IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 1, 2020, accepted July 12, 2020, date of publication July 20, 2020, date of current version July 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3009466

Secure Cooperative Spectrum Sensing Strategy Based on Reputation Mechanism for Cognitive Wireless Sensor Networks

XIANQUAN LUO
College of Artificial Intelligence, Yango University, Fuzhou 350015, China
e-mail: xqluo@ygu.edu.cn

ABSTRACT Cooperative spectrum sensing can be regarded as a promising method to resolve the spectrum scarcity owing to achieving spatial diversity gain in cognitive radio sensor networks. However, the spectrum sensing data falsification attack launched by the malicious nodes will result in the wrong decision in the fusion center owing to the falsified observations. It will cause a serious security threat and degrade the decision making process. In this paper, we propose a secure cooperative spectrum sensing strategy based on reputation mechanism for cognitive wireless sensor networks to counter above kind of attack. The beta reputation model is applied to assign reputation value to cognitive sensor nodes according to their historical sensing behavior, and a dynamic trust evaluation scheme of cooperative spectrum sensing is established. In the final decision, the fusion center allocates a reasonable weight value according to the evaluation of the submitted observations to improve the accuracy of the sensing results. Simulation results support that our proposed strategy can weaken the impact of sensing data falsification attacks in cooperative sensing and outperform some traditional methods.

INDEX TERMS Cooperative spectrum sensing, reputation mechanism, cognitive wireless sensor networks, cognitive radio.

I. INTRODUCTION

By employing the cognitive radio (CR) technology, the CR-enable sensor nodes can perform spectrum sensing to detect available licensed bands and reduce channel unordered competition. Owing to dynamically aware of the surrounding environment, CR sensor networks (CRSNs) can overcome the problem of overcrowded unlicensed spectrum bands and improve spectrum utilization [1]. IEEE, IITU-R, and other organizations and industry alliances have put forward a series of standards and specifications in the following aspects, including the network architecture, physical layer interface and medium access layer design of CR technology [2]. The current technologies for CRSNs are still in the development stage, and there are deficiencies in many aspects. Basically, the use of authorized frequency band by CR-enable sensor nodes are required to guarantee no interference to the primary user's signal strictly. However, false alarms and misdetection of PU's will be inevitable by shadowing and fading effect, especially under low signal-noise-ratio (SNR) conditions [3]. It brings about tremendous challenges in cognitive radio systems and influences the dynamic spectrum access for CR-enable sensor nodes to utilize idle licensed bands opportunistically. By combining the numerous sensor nodes' local sensing results, cooperative spectrum sensing (CSS) can alleviate the inaccuracy of single node's observation and enhance the spectrum sensing performance [4]. However, false reports included in cooperative nodes will cause a serious security threat and may disrupt the cognitive radio system [5].

Due to the open and time-varying characteristics of wireless channel, CRSNs are vulnerable to various security threats, e. g. interference, eavesdropping, deception and so on. Especially, spectrum sensing data falsification (SSDF) [6] or primary user emulation (PUE) [7] attacks are the most common and serious attacks, which will produce erroneous sensing decision and result in unwanted interference to the PU. Among them, the SSDF can be regarded as a particular case of the DoS (Deny of Service) attack [8]. During the process of collaborative spectrum sensing decision-making, the attackers will conduct a defective decision in term of the spectrum utilization by injecting falsified observations. More importantly, malicious users can illegally occupy spectrum

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

bandwidth by disrupting the proper functioning of the cooperative spectrum sensing. Even if there exists only a small number of malicious users in the CRSNs, that will lead to a serious degradation of detection performance and affect the robustness of the system [9]. When the number of malicious users exceeds to some extent, large-scale attacks will directly lead to the whole network collapse. Hence, when the fusion center (FC) adopts some conservative fusion strategies to protect the primary users as much as possible, only a few malicious users can mislead the FC to make a wrong decision [10]. Therefore, it is of great significance to design a secure cooperative spectrum sensing mechanism to resist SSDF attacks.

In this paper, we propose a secure cooperative spectrum sensing strategy based on reputation mechanism for cognitive wireless sensor networks to counter the SSDF attack. The main contributions of this paper are as follows:

- introducing the beta reputation model is applied to assign reputation value to cognitive sensor nodes according to their historical sensing behavior;
- proposing a dynamic trust evaluation scheme and assigning reasonable weight value to cooperative sensor node according to the evaluation of the submitted observations to improve the accuracy of the sensing results;
- proposing a attacker-identification method to detect attackers effectively.

II. RELATED WORK

By utilizing the cooperation of multi sensor nodes in different geographical locations, CSS can effectively alleviate the problem of spectrum allocation, which can reduce the interference inside the network under shadow fading and multipath effect. However, the corrupted sensing reports during transmission or sensing observations manipulated by malicious users will mislead the FC to make wrong decisions [11]. The countermeasures for secure cooperative sensing are discussed in many literatures, and different kinds of security attacks and defenses are studied recently.

Many anti-SSDF attack strategies employ analytical method with outlier detection for malicious user's detection. Li *et al.* [12] proposed a method combining spectrum sensing and outlier detection to distinguish the node's failure or malicious user's attack. Ghaznavi and Jamshidi [13] proposed a fast search algorithm based on the clustering network structure to detect the malicious nodes of each cluster, which can reduce the overhead by reducing the sensing information exchange between the cognitive users and the FC. By constructing a cooperative sensing network with double sparsity property, Qin *et al.* [14] introduced a compressive sensing technique and the strategy of adaptive outlier pursuit with low-rank matrix completion to detect malicious users. By utilizing the spatial characteristics of the CR sensors, Kaligineedi *et al.* [15] proposed an outlier detection technique with constraints of small size of the sensing data samples. Nath *et al.* [16] proposed a k-medoids clustering algorithm to isolate and distinguish the attackers without predefining the detection threshold.

Some countermeasures against SSDF attack are based on Dempter-Shafer theory of evidence, in which all recommendations are usually qualified as honest and accurate. Wang *et al.* [17] introduced a CSS algorithm based on Dempter-Shafer theory and defined the credibility of cognitive user's local results to improve the sensing accuracy. Considering the difference of cognitive users' sensing channel, Nguyen-Thanh and Koo [18] proposed an enhanced CSS mechanism to evaluate the degree of reliability of each sensing terminal, and assign different weight of sensing data based on Dempter-Shafer theory of evidence. By analyzing the distance between evidence vectors of different cooperative secondary users, Yu *et al.* [19] introduced an improved CSS scheme with the mathematical model from Dempster-Shafer evidence. Han *et al.* [20] proposed a detection method to resist SSDF attack, in which the FC removes the evidence with low reliable sensing nodes and fuses the reports with high reliability to obtain better detection performance. By exploiting the characteristics of sensing node's spatial diversity, Feng *et al.* [21] proposed a trustworthy cooperative spectrum sensing scheme and designed the factors of the current reliability and the historical reputation to estimate the trustworthiness degree of each sensing node.

To identifying attackers effectively and avoid detecting honest sensor nodes as attackers, trust mechanism can be regarded as more effective measure in many application scenarios. Chen and Xie [22] proposed a reputation-based CSS scheme based on hierarchical clustering architecture, which effectively reduced the impact of multipath fading, shadow and malicious attack by using the two-level reputation estimation. Gupta and Yerma [23] proposed a reliability-based weighting algorithm, which mainly improves the sensing performance in the low SNR conditions, and distinguishes the cognitive users according to the comparison between the user's historical sensing results and the FC. By exploiting the spatial and temporal correlation of sensing information, Huang *et al.* [24] employed the trust value of cognitive users to lessen the impact of malicious users on sensing results. To degrade the impact of malicious users, Wei *et al.* [25] applied a weighted average consistency algorithm to cooperative spectrum sensing, which can ensure reliable data transmission by direct and indirect trust value. In order to prevent malicious nodes from maintaining a high degree of trust in the alternate process of reporting real or erroneous sensing data, Feng *et al.* [26] proposed a novel trust scheme with dynamic evaluation against intermittent SSDF attack.

To alleviate the attacker's influence on the network performance, the punishment strategies are established to motivate the malicious nodes' falsified reports conservatively. Besides, the honest sensor nodes will acquire more fair distribution of data transmission owing to their local sensing information consistent with final results. To overcome the low spectrum access rate of normal nodes caused by cooperative malicious nodes' attack, Duan *et al.* [27] defined direct and indirect punishments and proposed two attack-prevention mechanisms, in which the FC is not required to identify or exclude attackers. Based on scheduling probability associated with each user's sensing data, Althunibat *et al.* [28] proposed an attacker identification and punishment strategy to assign each sensing node with proper scheduling probability. To minimize the Bayes risk, Sharifi and Niya [29] proposed an attack-aware cooperative spectrum sensing method to estimate the attack strength of SSDF, and deduced the optimal voting threshold in majority rule to improve the global decision-making accuracy.

Identifying the attacker is a critical process and should be conducted cautiously to avoid the detection of honest nodes as attackers. Therefore, the identification criteria of attackers should be reliable enough, and provide enough robustness for the system especially as the number of attackers is large.

III. METHODOLOGY

A. SYSTEM MODEL

We assume that the sensor nodes being deployed randomly in the monitoring region and a FC are organized into infrastructure-based CRSNs. All cognitive sensor nodes will perceive the PU's signal through the sensing channel, and then report the sensing information or local decision results to the FC via the reporting channel. Among them, the legitimate sensor nodes share the real energy values in spectrum sensing process, but the malicious sensor nodes send their falsified sensing data, to the FC for final combination. Based on binary hypotheses, the spectrum sensing for a specific frequency band can be generally formulated by:

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

where $s(t)$ the PU's transmit signal, h_i is the channel gain without delay, and $n_i(t)$ denotes the additive white Gaussian noise (AWGN) sample with mean 0 and variance σ_n^2.

Then, the energy detection method is employed to determine the spectrum sensing result [30]. Thus, the test statistics T_i of i-th sensor node for l samples can be given by:

$$T_i = \sum_{k=1}^{l} |x_i(k)|^2 \tag{2}$$

Comparing the energy threshold γ with the test statistics, the local sensing result will be obtained as:

$$g_i = \begin{cases} 0, & T_i < \gamma \\ 1, & T_i > \gamma \end{cases} \tag{3}$$

The sensor node participates in CSS and sends the local result 0 or 1, which indicates the channel being idle and occupied, to FC for subsequent global fusion decision. The FC fuses the received local results and makes the decision about the authorized spectrum according to the k-out-of-n rule [31]. The final decision $F(k)$ can be written as:

$$F(k) = \begin{cases} H_1, & if \ \sum_{i=1}^{N} g_i(k) \geq K \\ H_0, & otherwise \end{cases} \tag{4}$$

where H_0 and H_1 represent idle and occupied states of the channel respectively. $g_i(k)$ indicates that FC receives the local sensing results of the i-th sensing node at the k-th round. The majority fusion rule is applied, $K = \lceil (N+1)/2 \rceil$ and $\lceil \cdot \rceil$ is the integral function for upper limit.

Suppose that P_d and P_f represent the detection probability and false alarm probability of cognitive sensor node, the global detection probability and global false alarm probability can be given by [32]

$$\begin{cases} Q_d = \sum_{j=K}^{N} \binom{N}{j} P_d^j (1-P_d)^{N-j} \\ Q_f = \sum_{j=K}^{N} \binom{N}{n} P_f^j (1-P_f)^{N-j} \end{cases} \tag{5}$$

The FC can schedule the cognitive sensor node for data transferring only when the final decision about the channel is idle (i. e., $F(k) = 0$). Otherwise, $F(k) = 1$ and the FC will inform all sensor nodes remain silent to avoid interference to authorized users.

B. ATTACKING MODEL

During the phase of CSS, it is assumed that the attacking probability of each malicious node is θ. Once the attack is decided, the malicious node sends the report inconsistent with the local sensing result to the FC. Based on this attack strategy, the detection probability and false alarm probability of malicious nodes can be written as:

$$\begin{cases} P_{d\_MU} = \theta(1-\tilde{P}_d) + (1-\theta)\tilde{P}_d \\ P_{f\_MU} = \theta(1-\tilde{P}_f) + (1-\theta)\tilde{P}_f \end{cases} \tag{6}$$

where $\tilde{P}_d$ and $\tilde{P}_f$ represent the actual local detection probability and false alarm probability of the sensing node.

Considering that the main motivation of malicious nodes is to reduce the throughput of normal nodes and occupy the communication channel selfishly, malicious nodes will neglect the scheduling strategy of FC to access the channel directly for data transmission as global false alarm occurs. Specifically, malicious nodes cooperate with each other internally, and conduct majority criteria to obtain the global decisions $R(k)$ based on their local actual sensing results. Once $F(k) = 1$ but $R(k) = 0$, the malicious nodes will choose some of them randomly to access the frequency band and independently transmit their own data. The attack steps of malicious nodes mainly include:

(1) At the beginning of spectrum sensing, all malicious nodes have the same local spectrum sensing as normal nodes, and they also make their own local sensing decision.

(2) Each malicious node independently decides whether to attack or not with the probability of θ. If deciding to launch an attack, the malicious node will send the reporting inconsistent with the local sensing data to the FC. Otherwise, the malicious node does not launch the attack, and it will report the actual local sensing data.

(3) Malicious nodes share their local sensing results, and make a global decision $R(k)$ for internal notification.

(4) If the FC makes the global decision of CSS that the primary user does not exist, then it will select one of all nodes (possibly a malicious node), and schedule the node to access the channel for data transmission.

(5) Or else, once the global decision indicates that the primary user exists, the malicious nodes will check the internal global decision. If $R(k) = 0$, one of the malicious nodes will hand over the licensed channel.

Let P_{error} represent the sensing error probability of node i in spectrum sensing, we have

$$\begin{cases} P_{error} = P_f P(H_0) + (1 - P_d)P(H_1), & if\ i-th\ sensor\ node\ is\ honest, \\ P_{error\_MU} = P_{f\_MU} P(H_0) + (1 - P_{d\_MU})P(H_1), & otherwise. \end{cases} \tag{7}$$

C. REPUTATION MODEL

To solve the problem of SSDF attacks, the reputation system can be employed to integrate into the process of cooperative spectrum sensing. The theoretical basis of reputation system is originated from the collective measurement of the trustworthiness of other members to a certain one [33]. Furthermore, the reputation is often defined as the collective evaluation of a member's behavior in the system, which represents the reliability of the member and helps to determine the specific measures of some attributes. The basic idea of reputation system is to get a reputation value according to the historical behavior of members [34]. Generally, the members with higher reputation will get more opportunities and returns, and at the same time restrain the bad behavior of the members with lower reputation, so as to enhance the performance of the system.

During the phase of local sensing, the node's results have two possible types, which accord with binomial distribution. The probability distribution of binary events can be described by beta distribution. Therefore, we can employ Beta distribution function to build reputation model for credibility assignments to member nodes.

Suppose r indicate the events that the cognitive sensor node sends the local sensing results to the FC truthfully, and s indicate the events that the cognitive sensor node sends a report to the FC that is opposite of its local sensing decision. By setting $\alpha = r + 1$ and $\beta = s + 1$, the probability density function will be obtained by [35]

$$f(p|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \tag{8}$$

where $\Gamma(\cdot)$ is the Gamma function,p represents the probability of sensing behaviors and $0 \leq p \leq 1$. Besides, $\alpha > 0, \beta > 0$.

For the i-th sensor node, its reputation value will be evaluated by beta function: $R_i = Beta(r_i + 1, s_i + 1)$. Furthermore, the expectation value of the beta function can be calculated as: $E[Beta(\alpha, \beta)] = \alpha/(\alpha + \beta)$. Thus, the trust degree can be deduced by:

$$R_i = \frac{r_i + 1}{r_i + s_i + 2} \tag{9}$$

To resist the SSDF attacks launched by most malicious users effectively, the FC will utilize the beta reputation model to allocate the reputation value dynamically according to the historical behavior of cognitive sensor nodes. In the final fusion decision, the FC will assign the reasonable weight value for cognitive sensor nodes for sensing results combination.

The local sensing result of cognitive sensor node i in the k-th time interval is $g_i(k)$ and the FC aggregate all the results, which can be calculated as

$$G(k) = \sum_{i=1}^{N} w_i(k) g_i(k) \tag{10}$$

Next, according to the results of local sensing result and global fusion result, the sensing result deviation of the cognitive sensor node i at k-th time interval will be given by:

$$DIS(i, k) = \sqrt{\frac{\sum_{i=1}^{N} (g_i(k) - G(k))^2}{N}} \tag{11}$$

Hence, the mean value of the deviation of sensing results can be given by

$$AveDIS(i, k) = \frac{1}{N} \sum_{i=1}^{N} DIS(i, k) \tag{12}$$

Let $\mu_i(k)$ represent the positive or negative evaluation of the spectrum sensing results obtained by the i-th cognitive sensor node in the k-th time slot. If $AveDIS(i, k) \geq DIS(i, k)$, it indicates that the local sensing result of the cognitive sensor node in the k-th time slot is reliable and the positive evaluation to the cognitive sensor node should be increased as $\mu_i(k) = 1$. Otherwise, it means that the local sensing result is untrustworthy with respect to $\mu_i(k) = 0$, and then the negative evaluation will be assigned.

By analyzing the influence on the reputation of sensor node's report from the historical sensing results, the weight of reputation value should be updated with the varying of the sensing time. In order to ensure the robustness of the system, the model should have a certain tolerance for honest users who occasionally send error sensing data, and its reputation value can be gradually improved by continuously reporting correct data in subsequent period. Let m denote the maximum storage length of the cognitive sensor node's historical evaluation value, and according to the historical evaluation value, the positive evaluation $pos_i(k)$ and negative evaluation $neg_i(k)$ of cognitive sensor node i in the k-th sensing time slot can be obtained by

$$pos_i(k) = \begin{cases} \sum_{n=1}^{m} \mu_i(k)\,(w_i(k))^{m-n}, & if\ k < m, \\ \sum_{n=k-m+1}^{m} \mu_i(k)\,(w_i(k))^{m-n}, & otherwise. \end{cases} \tag{13}$$

$$neg_i(k) = \begin{cases} \sum_{n=1}^{m} (1-\mu_i(k))\,(w_i(k))^{m-n}, & if\ k < m, \\ \sum_{n=k-m+1}^{m} (1-\mu_i(k))\,(w_i(k))^{m-n}, & otherwise. \end{cases} \tag{14}$$

Taking the total evaluation into the beta reputation model, for the cognitive sensor node i, the reputation parameters $r_i(k)$ and $s_i(k)$ in the k-th time interval can be given by

$$r_i(k) = pos_i(k) + \omega_r \tag{15}$$

$$s_i(k) = neg_i(k) * \omega_s \tag{16}$$

where ω_r and ω_s denote the tuning parameters to reflect the linear and multiplier increase of different type of reports, respectively.

Therefore, based on Eq. (9), the reputation value $R_i(k)$ of cognitive sensor node i can be estimated expressed as

$$R_i(k) = w_i(k+1) = \frac{pos_i(k) + \omega_r + 1}{pos_i(k) + neg_i(k) * \omega_s + \omega_r + 2} \tag{17}$$

D. IDENTIFICATION OF ATTACKERS

The identification of malicious nodes is one of the key factors to enhance the overall performance of CRSN and enhance the sensing accuracy and energy efficiency [36]. During the process of malicious node identification, it should be avoided to identify normal nodes as malicious nodes. Once identified as a malicious node, the reports sent by the sensor node to the FC will be rejected before the final fusion.

According to the reputation model and data delivery, the credibility of sensing nodes can be estimated, and each sensing nodes increment their counters compared with the attackers. When the FC makes a global decision that the channel is idle, it will schedule a node to access the channel for data transmission, and evaluate the actual status of the channel through the success or failure of the data transmission of the node being scheduled. If the sensing report sent to the FC is inconsistent with the actual status of the channel, the counter value of the sensing node will be incremented by 1. Otherwise, the value of the counter will keep unchanged. After M sensing intervals, if the value of the counter is higher than the predetermined threshold, the relevant sensing node will be regarded as a malicious node. The counter value of the i-th sensing node at k-th time interval can be expressed as

$$U_i(k) = \begin{cases} U_i(k-1)+1, & if\ F(k) = 0\ and\ g_i(k) \neq \Theta(k) \\ U_i(k-1), & otherwise \end{cases} \tag{18}$$

where $\Theta(k)$ indicates the actual status of the channel at k-th time interval.

After k time intervals, the counter value follows the binomial distribution function and corresponding probability can be obtained by

$$\begin{cases} \Pr\{U_i(M) = u\} = \binom{M}{u} \pi_i^u (1-\pi_i)^{M-u} \\ \pi_i = \Pr(U_i(k) = U_i(k-1)+1) \\ = P(H_0)\,P_{f,i} \Pr(F(k) = 0 | g_i(k) = 1) + \\ P(H_1)\,P_{d,i} \Pr(F(k) = 0 | g_i(k) = 0) \end{cases} \tag{19}$$

where $P(H_0)$ and $P(H_1)$ represent the probability that the state of PU be idle and occupied respectively.

Then, the average value of the counter corresponding to the i-th sensing node can be expressed as

$$\begin{aligned} Ave\_U_i(t) &= \sum_{u=0}^{M} u \Pr\{U_i(M) = u\} \\ &= \sum_{u=0}^{M} u \binom{M}{u} \pi_i^u (1-\pi_i)^{M-u} \end{aligned} \tag{20}$$

Suppose λ be the identification threshold of malicious node. If $U_i(t) \geq \lambda$, the reputation model will detect and identify the attacker of malicious sensor nodes. Obviously, high values of λ may result in omitting the attackers, whereas some honest sensing nodes will be identified as attackers at low values of λ.

To optimize the threshold, we define the objective function as

$$\max \left\{ \left| \Pr\{Ave\_U(t) \geq \lambda\} - \Pr\{Ave\_\tilde{U}(t) \geq \lambda\} \right| \right\} \tag{21}$$

where $Ave\_U(t)$ and $Ave\_\tilde{U}(t)$ represent the average value of counter of all nodes and attackers being identified, respectively.

Bring the false alarm probability and detection probability of normal and malicious nodes into the Eq. (19), we can get the corresponding π_0 and π_0'. Thus, and the objective function can be written as

$$\begin{aligned} \max \Bigg\{ \Bigg| &\sum_{u=\lambda}^{M} \binom{M}{u} (\pi_0)^u (1-\pi_0)^{M-u} \\ &- \sum_{u=\lambda}^{M} \binom{M}{u} (\pi_0')^u (1-\pi_0')^{M-u} \Bigg| \Bigg\} \end{aligned} \tag{22}$$

Next, according to Lagrange method, the derivative of the function with respect to λ is equal to 0 and then the optimal threshold λ_{opt} can be obtained. Hence, we can deduce the derivative of part of objective function with respect to λ as follows:

$$\begin{cases} \dfrac{\partial \Pr\{Ave\_U(t) \geq \lambda\}}{\partial \lambda} = -M \begin{pmatrix} M \\ \lambda \end{pmatrix} (\pi_0)^{\lambda} (1-\pi_0)^{M-\lambda} \\ \dfrac{\partial \Pr\{Ave\_U(t) \geq \lambda\}}{\partial \lambda} = -M \begin{pmatrix} M \\ \lambda \end{pmatrix} (\pi_0')^{\lambda} (1-\pi_0')^{M-\lambda} \end{cases} \tag{23}$$

According to the objective function, the derivative of λ is equal to 0, and the following expression can be given by

$$\frac{\pi_0 (1-\pi_0')}{\pi_0' (1-\pi_0)} = \left(\frac{1-\pi_0'}{1-\pi_0}\right)^{M/\lambda} \tag{24}$$

Take logarithm on both sides of the equation, and finally get the optimal threshold can be estimated as

$$\lambda_{opt} = \frac{M}{\log_{\frac{1-\pi'}{1-\pi_0}} \frac{\pi_0}{\pi_0'} + 1} \tag{25}$$

IV. SIMULATION RESULTS

In this section, we conduct some simulations and compare it with the previous schemes to evaluate the performance of the proposed method. In the simulation experiment, the number of cooperative sensor nodes is assumed to be 40, the number of samples for energy detection is equal to 20, and the noise power σ_n^2 =1, $n = 1, 2, \cdots, N$. The local false alarm probability is fixed to constant value 0.1, and $P(H_1) = P(H_0) = 0.5$. Besides, the parameter δ is set to 0.6, $\omega_r = 1$ and $\omega_s = 2$. PU's signal is transmitted through AWGN channel, and all cooperative sensor nodes transmit their sensing data to the FC via ideal control channel.

To analyze the impact of the attacking probability on global error probability, we consider three typical SSDF attacks: Always-Yes, Always-No and Always-Opposite attacks [37], [38]. Among them, Always-Yes attack means that the attacker submits the sensing report "1" to show the PU signal being absent regardless of its local sensing result [39], [40]. Hence, the cognitive radio system mistakenly believes that the frequency band is occupied by PU, and the malicious sensor nodes can monopolize the spectrum band. Under the Always-No attack, the attacker submits the sensing report "0" to show the PU signal is absent, even though the PU is occupying the spectrum band. As a result, the final decision made by FC will show the PU spectrum bands to be absent and the interference to PU may be occurred by sensor node's data transmission. In the case of Always-Opposite attack, the attacker usually intends to cause either selfish grabbing or interference to the PU by submitting the sensing report that is opposite of its local sensing result [41], [42].

Figure 1 shows the results of global error probability under different attacking probability. The higher the attack probability is, the more frequent the attack is as well as the easier the malicious nodes to be exposed. It can be seen that with the increase of node attack probability, the error probability increases evidently and then decreases as the attack probability exceeds 30%. It illustrates that our method can distinguish the reports of the honest SUs and the reports of the attackers, thus identify the attackers effectively. Comparatively, the malicious nodes can obtain higher error probability by launching Always-Opposite attack, and it shows that the attack behavior is more hidden and destructive than other attacks. Also, it demonstrate that our proposed method can alleviate the effect of false sensing data caused by malicious nodes, which can oblige the malicious nodes to take into account of the trade-off between concealment and destructiveness as launching the attacks.

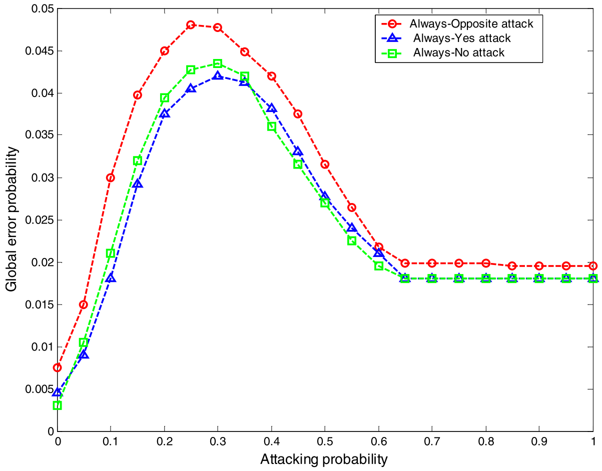

FIGURE 1. Global error probability under different attacking probability.

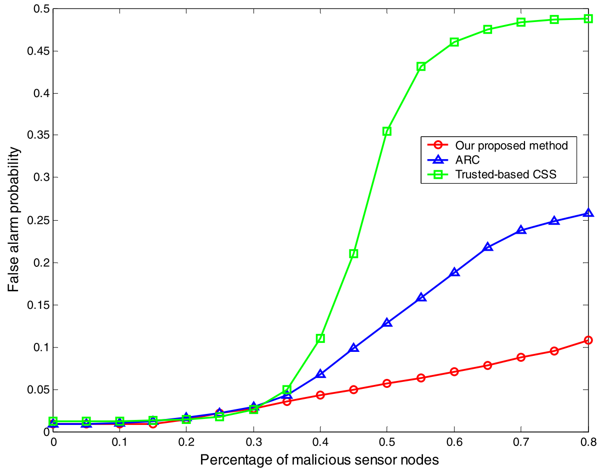

FIGURE 2. False alarm probability under Always-Yes attack.

Additionally, to evaluate the sensing performance of the proposed method, we compare with ARC [43] and Trusted-based CSS [44] in aspects of missed detection probability and false alarm probability under various attack models. Figure 2 and 3 respectively show the cooperative spectrum sensing performance under Always-Yes attack with different proportion of malicious sensor nodes. It can be found that the

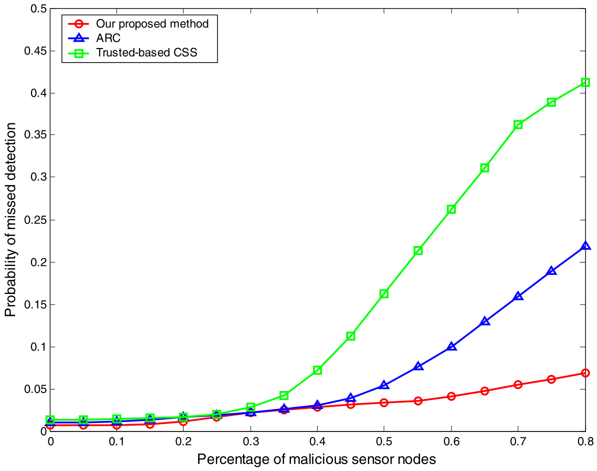

FIGURE 3. Missed detection probability under Always-Yes attack.

probability of false alarm and missed detection increases with the proportion of malicious sensor nodes. When the proportion of malicious sensor nodes exceeds 35%, the false alarm probability of the system of Trusted-based CSS deteriorates significantly. Compared with other methods, the false alarm probability in our proposed method varies from 0.011 to 0.12 even when the proportion of malicious sensor nodes reaches 80%. It is worth noting that the missed detection probability of ARC is better than that of the proposed method under the low proportion of malicious sensor nodes. However, when the high proportion of malicious sensor nodes will launch attacks, most of the sensing data are unreliable. It makes the anti SSDF attack strategy unable to play a role, and the performance drops obviously. In our method, the reputation mechanism based on historical perception data can help to eliminate the influence of falsified sensing information, and be proven to be an effective way to remove the effect of SSDF.

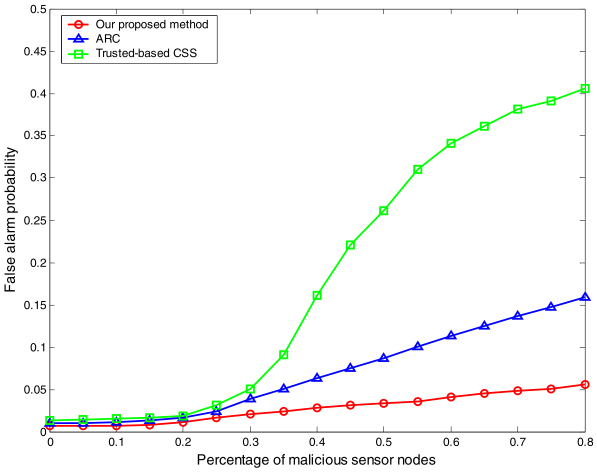

FIGURE 4. False alarm probability under Always-No attack.

Figs. 4 and 5 show the false alarm probability and the missed detection probability versus percentage of malicious SUs under the Always-No attacks. We observe that both our proposed method and ARC better performance than Trusted-based CSS. When the percentage of malicious presence becomes more than 50%, the false alarm probability of Trusted-based CSS has reached about 25%. Moreover, Trusted-based CSS shows the worse missed detection probability for different percentage of malicious sensor nodes as compared to our proposed method and ARC. After the proportion of malicious sensor nodes is more than 25%, the performance of ARC has deteriorated dramatically. The deterioration of our proposed method is relatively slow, and the probability of missed detection is increased to 0.165 in the case of 80% malicious sensor nodes.

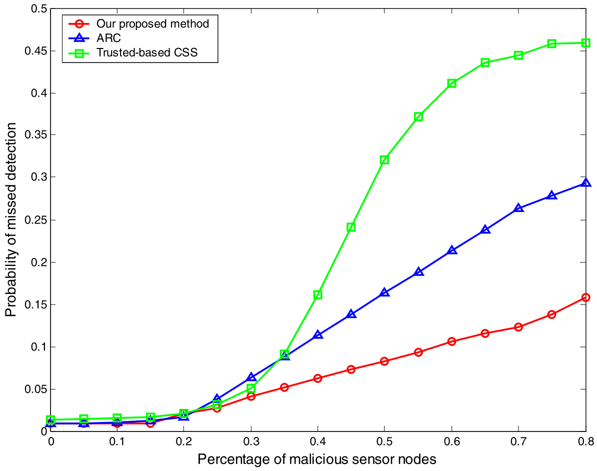

FIGURE 5. Missed detection probability under Always-No attack.

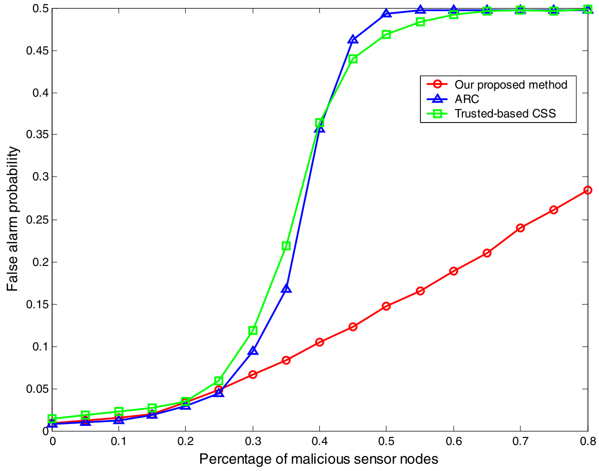

FIGURE 6. False alarm probability under Always-Opposite attack.

In addition, the simulation is performed under Always-Opposite attack to analyze the performance of our method. Figs. 6 and 7 show the false alarm probability and missed detection probability of different methods under Always-Opposite attack. It can be found that the probability of missed detection and false alarm under Always-Opposite mode increases with the proportion of malicious nodes, and the deterioration degree of all methods is significantly higher

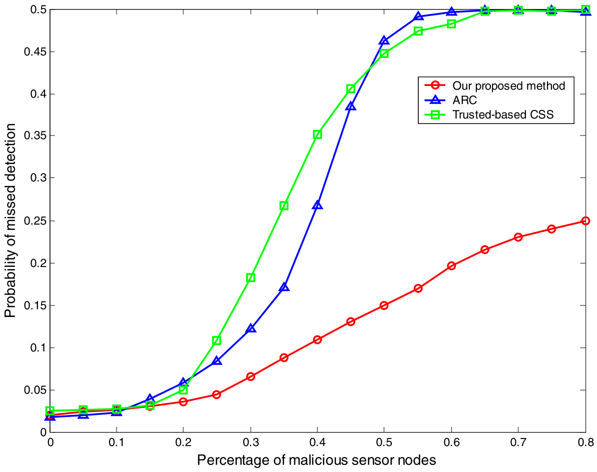

FIGURE 7. Missed detection probability under Always-Opposite attack.

than that in the previous two scenarios. It demonstrate that the opposite sensing data can cause a mass of more hazardous influence on the final fusion and result in more remarkable rise in the number of low detections and high false alarm circumstance at the FC. It also can be observed that our proposed method can obtain better sensing performance than other methods. This is due to the fact that our proposed approach succeeds in detecting and isolating the attackers, and avoids the confusion between the reports of the honest sensor nodes and the attackers.

V. CONCLUSION

In this paper, a secure CSS strategy based on reputation mechanism for cognitive wireless sensor networks is proposed to defense against SSDF attack. The beta reputation model is applied to assign reputation value to cognitive sensor nodes according to their historical sensing behavior, and a dynamic trust evaluation scheme of CSS is established. In the final fusion decision, the FC allocates a reasonable weight value according to the evaluation of the submitted observations to enhance the accuracy of the sensing system.

In this paper, we focus on the performance parameters of missed detection probability and false alarm probability. In the future, we will concentrate other network parameters, e. g., detection rate, false detection rate, and throughput at the presence of attackers. Additionally, we will further optimize the proposed reputation model to deal with the case when the attackers may improve their attack strategy adaptively based on the previous decisions.

REFERENCES

[1] H. Rifà-Pous, M. J. Blasco, and C. Garrigues, "Review of robust cooperative spectrum sensing techniques for cognitive radio networks," *Wireless Pers. Commun.*, vol. 67, no. 2, pp. 175–198, Nov. 2012.

[2] A. De Domenico, E. Calvanese Strinati, and M.-G. Di Benedetto, "A survey on MAC strategies for cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 1, pp. 21–44, 1st Quart., 2012.

[3] V. Jamali, N. Reisi, M. Ahmadian, and S. Salari, "Optimization of linear cooperation in spectrum sensing over correlated log-normal shadow fading channels," *Wireless Pers. Commun.*, vol. 72, no. 3, pp. 1691–1706, Oct. 2013.

[4] P. Prakash, S.-R. Lee, S.-K. Noh, and D.-Y. Choi, "Issues in realization of cognitive radio sensor networks," *Int. J. Control Autom.*, vol. 7, no. 1, pp. 141–152, Jan. 2014.

[5] J. Ren, Y. Zhang, Q. Ye, K. Yang, K. Zhang, and X. S. Shen, "Exploiting secure and energy-efficient collaborative spectrum sensing for cognitive radio sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6813–6827, Oct. 2016.

[6] R. Wan, L. Ding, N. Xiong, and X. Zhou, "Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 9, pp. 1–11, 2019.

[7] M. J. Saber and S. M. S. Sadough, "Optimisation of cooperative spectrum sensing for cognitive radio networks in the presence of smart primary user emulation attack," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 1, 2017, Art. no. e2885.

[8] S. Madbushi, R. Raut, and M. S. S. Rukmini, "Security issues in cognitive radio: A review," in *Proc. Int. Conf. Microelectron., Electromagn. Telecommun.*, Visakhapatnam, India, Dec. 2015, pp. 121–134.

[9] P. Subbulakshmi, M. Prakash, and V. Ramalakshmi, "Honest auction based spectrum assignment and exploiting spectrum sensing data falsification attack using stochastic game theory in wireless cognitive radio network," *Wireless Pers. Commun.*, vol. 102, no. 2, pp. 799–816, Sep. 2018.

[10] Y. Fang, X. Zhang, and Y. Li, "Comprehensive reputation-based security mechanism against dynamic SSDF attack in cognitive radio networks," *Symmetry*, vol. 8, no. 12, pp. 1–18, Dec. 2016.

[11] A. H. Hamed, A. A. Sharifi, M. J. M. Niya, and H. Seyedarabi, "Attack-aware cooperative spectrum sensing in cognitive radio networks under Byzantine attack," *J. Commun. Eng.*, vol. 6, no. 1, pp. 81–98, 2017.

[12] 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.

[13] M. Ghaznavi and A. Jamshidi, "A reliable spectrum sensing method in the presence of malicious sensors in distributed cognitive radio network," *IEEE Sensors J.*, vol. 15, no. 3, pp. 1810–1816, Mar. 2015.

[14] Z. Qin, Y. Gao, M. D. Plumbley, C. G. Parini, and L. G. Cuthbert, "Low-rank matrix completion based malicious user detection in cooperative spectrum sensing," in *Proc. IEEE Global Conf. Signal Inf. Process.*, Dec. 2013, pp. 1186–1189.

[15] 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.

[16] S. Nath, N. Marchang, and A. Taggu, "Mitigating SSDF attack using k-medoids clustering in cognitive radio networks," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 275–282.

[17] J. Wang, S. Feng, Q. Wu, X. Zheng, Y. Xu, and G. Ding, "A robust cooperative spectrum sensing scheme based on dempster-shafer theory and trustworthiness degree calculation in cognitive radio networks," *EURASIP J. Adv. Signal Process.*, vol. 2014, no. 1, pp. 35–42, Dec. 2014.

[18] 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.

[19] M. T. Yu, L. J. Zhao, and Z. Li, "Improved cooperative spectrum sensing scheme based on demp-ster-shafer theory in cognitive radio network," *J. Commun.*, vol. 35, no. 3, pp. 168–173, 2014.

[20] Y. Han, Q. Chen, and J.-X. Wang, "An enhanced D-S theory cooperative spectrum sensing algorithm against SSDF attack," in *Proc. IEEE 75th Veh. Technol. Conf. (VTC Spring)*, May 2012, pp. 1–5.

[21] S. Feng, X. Zheng, R. Liu, J. Chen, S. Xu, and L. Zhang, "Admissible evidence: Trustworthy cooperative spectrum sensing based on dempster-shafer theory in cognitive radio networks," in *Proc. IEEE/ACIS 13th Int. Conf. Comput. Inf. Sci. (ICIS)*, Jun. 2014, pp. 11–15.

[22] X. Ni, H. Chen, L. Xie, and K. Wang, "Reputation-based hierarchically cooperative spectrum sensing scheme in cognitive radio networks," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Aug. 2013, pp. 397–402.

[23] M. Gupta and G. Yerma, "Improved weighted cooperative spectrum sensing algorithm based on reliability in cognitive radio networks," in *Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2016, pp. 609–612.

[24] Z. Huang, X. Xu, J. Ni, H. Zhu, and C. Wang, "Multimodal representation learning for recommendation in Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10675–10685, Dec. 2019.

[25] Z. Wei, H. Tang, and F. R. Yu, "A trust based framework for both spectrum sensing and data transmission in CR-MANETs," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 562–567.

[26] J. Feng, Y. Zhang, G. Lu, and W. Zheng, "Securing cooperative spectrum sensing against ISSDF attack using dynamic trust evaluation in cognitive radio networks," *Secur. Commun. Netw.*, vol. 8, no. 17, pp. 3157–3166, Nov. 2015.

[27] 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.

[28] S. Althunibat, B. J. Denise, and F. Granelli, "Identification and punishment policies for spectrum sensing data falsification attackers using delivery-based assessment," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7308–7321, Sep. 2016.

[29] A. A. Sharifi and M. J. Musevi 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.

[30] N. Biswas, G. Das, and P. Ray, "Optimal hybrid spectrum sensing under control channel usage constraint," *IEEE Trans. Signal Process.*, vol. 66, no. 14, pp. 3875–3890, Jul. 2018.

[31] Y. Peng, F. Al-Hazemi, H. Kim, and C.-H. Youn, "Joint selection for cooperative spectrum sensing in wireless sensor networks," *IEEE Sensors J.*, vol. 16, no. 22, pp. 7837–7838, Nov. 2016.

[32] S. Nallagonda, A. Chandra, S. D. Roy, S. Kundu, P. Kukolev, and A. Prokes, "Detection performance of cooperative spectrum sensing with hard decision fusion in fading channels," *Int. J. Electron.*, vol. 103, no. 2, pp. 297–321, 2016.

[33] S. H. Chowdhury, B. Grebur, and L. Xiao, "Defense against spectrum sensing data falsification attacks in cognitive radio networks," in *Proc. Int. Conf. Secur. Privacy Commun. Netw.*, London, U.K., Sep. 2011, pp. 154–171.

[34] 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)*, Apr. 2013, pp. 614–619.

[35] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, "BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 59, pp. 88–94, Jan. 2016.

[36] M. Ndiaye, G. Hancke, and A. Abu-Mahfouz, "Software defined networking for improved wireless sensor network management: A survey," *Sensors*, vol. 17, no. 5, pp. 1031–1045, 2017.

[37] N. Marchang, A. Taggu, and A. K. Patra, "Detecting byzantine attack in cognitive radio networks by exploiting frequency and ordering properties," *IEEE Trans. Cognit. Commun. Netw.*, vol. 4, no. 4, pp. 816–824, Dec. 2018.

[38] M. Zhang, D. Zhang, H. Yao, and K. Zhang, "A probabilistic model of human error assessment for autonomous cargo ships focusing on human-autonomy collaboration," *Saf. Sci.*, vol. 130, Oct. 2020, Art. no. 104838.

[39] Y. F. Li and L. Z. Huang, "Cooperative spectrum sensing algorithm based on improved weighted sequential probability ratio test," *Appl. Res. Comput.*, vol. 33, no. 1, pp. 171–173, 2016.

[40] F. Hu and G. Wu, "Distributed error correction of EKF algorithm in multi-sensor fusion localization model," *IEEE Access*, vol. 8, pp. 93211–93218, 2020.

[41] C. Xu, "A novel recommendation method based on social network using matrix factorization technique," *Inf. Process. Manage.*, vol. 54, no. 3, pp. 463–474, May 2018.

[42] Z. Huang, X. Xu, H. Zhu, and M. Zhou, "An efficient group recommendation model with multiattention-based neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Jan. 15, 2020, doi: 10.1109/TNNLS.2019.2955567.

[43] 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.

[44] J. Wang, I.-R. Chen, J. J. P. Tsai, and D.-C. Wang, "Trust-based cooperative spectrum sensing against SSDF attacks in distributed cognitive radio networks," in *Proc. IEEE Int. Workshop Tech. Committee Commun. Qual. Rel. (CQR)*, May 2016, pp. 1–6.

XIANQUAN LUO was born in Fujian, China. He received the M.E. and D.E. degrees in navigation, guidance, and control from Ordnance Engineering College, China, in 2004 and 2007, respectively. He is currently an Associate Professor with the College of Artificial Intelligence, Yango University, China. His main research areas include radar technology, sensor detection technology, and artificial intelligence.