Research on Cognitive Radio Spectrum Sensing Security Mechanism Based on Blockchain

Guowei Zhang*
Shandong University of Political Science & Law, Shandong, China, 250014

*E-mail: jones134@163.com

Abstract. In cognitive wireless networks, the collusion attack of malicious users has brought great challenges to the safety perception of the spectrum. Based on the analysis of the characteristics of existing attacks, a hypothetical analysis of possible attack behaviors, and the effective combination of blockchain technology and existing mechanisms are introduced, and a new secure spectrum sensing method based on blockchain technology is proposed. This method can treat the user's historical interaction as a public ledger, and effectively monitor the user's collusion attacks.

Keywords: Cognitive Wireless Networks, Secure Spectrum Sensing, Blockchain

1. Introduction
With the increasing demand for wireless communications, spectrum resources have become more and more scarce, but the spectrum utilization rate is relatively low\(^\text{[1]}\). Cognitive radio is divided into primary users and secondary users according to spectrum usage priority. Primary users are legal users who are authorized by spectrum, and secondary users are users who are not authorized by spectrum and need to be used without causing interference to the primary user. Authorized frequency band \(^\text{[2-3]}\). The way to realize this function needs to introduce a loop control, namely the cognitive loop. The complete cognitive loop includes observation, guidance, planning, decision-making, action, and learning. Due to the different characteristics of different working stages, cognitive radio has many security risks \(^\text{[4-5]}\). According to the current status of cognitive radio network security research, the security threats of cognitive radio are mainly concentrated in the stages of spectrum sensing, decision-making and reconstruction. Cognitive Radio (CR) technology has proposed a method that allows dynamic spectrum access to solve the shortage of spectrum resources. This technology allows secondary users to access idle clips at the right opportunity while minimizing interference with the primary user. Integrating cognitive radio technology into wireless network communication, the formed cognitive radio network (Cognitive Radio Network, CRN) will greatly improve the utilization of spectrum resources. However, due to the nature of wireless propagation, spectrum sensing is extremely vulnerable to malicious attacks. Conscious link interruption and collusion attacks are the two main types of spectrum-aware malicious attacks in existence. In addition, some studies have detected possible malicious attacks through the principles of cognitive psychology; some scholars have proposed an economic principle based on evolutionary game theory, which gives real information to decision makers through incentive methods. Although the existing spectrum sensing
technology can greatly improve the utilization rate of spectrum resources, its security faces many problems\[6]\.

In view of the insufficiency in lack of the interaction history and the interaction history distance in existing frequency spectrum sensing technology in this paper, the blockchain technology is introduced into the process of spectrum cooperative sensing, and a new secure spectrum sensing method based on blockchain technology is proposed.

2. **System and attack model**

Mechanism design belongs to the field of microeconomics and is a comprehensive application of game theory and social choice theory. Through design rules, users are encouraged to act according to the rules designed in advance. The distributed cognitive wireless network is used as a scenario to introduce the reputation mechanism and aggressive behavior of various reputation models on it.

2.1. **Traditional threat**

When the number of interactions is small, a recommendation request needs to be sent to the neighboring secondary user with a high direct reputation value, and the recommendation value given by the recommender is used as the recommended reputation value, and the decision is made based on the final integrated reputation value.

General interference can be divided into natural interference and man-made interference. Among them, natural interference includes interference caused by nature such as cosmic interference and sky power interference. The former refers to interference caused by electromagnetic radiation from the Milky Way and the sun, and is an important source of ultra-short wave band interference. With large and fast fluctuation characteristics, mainly interfere with the low frequency band. The man-made interference mainly includes aiming interference, blocking interference, partial frequency band interference and scanning interference. These interferences cause the illusion of spectrum congestion in the spectrum sensing stage by the cognitive radio, but the premise of interference is that the interference signal A certain intensity and a certain effective interference duration.

2.2. **New threats**

Spectrum sensing is one of the key technologies of cognitive radio and the basis for other links. Spectrum sensing technology can be divided into single-user spectrum sensing, also known as local sensing and multi-user collaborative sensing. There are a variety of existing spectrum sensing methods, and there are different attack schemes according to the spectrum detection methods adopted by cognitive users. First, single-user perception technology can be divided into transmitter-based signal detection and receiver-based signal detection according to the detection target. Transmitter-based signal detection mainly includes energy detection, matched filter detection, and cyclostationary feature detection, and receiver-based signal detection mainly includes local Oscillator leakage power detection and detection based on interference temperature estimation.

2.3. **Attack model**

This article mainly considers the conspiracy attacks of malicious secondary users. In a scenario, secondary users at the same level do not know each other, and a secondary user can obtain a recommendation from another neighboring secondary user through transactions.

But malicious secondary users can also take advantage of this. If several malicious secondary users join together and collude with each other through a large number of fake transactions, when one of the malicious secondary users is recommended, their associates make the recommended person’s access request accepted by giving a high reputation value. In this way, the colluders continue to increase the reputation value and become secondary users with higher comprehensive reputation in the network.

3. **Security spectrum sensing method based on blockchain technology**

For traditional threats, you can first select favorable time, space, and frequency bands based on
existing experimental data to minimize the impact of natural interference; human interference is intended to seize or pollute channel resources, generally using energy detection or cycle feature detection. Get better perception performance.

This paper introduces the blockchain technology and reputation mechanism into the spectrum sensing process, and proposes a new secure spectrum sensing method.

The new reputation mechanism includes direct reputation and recommended reputation.

(1) Direct credibility evaluation.

In a local evaluation and transaction of a user, the historical interaction record obtained from the public account of the blockchain calculates the direct reputation \( T^D \) by the following formula:

\[
T^D = \left( N^S / NA \right) \times \rho \times W
\]  

Among them, NA represents the number of all perception cycles up to a certain period, \( N^S \) represents the correct number of interaction perceptions in history, and \( \rho \) represents the interaction density, which can be obtained by formula (2).

\[
\rho = 1 - e^{\left(1 - \frac{NA}{m \times n}\right)}
\]  

\( W \) is the influence coefficient of the number of interactions in the public ledger:

\[
W = \sum \left( \frac{h_i}{m \times \frac{1}{n}} \right)
\]  

Among them, \( h_i \) represents the number of interactions in period \( l \). From formula (3), it can be seen that the closer the interaction history in the public ledger is, the larger the proportion is, and the influence on the trust value will increase accordingly.

(2) Evaluation of recommendation credibility

When the requester's interaction history has fewer records in the public ledger, the requester needs to obtain other secondary user recommendations. Send a request to the neighbor sub-users with more interaction history and higher direct reputation value in the public ledger to obtain the recommended reputation value \( T^R \) of the neighbor sub-users.

\[
T^C = \alpha \times T^D + \beta \left( \sum_{i=0}^{\omega_i} + T^D \right)
\]  

\( \omega_i \), \( \alpha \), and \( \beta \) represent the recommendation value, direct reputation value, and recommender's comprehensive reputation value weight, respectively. Among them, \( \omega_i > 0 \), \( \alpha + \beta = 1 \), \( \alpha \geq 0 \), \( \beta \geq 0 \).

(3) Secure spectrum sensing based on blockchain technology.

When a certain cooperative user requests to access a certain frequency band, it needs to perceive and confirm whether the frequency band is idle. If it is idle, a recommendation request is sent to the neighbor secondary user. In order to avoid collusion attacks and malicious transaction behaviors, blockchain technology is adopted, and the history perception records and interaction history in the database are regarded as a public ledger, each neighboring secondary user can share, and any secondary user in this scenario cannot change ledger information. If the recommendation value given by a user or users is much higher than the reputation value of the requester in the public ledger, the recommended reputation value is given a smaller weight, and the correct reputation value given by other users is taken as recommend reputation value and give greater weight. Among them, the greater the recommendation value given by the collaborative secondary user deviates from the actual reputation value in the public ledger, the smaller the weight given.

In the decision-making process, the comprehensive reputation value is calculated by formula (5).
\[ PS = \left( \frac{\sum_{i=1,j \neq q}^{n} T^C \times state_i}{\sum_{i=1,j \neq q}^{n} T^C} \right) \]  \hspace{1cm} (5)

In formula (5), PS is the perception report of other neighboring secondary users obtained when the secondary user requests to access a certain frequency band. \( state \) means that the user perceives whether the frequency band is idle, \( state_i \in \{0,1\} \), 0 means the frequency band is idle, and 1 means busy. After calculating PS, the decision is made by formula (6).

\[ D^t_q = \begin{cases} 1, & PS \geq \text{threshold} \\ 0, & \text{others} \end{cases} \]  \hspace{1cm} (6)

Among them, \( D^t_q = 0 \) indicates that the frequency band status decision result is busy, and \( D^t_q = 1 \) indicates that the spectrum is confirmed to be idle.

4. Conclusion
In view of the security problems of collusion attacks existent in cognitive wireless networks (CRN), a blockchain-based spectrum sensing technology is proposed in this paper, which treats the user's interaction history and interaction distance as a public ledger, realizing the sharing of each node for providing convenience for the secondary user to make correct judgment. Compared with the traditional spectrum sensing technology and the simulation results, it is shown that the blockchain technology can improve the collusion attack and the sensing efficiency.

Acknowledgments
This work was financially supported by Scientific Research Funding for the Introduction of Talents, Shandong University of Political Science & Law fund.

References
[1] Fang Y, Xun Z, Yibing L. Comprehensive Reputation-Based Security Mechanism against Dynamic SSDF Attack in Cognitive Radio Networks[J]. Symmetry, 2016, 8(12):147-153.
[2] Wen H, Li S, Zhu X, et al. A framework of the PHY-layer approach to defense against security threats in cognitive radio networks[J]. IEEE Network, 2017, 27(3):34-39.
[3] Sucasas V, Althunibat S, Radwan A, et al. Lightweight security against combined IE and SSDF attacks in cooperative spectrum sensing for cognitive radio networks[J]. Security & Communications Networks, 2015, 8(18):3978-3994.
[4] Jingyu F, Man Z, Yun X, et al. Securing Cooperative Spectrum Sensing Against Collusive SSDF Attack using XOR Distance Analysis in Cognitive Radio Networks[J]. Sensors, 2018, 18(2):370-381.
[5] Guo J, Zhou X, Miao X, et al. Secure Minimum-Energy Multicast Tree Based on Trust Mechanism for Cognitive Radio Networks[J]. Wireless Personal Communications, 2017, 67(2):415-433.
[6] Li Z, Zheng G. Reliable Information Transmission: A Chaotic Sequence-Based Authentication Scheme for Radio Environment Maps Enabled Cognitive Radio Networks[J]. International Journal of Digital Content Technology & Its Applications, 2016, 4(4):48-57.