IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 31, 2020, accepted September 20, 2020, date of publication September 25, 2020, date of current version October 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3026738

An Enhanced Cooperative Spectrum Sensing Scheme Against SSDF Attack Based on Dempster-Shafer Evidence Theory for Cognitive Wireless Sensor Networks

DEGUI YAO, SHAOGUANG YUAN, ZHONGBIN LV, DIMING WAN, AND WANDENG MAO
Electric Power Research Institute, State Grid Henan Electric Power Company, Zhengzhou 450052, China

Corresponding author: Shaoguang Yuan (ysg_grid@tom.com)

This work was supported by the Science and Technology Project of State Grid Corporation of China under Grant 5200-201924303A-0-0-00.

ABSTRACT Due to the potential applicability of spectrum sensing, cognitive wireless sensor networks have attracted plenty of interest in the research community to improve the bandwidth utilization for practical applications. To alleviate the effect of multi-path fading and resolve the problem of hidden terminal, collaborative spectrum sensing (CSS) is regarded as effective technology to obtain better sensing accuracy. However, CSS is usually vulnerable to the attack behaviors originated from malicious sensor nodes. In this paper, an enhanced cooperative spectrum sensing scheme against SSDF attack based on Dempster-Shafer evidence theory for cognitive wireless sensor networks is introduced. First, the holistic credibility of sensor nodes can be evaluated according to the real-time difference between them and the statistical sensing behaviors. Furthermore, the basic probability assignment function can be defined based on evidence theory, and the credibility of sensor nodes can be estimated. Finally, by using the weighted probability assignment for each cognitive sensor node, the fusion center can reduce the influence of malicious sensor nodes on the final decision and ensure the reliability of reports from cooperative sensor nodes. Simulation results demonstrate that the proposed method can resist SSDF attacks significantly and outperform the traditional secure schemes in aspect of sensing accuracy.

INDEX TERMS Cooperative spectrum sensing, Dempster-Shafer evidence theory, data falsification, cognitive wireless sensor networks.

I. INTRODUCTION

By deploying spatially distributed autonomous sensor nodes, wireless sensor networks (WSNs) can monitor a wide range of ambient conditions and produce plenty of potential fields of applications [1]. Technically, most of the solutions for WSNs applications operate in unlicensed frequency bands and result in overcrowded status of the unlicensed spectrum bands, which degrades the performance of coexist systems significantly. To address above challenges, cognitive wireless sensor networks (CWSNs) has emerged to implement the opportunistic access to the spectrum and permit the sensor nodes to adapt their internal parameters for more reliable and efficient communication [2], [3]. It should be noted that the cognitive sensor node dynamically access the idle spectrum without affecting the authorized users, which provides a feasible measure to solve the problem of wireless spectrum resource scarcity for CWSNs. It also provides a new idea to solve the burst demand of wireless services to realize the utilization of spectrum resources [4].

To resolve the hidden terminal problem and alleviate the effect of multi-path fading, CSS is regarded as effective technology to obtain better sensing accuracy as well as reduce the probability of interference to authorized users. However, multiple sensor nodes jointly decide whether the primary user is occupying the spectrum resources, and there are some risks while obtaining benefits from spatial gains. During the process of CSS, the sensing results of each node need to be sent to the fusion center (FC) or other nodes for the data gathering or final decision making [5], [6]. Once the wrong

The associate editor coordinating the review of this manuscript and approving it for publication was Rongbo Zhu.

sensing information provided by malicious users is mixed in the fusion process, the wrong decision will be made, and the current status of authorization channels will be misjudged. Technically, spectrum sensing falsified data (SSDF) attack is one of the most serious threats in cooperative spectrum sensing [7]. For the sake of protecting the primary users from the interference, the FC require to gathering the reports from cooperative sensor nodes with conservative fusion strategies. Under the constraints, a small number of malicious users may mislead the FC to make a wrong decision [8], [9]. Therefore, it is of great significance to provide the CSS with secure mechanism against SSDF attacks. Therefore, in this paper, we propose an enhanced cooperative spectrum sensing scheme against SSDF attack, which employs Dempster-Shafer evidence theory to evaluate the credibility of sensor nodes. Generally, the major contributions of our paper can be summarized as follows:

i) evaluate the holistic credibility of sensor nodes according to the real-time difference between them and the statistical sensing behaviors.

ii) define the basic probability assignment function based on evidence theory, and propose a method to estimate the credibility of sensor nodes.

iii) utilize the weighted probability assignment for cooperative nodes to reduce the influence of malicious nodes on the fusion decision.

The remainder of the paper is organized as follows. Section 2 reviews the related works. Section 3 introduces the CSS method with energy detection and traditional SSDF attack types. The proposed cooperative spectrum sensing scheme against SSDF attack based on Dempster-Shafer evidence theory is presented in Section 4. The simulations and analysis are provided in Section 5, and the conclusions are presented in Section 6.

II. RELATED WORK

The emergence of cooperative spectrum sensing enables the secondary users (SUs) to acquire more reliable messages by sharing their sensing results, which improves the accuracy of sensing performance [10]. The whole process of CSS can be summarized as sensing stage and data fusion stage. SSDF attack often occurs in the stage of data fusion, in which malicious users can mislead the channel availability decision by sending false information [11].

Zhou *et al.* [12] proposed a defense algorithm based on Bayesian reputation model, and the main idea is to treat the cooperation process between cognitive radios as service and evaluation phase. The reputation value of SUs reflects their service quality, and the reputation value of secondary users will be updated by the reputation model. To resist probabilistic SSDF Attack, Wu *et al.* [13] introduced a weighted sequential probability ratio test scheme against SSDF attack, which integrates the reputation value of SUs into weight coefficient for sequential probability ratio test. By calculating the SU's suspicious degree, Liu *et al.* [14] proposed a defense model against SSDF attack, in which the defense model can distinguish malicious users and honest users and remove the incorrect report data of malicious nodes. By estimating attack strength, Sharifi *et al.* [15] proposed a novel method based on hard decision rule to obtain the optimum threshold value of voting and minimize the Bayes risk. By mathematical analysis of the upper and lower bounds of the theshold value, Wang *et al.* [16] proposed a dynamic threshold updating strategy based on the observations of the historical fusion value to defend against the probability SSDF attacks. When malicious users account for certain proportion of secondary users, the launch of large-scale SSDF attacks will make the system attain wrong sensing results. In such case, the above defense mechanisms are difficult to resist SSDF attacks.

To resolve the problem of distortion of data fusion in distributed spectrum sensing, Chen *et al.* [17] investigated some traditional data fusion techniques in terms of the robustness against Byzantine failures, and they proposed a reputation-based mechanism to the sequential probability ratio test. Chen *et al.* [18] applied Modified Grubbs test and employed Conjugate Prior-based theory to detect the malicious users based on the soft fusion scheme, in which the sensing reports is taken as a stochastic process. By investigating the malicious node's manipulation of sensing result independently or collaboratively, Hyder *et al.* [19] proposed an adaptive reputation-based clustering mechanism, which requires no prior knowledge of distribution of attacking nodes and is applicable for a wide range of attacking scenarios. Focusing on the massive attacks, Sharifi *et al.* [20] made use of Weighted Likelihood Ratio Test to estimate the credit value of each SU. Rawat *et al.* [21] presented a reputation based strategy to identify SSDF attackers. The shortage is mainly the inadequate identification of malicious and normal users as high percentage of independent attackers. Focusing on selfish attacks, Jo *et al.* [22] constructed an effective detection model for selfish cognitive radio attack, in which legitimate CR neighbors cooperate to prevent the selfish node from occupying all or partial resources of multiple channels.

Although plenty of the literature and comprehensive research on SSDF attack and defense has been made, most of them will be not specifically suited for CWSNs [23], [24]. Basically, the reason is that the framework of resource-constrained sensor nodes are not be considered, especially in aspect of the limitation of processing capacity and battery power. In addition, most CSS methods only decide whether a node is trusted according to the difference of the data upload in current sampling period, and do not make full use of the statistical information of its historical sensing behavior. However, due to the dynamic characteristics of wireless channel, those differences are unilateral, sometimes even inaccurate.

III. SYSTEM MODEL

A. COOPERATIVE SPECTRUM SENSING

CSS can overcome the shortcomings of individual spectrum sensing, so as to improve the spectrum sensing accuracy.

However, there exist certain security problems in either centralized or distributed cooperative spectrum sensing. Some malicious users will report falsified sensing information, which may be erroneous local detection results or modified sensing data, to maximize their personal interests rather than achieve high spectrum utilization [25], [26]. Therefore, the countermeasures will cope with the security threats only by determining the type of attack.

CSS usually consists of the following steps: local spectrum sensing, reporting transmission and global decision. Each cognitive sensor node first conducts local spectrum sensing independently for sampling the primary user's signals, and then sends the sensing result to the FC through the common control channel for final fusion. Finally, the received sensing results will be combined by linear fusion method, and the final decision results can be obtained according to the preset criteria.

Owing to easily implementation and not requiring any prior knowledge of signal characteristic about primary user, energy detection method is widely applied in CWSNs for local sensing [27]. Hence, the spectrum sensing will be modeled mathematically as a binary hypothesis test, and the sample of i-th sensor node at t-th interval can be expressed as:

$$E_i(t) = \begin{cases} n_i(t), & H_0 \\ h_i s_i(t) + n_i(t), & H_1 \end{cases} \tag{1}$$

where H_0 indicates that the detected channel is available for sensor nodes, and H_1 indicates that the detected channel is currently occupied by PU. $s_i(t)$ is the i-th sampling value of the transmitted signal from the primary user at t-th time interval. Besides, h_i represents the amplitude gain of the channel, and $n_i(t)$ is the sampling value of the noise signal by the i-th sensor node at t-th time interval. It is assumed that the noise signal by CR users is additive Gaussian white noise with mean value of 0 and variance of σ_i^2, and the noise and the transmitted signal from the primary user will be uncorrelated.

If each sensor node collects M samples during the signal observation interval, the energy detection result of the i-th sensor node can be expressed as

$$X_i = \sum_{t=1}^{M} [E_i(t)]^2 \tag{2}$$

Under the hypothesis H_0, X_i/σ_i^2 obeys the central chi square distribution with degree of freedom M. While under the hypothesis H_1, it obeys the non central chi square distribution of degree of freedom M, and the non central parameter is λ_i. Hence, the distribution of X_i/σ_i^2 can be expressed as:

$$X_i/\sigma_i^2 \sim \begin{cases} \chi_M^2, & H_0 \\ \chi_M^2(\lambda_i), & H_1 \end{cases} \tag{3}$$

where $\lambda_i = M\mu_i$ and $\mu_i = h_i^2 \sum_{t=1}^{M} (E_i(t))^2 / M\sigma_i^2$ means the average SNR of received signals.

According to the central limit theorem, if the number of the samples is large enough, X_i can be approximately normal distribution with the mean value

$$E(X_i) = \begin{cases} M\sigma_i^2, & H_0 \\ (M+\lambda_i)\sigma_i^2, & H_1 \end{cases} \tag{4}$$

and the variance

$$Var(X_i) = \begin{cases} 2M\sigma_i^4, & H_0 \\ 2(M+2\lambda_i)\sigma_i^4, & H_1 \end{cases} \tag{5}$$

Thus, the false alarm probability $P_{f,i}$ and detection probability $P_{d,i}$ of the i-th sensor node can be expressed as

$$P_{f,i} = \frac{1}{2} erfc\left(\frac{\gamma_i - M\sigma_i^2}{\sqrt{2M}\sigma_i^2}\right) \tag{6}$$

$$P_{d,i} = \frac{1}{2} erfc\left(\frac{\gamma_i - (M+\lambda_i)\sigma_i^2}{\sqrt{2(M+2\lambda_i)}\sigma_i^2}\right) \tag{7}$$

where γ_i denotes the local decision threshold of the i-th sensor node.

After completing the local spectrum sensing, all sensor nodes will send the local sensing results to the FC through the common control channel. Since error-correction coding in the physical layer can overcome the impact of noise on the transmitted information, we assumed that the sensor nodes report the sensing data to the FC through the error free common control channel.

B. SSDF ATTACK TYPES

By sending falsified observations, malicious nodes aim to create interference to primary transmitters. The four cases will be considered in common SSDF attack, which includes Always-busy, Always-free, Always-opposite and Random attack [28]–[30]. Among them, Always-opposite attack can be regarded as the combination of Always-busy and Always-free attack.

Always-opposite attack has a serious damage to the normal operation of the whole system. In soft fusion, two strategies launched by the attackers can achieve the always-opposite attack. The first strategy can be specifically described as: when the local decision of malicious user indicates the inexistence of the PU, the malicious user adds a component τ to the sensing data. Otherwise, the component τ will be subtracted to the sensing data, which result in the false impression of PU's existence. The secondary strategy is that the malicious user generates the reporting data in accordance with a certain distribution, i. e., when the local decision determines the PU's presence, the attacker falsifies the reports with the distribution under hypothesis H_1, and vice versa.

In addition, the probabilistic attack refers to that malicious users will launch SSDF attacks with specific probability. Malicious users can either choose always-busy, always-free or always-opposite attack strategies to change their reports when launching attacks, or send real sensing results directly when they do not launch attacks. Since it is very hard for

cognitive radio systems to deal with the probabilistic attacks based on always-opposite, this paper mainly studies the impact of such attacks on cooperative spectrum sensing based on soft fusion. The detailed discussions about the attack types are given as follows.

1) SCENARIO 1

Let θ_i denote the attacking probability of the malicious node. The larger value of θ_i indicates that the more frequent the malicious users launch attacks, which means that more serious damage can be created to the cognitive radio network.

The attack strategy of scenario 1 can be described as follows: the malicious user decides whether to launch an attack with probability θ_i. Once the malicious user launches an attack, it will first make a local decision and immediately generate the reporting which is opposite to the sensing result and send to the FC afterwards.

Let $X^*_{H_0,i}$ and $X^*_{H_1,i}$ be the energy sensing result sent by the i-th malicious user to fusion center under hypothesis H_0 and H_1, respectively. Then, the distribution of sensing results received by the fusion center from malicious users under hypothesis H_0 and H_1 can be expressed in (8) and (9), as shown at the bottom of the next page.

2) SCENARIO 2

The attack strategy by malicious node in scenario 2 is to add or subtract a component on the actual sensing data as we discussed before. When a malicious user decides to launch an attack, it will modify the sensing data based on the local decision so as to mislead the FC to make the wrong decision.

Suppose that the attacking probability of i-th malicious node is θ_i, and the modified component value of superposition or subtraction is τ_i. Thus, in scenario 2, the distribution of sensing results received by the fusion center from malicious users under hypothesis H_0 and H_1 can be expressed in (10) and (11), as shown at the bottom of the next page.

where $\tau_i = \omega\lambda_i\sigma_i^2$, and $\omega \in (0, 1)$

IV. PROPOSED METHOD

A. EVIDENCE THEORY

Owing to the advantage of reasoning with uncertainty, Dempster–Shafer theory is widely applied in network security, intelligent search and other fields [31]. Especially in information fusion, evidence theory can deal with the uncertain problems, such as signal detection, data classification, target recognition and so on [31]. Due to the randomness of the wireless channel, the detection of PU's signal is uncertain to detect. To resist the SSDF attack and enhance the accuracy of decision making in CWSNs, in this paper, we utilize the Dempster–Shafer theory to construct mathematical model for combining evidence from different sensor nodes and evaluate their credibility.

Definition 1: Assuming that $\Theta = \{\rho_1, \rho_2, \cdots, \rho_n\}$ is a limited recognition framework. The number of elements is finite and mutually exclusive framework [33], [34]. If exists $\Phi : 2^\Theta \to [0, 1]$ and

$$\begin{cases} \Phi(\emptyset) = 0, \\ \sum\limits_{A_k \subseteq \Theta} \Phi(A_k) = 1, \end{cases} \tag{12}$$

where Φ can be defined as the basic probability assignment (BPA) function. $\forall A_k \subseteq \Theta$ and $\Phi(A_k) > 0$, then A_k is a focal element of Θ. Meanwhile, it reflects the credibility of the evidence to A_k.

Considering that the detection of PU's activity can be regarded as a binary hypothesis testing, and the discernment framework based on Dempster-Shafer theory can be defined as $\Omega = \{H_0, H_1\}$ [35]. During the phase of energy detection, the BPA function of the i-th sensor node will be defined in the form of cumulative function as follows:

$$\begin{cases} \Phi_i^t(H_0) = \int_{x_{E_i}^t}^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{\left(x - M\sigma_i^2\right)^2}{2M\sigma_i^4}\right) dx \\ \Phi_i^t(H_1) = \int_{-\infty}^{x_{E_i}^t} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{\left(x - (M+\lambda_i)\sigma_i^2\right)^2}{2(M+2\lambda_i)\sigma_i^4}\right) dx \end{cases} \tag{13}$$

All sensor nodes will send their BPAs to FC, and the report of i-th sensor node at the t-th sensing slot can be represented as $\Phi_i^t = [\Phi_i^t(H_0), \Phi_i^t(H_1)]$.

In order to eliminate or mitigate the performance degradation caused by attackers, reports from different sensor nodes should be treated differently. In our scheme, the credibility of each sensor node is evaluated by its credibility, which involves two variables: current reliability and historical reputation. Among them, the current reliability of i-th sensor node is related to the BPA function of corresponding sensor node at certain time interval for spectrum sensing. In addition, the historical reputation should reflect the consistence of the sensor node's previous reporting with the final result. By combining those two variables, we can make good use of real-time and statistical information about sensor node's credibility.

B. FUSION DECISION BY DEMPSTER-SHAFER RULE

Since the reports from a malicious user are falsified occasionally according to the attacking probability, they will not be consistent with the ones from other sensor nodes all the time. Therefore, the current reliability of sensor node can be evaluated based on its reports' similarity with other sensor nodes at each time interval. Firstly, according to the reporting submitted by each sensing node, the probability allocation value of the decision result is calculated. The probability allocation vector of each node will be taken as evidence, and the Jousselme distance is estimated to evaluate the degree of conflict between evidences. Then, the trust degree of each sensing node is determined according to the obtained evidence conflict, and the weight value can be assigned. Secondly, the weighted combination of above evidences should be modified to achieve the purpose of reducing the evidence

conflict. Finally, the decision will be obtained through the fusion of evidence theory.

Definition 2: Suppose that Φ_i and Φ_j are BPA functions in recognition framework Θ, the Jousselme distance [36] between relevant evidences can be defined as:

$$d_J\left(\Phi_i, \Phi_j\right) = \sqrt{\frac{1}{2}\left(\Phi_i - \Phi_j\right)^T \Psi \left(\Phi_i - \Phi_j\right)} \tag{14}$$

where Ψ denotes a matrix with the dimensions of $\left(2^\Theta - 1\right) \times \left(2^\Theta - 1\right)$, and $\Psi(u, v) = \frac{u \cap v}{u \cup v}$, u and v is the subset of Θ.

Next, the Jousselme distance can be calculated by introducing the evidence from each sensing node into the Eq. (15), and then we can obtain the evidence distance matrix as:

$$D^\Omega = \begin{bmatrix} 0 & d_J\left(\Phi_1, \Phi_2\right) & \cdots & d_J\left(\Phi_1, \Phi_N\right) \\ d_J\left(\Phi_2, \Phi_1\right) & 0 & \cdots & d_J\left(\Phi_2, \Phi_N\right) \\ \vdots & \vdots & \ddots & \vdots \\ d_J\left(\Phi_N, \Phi_1\right) & d_J\left(\Phi_N, \Phi_2\right) & \cdots & 0 \end{bmatrix} \tag{15}$$

Also, the matrix D^Ω reflects the degree of conflict between the evidences obtained by each cooperative sensing node. The similarity coefficient in the original Jousselme distance shows that each element is calculated according to the same similarity criterion, which prove the basic probability assignment values in set Θ be positive. However, the basic probability distribution of test statistics of each sensor node is uneven in practical applications, and the similarity measurement of evidence is also different.

Therefore, the trust degree between the evidences can be deduced based on the degree of conflict among the evidences, and it can be expressed by the matrix R:

$$R = \begin{bmatrix} 1 & r_{12} & \cdots & r_{1N} \\ r_{21} & 1 & \cdots & r_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ r_{N1} & r_{N2} & \cdots & 1 \end{bmatrix} \tag{16}$$

where $r_{ij} = 1 - d_J\left(\Phi_i, \Phi_j\right)$.

According to the above matrix, the credibility of i-th sensor node's evidence relative to j-th node can be estimated as:

$$SP_i = \sum_{j=1, j\neq i}^{N} r_{ij} \tag{17}$$

By normalizing the credibility of each node's evidence, we can get their respective weights as follows

$$w_i = \frac{SP_i}{\sum_{i=1}^{N} SP_i} \tag{18}$$

Furthermore, the FC obtains the modified evidence by weighting the evidence of each node as:

$$\begin{cases} \hat{\Phi}_i^t\left(H_0\right) = w_i \times \Phi_i^t\left(H_0\right) \\ \hat{\Phi}_i^t\left(H_1\right) = w_i \times \Phi_i^t\left(H_1\right) \end{cases} \tag{19}$$

Consequently, by employing the combination rule of Dempster-Shafer theory, the aggregated result under different hypotheses can be expressed as:

$$\begin{aligned} \Phi^t\left(H_0\right) &= \hat{\Phi}_1^t\left(H_0\right) \oplus \hat{\Phi}_2^t\left(H_0\right) \oplus \cdots \oplus \hat{\Phi}_s^t\left(H_0\right) \\ &= \frac{\sum_{\cap A_k = H_0} \prod_{i=1}^{s} \hat{\Phi}_s^t\left(A_k\right)}{1 - \sum_{\cap A_k = \emptyset} \prod_{i=1}^{s} \hat{\Phi}_s^t\left(A_k\right)} \end{aligned} \tag{20}$$

$$\begin{aligned} \hat{\Phi}^t\left(H_1\right) &= \hat{\Phi}_1^t\left(H_1\right) \oplus \hat{\Phi}_2^t\left(H_1\right) \oplus \cdots \oplus \hat{\Phi}_s^t\left(H_1\right) \\ &= \frac{\sum_{\cap A_k = H_1} \prod_{i=1}^{s} \hat{\Phi}_s^t\left(A_k\right)}{1 - \sum_{\cap A_k = \emptyset} \prod_{i=1}^{s} \hat{\Phi}_s^t\left(A_k\right)} \end{aligned} \tag{21}$$

where s is the number of sensor nodes whose BPAs are selected for result aggregation at the t-th time interval.

Finally, the final decision will be conducted by the FC by combing the above aggregated result as follows:

$$FD = \begin{cases} 0, & Decide\ H_0\ if\ \frac{\hat{\Phi}^t(H_1)}{\hat{\Phi}^t(H_0)} \leq \eta, \\ 1, & Otherwise. \end{cases} \tag{22}$$

where η is the decision threshold.

$$X_{H_0,i}^* \sim \begin{cases} \mathcal{N}\left(M\sigma_i^2, 2M\sigma_i^4\right), & With\ probability\ \theta_i P_{f,i} + (1 - \theta_i), \\ \mathcal{N}\left((M + \lambda_i)\,\sigma_i^2, 2\,(M + 2\lambda_i)\,\sigma_i^4\right), & With\ probability\ \theta_i\left(1 - P_{f,i}\right), \end{cases} \tag{8}$$

$$X_{H_1,i}^* \sim \begin{cases} \mathcal{N}\left(M\sigma_i^2, 2M\sigma_i^4\right), & With\ probability\ \theta_i\, P_{d,i}, \\ \mathcal{N}\left((M + \lambda_i)\,\sigma_n^2, 2\,(M + 2\lambda_i)\,\sigma_i^4\right), & With\ probability\ 1 - \theta_i\, P_{d,i}, \end{cases} \tag{9}$$

$$X_{H_0,i}^* \sim \begin{cases} \mathcal{N}\left(M\sigma_i^2, 2M\sigma_i^4\right), & With\ probability\ 1 - \theta_i, \\ \mathcal{N}\left((M + \lambda_i)\,\sigma_n^2 - \tau_i, 2\,(M + 2\lambda_i)\,\sigma_i^4\right), & With\ probability\ \theta_i\, P_{f,i}, \\ \mathcal{N}\left((M + \lambda_i)\,\sigma_i^2 + \tau_i, 2\,(M + 2\lambda_i)\,\sigma_i^4\right), & With\ probability\ \theta_i\ \left(1 - P_{f,i}\right), \end{cases} \tag{10}$$

$$X_{H_1,i}^* \sim \begin{cases} \mathcal{N}\left(M\sigma_i^2, 2M\sigma_i^4\right), & With\ probability\ 1 - \theta_i, \\ \mathcal{N}\left((M + \lambda_i)\,\sigma_i^2 - \tau_i, 2\,(M + 2\lambda_i)\,\sigma_i^4\right), & With\ probability\ \theta_i\, P_{d,i}, \\ \mathcal{N}\left((M + \lambda_i)\,\sigma_i^2 + \tau_i, 2\,(M + 2\lambda_i)\,\sigma_i^4\right), & With\ probability\ \theta_i\ \left(1 - P_{d,i}\right), \end{cases} \tag{11}$$

C. IDENTIFICATION OF ATTACKERS

The historical reputation is based on the overall evaluation of sensor node's sensing data during the past time intervals. Although not real-time, it can provide useful references on the sensor node's behavior characteristics [37]. In addition, it is more stable and can be less affected by the results of random attacks. Only when a certain reputation value is reached, can it be proved that the sensing data and behavior of the sensor node are highly consistent with the overall analysis of the system during the continuous periods. Additionally, for malicious node, it is often necessary to launch an attack after the accumulated reputation value exceeds a certain threshold, so that the attack behavior will be effective.

The reputation update mechanism proposed in this paper assumes that all nodes are considered to be reliable during the initialization stage, and the reputation value is R_i^0. After receiving the sensing data from all nodes, FC will estimate the final state of PU and compare it with the local observation value received by each node. The reputation value will be updated according to the following criteria: (1) If the observation value of the participating node is rejected or not, the final decision will not be affected conversely and the PU's signal can be correctly detected. Then, the reputation will be increased. (2) For the case that the final decision is contrary to the observation value, the range of the reputation's reduction will be determined according to the average value of historical reputations. The detained update strategy is expressed as:

$$R_i^t = \begin{cases} R_i^{t-1} + 1, & \textit{if excluding } X_i \textit{ does not affect the fusion result}, \\ R_i^{t-1} - 1, & \textit{else if } \dfrac{1}{T}\displaystyle\sum_{i=1}^{T} R_i^t - R_i^0 > (1 - P_{error,i})t, \\ R_i^{t-1} - \xi, & \textit{otherwise}. \end{cases} \tag{23}$$

where ξ denotes the penalty factor, and $\xi > 1$. Besides, $P_{error,i} = P_{f,i}P_0 + (1 - P_{d,i})P_1$ and it represents the sensing error probability of i-th node, and P_0 and P_1 indicate the probability of PU's presence or absence respectively.

V. SIMULATIONS AND ANALYSIS

In this section, the simulation results are presented to evaluate the performance of the proposed method by MatLab. We setup a CWSN with 20 sensor nodes and a FC, and assume that the malicious nodes can change their sensing report to confuse the final decision. The additive white Gaussian noise (AWGN) channel is considered, and the idle and busy probabilities of the licensed channel are set as 90% and 10%, respectively. Initially, the FC chooses some of sensor nodes for CSS randomly. Through Monte-Carlo methods, the experimental scenario has been executed and all results are obtained over 10000 runs.

Figure 1 shows the effect of the proportion of malicious users and attacking probability on the total error probability of the system in attack scenario 1. From the experimental results, we can observe that the total error probability increases linearly with the increase of attack probability. In addition, more malicious nodes will result in high total error probability. The reason is that for a large number of attackers, their merging attack behaviors will become more severely.

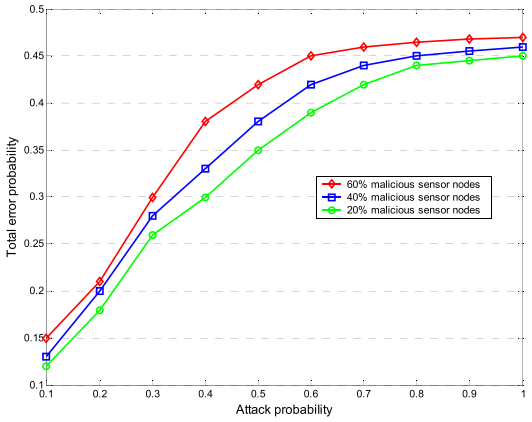


FIGURE 1. Total error probability under scenario 1.

Figure 2 also shows the total error probability under scenario 2. In contrast, when the attacking probability is low, the error probability in this scenario is lower than in scenario 1. Besides, it illustrates that when the number of malicious nodes is small, the attack strategy in scenario 2 is slightly less destructive to the whole CSS system. However, when the attacking probability exceeds 55%, the error probability will increase rapidly. Moreover, the size of the modified component also has a certain impact on the sensing performance. When the modified component is large and the attacking probability is high, the total error probability is significantly higher than other parameter settings. On the whole, the proposed method can effectively suppress the two attack strategies, and the total error probability is less than 50%. It can ensure that even when the attacking probability is close to 1, the system will not be completely useless.

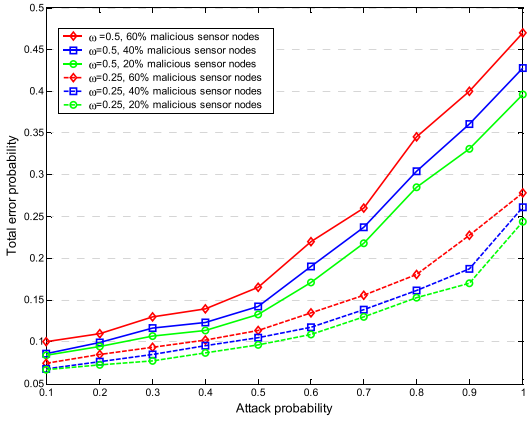


FIGURE 2. Total error probability under scenario 2.

Next, we compare with other traditional methods, including MTMS [38], Trusted-CSS [39] and TCAM [40], with respect to the detection probability, false alarm probability and the detection rate of malicious nodes being identified. Figure 3 shows the comparison of detection probability versus different percentage of malicious nodes under scenario 1. It can be found that when the proportion of malicious users is less than 30%, the detection probability performance of all algorithms is basically not affected. However, once the proportion of malicious users is more than 50%, this attack strategy obviously affects the performance of cooperative spectrum sensing. Compared with other methods, our proposed method has been able to show better detection probability.

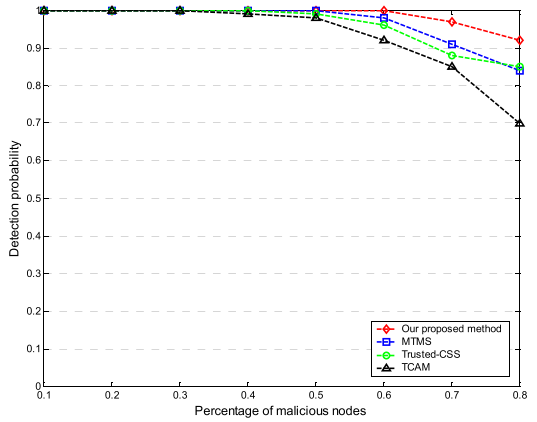


FIGURE 3. Comparison of the detection probability versus different percentage of malicious nodes under scenario 1.

Figure 4 shows the comparison of the false alarm probability versus different percentage of malicious nodes under scenario 1. When the proportion of malicious nodes exceeds 60%, the false alarm probability of TCAM increases rapidly and is significantly higher than other methods. It shows that TCAM is not robust enough to resist SSDF attack. When the proportion of malicious nodes is less than 50%, the curve corresponding to MTMS can better approximate Trusted-CSS. However, when the proportion of malicious users exceeds 50%, the false alarm probability of MTMS increases sharply, which indicates that the cooperative sensing method based on the coordination of trusted nodes can not effectively resist the cumulative attack when there are more malicious users in the cooperation.

The detection rate of malicious nodes is defined as the ratio of malicious nodes identified to the total number of actual malicious nodes. Figure 5 shows the comparison of the detection rate versus different percentage of malicious nodes under scenario 1. When the attacking probability is small, malicious users may disguise as normal users and do not launch attacks. In this way, the FC will treat them as trusted nodes and unable to effectively identify. Our proposed method and Trusted-CSS are obviously better than other methods. MTMS is sensitive to the selection of the trusted cooperative nodes set. When malicious users launch dynamic attacks non-uniformly, the attacking probability will be constantly varied. Therefore, MTMS can be easy to fall into local optimum.

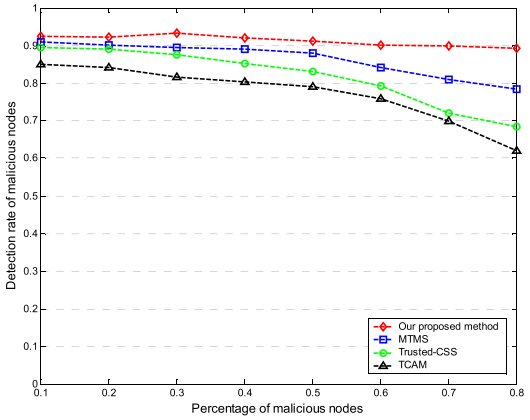


FIGURE 5. Comparison of the detection rate versus different percentage of malicious nodes under scenario 1.

Figures 6, 7, and 8 show the performance comparison versus different proportion of malicious nodes under scenario 2. It can be seen that with the increase of the proportion of

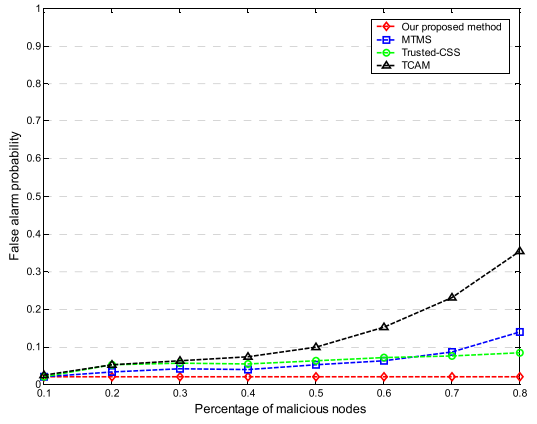


FIGURE 4. Comparison of the false alarm probability versus different percentage of malicious nodes under scenario 1.

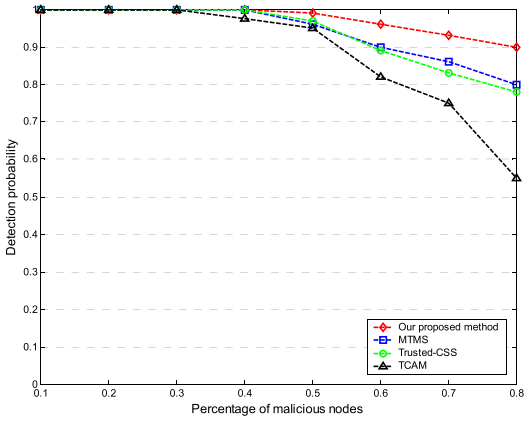


FIGURE 6. Comparison of the detection probability versus different percentage of malicious nodes under scenario 2.

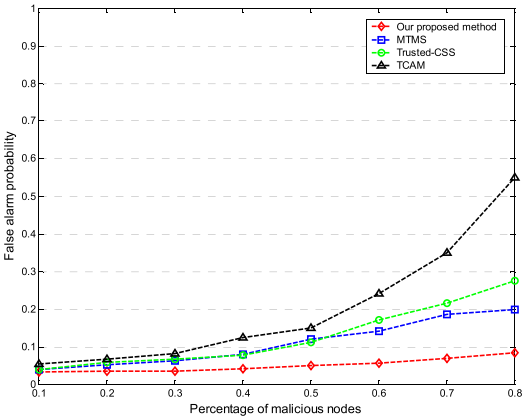


FIGURE 7. Comparison of the false alarm probability versus different percentage of malicious nodes under scenario 2.

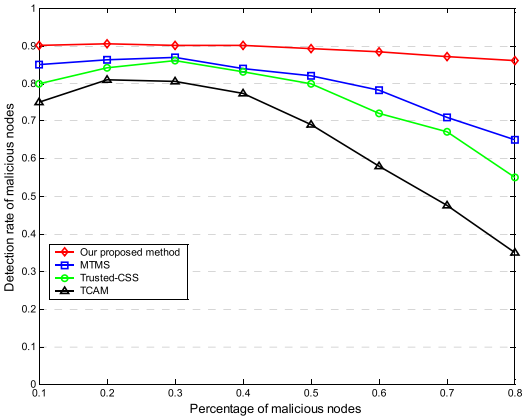


FIGURE 8. Comparison of the detection rate versus different percentage of malicious nodes under scenario 2.

malicious users, the decrease of global detection probability of cooperative spectrum sensing is significantly higher than that of attack scenario 1. When the proportion of malicious users in the network is 60%, the global detection probability of MTMS and Trusted-CSS is reduced to less than 0.9. The detection probability of TCAM is only 55.3% when the malicious node is 80%. At this time, the cognitive radio network can be considered as not working normally. Comparatively, when the proportion of malicious users reaches 80%, our proposed method can maintain high detection probability and low false alarm probability. It demonstrates that our proposed method can effectively compensate for the performance loss caused by these two SSDF attacks. In addition, we can observe that MTMS and Trusted-CSS can achieve approximate performance of false alarm probability when the proportion of malicious users is less than 50%. However, when the number of malicious users dominates the CSS system, i.e., the proportion of malicious users exceeds 50%, the performance of Trusted-CSS decreases significantly.

As for the malicious nodes being identified, the attacks in scenario 2 behave more confusedly than in scenario 1. Those malicious users with low attack probability may not launch attacks in some sensing slots, so their superimposed components have little impact on the final fusion results. And then, the fusion center cannot identify the malicious nodes explicitly. From the simulation results, with the increasing proportion of malicious users, if the malicious users can not be identified effectively, the normal nodes will be erroneously identified due to their reports contrary to the fusion result. As a result, the sensing process will be dominated by malicious users, which leads to a sharp decline in global sensing performance. Our proposed method based on D-S evidence theory can make full use of the cumulative reputation, i.e., the FC can still employ the irregularity of sending data to distinguish the normal users from the malicious users effectively. Thus, it can make the normal secondary users occupy the dominant position in the decision process, and improve the robustness of cooperative sensing.

VI. CONCLUSION

In this paper, an enhanced cooperative spectrum sensing scheme against SSDF attack based on Dempster-Shafer evidence theory for cognitive wireless sensor networks is introduced. First, the holistic credibility of sensor nodes can be evaluated according to the real-time difference between them and the statistical sensing behaviors. Furthermore, the basic probability assignment function can be defined based on evidence theory, and the credibility of sensor nodes can be estimated. Finally, by using the weighted probability assignment for each cognitive sensor node, the fusion center can reduce the influence of malicious sensor nodes on the final decision and ensure the reliability of reports from cooperative sensor nodes. Analytical and simulation results have shown that the proposed method can resist SSDF attacks significantly and outperform the traditional secure schemes in aspect of sensing accuracy.

REFERENCES

[1] W. Ejaz and M. Ibnkahla, "Multiband spectrum sensing and resource allocation for IoT in cognitive 5G networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 150–163, Feb. 2018.

[2] Y. Chen, S. Su, H. Yin, X. Guo, Z. Zuo, J. Wei, L. Zhang, "Optimized non-cooperative spectrum sensing algorithm in cognitive wireless sensor networks," *Sensors*, vol. 19, no. 9, pp. 1–23, 2019.

[3] Z. Liu, B. Hu, B. Huang, L. Lang, H. Guo, and Y. Zhao, "Decision optimization of low-carbon dual-channel supply chain of auto parts based on smart city architecture," *Complexity*, vol. 2020, pp. 1–14, May 2020.

[4] M. Shafiee and V. T. Vakili, "Comparative evaluation approach for spectrum sensing in cognitive wireless sensor networks (C-WSNs)," *Can. J. Electr. Comput. Eng.*, vol. 41, no. 2, pp. 77–86, 2018.

[5] A. Araujo, J. Blesa, E. Romero, and D. Villanueva, "Security in cognitive wireless sensor networks. Challenges and open problems," *EURASIP J. Wireless Commun. Netw.*, vol. 2012, no. 1, pp. 48–59, Dec. 2012.

[6] L. Dong, Q. Guo, and W. Wu, "Speech corpora subset selection based on time-continuous utterances features," *J. Combinat. Optim.*, vol. 37, no. 4, pp. 1237–1248, May 2019.

[7] J. Sen, "Security and privacy challenges in cognitive wireless sensor networks," 2013, *arXiv:1302.2253*. [Online]. Available: http://arxiv.org/abs/1302.2253

[8] A. Fragkiadakis, V. Angelakis, and E. Z. Tragos, "Securing cognitive wireless sensor networks: A survey," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 3, pp. 1–12, 2014.

[9] D. Jiang, G. Li, Y. Sun, J. Kong, and B. Tao, "Gesture recognition based on skeletonization algorithm and CNN with ASL database," *Multimedia Tools Appl.*, vol. 78, no. 21, pp. 29953–29970, Nov. 2019.

[10] G. Joshi, S. Nam, and S. Kim, "Cognitive radio wireless sensor networks: Applications, challenges and research trends," *Sensors*, vol. 13, no. 9, pp. 11196–11228, Aug. 2013.

[11] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2488–2497, Aug. 2010.

[12] M. Zhou, J. Shen, H. Chen, and L. Xie, "A cooperative spectrum sensing scheme based on the Bayesian reputation model in cognitive radio networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Shanghai, China, Apr. 2013, pp. 614–619.

[13] J. Wu, T. Song, C. Wang, Y. Yu, M. Liu, and J. Hu, "Robust cooperative spectrum sensing against probabilistic SSDF attack in cognitive radio networks," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Toronto, ON, Canada, Sep. 2017, pp. 1–6.

[14] S. Liu, J. Gao, and Q. Liu, "Defense against SSDF attack in cooperative spectrum sensing based on accumulated suspicious level," *J. Sichuan Univ.*, vol. s1, pp. 239–243, Oct. 2011.

[15] A. A. Sharifi and M. J. M. Niya, "Defense against SSDF attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach," *IEEE Commun. Lett.*, vol. 20, no. 1, pp. 93–96, Jan. 2016.

[16] L. Wang, L. Zhang, and X. Chen, "A dynamic threshold strategy against SSDF attack for cooperative spectrum sensing in cognitive radio networks," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2015, pp. 1–5.

[17] R. Chen, J.-M.-J. Park, and K. Bian, "Robustness against Byzantine failures in distributed spectrum sensing," *Comput. Commun.*, vol. 35, no. 17, pp. 2115–2124, Oct. 2012.

[18] C. Chen, M. Song, and C. Xin, "CoPD: A conjugate prior based detection scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks," *Wireless Netw.*, vol. 20, no. 8, pp. 2521–2528, Nov. 2014.

[19] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1707–1719, Aug. 2014.

[20] A. A. Sharifi, M. Sharifi, and J. Musevi Niya, "Reputation-based likelihood ratio test with anchor nodes assistance," in *Proc. 8th Int. Symp. Telecommun. (IST)*, Sep. 2016, pp. 51–56.

[21] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, Feb. 2011.

[22] M. Jo, L. Han, D. Kim, and H. P. In, "Selfish attacks and detection in cognitive radio ad-hoc networks," *IEEE Netw.*, vol. 27, no. 3, pp. 46–50, May 2013.

[23] P. S. Chatterjee and M. Roy, "A regression based spectrum-sensing Data–Falsification attack detection technique in CWSN," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Dec. 2015, pp. 48–53.

[24] P. Sankar Chatterjee and M. Roy, "Lightweight cloned-node detection algorithm for efficiently handling SSDF attacks and facilitating secure spectrum allocation in CWSNs," *IET Wireless Sensor Syst.*, vol. 8, no. 3, pp. 121–128, Jun. 2018.

[25] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3554–3565, Nov. 2010.

[26] W. Wei, X. Xia, M. Wozniak, X. Fan, R. Damaševicius, and Y. Li, "Multi-sink distributed power control algorithm for cyber-physical-systems in coal mine tunnels," *Comput. Netw.*, vol. 161, pp. 210–219, Oct. 2019.

[27] O. B. Akan, O. Karli, and O. Ergul, "Cognitive radio sensor networks," *IEEE Netw.*, vol. 23, no. 4, pp. 34–40, Jul./Aug. 2009.

[28] A. Vosoughi, J. R. Cavallaro, and A. Marshall, "A context-aware trust framework for resilient distributed cooperative spectrum sensing in dynamic settings," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9177–9191, Oct. 2017.

[29] L. Duan, A. W. Min, J. Huang, and K. G. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1658–1665, Oct. 2012.

[30] Q. Liu, "Attack-proof cooperative spectrum sensing based on consensus algorithm in cognitive radio networks," *KSII Trans. Internet Inf. Syst.*, vol. 4, pp. 1042–1062, Dec. 2010.

[31] R. R. Yager, J. Kacprzyk, and M. Fedrizzi, "Advances in the Dempster–Shafer theory of evidence," *J. Process Control*, vol. 8, no. 5, p. 517, 1994.

[32] Y. W. Du and C. Han, "Classical models and its applications in D-S evidence theory," *Appl. Mech. Mater.*, vols. 204–208, pp. 4958–4961, Oct. 2012.

[33] N. Nguyen-Thanh and I. Koo, "Evidence-theory-based cooperative spectrum sensing with efficient quantization method in cognitive radio," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 185–195, Jan. 2011.

[34] Z. Liu, B. Hu, Y. Zhao, L. Lang, H. Guo, K. Florence, and S. Zhang, "Research on intelligent decision of low carbon supply chain based on carbon tax constraints in human-driven edge computing," *IEEE Access*, vol. 8, pp. 48264–48273, 2020.

[35] O. Basir and X. Yuan, "Engine fault diagnosis based on multi-sensor information fusion using Dempster–Shafer evidence theory," *Inf. Fusion*, vol. 8, no. 4, pp. 379–386, Oct. 2007.

[36] A.-L. Jousselme, D. Grenier, and É. Bossé, "A new distance between two bodies of evidence," *Inf. Fusion*, vol. 2, no. 2, pp. 91–101, Jun. 2001.

[37] N. Nguyen-Thanh and I. Koo, "An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context," *IEEE Commun. Lett.*, vol. 13, no. 7, pp. 492–494, Jul. 2009.

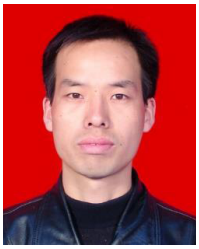
[38] S. Kar, S. Sethi, and R. K. Sahoo, "A multi-factor trust management scheme for secure spectrum sensing in cognitive radio networks," *Wireless Pers. Commun.*, vol. 97, no. 2, pp. 2523–2540, Jun. 2017.

[39] S. Jana, K. Zeng, W. Cheng, and P. Mohapatra, "Trusted collaborative spectrum sensing for mobile cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1497–1507, Sep. 2013.

[40] S. Bhattacharjee, S. Debroy, and M. Chatterjee, "Trust computation through anomaly monitoring in distributed cognitive radio networks," in *Proc. IEEE 22nd Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2011, pp. 593–597.

DEGUI YAO was born in Anhui, China. He received the D.E. degree from Chongqing University, China, in 2001. He is currently a Professor-Level Senior Engineer with the Electric Power Research Institute, State Grid Henan Electric Power Company. His research interest includes automation of electric power systems.

SHAOGUANG YUAN was born in Henan, China. He received the M.E. degree from North China Electric Power University, China, in 2015. He is currently an Engineer with the Electric Power Research Institute, State Grid Henan Electric Power Company. His research interest includes power big data.



ZHONGBIN LV was born in Henan, China. He received the D.E. degree from Zhengzhou University, China, in 2005. He is currently a Professor-Level Senior Engineer with the Electric Power Research Institute, State Grid Henan Electric Power Company. His research interests include power production management and informatization.

DIMING WAN was born in Jiangxi, China. He received the B.E. degree from North China Electric Power University, China, in 2011. He is currently an Engineer with the Electric Power Research Institute, State Grid Henan Electric Power Company. His research interest includes power informatization.

WANDENG MAO was born in Henan, China. He received the M.E. degree from Lanzhou University, China, in 2019. He is currently an Engineer with the Electric Power Research Institute, State Grid Henan Electric Power Company. His research interests include power big data analysis and electric IoT.