken into account. This means that the proposed D-S Cre scheme has the strongest ability for defense against FAMD attack from malicious SUs. The performance of all of the other CSS schemes suffer varying degrees of damage, especially for the OPT LIN method, which has extremely weak capability to counter the FAMD attacker. As illustrated in Figure 5, the performance of the proposed secure scheme has a slight advantage over the D-S Han and D-S Nhan schemes and outperforms the D-S Men and OPT LIN methods under the influence of a single FA attacker. Both the D-S Han and D-S Nhan methods performs equivalently under the presence of this sort of MU. The performance superiority of our faithworthy CSS scheme benefits from taking full advantage of the holistic credibility of SUs, meanwhile opting and ameliorating the forwarded basic probability assignment, as elaborated in Section 3.

Figures 6–8 have presented the performance comparison of each scheme when there exist two malicious SUs in the CRN. Without loss of generality, we consider the worst attack circumstance in the network, i.e., the cognitive node with the highest average SNR $\gamma_6 = -0$ dB (SU$_6$) and the node with average SNR $\gamma_5 = -1$ dB (SU$_5$) are assumed to be the two malicious users. In Figure 6, both SU$_5$ and SU$_6$ appear as FAMD attackers, whilst these two users adopt the FA attack pattern to launch the attack in the scenario in Figure 7. SU$_5$ in Figure 8 works as an FA attacker, while SU$_6$ employs the FAMD attack model to compromise the performance of the cognitive system.

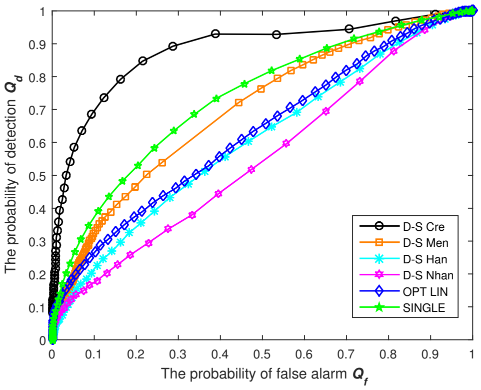

Figure 6. Detection performance comparison of each scheme when there are two FAMD attackers in the network.

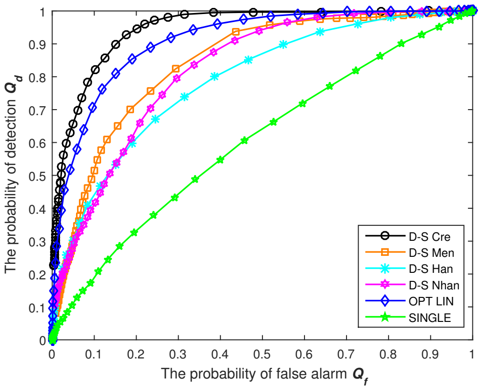

Figure 7. Detection performance comparison of each scheme when there are two FA attackers in the network.

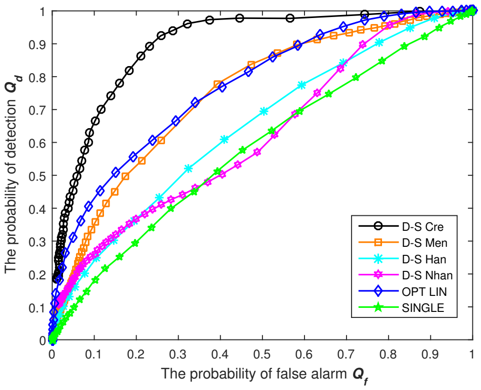

Figure 8. Detection performance comparison of each scheme when there are one FAMD attacker and one FA attacker in the network.

Under the impact of two FAMD attackers, as shown in Figure 6, the performance of all of the schemes within the scope of consideration have been seriously compromised, except for our proposed scheme. The performance of the comparison algorithm is even worse than that of the single node, which leads to an extremely detrimental effect on the cognitive system. On the contrary, the proposed D-S Cre scheme shows robust sensing capability, even under the situation of a destructive and powerful attack from MUs. This enables the CSS system to resist SSDF attack successfully.

Figure 7 evaluates the sensing performance of each scheme when there are two FA attackers in the network. It can be clearly seen that our proposed D-S Cre scheme possesses the most excellent performance compared to other CSS methods. The performance of the D-S Han scheme degrades dramatically in the presence of two FA attack users, and the OPT LIN method can maintaining relatively robust spectrum sensing performance.

In addition, the scenario of one FA attacker and one FAMD attacker existing in CRN is illustrated in Figure 8. Again, a sharp fall occurs in the contrast algorithms. The sensing performance of the D-S Men and OPT LIN schemes has a slight advantage over the D-S Han and D-S Nhan methods. However, none of them is capable of countering this sort of combined attack mode. Our proposed CSS scheme can still achieve preferable detection performance, i.e., detecting the LU signal and restraining malicious users in an effective and robust manner.

Ultimately, by comparing the performance of CSS schemes in Figures 6–8 with that in Figures 4 and 5, we can see that all CSS algorithms have different degrees of overall performance degradation with the increase of the number of malicious SUs. Therefore, the proposed D-S Cre method has obvious performance advantage both in detecting the licensed user and the malicious cognitive users; moreover, it has the strongest ability to defend against the typical SSDF attack behaviors.

5. Conclusions

In order to effectively defense against SSDF attack behaviors from malicious SUs, in this article, we propose a faithworthy CSS scheme based on the Dempster–Shafer theory of evidence and holistic credibility, including four consecutive procedures, which are basic probability assignment (BPA) with the PA approach, holistic credibility calculation, option and amelioration for BPA and evidence combination via the Dempster–Shafer rule, respectively. The projection approximation approach is introduced in this article to modify local BPA masses, which successfully reduces half of the required data volume transmitted from SUs to the DFC. Consequently, the transmitting bandwidth has been decreased, and the workload at DFC has been alleviated. Furthermore, through evaluating the credibility of SUs from both real-time difference and statistical sensing behavior, malicious SUs can be effectively distinguished from genuine ones. Abundant simulation experiments have been conducted and corroborated that the proposed scheme outperforms the existing ones under the influence of different attack modes and different numbers of malicious SUs. In the days ahead, more complex attack modes will be taken into account, meanwhile more effective approaches for holistic credibility calculation will be investigated.

Acknowledgments: This paper is funded by the National Key Foundation for Exploring Scientific Instrument of China (Grant No. 2016YFF0102806), the National Natural Science Foundation of China (Grant No. 51509049), the Natural Science Foundation of Heilongjiang Province, China (Grant No. F201345), and the Fundamental Research Funds for the Central Universities of China (Grant No. GK2080260140).

Author Contributions: Fang Ye conceived of the concept and performed the research. Xun Zhang conducted experiments to evaluate the performance of the proposed the CSS scheme and wrote the manuscript. Yibing Li and Chunrui Tang reviewed the manuscript. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Akyildiz, I.F.; Lee, W.; Vuran, M.C.; Mohanty, S. Next generation dynamic spectrum access cognitive radio wireless networks: A survey. *Comput. Netw.* **2006**, *50*, 2127–2159.
2. Chen, X.; Chen, H.; Meng, W. Cooperative communications for cognitive radio networks-from theory to applications. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1180–1192.
3. Zhang, J.; Yuen, C.; Wen, C.K.; Jin, S.; Wong, K.K.; Zhu, H. Large system secrecy rate analysis for SWIPT MIMO wiretap channels. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 74–85.
4. Digham, F.F.; Alouini, M.S.; Simon, M.K. On the energy detection of unknown signals over fading channels. *IEEE Trans. Commun.* **2007**, *55*, 21–24.
5. Cacciapuoti, A.S.; Akyildiz, I.F.; Paura, L. Correlation-aware user selection for cooperative spectrum sensing in cognitive radio Ad Hoc networks. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 297–306.
6. Cacciapuoti, A.S.; Caleffi, M.; Izzo, D.; Paura, L. Cooperative spectrum sensing techniques with temporal dispersive reporting channels. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 3392–3402.
7. Liu, Y.; Xie, S.; Yu, R.; Zhang, Y.; Yuen, C. An efficient MAC protocol with selective grouping and cooperative sensing in cognitive radio networks. *IEEE Trans. Veh. Technol.* **2013**, *62*, 3928–3941.
8. Deng, R.; Chen, J.; Yuen, C.; Cheng, P.; Sun, Y. Energy-efficient cooperative spectrum sensing by optimal scheduling in sensor-aided cognitive radio networks. *IEEE Trans. Veh. Technol.* **2013**, *61*, 716–725.
9. Zhang, L.; Ding, G.; Wu, Q.; Song, F. Defending against byzantine attack in cooperative spectrum sensing: Defense reference and performance analysis. *IEEE Access* **2016**, *4*, 4011–4024.
10. Varshney, P.K. *Distributed Detection and Data Fusion*; Springer: New York, NY, USA, 1997.
11. Kay, S.M. *Fundamentals of Statistical Signal Processing: Detection Theory*; Prentice-Hall: Saddle River, NJ, USA, 1998.
12. Chen, B.; Willett, P.K. On the optimality of the likelihood-ratio test for local sensor decision rules in the presence of non-ideal channels. *IEEE Trans. Inf. Theory* **2005**, *51*, 693–699.

13. Quan, Z.; Cui, S.G.; Sayed, A.H. Optimal linear cooperation for spectrum sensing in cognitive radio networks. *IEEE J. Sel. Top. Signal. Process.* **2008**, *2*, 28–40.
14. Peng, Q.H.; Zeng, K.; Wang, J.; Li, S.Q. A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context. In Proceedings of the 17th IEEE International Symposium on Personal, in Indoor and Mobile Radio Communications (IEEE PIMRC), Piscataway, NJ, USA, 11–14 September 2006; pp. 2511–2515.
15. Nhan, N.-T.; Insoo, K. An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context. *IEEE Commun. Lett.* **2009**, *13*, 492–494.
16. Han, Y.; Chen, Q.; Wang, J.X. An enhanced D-S theory cooperative spectrum sensing algorithm against SSDF attack. In Proceedings of the 75th IEEE Vehicular Technology Conference (IEEE VTC Spring), Piscataway, NJ, USA, 6–9 May 2012; pp. 1–5.
17. Men, S.Y.; Charge, P.; Pillement, S. A robust cooperative spectrum sensing method against faulty nodes in CWSNs. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICC), London, UK, 8–12 June 2015.
18. Nhan, N.-T.; Insoo, K. Evidence-theory-based cooperative spectrum sensing with efficient quantization method in cognitive radio. *IEEE Trans. Veh. Technol.* **2011**, *60*, 185–195.
19. Jana, S.; Zeng, K.; Cheng, W.; Mohapatra, P. Trusted collaborative spectrum sensing for mobile cognitive radio networks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1497–1507.
20. Wang, J.L.; Feng, S.; Wu, Q.H.; Zheng, X.Q.; Xu, Y.H.; Ding, G.R. A robust cooperative spectrum sensing scheme based on Dempster–Shafer theory and trustworthiness degree calculation in cognitive radio networks. *EURASIP J. Adv. Signal Process.* **2014**, *2014*, doi: 10.1186/1687-6180-2014-35.
21. Wang, W.K.; Li, H.S.; Sun, Y.; Han, Z. Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks. *EURASIP J. Adv. Signal Process.* **2010**, *4*, 1–15.
22. Shafer, G. *A Mathematical Theory of Evidence*; Princeton University Press: Princeton, NJ, USA, 1976.
23. Klir, G.J. *Uncertainty and Information: Foundations of Generalized Information Theory*; Wiley: Hoboken, NJ, USA, 2006.
24. Chen, R.L.; Park, J.M.; Bian, K. Robust distributed spectrum sensing in cognitive radio networks. In Proceedings of the 27th IEEE International Conference on Computer Communications (IEEE INFOCOM), Piscataway, NJ, USA, 13–18 April 2008.
25. Kun, Z.; Paweczak, P.; Cabric, D. Reputation-based cooperative spectrum sensing with trusted nodes assistance. *IEEE Commun. Lett.* **2010**, *14*, 226–228.
26. Lu, J.Q.; Wei, P. Improved cooperative spectrum sensing based on the reputation in cognitive radio networks. *Int. J. Electron.* **2015**, *102*, 855–863.