Hindawi
Security and Communication Networks
Volume 2023, Article ID 7844054, 8 pages
https://doi.org/10.1155/2023/7844054

Research Article

A Collaborative Spectrum Sensing Algorithm Based on Reputation Update against Malicious User Attacks

Hong Du and Long Chen

School of Electrical and Engineering, Chongqing University of Technology, Chongqing 400054, China

Correspondence should be addressed to Long Chen; chenlong118@cqut.edu.cn

Received 12 December 2022; Revised 28 February 2023; Accepted 7 March 2023; Published 14 April 2023

Academic Editor: Jegatha Deborah

In cognitive radio networks, collaborative spectrum sensing (CSS) algorithms could improve spectrum detection performance; however, most explorations are based on reliable network environments. In the real network environment, there may be malicious users that bring wrong spectrum sensing results and attacks designed by them remarkably reduce the spectrum efficiency. In order to resist the attacks of malicious users, this paper proposes a CSS method based on the reputation update. By setting an appropriate reputation threshold, the user fusion center selects the sensing user with a higher reputation to participate in the CSS. Each user's reputation value is then updated according to whether its local sensing result matches the final judgment result. This article chiefly discusses scenarios for application of three information fusion rules. The simulation results reveal that the proposed approach with reputation update outperforms the conventional CSS algorithm for a variety of judgment rules. The proposed algorithm is capable of preventing lower reputation users from participating in the CSS, filtering out malicious users, and eliminating the impact of malicious users' attacks.

1. Introduction

A cognitive radio network (CRN) can not only be compatible with the existing static spectrum allocation system but also substantially improve the spectrum efficiency at a low cost. Spectrum sensing is the primary problem to be solved in the CRN, and its main goal is to achieve the dynamic spectrum information in the surrounding environment quickly and reliably. As a result, each secondary user (SU) would be capable of sharing the spectrum based on the opportunistic access approach without interfering with the existing primary users (PUs) [1].

To reduce the adverse effects of multipath and shadow fading, multiple secondary users usually need to cooperate. Most existing collaborative spectrum sensing (CSS) schemes require specific base stations or fusion centers that collect local sensing results or decisions from all cooperating users and then fuse them with some rules to make a final decision.

In a real spectrum sensing environment, there may be malicious users sending false information. Malicious users send manipulated local sensing results to neighboring users, leading to a remarkable loss of spectrum sensing accuracy. Secure spectrum sensing algorithms to resist the attacks of malicious users have attracted more and more researchers' attention and research [2–5].

The CSS-based algorithm in cognitive radio is capable of improving the sensing performance but is not effective in defending against malicious users. The main purpose of the system proposed in the current investigation is to eliminate malicious users to prevent the CSS of the attack effect. The major contributions of this article are as follows:

(1) We propose an appropriate methodology to defend against attacks from malicious users in CRNs by calculating and updating the reputation value of secondary users. We show that our proposed defense mechanism outperforms the existing ones.

(2) The optimal decision rule for cooperative sensing is methodically examined with the proposed spectrum sensing scheme based on the reputation. Such

a scheme with the "majority" rule ensures higher detection probability and better spectrum sensing performance with a small false alarm probability. This approach is capable of noticeably improving the accuracy of spectrum sensing.

The rest of the present article is organized as follows. Section 2 presents the works associated with the CSS under malicious user attacks. In Section 3, we introduce the system model of a CSS algorithm based on reputation update and discuss various data fusion rules. In Section 4, we describe the traditional performance of the CSS and propose an approach to defend against attacks by evicting malicious users. In Section 5, we provide the simulation results and discussion. Finally, Section 6 presents the major obtained results in this paper.

2. Related Work

Most existing investigations on spectrum sensing performance in CRNs are essentially organized based on the premise that cognitive users are generally reliable. In a real spectrum sensing environment, there may be malicious users sending false information. Therefore, in recent years, more investigators have started to examine the impact of unreliable cognitive users on spectrum sensing performance and how to circumvent the interference of malicious users.

Rawat et al. [6] analyzed the performance limitations of CSS under Byzantine attacks where malicious users send false sensing data to the fusion center, which increases the probability of false sensing results. To defend against spectrum sensing data falsification (SSDF) attackers, Xu et al. [7] proposed an alternative optimization algorithm based on a dual reputation mechanism to maximize throughput. For this purpose, a dual reputation-based algorithm was proposed to distinguish the SSDF attackers and the honest secondary users were determined. Wang et al. [8] established a reputation-based CSS algorithm for mobile CRNs to resist malicious attacks. They proposed the idea of the "slide window" to increase the number of detected results during each iteration to enhance the stability and accuracy of the algorithm. Al-Mathehaji et al. [9] proposed a defense strategy to thwart SSDF attacks by intelligently verifying sensory data with the help of trusted nodes. The proposed scheme employed an efficient and fast reputation-based algorithm to analyze each user's behavior. Amjad et al. [10] presented a reputation system that works in the scenarios described above in conjunction with a semisupervised spatiospectral detection system, which could reduce the decision error rate and lead to a higher detection rate of malicious users. To improve malicious user detection and primary user identification in mobile CRN, Jana et al. [11] developed a primary user detection method based on the location reliability (LR) and a malicious user detection method based on the LR and Dempster–Shafer (DS) theories.

Mousavifar and Leung [12] proposed a secure and efficient cooperative spectrum sensing scheme to resist SSDF attacks and increase the energy efficiency in the CRSN. In order to maximize the energy efficiency of spectrum sensing, Ren et al. [13] evaluated the minimum number of sensor nodes required for spectrum sensing to ensure the optimal accuracy of the sensing results. The CSS in the presence of primary user emulation attackers (PUEA) was also explored by Pourgharehkhan et al. [14], which constituted a PUEA network in a cognitive radio network by impersonating primary users. In order to achieve the best performance and protect the predefined requirements of the CR, the authors proposed an algorithm to incorporate the help of secondary users in the spectrum sensing.

To reduce the effects of malicious users, a framework with high detection accuracy and low data acquisition costs in SUs was examined by Qin et al. [15]. Compared with the conventional approach, the proposed malicious user detection framework achieves high detection accuracy with lower data acquisition costs. To lessen the impact of interference and attacks, Zhang et al. [16] designed an ensemble machine learning framework that provides robust and accurate fusion performance. Ma et al. [17] analyzed the effect of an incomplete collaborative control channel on the identification of malicious secondary users under independent and cooperative attacks. To better distinguish honest users from malicious users, a reputation threshold was introduced for each secondary user (i.e., a reputation-based cooperative spectrum sensing method, which was robust against attacks). Yuan et al. [18] suggested a secure fusion strategy that utilizes a "soft decision" method and could distinguish between malicious users and honest users under any distribution of sensing reports using the maximum mean difference. The proposed scheme would be suitable for general CRN application scenarios. Zhang et al. [19] established the trained model to evaluate the reliability of nonanchor sensor data and also exploit them together with new anchor sensor data to retrain the model. Extensive experiments have confirmed the high efficiency and effectiveness of reliable spectrum occupancy detection, even when malicious spectrum sensors are in the majority. Cheng et al. [20] investigated the problem of malicious user identification against limited spectrum sensing data spoofing attacks in the CSS network. To identify interactive secondary users, a detection architecture was constructed with interactive secondary users divided into binary groups and performing distributed detection. The achieved results indicated the superiority of the proposed strategy over other detection algorithms.

In unreliable cognitive radio network environments, erroneous sensing results will interfere with primary users, thus affecting the normal use of authorized users, which defeats the original purpose of cognitive radio technology. In order to solve the problem of spectrum sensing uncertainty caused by malicious users, a CSS-based algorithm using reputation update is proposed to resist malicious user attacks.

3. System Model

As can be seen from Figure 1, the model of the CSS system consists of one primary user, M secondary users, a data fusion center (FC), and several malicious users. Let us

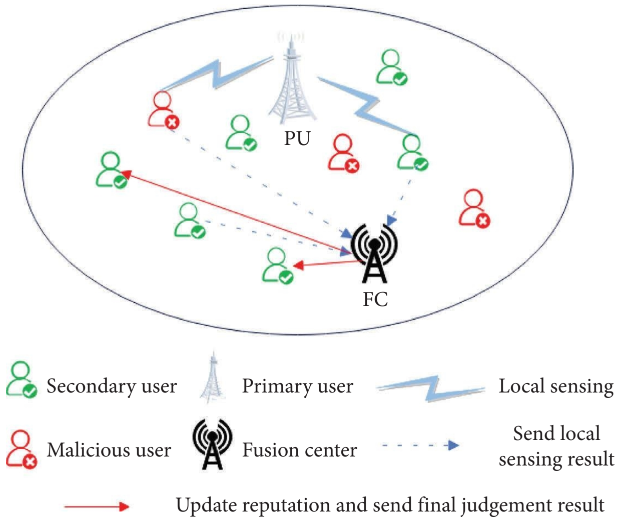
PU
FC
Secondary user
Primary user
Local sensing
Malicious user
Fusion center
Send local sensing result
Update reputation and send final judgement result

Figure 1: System model of collaborative spectrum sensing with the malicious user.

assume that the allowed band would be within the range of the user's cognitive spectrum sensing. First, each secondary user can sense independently, and then the sensed results are transmitted to the data fusion center. If there is an authorized primary user, the secondary user sends a "1" to the data fusion center; otherwise, a "0" is submitted. According to the integration rule, the data fusion center processes all sensing results, determines whether the primary user is present or not, and gives them to the secondary user.

The performance of the CSS scheme depends on the number and reputation of CR users in the CRN. If a CR user's local sensor returns a result that is less reliable, it will be given a low reputation level. Conversely, if the local sensing results of a CR user exhibit higher reliability, it will be given a high reputation level. The CR users' reputation results are accumulated from historical detection. The reputation could alter with time and environment; hence, the reputation level should be updated at any time.

In the present work, the centralized CSS approach is utilized. The fusion center receives the local sensing results and decides for the final result whether the primary user occupies the channel through the fusion rule. The main combinational methods used by the data fusion center are the "AND" rule, the "OR" rule, and the "K-out-of-N" rule. The flowchart of the fusion rule is presented in Figure 2. The information fusion center selects the adjudication rules based on the degree of spectrum required by the cognitive user service and the severity of interference restrictions by the licensed primary user.

The "AND" rule is more about maximizing the use of spectrum resources, and although the detection probability is reduced, it can be exchanged for a lower false alarm probability. The "AND" rule is suitable for scenarios where the cognitive user takes high demand for spectrum resources and the primary user exhibits low interference requirements. The advantage of collaborative sensing under the "OR" rule is the protection of primary users from harmful interference caused by cognitive users due to missed detections. This rule largely protects the primary users, but at the cost of more opportunities to use the spectrum. The "OR" rule is suitable for scenarios where the cognitive user has a low demand for spectrum resources and the primary user has a high demand for interference limits. The first two rules are extreme judgments that either focus only on protecting primary users from interference or on maximizing the use of spectrum resources, which necessities to implement a compromise solution in practical applications. The "K-out-of-N" rule is suitable for scenarios where primary users have low interference limit requirements and moderate spectrum resources.

4. A Collaborative Spectrum Sensing Algorithm Based on Reputation Update

4.1. Collaborative Spectrum Sensing Performance with Different Rules. The centralized collaborative spectrum is one of the most extensively utilized methodologies. There are two types of fusion methods that are often used, one is soft fusion and the other is hard fusion. Hard fusion means that a judgment threshold is set, and the presence of a primary user can only be determined if the information statistics would be greater than or equal to the threshold value. The fusion center receives the results of the local sensing and obtains the final result whether the original user occupies the channel through the fusion rule or not. The main fusion-based methods employed by the data fusion center are the "AND" rule, the "OR" rule, and the "K-out-of-N" rule.

The "AND" rule means that all CR users send their reputation value to the FC, and the FC receives all the results and performs a logical "AND" calculation. In other words, the FC determines that the primary user exists only when all CR users involved in the collaboration detect the presence of the primary user's signal. Until a CR user detects the presence of the primary user, the FC detects that the primary user does not exist. Assuming that the local detection probability and the false alarm probability of the i-th CR user

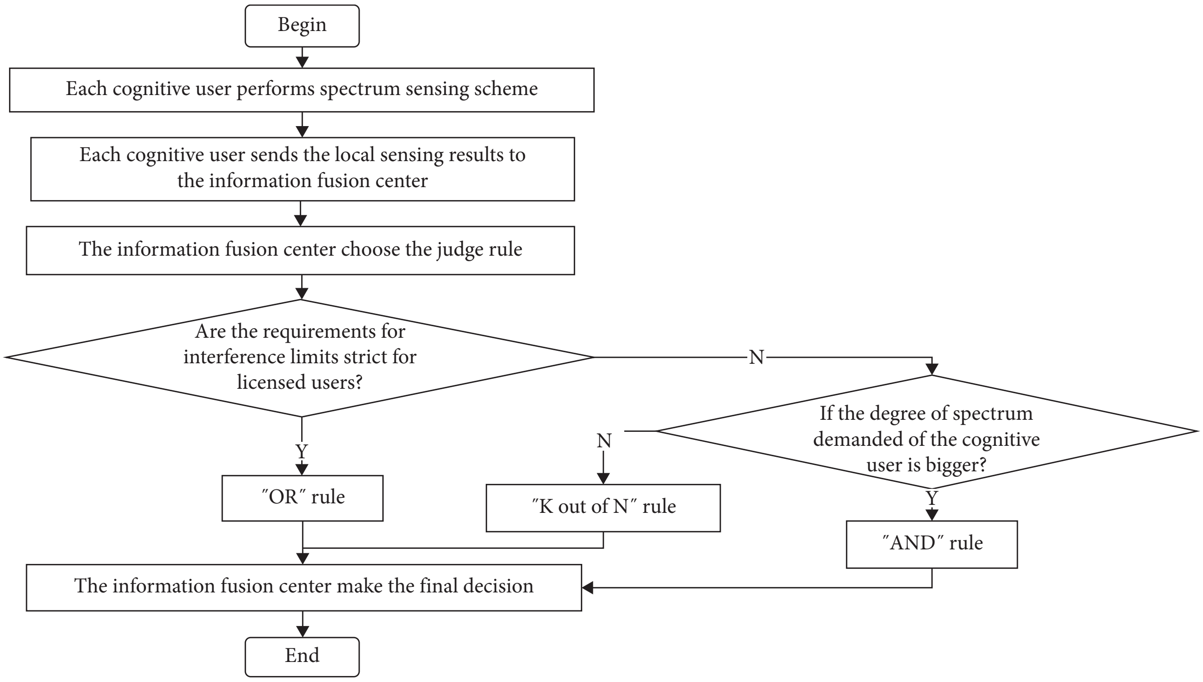
Begin
Each cognitive user performs spectrum sensing scheme
Each cognitive user sends the local sensing results to the information fusion center
The information fusion center choose the judge rule
Are the requirements for interference limits strict for licensed users?
N
Y
If the degree of spectrum demanded of the cognitive user is bigger?
N
Y
″OR″ rule
″K out of N″ rule
″AND″ rule
The information fusion center make the final decision
End

Figure 2: The flow diagram of the fusion rule.

are $p_{d,i}$ and $p_{f,i}$, respectively, the final false alarm probability Q_j and the detection probability Q_d are calculated by "AND" rule which can be evaluated as follows:

$$\begin{aligned} Q_d &= \prod_{i=1}^{M} p_{d,i}, \\ Q_f &= \prod_{i=1}^{M} p_{f,i}, \end{aligned} \tag{1}$$

where M represents the number of local CR users involved in the collaboration.

The "OR" rule means that all CR users send their sensing results to the FC, which receives all the results of the logical "OR" rule. As long as a CR user detects the presence of the primary user, the FC determines the presence of the primary user. This rule properly protects the primary user from the interference of CR users, but the spectrum utilization will be noticeably reduced, leading to the waste of spectrum resources. Assuming that the local detection probability and the false alarm probability of the i-th CR user are denoted by $p_{d,i}$ and $p_{f,i}$, respectively, the final false alarm probability Q_j and the false detection probability Q_d are calculated by "OR." By this virtue, the logic is obtained as follows:

$$Q_d = 1 - \prod_{i=1}^{M}\left(1 - p_{d,i}\right), Q_f = 1 - \prod_{i=1}^{M}\left(1 - p_{f,i}\right). \tag{2}$$

The "K-out-of-N" rule is that among M cognitive users, if the number of CR users is greater than or equal to K, it detects the presence of the primary user such that the presence of the primary user is judged to exist. Otherwise, if the number of CR users is less than K, it detects the presence of the primary user such that the primary user is judged not to exist.

$$\begin{cases} H_1\colon \sum_{i=1}^{M} D_i \geq K, \\ H_0\colon \sum_{i=1}^{M} D_i < K, \end{cases} \tag{3}$$

where D_i is the judgment result of the i-th CR user.

Assuming that the local detection probability and the false alarm probability of the i-th CR user are represented by $p_{d,i}$ and $p_{f,i}$, respectively, the final false alarm probability Q_j and the false detection probability Q_d are calculated by the "K-out-of-N" rule, as evaluated in the following form:

$$\begin{aligned} Q_d &= \sum_{j=k}^{M} \sum_{\Sigma D_i = j} \prod_{i=1}^{M} \left(p_{d,i}\right)^{D_i}\left(1 - p_{d,i}\right)^{1-D_i}, \\ Q_f &= \sum_{j=k}^{M} \sum_{\Sigma D_i = j} \prod_{i=1}^{M} \left(p_{f,i}\right)^{D_i}\left(1 - p_{f,i}\right)^{1-D_i}. \end{aligned} \tag{4}$$

4.2. Collaborative Spectrum Sensing Performance Based on Reputation Update. The proposed algorithm in this paper is also allowed to set a suitable reputation threshold. To this end, each CR user obtains sensing results through local energy detection and compares them with the reputation threshold value. However, the FC only receives sensing results from CR users above the threshold value and fuses them. It implies that the FC selects the sensing CR users with a higher reputation to participate in spectrum sensing collaboration and filters CR users with a low reputation. Finally, the reputation value of each CR user is updated according to whether the local sensing result of each CR user is consistent with the corresponding global one.

$p_{\mathrm{di}}(z)$ refers to the probability that the FC judges the presence of PU signal $x(t)$ ($d_{FC} = 1$) and the i-th CR user also judges the presence of PU signal ($d_i = 1$) at the z-th spectrum sensing, which is the detection probability of the i-th CR user at the z-th spectrum sensing. $p_{fi}(z)$ stands for the probability that the FC judges the absence of PU signal $x(t)(d_{FC} = 0)$ and the i-th CR user judges that the PU signal is present ($d_i = 1$), which is the false alarm probability of the i-th sensing node at the z-th spectrum sensing.

$$\begin{aligned} p_{\mathrm{di}}(z) &= p\left\{d_i = 1 \middle| d_{\mathrm{FC}} = 1\right\}, \\ p_{\mathrm{fi}}(z) &= p\left\{d_i = 1 \middle| d_{\mathrm{FC}} = 0\right\}, \end{aligned} \tag{5}$$

where d_i represents the local sensing result of the i-th CR user, d_{FC} denotes the sensing result of the FC, and z stands for the number of spectrum sensing, $i = 1,2, \ldots, z$.

$$\begin{aligned} H_0&: d_i = 0, \\ H_1&: d_i = 1, \end{aligned} \tag{6}$$

where H_0 and H_1 represent the local sensing result of the i-th CR user.

The reputation degree R_i is set appropriately for each user, and two threshold values are set as λ and θ, where λ represents the energy detection threshold and θ denotes the reputation degree threshold. Based on their trust values $R_i(z)$, the users can be generally classified into three states:

(1) When $R_i < \lambda$, the user is in an untrusted state, and it is filtered out and cannot participate in CSS.

(2) When $\lambda < R_i < \theta$, the user is in a waiting state, and the fusion center will not receive its sensed results, but the user's reputation value is still updated.

(3) When $R_i > \theta$, the user is in a reliable state, and the fusion center allows it to participate in the CSS.

The reputation can be updated as follows:

$$R_i(z+1) = R_i(z) + (-1)^{\left(f_i(z) + D(z)\right)}. \tag{7}$$

The result of the local spectrum sensing is given as

$$f_i(z) = \begin{cases} 1, & \Gamma_i(z) \geq \lambda, \\ 0, & \text{otherwise}. \end{cases} \tag{8}$$

According to the above equation, the reputation value of the i-th CR user in the z-th spectrum sensing can be evaluated.

$R_i(z)$ denotes the reputation of the i-th CR user at the z-th sensing, μ represents the judgment threshold of the fusion center, and $G = \{i, R_i(z) > \theta\}$.

$$D(z) = \begin{cases} 1, & \sum\limits_{i \in G} w_i(z)\Gamma_i(z) \geq \mu, \\ 0, & \text{otherwise}. \end{cases} \tag{9}$$

The weights can be expressed as follows:

$$\begin{aligned} w_i(z) &= \frac{w_i'(z)}{\sum\limits_i w_i'(z)}, \\ w_i'(z) &= \frac{R_i(z)}{\max\ \left(R_i(z)\right)}. \end{aligned} \tag{10}$$

5. Simulation Results and Discussion

Let us assume that the proportion of malicious users is $n = 0.4$, the number of CR users is $M = 30$, the signal-to-noise ratio is SNR = −8 dB, a sinusoidal signal is taken as the PU signal, sampling frequency is FS = 100 MHz, sampling points is 10000, and a sinusoidal signal and a randomly generated Gaussian white noise represent the signal detected by the SU in the simulation environment.

The performance comparison of the proposed scheme with reputation and traditional scheme using the "AND" rule is illustrated in Figure 3. The detection probability of the reputation-based algorithm is higher than that of the traditional CSS with the "AND" rule. In the case of the false alarm probability equal to 0.1, the detection probability of the traditional algorithm is obtained as 0.35, and the detection probability of the reputation-based algorithm is predicted to be 0.75. This is mainly attributed to the fact that the malicious users are eliminated due to low reputation in the proposed algorithm, and the sensing results of the cognitive users with high reputations are chosen to participate in the final decision.

Figure 4 compares the spectrum sensing performance of the proposed algorithm with reputation and the traditional CSS scheme using the "OR" rule. The plotted results indicate that the detection probability of the CSS with the reputation-based algorithm is higher than that of the traditional CSS-based algorithm for the "OR" rule. When the false alarm probability is set as 0.1, the detection probability of the traditional algorithm is predicted to be 0.83, and the detection probability of the reputation-based algorithm is gained as 0.98. This issue is essentially ascribed to the fact that in the traditional CSS algorithm, the final decision using the "OR" rule is more prone to malicious users, resulting in poor spectrum detection performance.

Figure 5 compares the spectrum sensing performance of the algorithm with and without the "majority" rule reputation. The "majority" rule is achieved in the case of $K = N/2$ for the "K-out-of-N" rule, that is, more than half of the secondary users judge that the primary user exists, and the final decision is that the primary user exists. The demonstrated results reveal that the detection probability of the CSS with the reputation-based algorithm is higher than that of the traditional CSS algorithm for the "majority" rule. When the false alarm probability is set equal to 0.1, the detection probability of the traditional algorithm is obtained as 0.93, and the detection probability of the reputation-based algorithm is predicted to be 1. The "majority" rule means that the judgment of more than half of the cognitive users is the final decision. Therefore, the influence of the spectrum

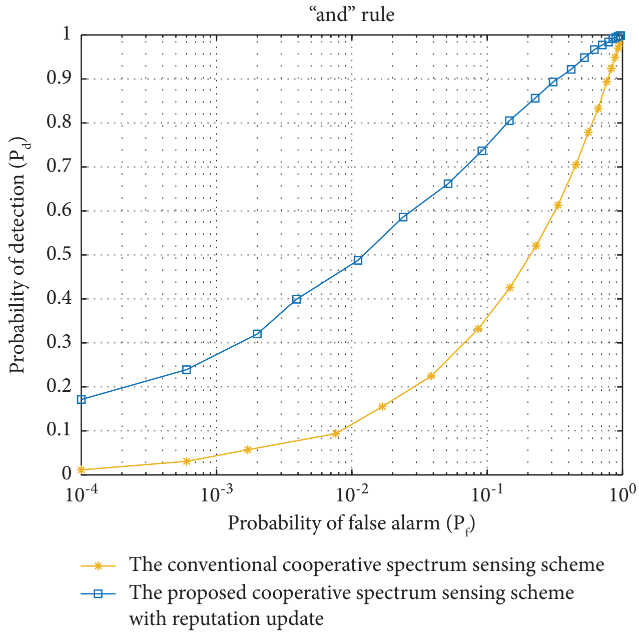

Figure 3: Comparison of the performance of proposed scheme with reputation and traditional scheme (“AND” rule).

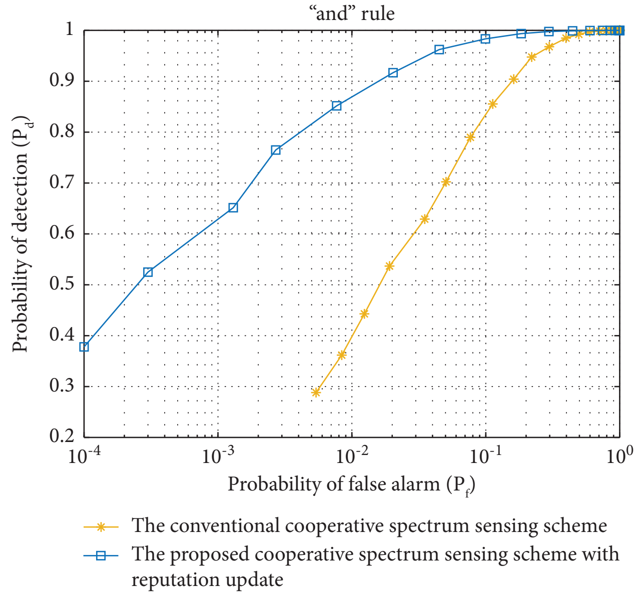

Figure 4: Comparison of the performance of proposed scheme with reputation and traditional scheme (“OR” rule).

sensing inaccuracy due to the malicious users is relatively small compared to the proposed scheme.

The simulation results reveal that the CSS with a reputation-based algorithm outperforms the traditional algorithm, and the proposed reputation-based algorithm is capable of improving the detection probability and effectively resisting the malicious users.

Figure 6 compares the spectrum sensing performance of the reputation-based CSS algorithm based on the “AND” rule, “OR” rule, and “majority” rule. For the proposed algorithm based on reputation update, when the false alarm probability is set as 0.1, the spectrum detection probability with the “AND” rule is predicted to be 0.75, and the spectrum detection probability with the “OR” rule is obtained as 0.98. The probability of detecting the “majority” rule for spectrum sensing would be 1. The “majority” rule is a compromise solution in practical CRNs, which is appropriate for scenarios where the primary user has low interference limit requirements and moderate spectrum resource needs.

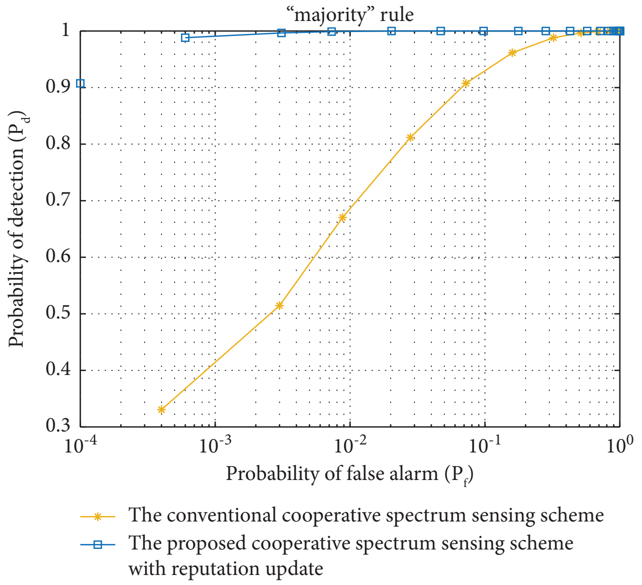

Figure 5: Comparison of the performance of proposed scheme with reputation and traditional scheme (“majority” rule).

According to the simulation results, the CSS algorithm based on the “majority” rule has a higher detection probability and performs better in spectrum sensing.

In the case of the “majority” rule, the effectiveness of the CSS-based approach has been compared for both cases with and without reputations. The percentage of malicious users is set as 0.1, 0.3, and 0.5, respectively. Figure 7 and Table 1 represent that the reputation-based CSS performs better as the percentage of malicious users raises. The performance of the proposed algorithm on the basis of the reputation update is better than the conventional method when the percentage of malicious users is known.

When the proportion of malicious users is high and the probability of a false alarm is certain, the detection probability of the algorithm proposed in this paper is significantly higher than that of the traditional algorithm. The proposed algorithm is capable of effectively enhancing the performance of the spectrum sensing in the environment subjected to the attacks of multiple malicious users.

The simulation results indicate that the reputation-based CSS algorithm with the “majority” rule performs better and would be more effective against malicious users. This fact

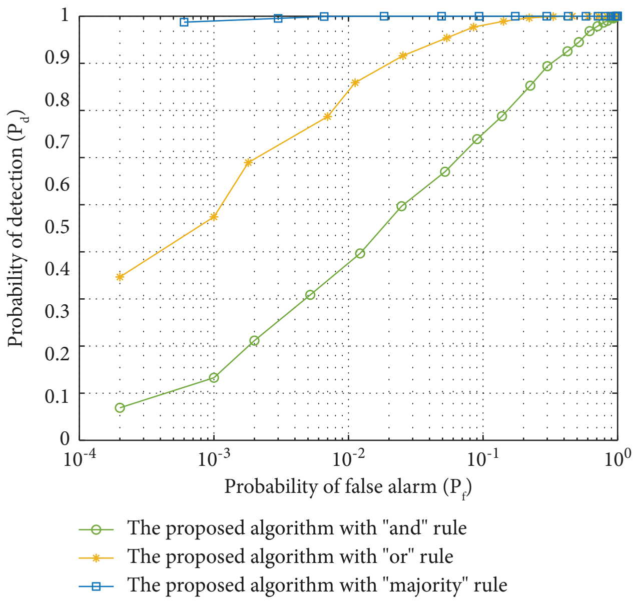

FIGURE 6: Comparison of collaborative spectrum sensing performance with reputation for different rules.

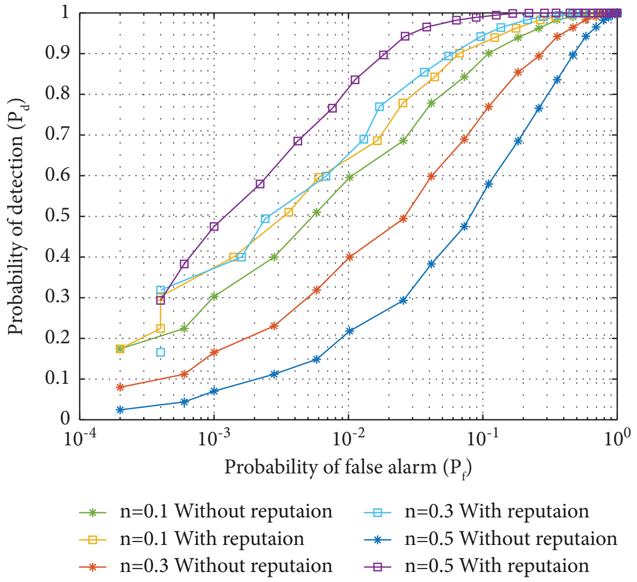

FIGURE 7: Comparison of the performance of proposed scheme with reputation and traditional scheme without reputation under different proportion of malicious users.

TABLE 1: Probability of detection for the algorithm with and without reputation in different proportion of malicious users.

Algorithm	The proportion of malicious users		
	0.1	0.3	0.5
Traditional algorithm	0.88	0.79	0.59
Proposed algorithm	0.92	0.94	0.99

ensures efficient and secure spectrum sensing in environments with a high number of malicious users.

6. Conclusions

The CSS in cognitive radio is capable of enhancing the sensing performance; however, it is ineffective against malicious user attacks. In order to effectively repel the attacks of malicious users, in this paper, we establish a CSS algorithm based on the reputation update. By analyzing the simulation results and contrasting them with the CSS algorithm, we are able to improve the spectrum detection performance. The achieved results reveal that the proposed reputation-based algorithm with the "majority" rule performs better and is the most effective against malicious users.

Data Availability

The data are available on reasonable request from the corresponding author.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This study was supported by the Science and Technology Research Program of Chongqing Municipal Education Commission (grant nos. KJQN202101123, KJQN202101110, and KJQN202101128), 2021 Chongqing Doctoral "Through Train" Scientific Research Project (nos. CSTB2022BSXM-JCX0118 and CSTB2022BSXM-JCX0119), and Scientific Research Start-Up Fund Project of Chongqing University of Technology (no. 2020ZDZ013).

References

[1] Y. C. Liang, K. C. Chen, G. Y. Li, and P. Mahonen, "Cognitive radio networking and communications: an overview," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 7, pp. 3386–3407, 2011.

[2] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Communications*, vol. 19, no. 6, pp. 106–112, 2012.

[3] S. A. Mousavifar and C. Leung, "Transient analysis for a trust-based cognitive radio collaborative spectrum sensing scheme," *IEEE Wireless Communications Letters*, vol. 4, no. 4, pp. 377–380, 2015.

[4] X. Wang, M. Jia, and Q. Guo, "A trust-value based cooperative spectrum sensing algorithm for mobile secondary users," *IEEE International Conference on Communication Workshop (ICCW)*, vol. 24, pp. 1635–1639, 2015.

[5] Y. Gan, C. Jiang, N. C. Beaulieu, J. Wang, and Y. Ren, "Secure collaborative spectrum sensing: a peer-prediction method," *IEEE Transactions on Communications*, vol. 64, no. 10, pp. 1–4294, 2016.

[6] 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 Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, 2011.

[7] Z. Xu, Z. Sun, and L. Guo, "Throughput maximization of collaborative spectrum sensing under SSDF attacks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 8378–8383, 2021.

[8] X. Wang, M. Jia, Q. Guo, X. Gu, and G. Zhang, "Reputation-based cooperative spectrum sensing algorithm for mobile cognitive radio networks," *China Communications*, vol. 14, no. 1, pp. 124–134, 2017.

[9] Y. Al-Mathehaji, S. Boussakta, M. Johnston, and H. Fakhrey, "Defeating SSDF attacks with trusted nodes assistance in cognitive radio networks," *IEEE Sensors Letters*, vol. 1, no. 4, pp. 1–4, 2017.

[10] M. F. Amjad, B. Aslam, and C. C. Zou, "Reputation aware collaborative spectrum sensing for mobile cognitive radio networks," in *Proceedings of the MILCOM 2013 - 2013 IEEE Military Communications Conference*, pp. 951–956, San Diego, CA, USA, November 2013.

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

[12] S. A. Mousavifar and C. Leung, "Energy efficient collaborative spectrum sensing based on trust management in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 4, pp. 1927–1939, 2015.

[13] 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 Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6813–6827, 2016.

[14] Z. Pourgharehkhan, A. Taherpour, and T. Khattab, "Efficient collaborative spectrum sensing under the smart primary user emulation attacker network," in *Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, San Diego, CA, USA, December 2015.

[15] Z. Qin, Y. Gao, and M. D. Plumbley, "Malicious user detection based on low-rank matrix completion in wideband spectrum sensing," *IEEE Transactions on Signal Processing*, vol. 66, no. 1, pp. 5–17, 2018.

[16] Y. Zhang, Q. Wu, and M. R. Shikh-Bahaei, "On ensemble learning-based secure fusion strategy for robust cooperative sensing in full-duplex cognitive radio networks," *IEEE Transactions on Communications*, vol. 68, no. 10, pp. 6086–6100, 2020.

[17] L. Ma, Y. Xiang, Q. Pei, Y. Xiang, and H. Zhu, "Robust reputation-based cooperative spectrum sensing via imperfect common control channel," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 3950–3963, 2018.

[18] S. Yuan, L. Li, and C. Chigan, "On MMD-based secure fusion strategy for robust cooperative spectrum sensing," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 504–516, Sept. 2019.

[19] Y. Zhang, A. Li, J. Li et al., "SpecKriging: GNN-based secure cooperative spectrum sensing," *IEEE Transactions on Wireless Communications*, vol. 21, no. 11, pp. 9936–9946, 2022.

[20] Z. Cheng, J. Zhang, T. Song, J. Hu, and X. Bao, "Detection strategy against restricted SSDF attack with potential interaction assistance," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 2, pp. 553–566, 2021.