Reward-Based Spectrum Sensing and Allocation Mechanism Defending Against SSDF Attacks

Liubi Huang[1], Wei Wang[1(✉)], Xiaozhen Lu[2], Jinge Sun[1], Bo Zhou[1], and Mingjie Wang[3]

[1] College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
{huanglb,wei_wang,sjg834,b.zhou}@nuaa.edu.cn
[2] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
luxiaozhen@nuaa.edu.cn
[3] Academy for Network and Communications of China Electronics Technology Group Corporation, Shijiazhuang 050081, China

Abstract. The acquisition of reliable spectrum data is a prerequisite for spectrum sharing. However, current spectrum sensing faces serious Spectrum Sensing Data Falsification (SSDF) attacks. To mitigate this challenging issue, we propose a reward-based joint spectrum sensing and channel allocation scheme, where secondary users are required to submit estimated revenue values along with their sensing results to the fusion center, the center then allocates channels based on the revenue results. The channel allocation problem is formulated as an optimization problem to maximize revenue, which is then solved using the Hungarian algorithm. Simulation results show that the obtained revenue of the secondary user with normal sensing is significantly higher than that of when launching SSDF attacks, demonstrating the effectiveness of the proposed scheme in mitigating SSDF attacks. Moreover, the proposed scheme outperforms existing spectrum sensing and channel allocation schemes when the number of trusted users is small.

Keywords: Credible Spectrum Sensing · Spectrum Access · SSDF Attacks

1 Introduction

The new features and application scenarios brought by the sixth-generation mobile communication technology (6G), such as augmented reality, virtual reality, remote healthcare, autonomous driving, and intelligent manufacturing, pose higher demands on network performance and spectrum resources [1]. It is necessary to build networks with higher data rates, lower latency, and greater connection density to ensure stable and efficient communications. As limited

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2025
Published by Springer Nature Switzerland AG 2025. All Rights Reserved
H.-H. Chen and W. Meng (Eds.): WiSATS 2024, LNICST 606, pp. 319–330, 2025.
https://doi.org/10.1007/978-3-031-86203-8_25

spectrum resources cannot meet the growing demand, it has become imperative to adopt new technologies such as cognitive radio to alleviate the pressure on spectrum resources.

By leasing idle spectrum bands owned by primary users (PUs) to secondary users (SUs), spectrum utilization can be improved with dynamic spectrum sharing [2,3]. Traditional dynamic spectrum sharing usually involves Observe, Orient, Decide, and Access (OODA) [4]. The fusion center (FC) first collects spectrum information sensed by SUs, performs data fusion, and then allocates spectrum resources [5].

Notably, reliable and trustworthy spectrum situation information is crucial for secure and efficient dynamic spectrum sharing. However, in traditional spectrum sensing, malicious and lazy users may falsify spectrum sensing results for their own benefit, resulting in decreased spectrum utilization and system efficiency. To defend against SSDF attacks and obtain true spectrum information, it is important to mitigate the impact of malicious and lazy users. In [6], the authors utilized the inconsistency in historical data, while in [7] the authors exploited the inconsistency between the location and the submitted sensing results for identifying malicious users. In [8], SUs are assigned different trust values based on sensing results, and trust scores are continually updated. SUs engaged in malicious behavior experience a decrease in their trust value, which makes them easier to detect. However, the computational complexity in these approaches is high and often inefficient. The spectrum sensing and access operate independently, failing to ensure entirely reliable spectrum sharing. Lazy users detection was proposed in [9] and the computational complexity was reduced by validating sensing behavior rather than sensing results, but this scheme may disrupt normal communications with pilot injection and lack a proper method to defend against malicious users.

Different from the aforementioned works, we propose a reward-based spectrum sensing and allocation mechanism to defend against SSDF attacks. This mechanism requires SUs to submit not only sensing results but also the estimated revenue after sensing the channel, and only the users who conduct normal sensing and true sensing results would be more likely to access the spectrum and obtain the highest revenue, thus motivating SUs to obey the rules. The scheme does not require a complex sensing data fusion process or pilot emission that interferes with normal communications. Our main contributions are summarized as follows:

- To defend against SSDF attacks from malicious and lazy users in spectrum sensing, we proposed a reward-based spectrum allocation mechanism, where SUs first conduct spectrum sensing, and then they are required to report an expected revenue based on the sensing results to the FC for subsequent spectrum allocation. In this way, the malicious or lazy users may not obtain the expected values without reporting the true sensing results, which can mitigate the SSDF attack to some extent.
- We model the channel allocation problem based on estimated revenue as an optimization problem. The Hungarian algorithm is used to obtain the

allocation strategy. Only the user who submits the primary user is absent and has the largest estimated revenue may be allocated the channel.
– We conduct simulations to verify the effectiveness of the proposed scheme. Simulation results show that the proposed mechanism can motivate rational users to submit reliable sensing results. When the number of trusted users is small, this scheme is able to maintain higher spectrum utilization as compared to existing schemes.

The remainder of this paper is organized as follows. We introduce the system model and SSDF attacks in Sect. 2. The reward-based spectrum allocation mechanism is shown in Sect. 3. The simulation results and discusses the performance are presented in Sect. 4. Finally, conclusions are given in Sect. 5.

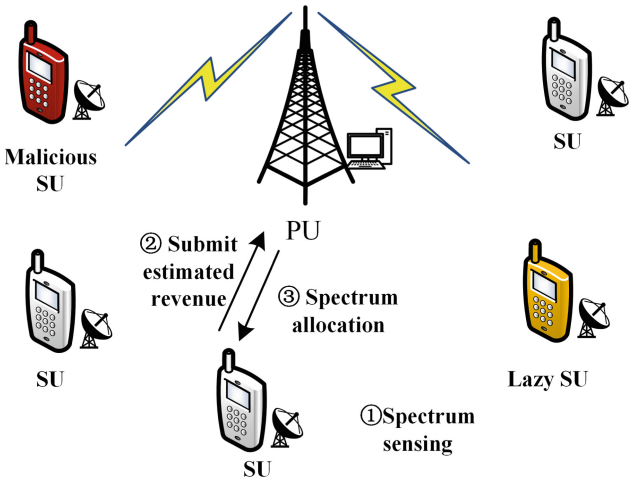

Fig. 1. System scenario.

2 System Model

We consider a spectrum sharing scenario with one PU and multiple SUs, as shown in Fig. 1. All SUs in the network constitute the set: $\{SU_i\}(1 \leq i \leq N)$. Specifically, the SUs are required to conduct spectrum sensing before accessing, and the sensing results are required to be reported to the FC. Along with the sensing results, they must submit estimated revenue, which represents their reward when accessing spectrum. When SUs detect no primary user, they can transmit at higher power to earn more revenue. Meanwhile, the FC imposes access fees based on estimated revenue during channel allocation, where higher estimates result in higher charges. There are lazy users who do not perform sensing and malicious users who report false sensing results in the network. Our model defends against attacks by analyzing the benefits of a user's current action.

2.1 Spectrum Sensing

Each time slot of spectrum sharing involves three phases: spectrum sensing, data processing, and data transmission [10]. During spectrum sensing, the SUs sample the PU's signal at rate F_s.

For a single SU, the problem of detecting a PU is modeled as a binary hypothesis test: H_0 indicates absence of PU, while H_1 indicates presence. The SU's received signal can be modeled:

$$y(n) = \begin{cases} w(n), & H_0 \\ x(n) + w(n), & H_1 \end{cases}, \tag{1}$$

where $x(n)$ represents the signal component with power P_S, and $w(n)$ denotes the zero-mean additive white Gaussian noise with power P_N. SUs are assumed to use the energy detection algorithm to construct the judgment statistic Y:

$$Y = \frac{1}{K} \sum_{n=1}^{K} |y(n)|^2, \tag{2}$$

where K represents the number of samples per unit cycle. Utilizing the central limit theorem, it can be demonstrated that for sufficiently large K, the detection statistic for a detector closely approximates a normal distribution [11]:

$$Y \sim \begin{cases} N(P_N, 2{P_N}^2/K), & H_0 \\ N(P_S + P_N, 2(P_S + P_N)^2/K), & H_1 \end{cases}. \tag{3}$$

It can be concluded that the judgment statistic Y follows a normal distribution, where the mean and variance are related to the signal power P_S and the noise power P_N.

The SUs discern the presence or absence of the PU by comparing their judgment statistic Y with the detection threshold γ. At this point the expressions for the detection probability P_D and the false alarm probability P_F are as follows [12]:

$$P_D = \Pr\{Y > \gamma | H_1\} = Q\left(\frac{\gamma - (P_S + P_N)}{\sqrt{2/K}\,(P_S + P_N)}\right), \tag{4}$$

$$P_F = \Pr\{Y > \gamma | H_0\} = Q\left(\frac{\gamma - P_N}{\sqrt{2/K} P_N}\right), \tag{5}$$

where $Q(x)$ is complement distribution function for standard normal distribution, $Q(x) = \int_x^{+\infty} \exp\left(-t^2/2\right) dt/\sqrt{2\pi}$. By setting the false alarm probability P_F to a constant value such as 0.01, a suitable threshold γ can be determined. Subsequently, the detection probability P_D can be derived based on the Eq. (4) and (5). For a trusted user SU_i^T, its sensing result of the j-th spectrum channel $S_{i,j}^T$ $(1 \le i \le N, 1 \le j \le M)$ can be denoted:

$$S_{i,j}^T = \begin{cases} 1, & \mathrm{Y} \ge \lambda \\ 0, & \mathrm{Y} < \lambda \end{cases}. \tag{6}$$

SUs use a set $\mathbf{S}_i = \{S_{i,1}, ..., S_{i,j}, ..., S_{i,M}\}$ $(1 \leq i \leq N, 1 \leq j \leq M)$ to store its sensing result for each channel.

2.2 SSDF Attacks

We improve the model to accommodate N SUs (comprising N_1 trusted users, N_2 malicious users, and N_3 lazy users), along with M PUs and one FC. Both lazy and malicious users pose threats to the system. Lazy users are very frugal with their sensing cost and refrain from sensing. They repeatedly claim PU absence to opportunistically access channels. Malicious users intend to disrupt network performance, conducting sensing but providing false results to interfere with spectrum allocation.

Lazy users are denoted by SU_i^L, and malicious users are denoted by SU_i^M. Their sensing results for the j-th channel ($S_{i,j}^L$ and $S_{i,j}^M$) can be denoted:

$$S_{i,j}^L = 0, (1 \leq i \leq N, 1 \leq j \leq M) \tag{7}$$

$$S_{i,j}^M = \begin{cases} 0, & Y \geq \lambda \\ 1, & Y < \lambda \end{cases} .(1 \leq i \leq N, 1 \leq j \leq \text{ M}) \tag{8}$$

These false sensing results will be submitted to the FC for data fusion together with normal sensing results, thus interfering with the FC's judgment of the real channel state.

3 Proposed Reward-Based Sensing and Allocation Scheme

3.1 Estimated Revenue of SUs

As shown in Fig. 1, the SU is required to provide the user ID, channel status, and estimated revenue to the FC post-spectrum sensing. This revenue estimation is derived from sensing results and mainly depends on the SU's transmission rate in the channel. Assuming the transmit power of SU_i is P_i, the channel gain is g_j, and channel noise is P_N, the estimated transmission $SNR_{i,j}$ and the estimated channel capacity $C_{i,j}$ can be expressed as follows:

$$SNR_{i,j} = P_i |g_j|^2 / P_N, \tag{9}$$

$$C_{i,j} = B \log_2 (1 + SNR_{i,j}), \tag{10}$$

where B is the band of the channel. Assume that the probability of the PU signal being absent is P_0, and the probability of it being present is $P_1 = 1 - P_0$. $R_{i,j}$ represents the estimated revenue of the SU, assuming the primary user is absent and the SU accesses the spectrum. The estimated revenue of the trusted user $R_{i,j}^T$ can be expressed as follows:

$$R_{i,j}^T = \eta \left[P_1 (1 - P_D) + P_0 (1 - P_F) \right] C_{i,j} - F_i, \tag{11}$$

where η is a constant parameter, and F_i is the sensing cost of SU. The estimated revenue for malicious user can be expressed as:

$$R_{i,j}^{M} = \eta \left(P_1 P_D + P_0 P_F\right) C_{i,j} - F_i. \tag{12}$$

Lazy user does not perform sensing, and its estimated revenue is independent of the detection probability and the false alarms probability. It can be expressed as:

$$R_{i,j}^{L} = \eta C_{i,j}. \tag{13}$$

3.2 Spectrum Allocation

The FC allocates available channels to users based on their reported estimated revenue and channel states.

SUs submit their estimated revenue vectors $\mathbf{R}_i = [R_{i,1}, ..., R_{i,j}, ..., R_{i,M}]$ $(1 \leq i \leq N, 1 \leq j \leq M)$ to the fusion center. The fusion center selects accessible users and assigns a selection vector $\mathbf{x}_i = [x_{i,1}, ..., x_{i,j}, ..., x_{i,M}]$ $(1 \leq i \leq N, 1 \leq j \leq M)$ to each SU. When $x_{i,j} = 1$, it signifies permission to access the j-th channel, whereas $x_{i,j} = 0$ denotes lack of permission. Each channel is assigned to a user individually, with no sharing among SUs. Consequently, a user can only use one channel at a time, ensuring that channels are allocated efficiently and without overlap.

Fusion center needs to solve such an optimization problem [13]:

$$\begin{aligned} &\max_{\mathbf{x}} \sum_{i=1}^{N} \mathbf{R}_i {\mathbf{x}_i}^H. \\ &s.t.\ x_{i,j} \in \{0, 1\} \\ &\quad \sum_{j=1}^{M} x_{i,j} \leq 1, i = 1, 2, ..., N \\ &\quad \sum_{i=1}^{N} x_{i,j} \leq 1, j = 1, 2, ..., M \end{aligned} \tag{14}$$

This is a classic combinatorial optimization problem under finite resources, which describes channels and users matching problem. The problem is solved by Algorithm 1. Once the fusion center assigns a channel, the SU is required to pay an access fee $\eta_2 R_{i,j}$ before utilizing the channel for communications. Considering that not all SUs are allocated channels, a disparity arises between the user's estimated revenue $R_{i,j}$ and the actual revenue $Reward_{i,j}$. Only the user reporting the highest estimated gain is granted access, enabling them to obtain actual revenue similar to the estimated revenue. η_1 and η_2 represent the ratios of user access benefits and access costs, respectively. For SUs, the actual revenue is denoted as:

$$Reward_{i,j} = P_0 x_{i,j} \left(\eta_1 - \eta_2\right) R_{i,j} - P_1 x_{i,j} \eta_2 R_{i,j} - F_i, \tag{15}$$

where F_i denotes the user's sensing cost, which correlates with the number of cycle samples K. Since the lazy users do not sense, $F_i = 0$.

3.3 Review of Defenses

During malicious attacks, an idle report indicates the presence of the PU, while a busy report indicates its absence. Because of the way it attacks, malicious users report higher estimated revenue for busy channels. Consequently, the busy channels are more likely to be assigned to malicious users, rendering them unable to utilize the spectrum effectively and generate revenue. Moreover, the mechanism imposes an access fee on users based on their reported estimated revenue, even if they do not really utilize the channel, thereby imposing a high cost on attacking the system. This attack becomes ineffective if malicious users choose to report lower estimated revenue to evade costly access fee, because lower estimated revenue prevents malicious users from accessing, naturally thwarting attacks on the system.

Algorithm 1: Select Matrix Algorithm

Input: ID, $\mathbf{R_i}$, $\mathbf{S_i}$
Output: x, $Reward_{i,j}$
Verify ID;
Calculate the greatest total revenue: $\max_{\mathbf{x}} \sum_{i=1}^{N} \mathbf{R}_i {\mathbf{x}_i}^H$;
(A, TR) = Hungarian ($\mathbf{R_i}$);
$x = A * \mathbf{S_i}$;
Charge access fee: $\eta_2 * x_{i,j} * R_{i,j}$;
Calculate actual revenue: $Reward_{i,j}$;

As for lazy users, they persistently report the absence of the primary user and high estimated revenue. While this strategy is risky, it does not significantly disrupt the system. Lazy users can easily access channels when the primary user is absent. Once spectrum resources become scarce, constantly reporting channel idleness will only cause them to pay high access fee.

In conclusion, the proposed mechanism is well defended against SSDF attacks. As this mechanism does not rely on the fusion of sensing results, attacks by malicious and lazy users do not impact the benefits of other normal users.

4 Simulation Results

This section focuses on analyzing and confirming the feasibility and effectiveness of the proposed scheme. We set the simulation parameters according to Table 1.

4.1 Analysis of Scheme Feasibility

Comparison of Users' Revenue: To demonstrate the feasibility of the scheme, we simulate the revenue of the same user as a trusted user, a malicious user, and a lazy user, respectively. As shown in Fig. 2, when the number of available

Table 1. Simulation parameters

Simulation parameters	Simulation presets
The number of channels M	10
The number of trusted users N_1	8
The number of malicious users N_2	1
The number of lazy users N_3	1
The number of cycle samples K	50
Receiving S/N ratio γ	2 dB
The probability of false alarm P_F	0.01
The rate of access revenue η_1	3
The rate of access fee η_2	0.8

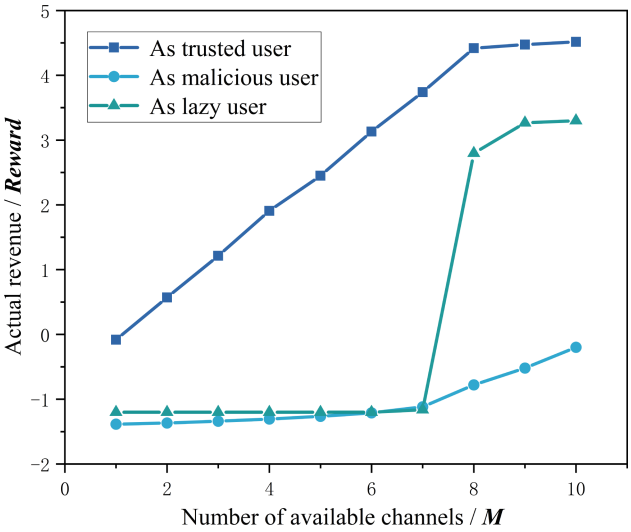

Fig. 2. Actual revenue of a user when it behaves as a trusted user, malicious user, and lazy user, respectively.

channels is small, there are insufficient channels for allocation, and all types of users gain low revenue due to sensing costs. With an increase in the number of available channels, the revenue of trusted users gradually increases, while the revenues of malicious and lazy users remain low. Simulation results show that the proposed scheme prioritizes the spectrum demand of trusted users. Only when the available channels already fully satisfy the demand of trusted users, malicious and lazy users have the opportunity to access the channel and gain revenue. In addition, when the environmental conditions become more severe (the number of trusted users is 3, which means that malicious users are the majority of SUs), the simulation results are shown in Fig. 3. Trusted users also gain higher revenue

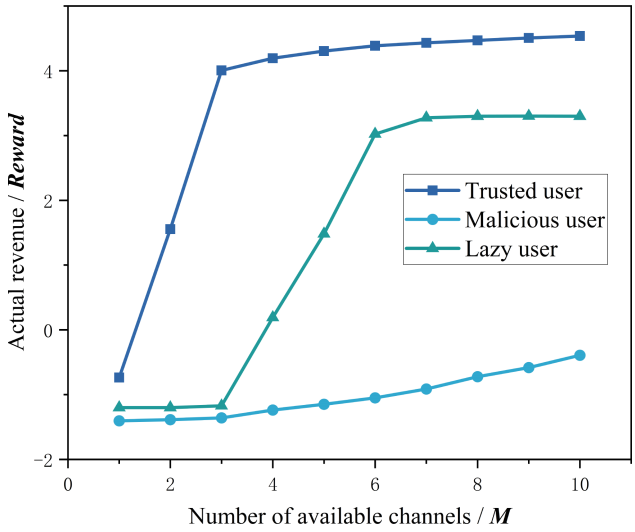

Fig. 3. Actual revenue of different users in severe environment (the number of trusted users is only 3).

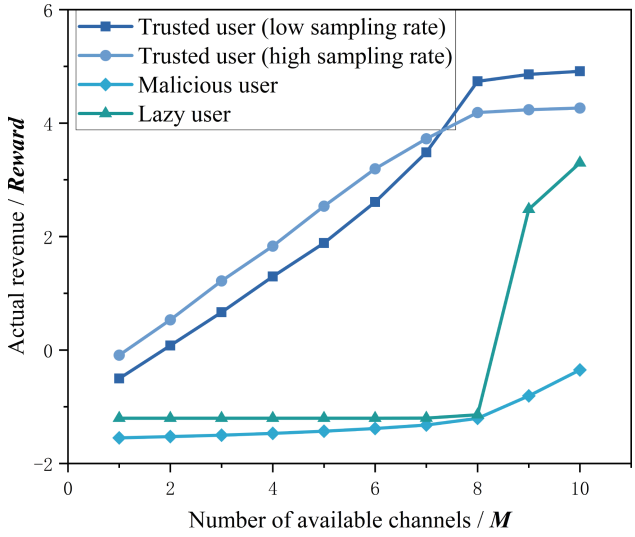

Fig. 4. Actual revenue of different users at high and low sampling rates.

than malicious users. In conclusion, rational users will choose to be trusted users to ensure their high revenue, which proves that the mechanism can effectively motivate users to perform trusted behaviors and avoid being malicious.

The Effect of Sensing Cost: To demonstrate the impact of sensing cost on actual revenue, we vary the number of cycle samples, which ranges from 30 to 65

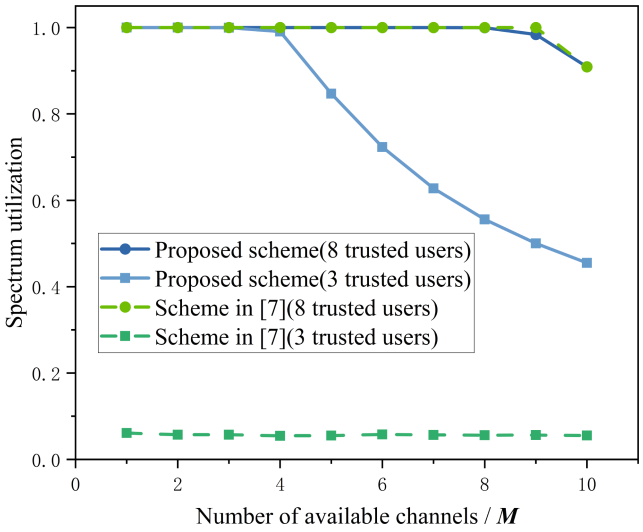

Fig. 5. Comparison of spectrum utilization between the proposed scheme and the scheme in [7].

for the 8 trusted users, while the cycle samples are kept at 50 for malicious and lazy users. The simulation results are shown in Fig. 4. Users with high sampling rates have higher revenue than low sampling rate users only when the number of available channels is small. For the trusted users, a high sampling rate means that the accuracy of the sensing results improves and they can make a correct judgment of the current channel state. At the same time, the sensing cost will increase. When the number of available channels is small, the high sampling rate can help users avoid the loss caused by inaccurate sensing. Consequently, the revenue is higher than the low sampling rate. When the number of available channels is large, users with high sampling rates cannot have higher access rates, and the problem of the high cost associated with a high sampling rate comes to light. As a result, the actual revenue is lower than that of a low sampling rate.

4.2 Comparison of Spectrum Utilization

To demonstrate the effectiveness of the proposed scheme in increasing spectrum utilization, we compare the performance of the proposed scheme with the scheme in [7]. Spectrum utilization represents the percentage of spectrum that is successfully accessed and normally used by trusted users. It reflects the effectiveness of the mechanism in fully utilizing the spectrum. As shown in Fig. 5, the simulation results show that both the proposed scheme and the scheme in [7] are able to maintain a high spectrum utilization when the number of trusted users is large. When the number of trusted users is small, the performance of the scheme in [7] deteriorates drastically, and the proposed scheme has been successful in maintaining a high spectrum utilization to some extent. It can be

observed that when the number of available channels is larger than the number of trusted users, the spectrum utilization of both schemes shows a decreasing trend. When the number of available channels is larger, all the trusted users successfully accessed the channel, but the malicious users are unable to allocate the available channels due to the wrong reporting, and the total spectrum utilization decreases. The proposed mechanism successfully ensures the priority of trusted users in using the spectrum and performs well in the face of severe environments.

5 Conclusion

In this paper, we have proposed a reward-based spectrum sensing and allocation mechanism to defend against SSDF attacks. The mechanism models the access process as an optimization problem on the basis of the estimated revenue, which is solved by the Hungarian algorithm. Simulation results demonstrate that the proposed scheme is able to successfully motivate rational users to perform trustworthy behaviors. In addition, the scheme is also able to maintain higher spectrum utilization and higher stability in severe environments.

Acknowledgment. This work was supported in part by the National Natural Science Foundation of China under Grant 62371231, 62201255, the Natural Science Foundation on Frontier Leading Technology Basic Research Project of Jiangsu under Grant BK20222001, and the Jiangsu Provincial Key Research and Development Program under Grants BE2023027.

References

1. Mahmood, N.H., Berardinelli, G., Khatib, E.J., Hashemi, R., De Lima, C., Latva-aho, M.: A functional architecture for 6G special-purpose industrial IoT networks. IEEE Trans. Industr. Inform. **19**(3), 2530–2540 (2023)
2. Hu, S., Liang, Y.-C., Xiong, Z., Niyato, D.: Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond. IEEE Wirel. Commun. **28**(4), 145–151 (2021)
3. Wu, Q., Wang, W., Li, Z., Zhou, B., Huang, Y., Wang, X.: SpectrumChain: a disruptive dynamic spectrum-sharing framework for 6G. Sci. China Inf. Sci. **66**(3) (2023). Art. no. 130302
4. Sun, Z., Liang, W., Qi, F., Dong, Z., Cai, Y.: Blockchain-based dynamic spectrum sharing for 6G UIoT networks. IEEE Netw. **35**(5), 143–149 (2021)
5. Hajian, G., Shahgholi Ghahfarokhi, B., Asadi Vasfi, M., Tork Ladani, B.: Privacy, trust, and secure rewarding in mobile crowd-sensing based spectrum monitoring. J. Ambient Intell. Humaniz. Comput.**14**(1), 655–675 (2023)
6. Miah, M.S., Hossain, M.S., Armada, A.G.: Machine learning-based malicious users detection in blockchain-enabled CR-IoT network for secured spectrum access. In: IEEE Symposium Broadband Multimedia System Broadcast. (BMSB), Spain (2022)
7. Wang, S.-L., Tsai, T.-H., Chung, W.-H.: The novel crowdsourcing algorithm for cooperative spectrum sensing. In: IEEE International Symposium on Dynamic Spectrum Access Network (DySPAN), pp. 1–5, Seoul, Korea (South) (2018)

8. Xiangbei, C., Lina, Q., Chengbing, C.: An improved information transmission technology based on trust value against SSDF attack. In: IEEE 22 International Conference on Communication Technology (ICCT), Nanjing, China, pp. 1346–1352 (2022)
9. Fernando, P., et al.: Distributed-proof-of-sense: blockchain consensus mechanisms for detecting spectrum access violations of the radio spectrum. IEEE Trans. Cogn. Commun. Netw. **9**(5), 1110–1125 (2023)
10. Li, F., Lin, R., Wang, J., Hu, J., Shu, F., Wu, L.: A fast method to defend against SSDF attacks in the CIoV network: based on DAG blockchain and evolutionary game. IEEE Commun. Lett. **27**(12), 3171–3175 (2023)
11. Liu, X., Zheng, K., Chi, K., Zhu, Y.-H.: Cooperative spectrum sensing optimization in energy-harvesting cognitive radio networks. IEEE Trans. Wirel. Commun. **10**(11), 7663–7676 (2020)
12. Vosoughi, A., Cavallaro, J.R., Marshall, A.: Trust-aware consensus-inspired distributed cooperative spectrum sensing for cognitive radio Ad Hoc networks. IEEE Trans. Cogn. Commun. Netw. **2**(1), 24–37 (2016)
13. Wang, Z., Feng, Z., Zhang, P.: An iterative Hungarian Algorithm based coordinated spectrum sensing strategy. IEEE Commun. Lett. **15**(1), 49–51 (2011)