IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 29, 2020, accepted November 11, 2020, date of publication November 16, 2020,
date of current version November 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3038321

A Blockchain-Based Node Selection Algorithm in Cognitive Wireless Networks

HUANG TANGSEN, XIAOWU LI, AND XIANGDONG YING
School of Electronics and Information Engineering, Hunan University of Science and Engineering, Yongzhou 425199, China

Corresponding author: Xiaowu Li (lixiaowu555@163.com)

This work was supported in part by the Hunan Natural Science Foundation under Grant 2019JJ40096 and Grant 2019JJ40097, in part by the Youth Research Foundation of Hunan Education Department under Grant 20B247 and Grant 17B107, in part by the Outstanding Youth Research Foundation of Hunan Province under Grant 2020JJ2015, in part by the Key Research Foundation of Hunan Science and Technology Department under Grant 2017NK2390, in part by the Research Foundation of Science and Technology Bureau of Yongzhou, China, under Grant 2019YZKJ08 and Grant 2019YZKJ10, and in part by the construct program of applied characteristic discipline in Hunan University of Science and Engineering.

ABSTRACT In cognitive wireless networks, multi-node cooperative spectrum sensing can effectively improve the accuracy of spectrum sensing, but there is a non-linear relationship between the number of nodes and sensing accuracy. Nodes with low reliability participate in cooperative sensing, which is not conducive to the improvement of sensing accuracy, and reduces the energy efficiency of spectrum sensing, which poses challenges to the normal operation of cognitive wireless networks. In order to improve energy efficiency and sensing performance, this paper proposes the node evaluation and scheduling (NES) algorithm and the Secure Spectrum Sensing based on Blockchain (SSSB) algorithm, which can evaluate the reliability of sensing nodes in real time, and obtain the trust value of the node. The nodes information is stored in the management center of blockchain. Blockchain encrypts nodes information to ensure that a node corresponds to its own trust value without confusion. Fusion Center of cognitive wireless networks select good performance nodes to participate in cooperative spectrum sensing. Which can reduce energy consumption while improving the sensing performance. The simulation experiment results show that the new algorithm in this paper is far superior to the traditional algorithm. Under the same other conditions, the detection probability is increased by 5%, and the energy consumption is reduced by 10%, and the safety index has also been greatly improved.

INDEX TERMS Cognitive wireless networks, blockchain, energy efficiency, sensing accuracy.

I. INTRODUCTION

With the ever-increasing demand for wireless communication, spectrum resources are becoming more and more tense [1], [2], but the spectrum utilization rate is relatively low [3], [4]. Cognitive wireless networks proposes to allow dynamic spectrum access to authorized frequency bands to make full use of spectrum holes, improve spectrum utilization, and ease spectrum resources shortage [5].

In the process of spectrum sensing, the sensing performance of a single node cannot be well achieved due to the influence of geographic location [6], while multi-node cooperative sensing can overcome the sensing shortcomings of a single node and make preparations by combining information from different geographic locations [7]. Therefore, multi-node cooperative sensing is a commonly used sensing method in cognitive wireless networks [8]. Multi-node cooperative perception can effectively improve the accuracy of perception, but the increase in the number of nodes will bring additional energy costs, increasing the energy consumption of the cognitive wireless network, and the front end of the cognitive network is battery-powered [9], so the energy consumption increases. It will reduce the battery life, which will also reduce the working life of the cognitive wireless network [10].

In order to extend the working life of cognitive wireless networks, many improved methods are used,the method of switching on and off time is adopted to extend the working life of the cognitive network [11], but this method has low perception efficiency and misses many opportunities for spectrum access. The method of cooperating between nodes and the primary user according to the agreement is used to reduce the workload of the cognitive network [12]. This method can effectively reduce energy consumption, but this

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

method gives priority to meeting the requirements of the main user and will reduce the throughput of the cognitive user. The method of grouping relay is used to reduce the energy loss caused by information transmission [13]. In this method, each node does not need to send the local sensing result to the fusion center, but each node first sends it to the patriarch, and then the patriarch decides later sent to the fusion center, this method reduces communication overhead, but the sensing accuracy is compromised.

The method of purchasing the primary user information is used to reduce workload of the cognitive network [14]. The modified method can greatly reduce the workload of the cognitive user to perform spectrum sensing because the primary user's working time is known in advance. But user information costs are high, only used in special occasions, and does not have universal significance. A review method is proposed to reduce the number of cooperative sensing nodes [15], so as to achieve the purpose of reducing energy consumption and communication overhead. In this algorithm, nodes with low reliability can be removed, but the sensing performance of all nodes is considered to be unchanged. In fact, when the radio environment changes, the performance of the nodes will change, which is not reflected in the algorithm.

In order to improve the energy efficiency of cognitive networks, a dynamic node selection algorithm is proposed [16]. The algorithm selects a fixed number of nodes to participate in cooperative perception according to the trust value of nodes, which can reduce energy consumption, but can not change the number of nodes according to the change of environment. In order to improve the energy efficiency and the operation efficiency of cognitive network [17], a time-sharing algorithm is proposed. This algorithm makes nodes work in turn, which can reduce the energy consumption of each node, but all nodes are involved in the work, and some nodes with poor sensing performance will not help cooperative sensing, which will affect the operation performance of cognitive radio network. In order to overcome the shortcomings of the algorithm [17], a node selection algorithm based on deep learning is proposed [18].

The algorithm still allows nodes to work in turn, and learns the sensing operation of each node, removing the nodes with large energy consumption to participate in the cooperative sensing, which can improve the energy-efficiency of cognitive wireless network. But in fact, external radio environment is a time-varying, the algorithm is not considering the influence of environmental changes on the node sensing performance, lack of environment interaction with the outside world radio link, failing to reflect changes in the environment [19].

The above method does not take into account the energy-efficiency and sensing performance of cognitive wireless network, and does not take into account the impact of changes in radio environment on sensing performance and energy-efficiency.

In fact, the nodes with poor sensing performance will not help the cooperative sensing, but will affect the global decision of the fusion center [20]. Therefore, in cognitive wireless networks, the nodes with poor sensing performance should be removed, and only the reliable nodes should be selected to participate in cooperative sensing [21]. However, the performance of the node is not fixed, it will change due to its own factors and the changes of the external environment. Therefore, in the actual cognitive wireless radio, need to consider the impact of environmental changes [22], and improve sensing accuracy and energy efficiency. But previous literature did not consider the impact of environmental, and did not consider using the blockchain method to select nodes with good performance [23].

In this paper, in order to simultaneously improve the energy efficiency and sensing accuracy of cognitive wireless networks, a secure spectrum sensing mechanism based on blockchain is proposed. The mechanism can reflect the change of environment and timely modify the number of nodes participating in cooperative sensing, and can evaluate the reliability of sensing nodes in real time, and obtain the trust value of the node through the evaluation algorithm. The mechanism not only memorizes the energy consumption and sensing performance of each node, but also remembers the trust value of a single node. The trust value is stored in the reliability list of the blockchain, the management center of the blockchain encrypts the list to ensure that a node corresponds to its own trust value without confusion. Experimental results show that the proposed algorithm in this paper can give a good consideration to both energy efficiency and sensing accuracy, and extend the working life of cognitive wireless networks.

The rest of the research paper is structured as follows. The second section introduces the network model proposed in this paper. In the third section, the node estimation and selection algorithm is given. In the fourth section, the blockchain-based cognitive wireless network security work algorithm is given. In the fifth section, the algorithm's experimental results and analysis is given. Finally, a conclusion is given.

II. SYSTEM MODEL

This paper designs a cognitive wireless network model based on blockchain. The model includes the management center of the blockchain, a primary user, a cognitive base station (fusion center), and multiple nodes (cognitive users). Some nodes are in spectrum sensing state, and the other nodes are in silent state. This model is a centralized cooperative spectrum sensing model [24]. Each node can only exchange information with the fusion center. The sensing information of each node is sent to the fusion center for processing, and the fusion center feeds back information to each node [25]. There is no direct communication between nodes, so a centralized architecture helps to improve information processing efficiency [26]. The fusion center is not only responsible for communication with the nodes, but also for communication with the blockchain management center, sending the node information to the management center for storage, and the blockchain management center will also call the node information to the fusion center. The blockchain management center and the fusion center are an important interaction mechanism for selecting reliable nodes. The detailed system model is shown in Figure 1.

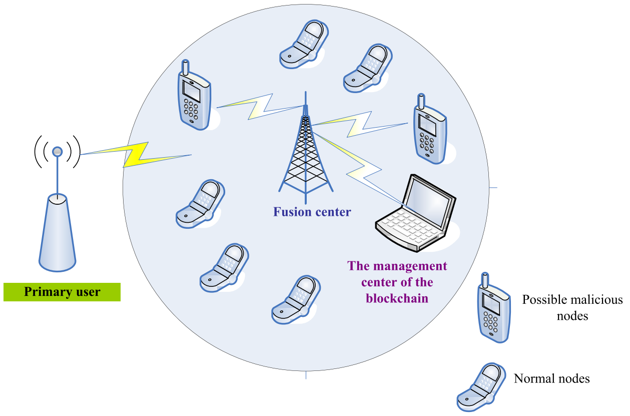

FIGURE 1. Cognitive wireless network model based on blockchain.

In Figure 1, it can be seen that not all nodes participate in cooperative sensing at the same time, but some nodes are possible malicious nodes. This is because the nodes are grouped, and the node with the highest trust value is selected to participate in cooperative sensing, malicious nodes are blocked from participating in cooperative sensing. The purpose is to improve energy efficiency and maximize the extension the working life of cognitive network. In the premise of satisfying the sensing performance, the energy consumption is reduced.

The reason for grouping the nodes and evaluating the trust value of the nodes is mainly because the geographical locations of the nodes are different, and the nodes close to the primary user receive strong signals, which can be obtained good perception accuracy on the basis of consuming less energy. When the path loss caused by the long distance from the primary user is larger, or the channel is not good, and the node with severe Rayleigh fading receives weaker signals from the primary user, and needs to perform longer sensing operations, and consumes more energy can make sensing judgments. Because the primary user's signal is weak and easily affected by interference, these nodes are prone to make wrong judgments. Such judgment results are not conducive to the protection of the primary user, which brings challenges to the security of cognitive wireless networks. Therefore, it is necessary for the security work of cognitive wireless networks to estimate nodes and select nodes with high reliability to participate in cooperative sensing.

III. NODE ESTIMATION AND SELECTION ALGORITHM

In order to improve the security of cognitive wireless networks, it is necessary to take the node trust value as an important index to participate in cooperative sensing. Therefore, the combination of node trust value and basic system architecture can meet the sensing accuracy and reduce energy consumption. The blockchain management center can be more effective in preventing data confusion.

A weighted combination mechanism based on reputation [27] can improve the sensing performance of cognitive wireless networks. The algorithm first estimates the reliability of all nodes in the system. This estimation is based on the historical interactive data. Once a suspicious node is found, it immediately makes an isolation decision for the sensing data of the node. The algorithm improves the robustness of the system, but increases the additional energy consumption, and the impact of environmental changes on the node itself is not considered.

In fact, the radio environment is time-varying, and changes in the working status of the primary user will also affect the sensing of nodes, especially when the location of the primary user moves, the nodes with good sensing may become malicious in the next moment, while the node with poor performance may become a reliable node. Therefore, in order to track changes in the status of nodes, it is necessary to establish a real-time evaluation mechanism for nodes. When the node performance deteriorates, it can stop its sensing work in time, and when the node performance becomes better, it can be transferred to work in time.

In order to evaluate and select nodes more efficiently, this paper establishes an node evaluation algorithm and nodes selection mechanism. The nodes selection algorithm flow chart is shown in Figure 2.

In Figure 2, the cognitive wireless network estimates the reliability of each node before performing spectrum sensing operations, and this estimation is based on historical data. When the external environment is stable, the original scheme will continue to work, but when the external environment changes, the reliability of the node needs to be re-estimated. The trustworthiness value of the node is recalculated according to formula (1) [28], and the fusion center will establish nodes list and nodes information are sent to the management center of the blockchain to avoid errors. The management center intelligently provides node information and is responsible for scheduling nodes to participate in cooperative sensing according to the requirements of the fusion center.

$$q_j = \frac{\sum_{i=1}^{k} \left|R_{j,i}\right| \cdot r_{j,i}}{\sum_{i=1}^{k} \left|R_{j,i}\right|} \tag{1}$$

In formula (1), q_j is the initial trust value of the j-th node, $\left|R_{j,i}\right|$ is the sensing result of the j-th node in the i-th sensing cycle, and $r_{j,i}$ is the reward value obtained by the j-th sensing node in the i-th sensing cycle. The value of $r_{j,i}$ follows the following principles: when the judgment result of the j-th node in a sensing cycle is consistent with the fusion center, then $r_{j,i} = 1$, otherwise $r_{j,i} = 0$, k is the number of statistical sensing cycles.

Calculate the initial value of the reliability of each node by formula (1), and save the value in the management center of the blockchain. When the environment changes, the reliability of the nodes will be re-estimated, and the nodes participating in sensing will be adjusted according to the node evaluation and scheduling (NES) algorithm.

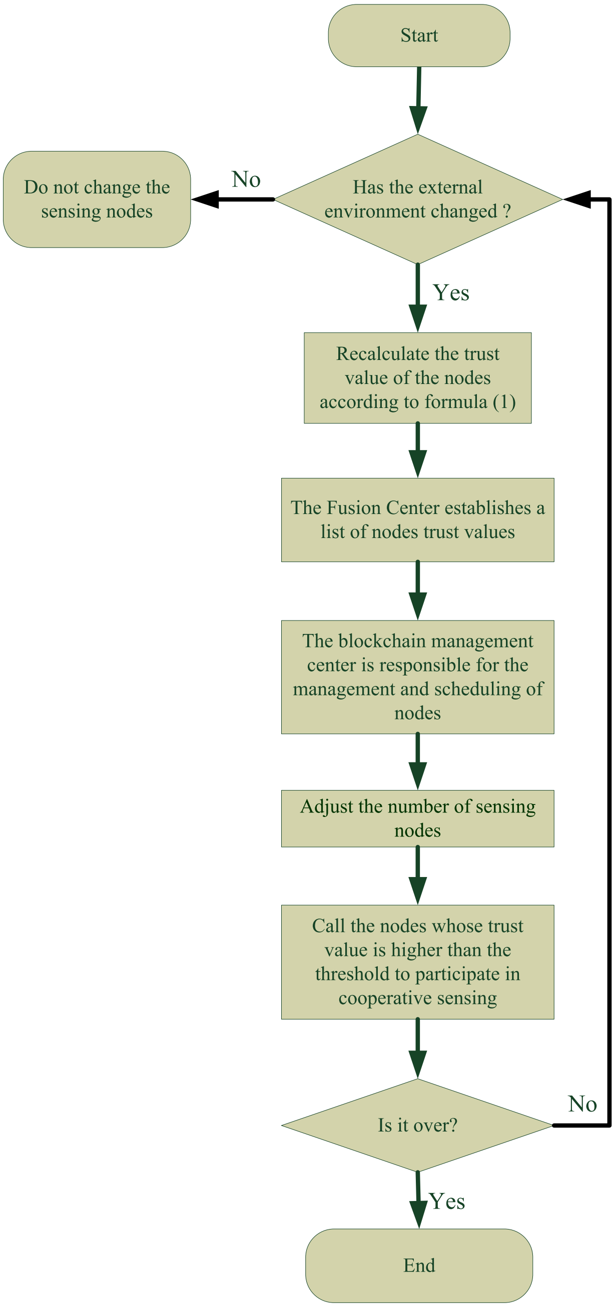
Start
Has the external environment changed ?
No
Do not change the sensing nodes
Yes
Recalculate the trust value of the nodes according to formula (1)
The Fusion Center establishes a list of nodes trust values
The blockchain management center is responsible for the management and scheduling of nodes
Adjust the number of sensing nodes
Call the nodes whose trust value is higher than the threshold to participate in cooperative sensing
Is it over?
No
Yes
End

FIGURE 2. **Flow chart of the node evaluation and scheduling algorithm.**

In NES algorithm, three return values and three correction coefficients are set, they are performance return value r, energy consumption return value g, comprehensive return value υ, performance correction coefficient ρ, energy consumption correction coefficient ξ and comprehensive correction coefficient ν.

The calculation formula of performance return value r is shown in formula (2):

$$r = \frac{1}{k}\sum_{i=1}^{k}[(1-X_i)(\alpha_i \cdot C_G + (1-\alpha_t)C_B) + X_i\,(\beta_i \cdot C_G + (1-\beta_i)\cdot C_B)] \quad (2)$$

In formula (2), the value of X_i is 1 or 0, when the primary user band is busy, it is taken as 1, while the primary user band is idle, it is taken as 0.

The value of k is the same as that in formula (1), which represents the statistical times of sensing period. C_G is the reward coefficient, and C_B is the punishment coefficient. α_i and β_i are weighted coefficients, and their values are shown in formula (3):

$$\alpha_i = \begin{cases} 1, & X_i = 0\,|H_0 \\ 0, & X_i = 0\,|H_1 \end{cases}, \quad \beta_i = \begin{cases} 1, & X_i = 1\,|H_1 \\ 0, & X_i = 1\,|H_0 \end{cases} \quad (3)$$

The value of return coefficient g of energy consumption is calculated by formula (4):

$$g = \frac{1}{k}\sum_{i=1}^{k}[D_G Y_i + D_B(1-Y_i)] \quad (4)$$

In formula (4), D_G is the energy consumption reward coefficient, indicating that the node energy consumption is less than the threshold value, D_B is the energy consumption penalty coefficient, indicating that the node energy consumption is greater than the threshold value. Y_i is the weighting coefficient of energy return value, and its value is calculated by formula (5):

$$Y_i = \begin{cases} 1, & \lambda_0 - \sum_{j=1}^{M} e_{i,j} \geq 0 \\ 0, & \lambda_0 - \sum_{j=1}^{M} e_{i,j} < 0 \end{cases} \quad (5)$$

In formula (5), λ_0 is a preset energy consumption threshold in a sensing period.

The calculation of the comprehensive return value υ is shown in formula (6):

$$\upsilon = 0.4r + 0.6g \quad (6)$$

Formula (6) shows that the weight of energy consumption return value accounts for 60% and the weight of performance return value accounts for 40%. This shows that in this paper, we emphasize on satisfying the sensing performance (sensing accuracy) while paying more attention to reducing energy consumption.

The value of the performance correction coefficient ρ is calculated by formula (7):

$$\rho_j = \sum_i \left[x_{i,j} - X_i\right] \quad (7)$$

The correction coefficient ρ_j represents the number of times that the j-th node transmits wrong information to the fusion center, and also represents the risk factor of the node. $x_{i,j}$ represents the result reported by the j-th node to the fusion center in the i-th sensing cycle, and X_i represents the decision result of the i-th sensing cycle.

The value of energy consumption correction coefficient ξ is calculated by formula (8):

$$\xi_j = \sum_i O_{i,\mathrm{j}} \cdot Y_{i,j} \tag{8}$$

ξ_j represents the number of times that the energy consumption of the j-th node exceeds the energy threshold, and also represents the severity of punishment. $O_{i,\mathrm{j}}$ represents the switch, with a value of 1 or 0, when the j-th node participates in cooperative sensing in the i-th cycle, it is taken as 1, otherwise it is taken as 0. $Y_{i,j}$ indicates whether the energy consumption of the j-th node in the i-th sensing cycle exceeds the energy consumption threshold, and its value is calculated by formula (9).

$$Y_{i,j} = \begin{cases} 1, & \mathrm{e}_{i,j} - \lambda_0 \geq 0 \\ 0, & \mathrm{e}_{i,j} - \lambda_0 < 0 \end{cases} \tag{9}$$

λ_0 in formula (9) represents the energy consumption threshold, and its value is calculated by formula (10).

$$\lambda_0 = \frac{\sum\limits_{j=1}^{M} e_{i,j}}{M} \tag{10}$$

In formula (10), M represents the number of all nodes in the cognitive wireless network. $e_{i,j}$ represents the energy consumption of the j-th node in the i-th cycle.

The value of comprehensive correction coefficient ν is calculated by formula (11).

$$\nu_j = 0.4\rho_j + 0.6\xi_j \tag{11}$$

ν_j represents the comprehensive correction coefficient of the j-th node, which is obtained by the weighted sum of the performance correction coefficient and energy consumption correction coefficient. The performance correction coefficient accounts for 40% and the energy consumption correction coefficient accounts for 60%. That is, on the premise of satisfying the perceptual performance, more energy consumption will be punished more severely.

The update process of node trust value is shown in equation (12).

$$q_j^{n+1} = q_j^n + [\vartheta \upsilon - (1 - \vartheta)\nu_j^n] q_j^n \tag{12}$$

In formula (12), q_j^n is the trust value of the j-th node in the previous perception cycle, q_j^{n+1} is the current trust value of the j-th node, υ represents the comprehensive return value of the previous cycle, and ν_j^n represents the comprehensive correction coefficient of the previous cycle. ϑ is a weighting factor, $\vartheta \in [0, 1]$. The larger the value of ϑ, the larger the proportion of the feedback coefficient, and the better the sensing performance or energy consumption index. On the contrary, it indicates that the sensing node needs to be adjusted to improve the sensing performance and energy consumption index.

The detailed description of node evaluation and selection algorithm is shown in algorithm 1.

Algorithm 1 Node Evaluation and Selection Algorithm

```
1: Input: $M$, $k$, $R_{j,\mathrm{i}}$, $r_{j,i}$;
2: Output: energy consumption value $E$, sensing accuracy
   value $P$;
3: Set the value of $C_G$,$C_B$, $X_i$;
     Calculate $q_j$ according to (1), $j = 0, 1, \cdots, M - 1$;
   Calculate the $\alpha_i$, $\beta_i$ according to (3);
   Calculate the $r$ according to (2);
   If $C_G < C_B$, $r$ becomes smaller, saying that the sensing
     performance is decreasing;
     else if $C_G = C_B$, $r$ increases, saying that the sensing
          performance is getting better;
     Else $C_G = C_B$, $r$ does not change, the sensing
        performance will not change;
4: Set the value of $D_G$,$D_B$, $Y_i$;
Calculate the $Y_i$ according to (5);
Calculate the $g$ according to (4);
If $D_G > D_B$, $g$ becomes smaller, saying that
   energy consumption is decreasing;
   else if $D_G < D_B$, $g$ will become larger, indicating that
         the energy consumed is increasing;
     else $D_G = D_B$, $g$ does not change, the energy
        consumed will not change;
Calculate the $\upsilon$ according to (6);
5: Set the value of $x_{i,j}$, $Y_{i,j}$,$\mathrm{e}_{i,j}$, $\lambda_0$, $O_{i,j}$;
  Calculate the $\rho$ according to (7);
  Calculate the $\xi$ according to (8);
  Calculate the $\nu$ according to (11);
6: Set the value $\upsilon$, $\nu$, $q_j$, $\vartheta$
  Calculate the $q_j^{n+1}$ according to (12);
  if $\vartheta < 0.5$, indicating a decrease in sensing performance
      and an increase in energy consumption;
    else if $\vartheta > 0.5$, indicating that the sensing performance
           has increased and the energy consumption has
           decreased;
else $\vartheta = 0.5$, indicating that the two indicators of
       sensing performance and energy consumption
       maintain a balance;
7: The updated $q_j^{n+1}$ is saved in the blockchain management
   center for calling when needed;
8: The fusion center chooses nodes with high trust value to
   participate in cooperative sensing;
   If the external environment does not change, the
   cognitive wireless network is stable, otherwise return to
   step 1 and re-evaluate the nodes;
9: End
```

The node estimation and selection algorithm can run stably in a constant environment, which can reduce the time for re-evaluation and node selection. Only when the environment changes greatly, such as the primary user moves, there is a new obstacle, a node fails or there is no battery and other sudden conditions, the Fusion Center will re-evaluate the nodes, and call the nodes with high trust values from the blockchain management center to perform spectrum sensing.

It is can greatly improve the efficiency of spectrum sensing, and reduce the useless energy consumption and enhancing the robustness of cognitive wireless networks.

IV. COGNITIVE WIRELESS NETWORK SECURITY WORK ALGORITHM BASED ON BLOCKCHAIN

Blockchain is an underlying technology abstracted from Bitcoin. It is a new application of traditional technology in the Internet era, which includes distributed data storage technology, wireless networks, consensus mechanism and cryptography [29]. As a decentralized public database, blockchain uses public key cryptographic algorithms, hash functions, consensus mechanisms and other technologies to build a decentralized non-authentication system that can be used in e-commerce to ensure user information security. Simply put, blockchain can be widely used in Internet finance or a wider market. It will further promote the process of economic globalization and will have a great impact on the existing financial market structure and even the social structure [30].

Blockchain technology has the advantages of low transaction costs, strong transparency, and high security. It can effectively improve the efficiency of information use, make the transaction process transparent, share supervision, and protect the legitimate rights and interests of all parties to the transaction. Common problems such as high cost, low efficiency, and low data storage security in the standardized database provide new ideas [31]. Blockchain is a kind of tamper proof, full history database storage technology, usually uses point-to-point technology to organize each node. Each node realizes the functions of routing, new node identification and data dissemination through multicast. It can appear at any node in the system. By using cryptography, it can generate related data blocks. The generated data can check the validity of the information, and can also realize the reliable link with the next data [32].

In wireless network communication, blockchain technology is a kind of technology that can not be tampered with among the same level secondary users who do not trust each other or have weak trust without intermediary participation. Regarding the historical interaction in the database as a public account book, each node stores the historical interaction records of the whole network, and the records of data collection, transaction, circulation and calculation and analysis are kept on the blockchain, which makes the quality of data obtain unprecedented strong trust endorsement, and ensures the correctness of data analysis results and the effect of data mining [33]. In view of the advantages of blockchain technology, this paper proposes a cognitive wireless network security algorithm based on blockchain.

A. ALGORITHM DESIGN STRUCTURE

The research object of this article is the two-way authentication problem between the blockchain IoT device and the cognitive wireless network convergence center. Therefore, the system in this article is mainly composed of the blockchain system, the cognitive wireless network convergence center, and the blockchain IoT device. Users communicate with the blockchain system through the fusion center. The specific structure is shown in Figure 3. The IoT device sends node information to the fusion center, and the fusion center queries the blockchain system for the existence of its node information, and then the node sends the data signed by the private key to the fusion center, and verifies whether the sensing node has a corresponding private key pair Sign it. If it is, then forward the node's request to the blockchain system, and forward the response of the blockchain system back to the sensing node. The data signed by the sensing node can confirm the identity of participating in spectrum sensing, and can also ensure that its data has not been tampered with or forged.

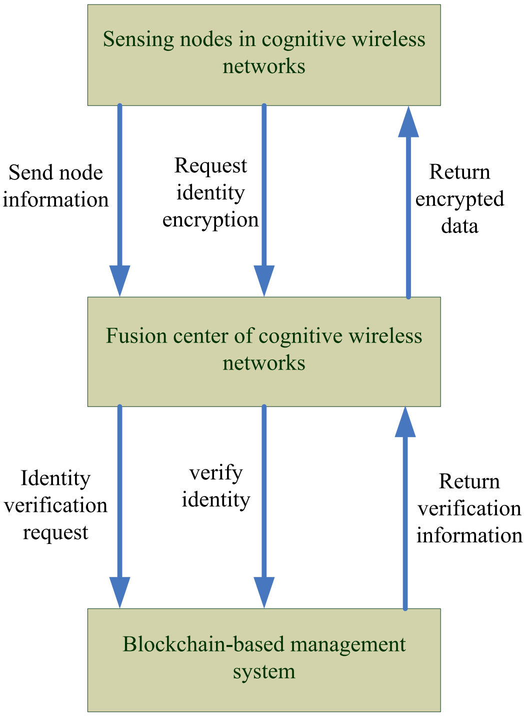
Sensing nodes in cognitive wireless networks
Send node information
Request identity encryption
Return encrypted data
Fusion center of cognitive wireless networks
Identity verification request
verify identity
Return verification information
Blockchain-based management system

FIGURE 3. Security algorithm structure of cognitive wireless network.

B. SECURE SPECTRUM SENSING BASED ON BLOCKCHAIN TECHNOLOGY

This paper introduces the blockchain technology and reputation mechanism into the spectrum sensing process. A new secure spectrum sensing method is proposed. This security sensing method includes the evaluation of the user's direct reputation and recommendation reputation.

When a cooperative node requests to access a certain frequency band, it needs to sense whether the frequency band is idle. If it is idle, it will send a recommendation request to the fusion center. In order to avoid collusion attack and malicious node behavior, the sensing results are more accurate. Using the blockchain technology, the historical sensing records in the database and the distance of interaction history is regarded as a public ledger, which can be shared by each neighbor node, and no node in this scenario can change the

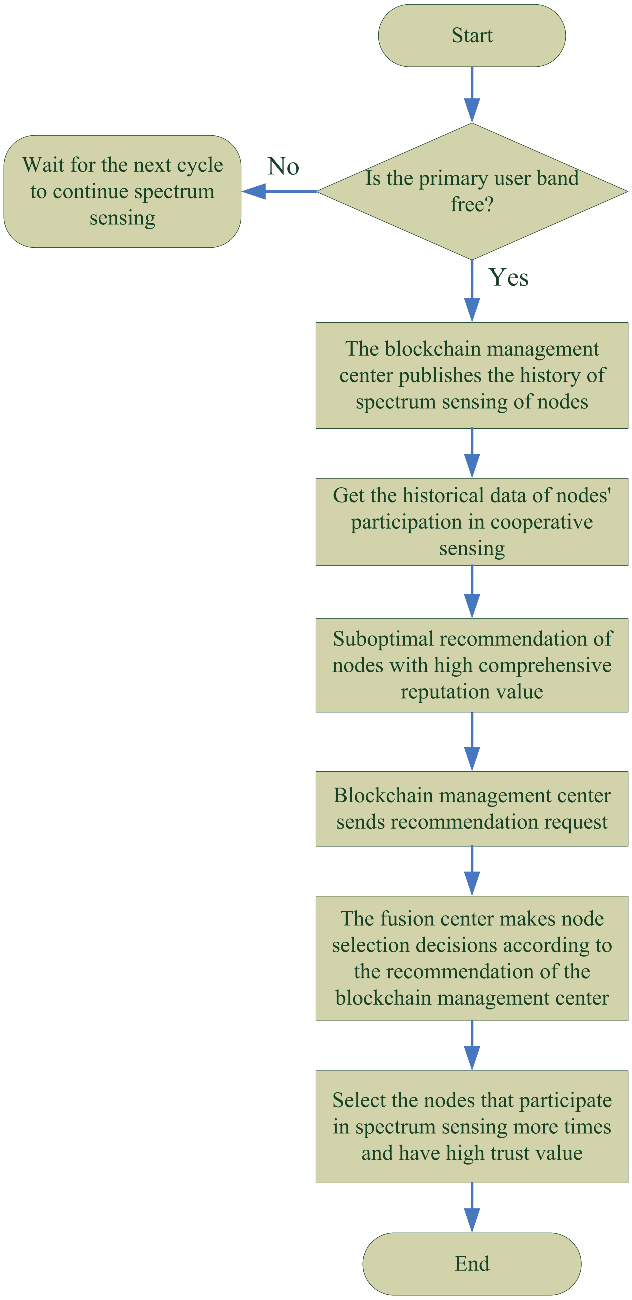
Start
Is the primary user band free?
No
Wait for the next cycle to continue spectrum sensing
Yes
The blockchain management center publishes the history of spectrum sensing of nodes
Get the historical data of nodes' participation in cooperative sensing
Suboptimal recommendation of nodes with high comprehensive reputation value
Blockchain management center sends recommendation request
The fusion center makes node selection decisions according to the recommendation of the blockchain management center
Select the nodes that participate in spectrum sensing more times and have high trust value
End

FIGURE 4. Secure spectrum sensing algorithm based on blockchain (SSSB) in cognitive wireless networks.

ledger information. The specific working process of security spectrum sensing based on blockchain technology is shown in Figure 4.

After the fusion center sends a perception request, the evaluation of a node's local reputation value is related to the peer requester. It is necessary to obtain the requester's perception calculation record from the public account book of the blockchain to calculate its direct reputation value. For the sender, the local direct reputation value is calculated by formula (13).

$$T_i = \frac{N_i}{k}\theta\omega_i \tag{13}$$

In formula (13), T_i represents the i-th sensing period, N_i is the number of all the sensing periods up to T_i time period. The meaning of k is the same as in formula (1), indicating the correct number of interactive sensing in history [34], θ means the sensing operation intensity, and its value is calculated by formula (14), ω_i is the influence coefficient of the sensing times in the public account book, and its value is calculated by formula (15).

$$\theta = 1 - e^{\left|-\frac{k}{mn}\right|} \tag{14}$$

$$\omega_i = \sum_{i=1}^{n} \left|\frac{h_1}{m} \cdot \frac{l}{n}\right| \tag{15}$$

where h_1 is the number of interactions in l period and m is the size of sensing period in each period, n is the total interaction period. It can be seen from formula (14) and (15) that the closer is the interaction history in the public account book, the proportion will be the greater, and the impact on trust value will increase accordingly [35].

When the trust value of the node is not in the forefront of all nodes, the node is selected by calculating the comprehensive trust value, and the comprehensive trust value of the node is calculated by (16).

$$T_{i,c} = \phi T_i + \varphi \left|T_i + \theta \sum_i \omega_i\right| \tag{16}$$

where ϕ, φ, ω_i respectively represent the weight of the trust value, the direct reputation value and the comprehensive reputation value of the node. Among them, the values of ϕ, φ, ω_i meet the conditions $\phi > 0$, $\phi \geq 0$, $\omega_i \geq 0$,$\phi + \varphi = 1$. Every time a recommendation is made, the user's recommendation reputation value will be updated.

The security spectrum sensing technology based on the blockchain, through the calculation of the comprehensive trust value of the nodes in the network. The final decision-making process uses the classic trust value decision-making algorithm. The nodes in the network are classified by setting the corresponding rejection threshold and trust threshold. If the comprehensive trust value is less than the rejection threshold, the node is considered a malicious user; if the comprehensive trust value is greater than the trust threshold, the node is considered a normal user; if the comprehensive trust value is between the rejection threshold and the trust threshold, the node is considered to be a node to be observed. The node obtains the right to participate in cooperative sensing through the continuous update of the trust value.

V. ANALYSIS OF THE SIMULATION EXPERIMENT

The experiment was carried out by the Monte Carlo simulation in this paper. This test runs VMware esxi 6.7.0 (build 8169922) bare metal virtual machine system on a workstation using two Intel Xeon Gold6128 3.7GHz processors, 256 Gb memory and Samsung SM961 / PM961 SSD [36].

In the simulated cognitive wireless network, there are 3 auxiliary nodes and 15 sensing nodes [37]. The corresponding parameters are set as shown in Table 1 [38].

TABLE 1. Simulation parameter setting.

Parameter	Value
Simulation area setting	A circular area with a radius of 100m
Primary user	Place a primary user anywhere on the edge of the circular area
Working parameters of primary user	BPSK signal with power of 100MW and bandwidth of 100kHz
Number of nodes	Randomly place 15 nodes (5 nodes with SNR = - 18 dB, - 16 dB and - 14 dB respectively)
Noise settings	AWGN
Average detection times	10000
Auxiliary node	3 (SNR = - 14 dB)
Spectrum detection method of node front end	Energy detection

The always occupied class means that the frequency band is considered to be in the occupied state, i.e. it is always sent 1 whether the primary user is using the detected frequency band or not; the always idle class is that the frequency band is considered to be in the idle state, that is to say, it is always sent whether the primary user is using the detected frequency band or not For the actual use of the frequency band, if it does not follow any rules, it is considered to be in the idle state or occupied state, that is, random transmission 0 and 1 [39].

In the simulation experiment of the algorithm, the number of malicious users in the system is mainly considered in two cases, as shown in Table 2.

TABLE 2. Malicious user (MU) parameter values.

Total number of Mu	SNR	Mu number under different SNR
4	SNR=-18d B	2
4	SNR=-16d B	1
4	SNR=-14d B	1
8	SNR=-18d B	3
8	SNR=-16d B	3
8	SNR=-14d B	3

In the experiment based on the auxiliary node, assuming that the primary user band is in a half busy state. The NES algorithm in this paper is compared with 4 classical algorithms, which are AND rule, OR rule, Majority rule and K-out-of rule respectively [40]. When using the traditional 4 fusion methods, the number of malicious nodes is set to 4, and the number of normal nodes is 15. When using the node evaluation and scheduling (NES) algorithm in this paper, the number of malicious nodes is set to 8, and other parameters are consistent with the settings in the traditional method.

In order to verify the sensing performance of the algorithm in this article, the ROC curves of the comparison of sensing performance are shown in Figures 5. As can be seen from Figure 5, in the case of four malicious nodes in cognitive wireless network, the detection probability of the algorithm in this paper is higher than that of the classical algorithm under the same false alarm probability. This is because the algorithm in this paper considers the environment and other variable factors, and the cognitive wireless network has stronger robustness and stronger anti attack ability. No matter in any environment, the node information can be updated in time, and the node information is encrypted by blockchain technology. The fusion center can request the nodes with good performance to participate in cooperative sensing, so the sensing performance is always better than the classic algorithm.

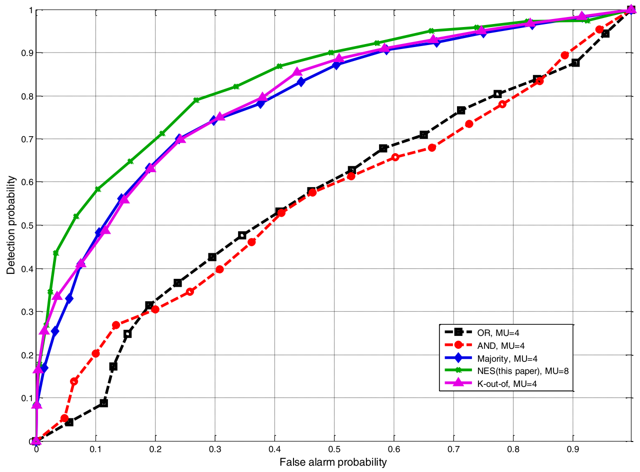

FIGURE 5. Comparison of sensing performance between four classical algorithms and NES algorithm in this paper.

Figure 6 shows the energy consumption comparison between the NES algorithm and the classical algorithm under the same conditions. Other simulation experiment parameters are the same as the experiment in Figure 5.

It can be seen from Figure 6 that after the number of sensing cycles exceeds 60, the energy consumption of the algorithm in this paper is significantly less than that of the other 4 classic algorithms. The more the number of sensing cycles, the longer the sensing time, the more energy will be saved. Greatly help cognitive wireless network to extend the working life. This is because the algorithm in this paper can always select the node with the best performance to

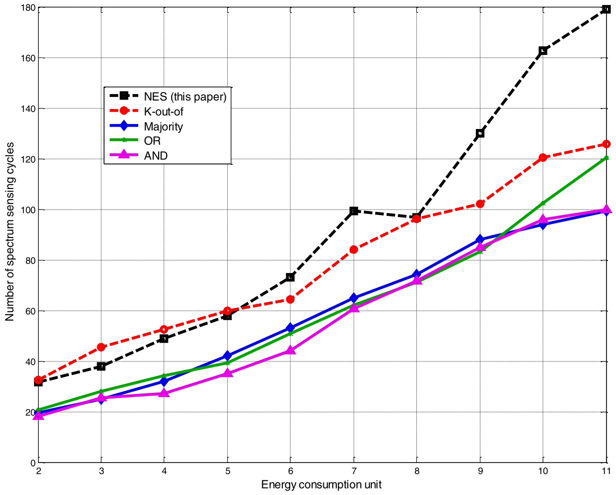

FIGURE 6. Comparison of energy consumption between four classical algorithms and NES algorithm in this paper.

participate in cooperative sensing in time, so it can save more energy when the sensing performance is better than the traditional method.

Figure 7 describes the anti-attack ability of the Secure Spectrum Sensing based on Blockchain (SSSB) algorithm in the cognitive wireless network.

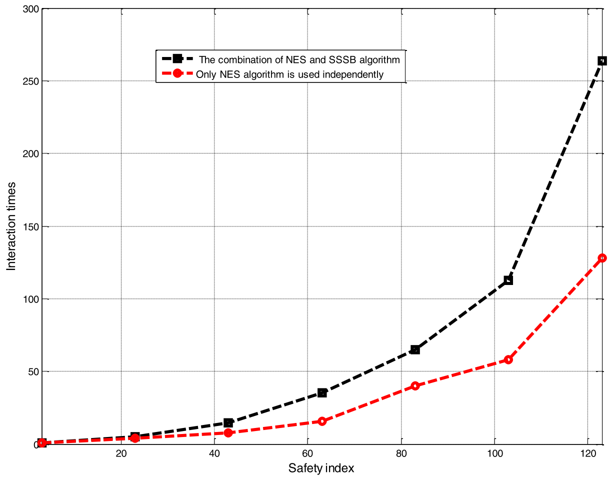

FIGURE 7. Security performance comparison of cognitive wireless networks.

It can be seen from Figure 7 that when the NES and SSSB algorithms are used in combination, as increasing the number of interactions between the sensing node, fusion center and blockchain management center, the security index of the cognitive wireless network rises significantly faster. When the number of interactions exceeds 50 times, the safety index using the SSSB algorithm rose faster than the safety index using only the NES algorithm, which fully reflects the effectiveness of the SSSB algorithm. This is because the SSSB algorithm incorporates blockchain technology. It can greatly improve the anti attack ability and security ability of cognitive wireless network.

This article incorporates blockchain technology. In order to prove that the new algorithm does not increase network overhead, a network traffic test experiment was deliberately done. Network traffic test aims to test the algorithm and no identity in this paper. To verify the difference of network traffic between wireless access points. This protocol increases the network traffic pressure. Network traffic test enables. If the network traffic is tested with iftop, the query will be sent directly to the blockchain. Compare the request traffic with the request traffic authenticated by this algorithm, Query per second (QPS) and calculate the network traffic utilization. In order to make the request timely. In order to get a response, and thus more accurately measure the impact on the network. The number of service nodes selected by the machine is 1 [40]. The network traffic test results are shown in Table 3.

TABLE 3. Network traffic test results.

QPS	Direct interactive traffic (MB/S)	Encrypted authentication traffic (MB/S)	Traffic utilization (%)
1	1	1	100
2	2	2.001	99.95
5	5	5.002	99.96
10	10.001	10.005	99.96
20	20.002	20.011	99.955
40	20.004	20.02	99.95

It can be seen from the observation results in Table 3, it is concluded that the algorithm in this paper has a 0.1% impact on network traffic, and has minimal impact on cognitive wireless network performance.This also proves that the algorithm in this paper not only has the advantages of improving sensing performance and reducing energy consumption, but also has no disadvantages of increasing network overhead.

VI. CONCLUSION

This paper makes an in-depth study on the model of cognitive wireless networks. In the practical application scenarios of cognitive wireless networks, there are usually serious errors when the nodes sensing the data, which causes the sensing values to deviate from the normal range, or some nodes deliberately send the wrong data to the fusion center. Therefore, aiming at the security problem of malicious node attack in cognitive wireless network, this paper proposes the node evaluation and scheduling (NES) algorithm and the Secure Spectrum Sensing based on Blockchain (SSSB) algorithm, which regards the user's interaction history and interaction distance as a public account book, and is managed by the blockchain management center, which is convenient for the fusion center to call nodes with excellent performance to participate in cooperative sensing. Finally, the simulation results show that the proposed algorithm is much better than the traditional algorithm, which can not only effectively improve the spectrum sensing performance, but also reduce the energy consumption, and will not increase the communication overhead of cognitive wireless network.

There are still many shortcomings in the field of cognitive wireless research. For example, in the case of low signal-to-noise ratio, the sensory performance of nodes will deteriorate rapidly. The existing methods cannot solve the problem of sensory performance under low signal-to-noise ratio. Secondly, the existing research does not pay enough attention to network throughput, and follow-up research needs to strengthen the research of throughput. Secondly, the application of blockchain in cognitive wireless networks needs to be further strengthened. Network security is a current research hotspot. Research needs to further use blockchain technology to enhance the robustness of cognitive wireless networks.

REFERENCES

[1] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2789–2800, Mar. 2017.

[2] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, Apr. 2019.

[3] S. Iqbal, A. W. Malik, A. U. Rahman, and R. M. Noor, "Blockchain-based reputation management for task offloading in micro-level vehicular fog network," *IEEE Access*, vol. 8, pp. 52968–52980, Mar. 2020.

[4] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 289–300, Mar. 2020.

[5] X. Zhou, W. Liang, K. Wang, H. Wang, L. T. Yang, and Q. Jin, "Deep learning enhanced human activity recognition for Internet of healthcare things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6429–6438, Jul. 2020.

[6] J. Shi, R. Li, and W. Hou, "A mechanism to resolve the unauthorized access vulnerability caused by permission delegation in blockchain-based access control," *IEEE Access*, vol. 8, pp. 156027–156042, Aug. 2020.

[7] T.-H. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, and R. Thomas, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184133–184144, Dec. 2019.

[8] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchain-enabled deduplicatable data auditing mechanism for network storage services," *IEEE Trans. Emerg. Topics Comput.*, early access, Jun. 29, 2020, doi: 10.1109/TETC.2020.3005610.

[9] S. Zhu, Z. Cai, H. Hu, Y. Li, and W. Li, "ZkCrowd: A hybrid blockchain-based crowdsourcing platform," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4196–4205, Jun. 2020.

[10] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in DWSNs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6193–6202, Sep. 2020.

[11] H. Tangsen, L. Xiaowu, and C. Qingjiao, "Research on an evaluation algorithm of sensing node reliability in cognitive networks," *IEEE Access*, vol. 8, pp. 11848–11855, Jan. 2020.

[12] X. Zhou, W. Liang, K. I.-K. Wang, R. Huang, and Q. Jin, "Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data," *IEEE Trans. Emerg. Topics Comput.*, early access, Jul. 26, 2019, doi: 10.1109/TETC.2018.2860051.

[13] M. Salah, O. A. Omer, and U. S. Mohammed, "Spectral efficiency enhancement based on sparsely indexed modulation for green radio communication," *IEEE Access*, vol. 7, pp. 31913–31925, Jul. 2019.

[14] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social Internet OS vehicles: Review, challenges and blochchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, Jun. 2019.

[15] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6492–6499, Dec. 2019.

[16] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Mar. 2019.

[17] Y. Wang, M. Liu, J. Yang, and G. Gui, "Data-driven deep learning for automatic modulation recognition in cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4074–4077, Apr. 2019.

[18] Y. Xu, Q. Zeng, G. Wang, C. Zhang, J. Ren, and Y. Zhang, "An efficient privacy-enhanced attribute-based access control mechanism," *Concurrency Comput. Pract. Exper.*, vol. 32, no. 5, p. e5556, Mar. 2020, doi: 10.1002/cpe.5556.

[19] X. Zhou, W. Liang, K. I.-K. Wang, and S. Shimizu, "Multi-modality behavioral influence analysis for personalized recommendations in health social media environment," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 5, pp. 888–897, Oct. 2019.

[20] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101–4112, May 2020.

[21] Y. Lin, Z. Cai, X. Wang, and F. Hao, "Incentive mechanisms for crowdblocking rumors in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9220–9232, Sep. 2019.

[22] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, Sep. 2019.

[23] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," *IEEE Trans. Ind. Informat.*, early access, Sep. 11, 2020, doi: 10.1109/TII.2020.3022432.

[24] C. Xu, K. Wang, P. Li, S. Gou, J. Luo, B. Ye, and M. Guo, "Making big data open in edges: A resource-efficient block-based approach," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 4, pp. 870–882, Apr. 2019.

[25] T. Shu, W. Liu, T. Wang, Q. Deng, M. Zhao, N. N. Xiong, X. Li, and A. Liu, "Broadcast based code dissemination scheme for duty cycle based wireless sensor networks," *IEEE Access*, vol. 7, pp. 105258–105286, Jul. 2019.

[26] Z. He, Z. Cai, and X. Wang, "Modeling propagation dynamics and developing optimized countermeasures for rumor spreading in online social networks," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2015, pp. 205–214.

[27] H. Feng, W. Wang, B. Chen, and X. Zhang, "Evaluation on frozen shellfish quality by blockchain based multi-sensors monitoring and SVM algorithm during cold storage," *IEEE Access*, vol. 8, pp. 54361–54370, Mar. 2020.

[28] Z. Liu, D. Wang, J. Wang, X. Wang, and H. Li, "A blockchain-enabled secure power trading mechanism for smart grid employing wireless networks," *IEEE Access*, vol. 8, pp. 177745–177756, Sep. 2020.

[29] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, "Blockchain-enabled accountability mechanism against information leakage in vertical industry services," *IEEE Trans. Netw. Sci. Eng.*, early access, Feb. 27, 2020, doi: 10.1109/TNSE.2020.2976697.

[30] R. T. Yazicigil, T. Haque, P. R. Kinget, and J. Wright, "Taking compressive sensing to the hardware level: Breaking fundamental radio-frequency hardware performance tradeoffs," *IEEE Signal Process. Mag.*, vol. 36, no. 2, pp. 81–100, Mar. 2019.

[31] X. Zhou, Y. Li, and W. Liang, "CNN-RNN based intelligent recommendation for online medical pre-diagnosis support," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, early access, May 14, 2020, doi: 10.1109/TCBB.2020.2994780.

[32] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3632–3641, Jun. 2019.

[33] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017.

[34] T. Huang, X. Yin, and Q. Cao, "A new algorithm for considering green communication and excellent sensing performance in cognitive radio," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 6, pp. 1–11, Jun. 2020.

[35] Z. Cai and Z. He, "Trading private range counting over big IoT data," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2019, pp. 144–153.

[36] G. Chen and T. Huang, "Community privacy estimation method based on key node method in space social Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 10, pp. 1–13, Oct. 2019.

[37] Y. Xu, G. Wang, J. Ren, and Y. Zhang, "An adaptive and configurable protection framework against Android privilege escalation threats," *Future Gener. Comput. Syst.*, vol. 92, pp. 210–224, Mar. 2019.

[38] X. Yan, B. Cui, Y. Xu, P. Shi, and Z. Wang, "A method of information protection for collaborative deep learning under GAN model attack," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, early access, Sep. 10, 2019, doi: 10.1109/TCBB.2019.2940583.

[39] X. Zhou, B. Wu, and Q. Jin, "Analysis of user network and correlation for community discovery based on topic-aware similarity and behavioral influence," *IEEE Trans. Human-Mach. Syst.*, vol. 48, no. 6, pp. 559–571, Dec. 2018.

[40] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, Feb. 2018.

HUANG TANGSEN received the B.Eng. degree in electronic information engineering from the Hunan University of Technology, Zhuzhou, China, in 2004, and the M.Eng. degree in signal and information processing from the Guilin University of Electronic Science and Technology, Guilin, China, in 2007. He is currently pursuing the Ph.D. degree with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China. He worked as a Teacher with the Hunan University of Science and Engineering, Yongzhou, China. His research interests include cognitive radio, ultra-wideband communication, and compressed sensing.

XIAOWU LI received the Ph.D. degree in digital image processing from Hunan Normal University, Changsha, China, in 2018. He worked as a Teacher with the Hunan University of Science and Engineering, Yongzhou, China. He is currently an Associate Professor. His current research interests include three-dimensional reconstruction of icosahedral virus and communication signal processing.

XIANGDONG YING is currently a Professor with the School of Electronics and Information Engineering, Hunan University of Science and Engineering. He is also the Associate Dean of the School of Electronics and Information Engineering. His research interests include network and information security, the Internet of Things, and cloud computing. He is also a member of CCF.