electronics

MDPI

Article

An Active and Passive Reputation Method for Secure Wideband Spectrum Sensing Based on Blockchain

Xinyu Xie [1], Zhuhua Hu [1,*], Min Chen [1,*], Yaochi Zhao [2] and Yong Bai [1]

[1] School of Information and Communication Engineering, Hainan University, Haikou 570228, China; xxy976862680@gmail.com (X.X.); bai@hainanu.edu.cn (Y.B.)
[2] School of Computer Science and Cyberspace Security, Hainan University, Haikou 570228, China; zhyc@hainanu.edu.cn
* Correspondence: eagler_hu@hainanu.edu.cn (Z.H.); chenmin@hainanu.edu.cn (M.C.)

Abstract: Spectrum is a kind of non-reproducible scarce strategic resource. A secure wideband spectrum sensing technology provides the possibility for the next generation of ultra-dense, ultra-large-capacity communications to realize the shared utilization of spectrum resources. However, for the open collaborative sensing in cognitive radio networks, the collusion attacks of malicious users greatly affect the accuracy of the sensing results and the security of the entire network. To address this problem, this paper proposes a weighted fusion decision algorithm by using the blockchain technology. The proposed algorithm divides the single-node reputation into active reputation and passive reputation. Through the proposed token threshold concept, the active reputation is set to increase the malicious cost of the node; the passive reputation of the node is determined according to the historical data and recent performance of the blockchain. The final node weight is obtained by considering both kinds of reputation. The proposed scheme can build a trust-free platform for the cognitive radio collaborative networks. Compared with the traditional equal-gain combination algorithm and the centralized sensing algorithm based on the beta reputation system, the simulation results show that the proposed algorithm can obtain reliable sensing results with a lower number of assistants and sampling rate, and can effectively resist malicious users' collusion attacks. Therefore, the security and the accuracy of cooperative spectrum sensing can be significantly improved in cognitive radio networks.

Keywords: cognitive radio; spectrum sensing; blockchain; malicious users; collusion attacks

Citation: Xie, X.; Hu, Z.; Chen, M.; Zhao, Y.; Bai, Y. An Active and Passive Reputation Method for Secure Wideband Spectrum Sensing Based on Blockchain. *Electronics* **2021**, *10*, 1346. https://doi.org/10.3390/electronics10111346

Academic Editor: Rameez Asif

Received: 6 May 2021
Accepted: 31 May 2021
Published: 4 June 2021

1. Introduction

In cognitive radio (CR) networks, spectrum sharing strategy based on dynamic access provides a feasible scheme for efficient spectrum utilization [1–4]. This technology allows the secondary user (SU) to access the idle spectrum when the signal of the primary user (PU) is not detected. However, when the authorized frequency band is occupied by the PU, the SU must withdraw from the frequency band and search other idle frequency bands for communication. In 5G heterogeneous networks, the implementation of large-scale spectrum sharing faces many challenges [5]. For example, one challenge is how to obtain accurate perception results with as little prior information as possible [6]. Collaborative spectrum sensing (CSS) technology is one of the key solutions to CR technical problems. Most of the existing research builds models and algorithms under fading channel conditions, and use the spatial diversity of multi-nodes sensing to achieve the purpose of reducing sensing cost or improving sensing robustness [7–12]. However, when users provide false sensing results maliciously, the performance and security of spectrum sensing will be significantly affected [13] Zhang Linyuan et al. discuss various situations of Byzantine attack and defense in reputation-based cooperative spectrum sensing [14]. Therefore, how to reduce the impact of malicious users (MU) uploading false sensing data and how to ensure the accuracy and security of spectrum sensing are hot issues worthy of research [15,16].

The existing collaborative network of swarm intelligence can provide an operating platform for CSS, and the related research on swarm intelligence sensing mainly focuses on reputation mechanism, reciprocity mechanism, fairness and incentive mechanism based on electronic currency [17,18]. As a decentralized ledger [19], blockchain can record the reputation value and sensing results of all nodes under the consensus mechanism [20]. In addition, in recent years, the proposal of quantum technology has threatened the one-way encryption in blockchain on the one hand, and on the other hand, it has improved the security of the blockchain and its performance [21–23]. Ikeda, K. innovatively proposed a decentralized online quantum cash system called qBitcoin, which eliminates the double-spending problem and ensures the security of the blockchain from the quantum perspective. This work is the first blockchain-related research using the unclonable theorem and quantum digital signature [24]. Gao, YL. et al. proposed a safe and efficient quantum blockchain scheme based on the quantum non-cloning theorem [25]. Current blockchain security relies on 'one-way' mathematical functions. Kiktenko E. O. et al. reported an experimental realization of a quantum-safe blockchain platform [26]. This platform can solve the problem of the digital signature using 'one-way' mathematical functions which makes it vulnerable to the attack of quantum computers. Therefore, secure spectrum sensing can be achieved with the help of blockchain. Meanwhile, it encourages nodes to participate in sensing tasks to obtain higher rewards through the incentive system, and it can realize a new way of spectrum sharing [27]. The innovative application of this technique can promote the development of 5G and future 6G technology [28–30].

1.1. Related Work and Motivation

At present, the application of blockchain in CSS is mainly to solve the following three issues.

(1) How can we build a decentralized collaborative sensing platform to positively motivate users to carry out sensing tasks, and how can the platform obtain benefits under the consideration of energy consumption and other factors at the same time? In part of the research, the requirements of platform users for sensing services were specified through smart contracts. Only within the scope of requirements described in the contract, can users join the sensing task to obtain benefits [31,32]. Lv, P. et al. proposed a blockchain-based spectrum sensing (BBSS) system, which uses the characteristics of the blockchain to ensure the security and correctness of the spectrum transaction process. Both requesters and participants of spectrum sensing can undertake strategies to maximize their own interests [33]. In [34], the operation of a smart contract can avoid the interference and capacity loss caused by chaotic spectrum sharing. In [35,36], a node access competition protocol for blockchain verification was proposed to build a secure decentralized database, which also introduced a virtual currency named Specoins for spectrum access cost. A virtual wireless network based on blockchain technology was constructed to realize spectrum resource allocation in [37].

(2) How can we accurately identify the malicious nodes in the distributed collaborative network? Careem M.A.A. and Dutta A. defined and analyzed a detection mechanism that used the signal-to-noise ratio (SNR) and the spatial distance between nodes to detect abnormal sensing nodes, forming a highly reliable and accurate law enforcement system [38]. In [39], the expected distance between honest and malicious users was obtained through the probability of detection and the probability of false alarm, and abnormal nodes were judged by the Hamming distance difference of the sensing results among distributed nodes.

(3) How can we ensure the security and accuracy of collaborative sensing fusion results in the presence of malicious nodes? In the sensing task, if the behavior of SUs and their requirements for spectrum attributes were not paid attention to, the performance of CR would be reduced [40]. In this regard, reputation value can be set for each sensing node and given different weights [41]. For distributed collaborative sensing, a sensing-based dynamic spectrum access framework was proposed, which was supported by blockchain to ensure the security and reliability of sensing results without a fusion center [42]. Patnaik,

M. et al. proposed the ProBLeSS protocol, which can be used to resist SSDF attacks in CR-IoBT networks without a resource-intensive key management architecture [43]. For centralized CSS, the blockchain can be regarded as an unchangeable distributed ledger with historical data to obtain the reputation information of sensing nodes [44–46]. The existing collaborative centralized fusion algorithms generally adopted equal weight fusion for the upload results, and its performance dropped sharply when a large number of MUs colluded with each other. On this basis, a fusion algorithm based on historical data correction weight was proposed, in which weights for each node were set through historical sensing records [47]. However, in the collaborative sensing task involving multiple nodes, if only the influence of a single historical record is considered, the sensing performance of nodes under some specific scenarios cannot be fully satisfied. Moreover, when the nodes need to consider too many historical records, it results in an increase in computing power and time cost, which will affect the overall performance of collaborative fusion sensing.

1.2. Our Contributions

In order to solve the above issues, this paper proposes an active and passive reputation method for secure wideband spectrum sensing based on blockchain technology (APR_SWSS). In this algorithm, users' reputation can be divided into two categories: active sensing reputation (ASR) and passive sensing reputation (PSR). ASR is judged by the number of tokens attached when the node submits the sensing results, while PSR is determined by the number of balance tokens and recent sensing task records. In the blockchain network, the number of balance tokens of a node can be regarded as the accumulation of credibility of the node in each task, which can also be regarded as the overall measurement of its reputation by the fusion center. Meanwhile, for each node, the recent sensing task records can modify its passive reputation, and quickly reduce the sensing weight of the malicious node. Simulation results show that the proposed APR_SWSS algorithm can reduce the burden of sampling combined with compressed sensing technology, and can achieve more accurate sensing results with fewer assistants. Meanwhile, it can quickly find the malicious nodes, realize the reasonable weight allocation of each node, and effectively resist the spectrum sensing data falsification (SSDF) attack of MUs.

1.3. Paper Organization

The rest of this paper is organized as follows. Section 2 gives system model with SSDF attack, which uses compressed sampling technology, including a blockchain module and a CSS module. Section 3 describes the overall system scheme and the proposed APR_SWSS algorithm in detail. The simulation results and performance analysis of the APR_SWSS algorithm are presented in Section 4. Finally, Section 5 concludes this paper.

2. System Model and Proposed Methods

2.1. System Model

The system model is shown in Figure 1. In the CR network, the method of CSS can obtain spatial diversity gain by fusing the results of spectrum sensing from multiple cognitive users, which effectively improves the accuracy of spectrum sensing and solves the hidden-terminal problem. However, MUs may carry out SSDF attacks, that is, sending wrong data maliciously in the sensing task, which leads to a large deviation between the judgment result and the actual result, and greatly deteriorates the sensing performance of the system. In the cognitive wireless network, the SUs that perform spectrum sensing are called sensing nodes, and the nodes performing a sensing task are called assistants. When performing sensing tasks, the sensing node and the assistant are equivalent.

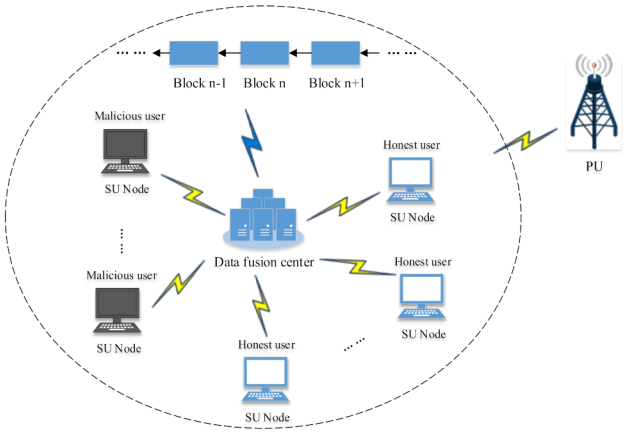

Figure 1. CSS system model with malicious users.

Firstly, in wideband spectrum sensing technology, compressed sensing technology can realize signal sampling in a very wide frequency range. The core is that if a signal is K-sparse, then the original high-dimensional signal can be projected onto a low-dimensional space with an observation matrix, and can be recovered with high probability from a small number of linear random measurements. In the actual environment of spectrum sensing, a signal with a very wide frequency range is usually a sparse multi-band signal. Therefore, the compressed sampling method can effectively reduce the requirements of the receiver for the signal sampling rate, thus reducing the performance requirements of ADC hardware.

The compressed observation is

$$y = Ax, \tag{1}$$

where $A \in R^{m \times n}$ is an observation matrix, $y \in R^m$ and $x \in R^n$ are the observation vector and the original signal, respectively. x can be represented by a few bases with the suitable reference base, i.e., in a transform domain, $x = \Psi\alpha$, where Ψ is the transform base, and α is the sparse representation on transform base of x. If the l_0 norm of α satisfies $\|\alpha\|_0 \leq K$, then x is K-sparse. When K is small enough, the compression can be achieved. Assuming $V = A\Psi$, $V \in R^{m \times n}$, we can find:

$$y = A\Psi\alpha = V\alpha. \tag{2}$$

For the K-sparse signal x, M samples are extracted from the signal x by the measuring matrix, and the receiver can use these sampled values to solve the minimum norm l_0:

$$\min\|x\|_0 s.t. \|Ax - y\|_2 \leq \varepsilon. \tag{3}$$

By using (3), the high-precision reconstruction of the sparse signal can be realized.

The perceived spectrum bandwidth is divided into N non-overlapping sub-bands, and f_n is the center frequency. Assuming that the position and bandwidth of each sub-channel are known, during the time of spectrum sensing, the following binary assumptions are made:

$$\begin{cases} H_0 : s = n \\ H_1 : s = x + n \end{cases}, \tag{4}$$

where $n \sim N(0, \delta^2 I_N)$ is $N \times N$ white Gaussian noise, and its probability density function is

$$f_n = \frac{1}{2\pi^{\frac{N}{2}}} \cdot \frac{1}{(\delta^2)^{\frac{1}{2}}} \cdot e^{\frac{1}{2} \cdot n^T (\delta^2)^{-1} \cdot n}. \tag{5}$$

From the compressed sensing theory, x should be sparse,

$$x = \Psi\alpha, \ \|\alpha\|_0 = K. \tag{6}$$

where K is the sparsity of α. Considering (1), a new dual hypothesis can be obtained

$$\begin{cases} H_0 : s = An \\ H_1 : s = A(x + n) \end{cases} \tag{7}$$

According to the Neyman–Pearson binary hypothesis test criterion, we can obtain the relationship among compression ratio M/N, the false alarm probability P_f, SNR and the correct detection probability P_d,

$$P_d = Q(Q^{-1}(P_f) - \sqrt{\frac{M}{N}}.\sqrt{\text{SNR}}), \tag{8}$$

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} e^{\frac{-t^2}{2}} dt \tag{9}$$

For a single user, the sensing result can be finally obtained through compressed sensing. The support set of spectrums represented by the sequence of spectrum state $d \in \{0, 1\}^{1 \times N}$ can be used to describe the result:

$$d[k] = \begin{cases} 1, k \in \Lambda \\ 0, k \notin \Lambda \end{cases} \tag{10}$$

where Λ is the support set of spectrums.

For the sequence of judgment results $d^{1 \times K}$, $d[k] = 1$ means the user determines the sub-band has been occupied after detection, while $d[k] = 0$ means the judgment on this sub-band is currently idle.

Secondly, there are three common SSDF attacks in CSS: false alarm attack, missed detection attack and probabilistic attack. The false alarm attack means that malicious nodes send 1 with 100% probability, and the missed detection attack means that malicious nodes send 0 with 100% probability. Both false alarm attack and missed detection attack can be regarded as special cases of probabilistic attack. Therefore, this paper mainly considers how to improve the accuracy of the judgment results in the CSS system with probabilistic attacks.

The scenario is described as follows: in the CR environment, each malicious user sends wrong data to the fusion center in the form of a probabilistic attack to affect the final judgment result. That is, after the malicious user detects the correct sensing result, for some purpose, the spectrum sensing result displayed as an occupied state will be tampered with the idle state with the probability of P_{10} locally, while the spectrum sensing result displayed as the idle state will be tampered with the occupied state with the probability of P_{01}, locally. Malicious users upload the falsified results to the fusion center for judgment. In this case, the false alarm probability and the missed detection probability from the entire CSS system will increase simultaneously. From the data fusion center, the correct detection probability and the false alarm probability for a single malicious user can be obtained:

$$P_d^{\text{m}} = (1 - P_{10})P_d + P_{01}(1 - P_d) \tag{11}$$

$$P_f^{\text{m}} = (1 - P_{10})P_f + P_{01}\left(1 - P_f\right) \tag{12}$$

where P_f^{m} is the false alarm probability of a malicious user and P_d^{m} is the correct detection probability of a malicious user.

Finally, the blockchain technology mentioned in [16] is essentially a decentralized database, which involves a variety of new application modes of computer technology, such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm. As shown in Figures 2 and 3, the blockchain is a chained data structure with blocks, which realizes the link between blocks by random hashing, and ensures the rationality of the generated blocks with the timestamp. Its characteristics

include decentralization, openness, autonomy, no falsity, and anonymity. Through the blockchain, users can achieve trust-free interaction. The data recorded on the blockchain is the result of consensus reached by most nodes on the network, so the quality of the data can be strongly guaranteed.

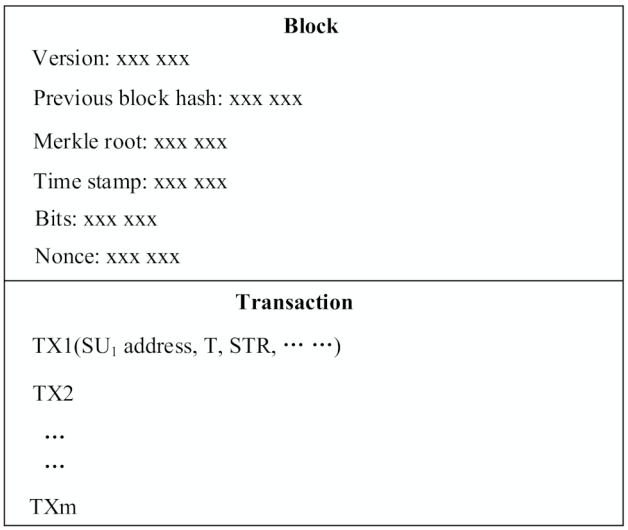

Figure 2. Structure of block.

Figure 3. Blockchain hash connection model.

Through the blockchain, we can get the transaction information in the network, including the transaction time, transaction number, transaction amount (T), transaction account (address), account token balance (R), and additional content segment in transaction (STX) of both transaction parties. Based on the above information, the weight of the i-th user in a spectrum sensing task can be set as:

$$W_i = f(T_i, R_i, STX_i) \tag{13}$$

For a sub-band, the final judgment result is determined by the K-N rule, which supports the judgment of nodes with weight greater than 0.5. Then the judgment result of the k-th sub-band is as follows:

$$\overline{d}[k] = \begin{cases} 0, \sum_{1}^{B} W_i < 0.5 \\ 1, \sum_{1}^{B} W_i \geq 0.5 \end{cases} \tag{14}$$

where W_i is the weight of the i-th sensing node that determines how the sub-band is occupied and B is the number of the sensing nodes that determines how the sub-band is occupied. Then the level of spectrum sensing results obtained by the CR network fusion center can be expressed as the average correct detection probability $\overline{P}_d$ and the average false alarm probability $\overline{P}_f$.

$$\overline{P_d} = \sum_{a=1}^{r} W_a^{\mathrm{m}} P_d^{\mathrm{m}} + \sum_{b=1}^{H-r} W_b^{\mathrm{h}} P_d^{\mathrm{h}} \tag{15}$$

$$\overline{P_f} = \sum_{a=1}^{r} W_a^{\mathrm{m}} P_f^{\mathrm{m}} + \sum_{b=1}^{H-r} W_b^{\mathrm{h}} P_f^{\mathrm{h}} \tag{16}$$

where P_f^{h} is the false alarm probability of a honest user and P_d^{h} is the correct detection probability of a honest user. P_f^{m} is the false alarm probability of a malicious user and P_d^{m} is the correct detection probability of a malicious user. ${W_a}^{\mathrm{m}}$ is the weight of the a-th malicious users and W_b^{h} is the weight of the b-th honest users. H is the number of users and r is the number of malicious users.

2.2. The Proposed System Scheme

Figure 4 shows an overview of the overall system scheme based on APR_SWSS algorithm. After compressed sensing, the user uploads the generated result sequence to the blockchain network in the form of transaction, and is packaged into blocks after verification by miner nodes. The fusion center obtains the sensing information of the node from the network, adjusts the weight of the node through the proposed APR_SWSS algorithm, and obtains the final fusion result.

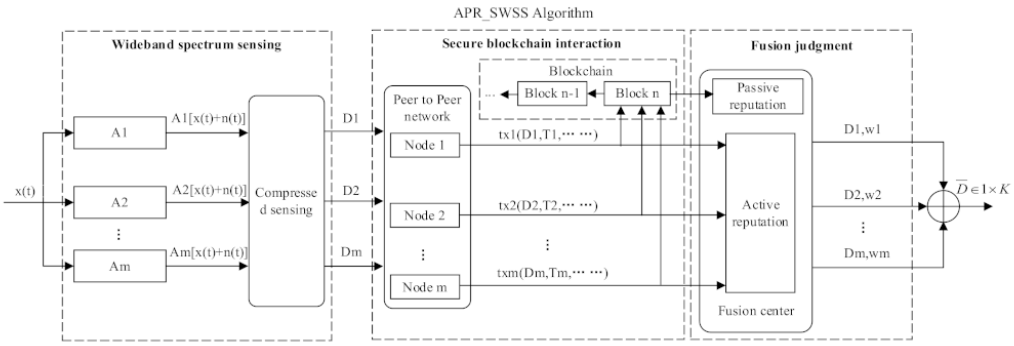

Figure 4. Overview of the framework of APR_SWSS algorithm.

The blockchain technique can ensure the users' privacy and data security. Firstly, in the blockchain network, the user sends sensing results to the fusion center, and the fusion center can only obtain the transaction and balance information of the account through the user's wallet address. Secondly, as a decentralized database, blockchain can guarantee data security. Once the data is recorded in the blockchain ledger, it cannot be tampered with. Finally, the transaction between a sensing node and the fusion center on the blockchain can ensure the safety of the fusion results through multiparty games. If users who are quite sure of the high accuracy of their results will send more tokens, the critical value of tokens obtained by the fusion center will also rise accordingly through comprehensive judgment. However, users who have no confidence in their results usually send the number of tokens below the threshold, which leads to the decrease of decision weight. Therefore, the result of fusion judgment will approach the higher accuracy side.

2.2.1. CSS Process Based on Blockchain

In the sensing task, CSS is a decision made by the data fusion center after synthesizing the sensing results of all involved nodes. On this basis, the model used in this paper introduces the blockchain network and incentive mechanism, which can provide a trust-free working environment for CR network nodes, and encourage more nodes to participate in sensing tasks and obtain more token rewards.

As shown in Figure 5, the CSS model mainly includes sensing users, the data fusion center and blockchain network. The SU is the executor of the sensing task. As a decentralized database, a single SU will send the result to the fusion center through the blockchain network in the form of a transaction after analyzing the sensing results. All information will be synchronously recorded on the chain. After obtaining the sensing

results of multiple users, the data fusion center will make a fusion judgment through the data on the blockchain, and get the final result.

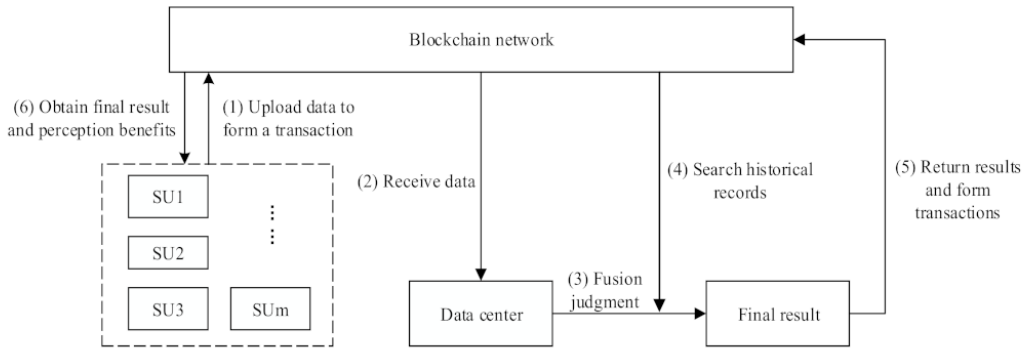

Figure 5. CSS model based on blockchain.

The detailed steps of a sensing task are as follows:

Step 1: The task is first released, and then each CR SU node perceives the range of the target frequency band and sends the detected results to the data fusion center account in the form of transaction on the blockchain.

Step 2: After the transaction is broadcast, the miner packs and generates blocks. The data center receives the transaction through the blockchain network, and gets the sensing information attached to the transaction at the same time.

Step 3: The data center judges all transactions with destination address pointing to itself as the transaction with sensing results, and searches the additional information of the transaction including the task number. The transaction, which is confirmed as the uploaded result of the sensing task, will be included in the data set to be fused, and then the weight is set.

Step 4: For each uploaded sensing result, the fusion center obtains its wallet address from the transaction, and adjusts the weight of the user's sensing data by retrieving the basic account data and historical data related to the user recorded on the blockchain.

Step 5: After the final sensing result is obtained by fusion decision, the data center will send a transaction to the nodes participating in the sensing task, which is attached with the correct sensing result, showing whether the sensing result is valid or not, and if the token incentive is rewarded by successful sensing.

Step 6: The node participating in the sensing task receives the transaction containing the fusion result and the reward token, and then the token balance changes accordingly.

The consensus mechanism of this blockchain network is implemented based on POW (roof of work), and the nodes on the chain are managed by the fusion center. Since the confirmation of the sensing node in this scheme is based on the task number in the transaction additional segment, we adopt the block generation strategy to generate blocks in time. The generation time of each block is fixed, but its number of internal transactions is not fixed. Due to the timeliness and rapidity required for spectrum sensing, the fusion center will also receive sensing data for a limited time, that is, it will no longer receive data for this sensing task after a certain period of time.

2.2.2. Blockchain Transaction Model

In the blockchain network, a single sensing user uploads the sensing results to the fusion center in the form of transaction. As shown in Figure 6, the transaction includes not only the sensing task number and the uploaded sensing results, but also any number of transaction tokens.

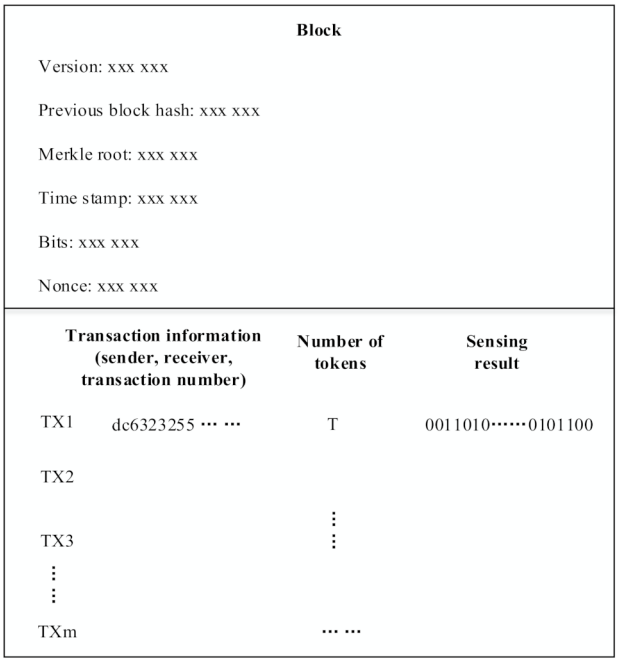

Figure 6. Block of transaction uploaded by node sensing result.

The sensing task number can prove that the data in the transaction belongs to the sensing task corresponding to the number. After determining the range of the sensing frequency band and the number of sub-bands divided in this range, the uploaded sensing results are represented by a sequence $D \in 1 \times N$ composed of 0 and 1, which is equal to $\overline{d}$.

Generally, based on experience and the number of token balances owned by the whole blockchain account, the fusion center will set a threshold value for the number of transaction tokens submitted by the sensing user. When the number of tokens attached by the sensing user exceeds the threshold, the fusion center will give some extra weight to the user in the final fusion decision.

Similarly, after the fusion decision, the fusion center will send a transaction to the user node that participated in the sensing task before. As shown in Figure 7, the transaction contains the sensing task number, the final decision results, the accuracy judgment and the number of returned tokens. The final decision results are also given in the sequence structure of 0 and 1. The accuracy judgment is to determine the validity of the results uploaded by the sensing node, which will be an important basis for the fusion center to set or adjust the weight of the node in the future. After confirming that the user's sensing data is valid, the fusion center will send a certain number of tokens according to the weight of the uploaded results of the node in the judgment. In order to positively motivate the sensing nodes to perform sensing tasks, and reward the sensing nodes that make contributions to setting the active reputation, the fusion center will not only return the number of transaction tokens attached to the user when submitting the sensing results, but also reward the user with additional tokens. The higher the number of tokens a user has, the greater the chance to access the spectrum. If users' sensing results are valid after the decision of the fusion center, they will receive T^* tokens as a reward, where T^* denotes the number of tokens that fusion center sends to the sensing nodes.

$$T_i^* = 1.25T_i(1 + W_i) \tag{17}$$

for the i-th sensing node, T_i is the number of tokens handed in during the setting of active reputation, and W_i is the weight judged by the fusion center finally.

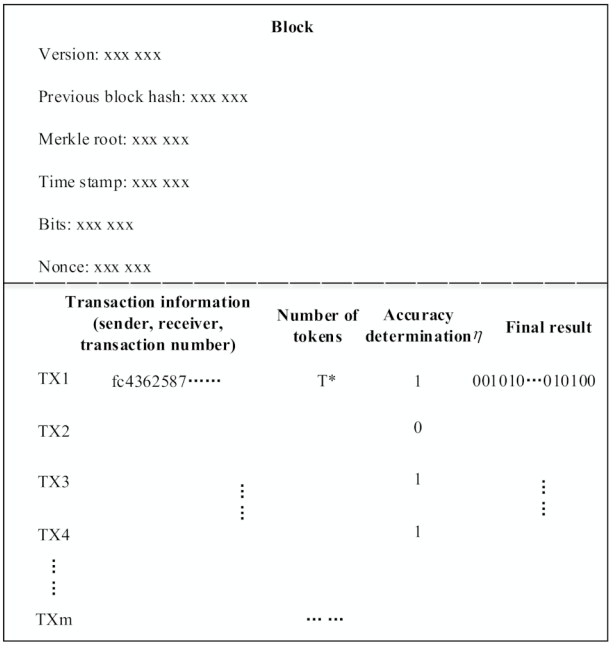

Figure 7. Block of transaction returned by fusion decision result.

2.2.3. The APR_SWSS Algorithm

In CSS, the common weighted fusion decision algorithm is usually used for fusion decision, that is, all nodes participating in the sensing task are allocated the same weight for fusion calculation. When the joint decision amount $\overline{D}_{[i]}$ for a certain sub-band exceeds the threshold value D_{th}, this sub-band is judged to be occupied, otherwise, it is idle.

This paper proposes an APR_SWSS algorithm based on blockchain technology. By combining with the blockchain mechanism, it can adjust the sensing weight of each sensing node, and then get a more stable and accurate sensing result. The details of the proposed algorithm are as follows.

For the i-th user, the reputation is divided into ASR and PSR. As discussed above, ASR is judged by whether the number of tokens attached by the user when uploading the sensing results meets the critical value. The threshold value set in the whole CR network is $\overline{T}$. For the $\overline{T}$ value, under normal circumstances, we can obtain it through the OTSU method by T_i:

Put all the numbers of the tokens T_i from small to large in set $\boldsymbol{G}$, and get the average value μ_T:

$$\mu_T = \frac{\sum_{i=1}^{I} T_i}{I} \tag{18}$$

where I is the number of nodes uploaded tokens in the sensing task, and T_i is the number of tokens uploaded by the i-th node. Assuming that the threshold $\overline{T_s} \in \boldsymbol{G}$ is used to divide $\boldsymbol{G}$ into two sets of the number of tokens uploaded by honest nodes and malicious nodes, then calculate the between-class variance σ_t^{*2} iteratively:

$$\overline{T_{si}} = T_i, i = 1, 2, \ldots, \tag{19}$$

$$p_m^* = \frac{n_{tm}}{I} \tag{20}$$

$$p_h^* = \frac{n_{th}}{I} \tag{21}$$

$$\mu_m^* = \frac{\sum_{i=1}^{n_{tm}} T_i}{n_{tm}} \tag{22}$$

$$\mu_h^* = \frac{\sum_{i=n_{tm+1}}^{I} T_i}{n_{th}} \tag{23}$$

where n_{th} is the number of elements in **G** larger than $\overline{T_s}$, and n_{tm} is the number of elements in **G** smaller than $\overline{T_s}$. p_m^* is the probability of elements in **G** smaller than $\overline{T_s}$ and p_h^* is the probability of elements in **G** larger than $\overline{T_s}$.μ_m^* is the mean of elements in set of the number of tokens uploaded by malicious nodes, μ_h^* is the mean of elements in set of the number of tokens uploaded by honest nodes.

Calculate the between-class variance σ_t^{*2}:

$$\sigma_t^{*2} = p_m^*(\mu_T - \mu*_m)^2 + p_h^*(\mu_T - \mu_h^*)^2 \tag{24}$$

Then find the $\overline{T_{si}}$ that results in maximum between-class variance:

$$\overline{T} = Arg\max_{i=1\sim I} \sigma_t^{*2}(\overline{T_{si}}) \tag{25}$$

In this way, we can obtain additional prior information from the game in a trust-free environment. The number of tokens attached to the transaction submitted by the *i*-th user is T_i, then the ASR of this user is ψ_i, $\overline{T}$ is the threshold value.

$$\psi_i = \begin{cases} 0, T_i < \overline{T} \\ 1, T_i \geq \overline{T} \end{cases} \tag{26}$$

Historical Reputation

In the blockchain technology network introduced in this paper, a number of token balances perceived by a user can be regarded as the accumulation of token gains obtained through effective sensing in all sensing tasks of the user in the past history. For users, the more tasks they participate in, the more accurate the sensing results, and the more tokens they will have on their account. Based on this, we can take the number of balance tokens of the sensing users as the overall measurement value of their PSR.

Assume that there are m sensing users participating in a sensing task. By querying the transaction, the fusion center gets all the wallet addresses of the accounts that initiate the transaction with the sensing result information, and obtains the balance token number R on these accounts. Through the above operation, m balance tokens are obtained, forming a $1 \times$ m matrix [R1, R2, R3,..., Rm]. When the median R0.5 is found, the historical reputation value μ_i of the *i*-th sensing user can be obtained by Sigmod function,

$$\mu_i = \frac{1}{1 + e^{-\frac{R_i}{R_{0.5}}}} \tag{27}$$

Recent Correction

If a sensing node with high historical reputation value continuously sends wrong sensing data, the final fusion decision will be greatly affected. In order to avoid a previously honest sensing node from starting to do malicious behavior under certain motives, the fusion center is required to quickly modify the weight of the malicious node with high historical reputation value.

For the *i*-th sensing user, the fusion center will retrieve the accuracy judgment value η of the user's recent L times sensing tasks while setting its historical reputation value, where η is the accuracy determination in Figure 7. For L times of sensing tasks, the memory weight θ is set to decrease according to the time sequence,

$$\eta = \begin{cases} 0, \text{the sensing result is invalid} \\ 1, \text{the sensing result is valid} \end{cases} \tag{28}$$

$$\sum_{i}^{L} \theta_i = 1 \tag{29}$$

Then the user's recent reputation correction value γ can be expressed as:

$$\gamma_i = \sum_{i}^{L} \eta_i \cdot \theta_i \tag{30}$$

Finally, in order to meet the weight calculation requirements in different situations, the decision parameter β is introduced to adjust the weight proportion of ASR and PSR, and the final weight calculation expression is obtained,

$$W_i = \beta \cdot \psi_i + (1 - \beta) \cdot \mu_i \cdot \gamma_i \tag{31}$$

The algorithm can be expressed as Algorithm 1.

Algorithm 1. The APR_SWSS.

Input: T_i, R_i, β, θ_i, L, η_i

1. Determine the critical value $\overline{T}$ by T_i though OTSU method.
2. Calculate ASR:
$$\psi_i = \begin{cases} 0, T_i < \overline{T} \\ 1, T_i \geq \overline{T} \end{cases}$$
3. Obtain the median $R_{0.5}$ from the token balance of the nodes participating in the task.
4. Calculate PSR:
$$\mu_i = \frac{1}{1 + e^{-R_i / R_{0.5}}}$$
5. Calculate the recent reputation correction:
$$\gamma_i = \sum_{i}^{L} \eta_i \cdot \theta_i$$
6. Get the final node weight:
$$W_i = \beta \cdot \psi_i + (1 - \beta) \cdot \mu_i \cdot \gamma_i$$

Output: Node weight W_i

3. Results

The performance of APR_SWSS algorithm based on blockchain under SSDF attack is verified by simulation. The software environment of the simulation experiment is as follows: 64-bit Win7 operating system, MATLAB R2018b.

Blockchain running environment: Testnet under Ethereum geth client.

Hardware environment: Intel (R) core (TM) i5–5200u CPU @ 2.20 GHz and 8 GB RAM.

The detection results are assumed to be independent of each other. For a single node, the detection probability is 80% and the false alarm probability is 30%. The sensing frequency band is divided into 100 sub-bands. The CR network includes one fusion center, two PUs and 20 SUs. Meanwhile, there are two pseudo honest users (nodes that send false sensing results and submit a low number of tokens but have high reputation, and have higher historical reputation than malicious nodes) in the honest users.

Assume that the probability of MUs producing malicious behavior is 80% and the probability of honest users being misjudged is 5%.

Define $SNR = E/\sigma^2$, compression ratio M/N, where M is the sampling rate of local compression measurement, and N is the dimension of the signal itself. The lower the compression ratio, then the lower the system compression sampling cost is.

The probability of submitting the full quantity of tokens for honest users is 80%, and for MUs it is 20%. For the correction value of recent credibility, the nearest accuracy judgment value of L = 4 times is taken into account, and the memory weight is respectively

taken as $\theta_{n-1} = 0.4$, $\theta_{n-2} = 0.3$, $\theta_{n-3} = 0.2$, $\theta_{n-4} = 0.1$, and the decision parameter is $\beta = 0.5$. The description of the symbols mentioned in this section is shown in Table 1.

Table 1. Nomenclature.

Symbol	Description
SNR	Signal to noise ratio
M	Sampling dimension of local compressed measurement
N	Signal dimension
m	No. of sensing users
h	No. of malicious nodes
P_d	Detection probability
P_f	False alarm probability
L	No. of recent check of history
θ	Memory weight
β	Decision parameter

Assume that a single user performs 1000 sensing tasks, and the probability of this node performing SSDF attack is 30% for the first 400 times, 80% from 400 to 800 times and 10% for the last 200 times. The change of recent reputation correction value under different probability of malicious behavior is shown in Figure 8. When the malicious rate of malicious nodes changes, the modified parameters can be quickly adjusted to a stable range. It can be seen that setting the recent reputation correction value can resist on–off attacks to a certain extent.

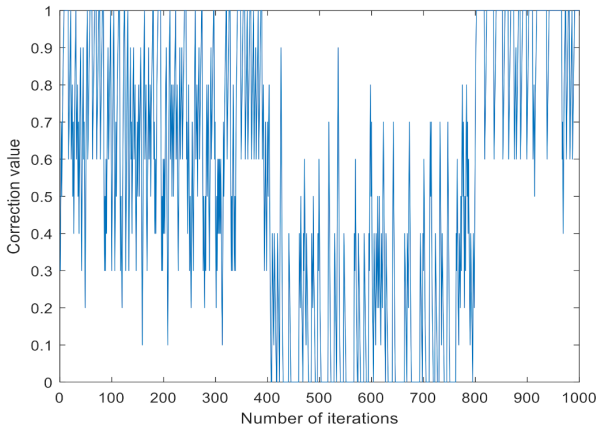

Figure 8. The change of 1000 recent reputation correction values.

In order to further obtain the sensitivity and distribution of the parameter, 100 times of sensing are carried out. The node carries out SSDF attack with probability 30% during the first 40 times, 80% from 40 to 80 times, and 10% for the last 20 times. Figure 9a describes the change of the node's recent reputation correction value under different probabilities of malicious behavior, and Figure 9b–d show the statistical pie charts of the modified value under different probabilities of malicious behavior, respectively. When the probability is 30%, the correction value is concentrated in the range of 0.4–1; when the probability is 80%, the range is 0–0.4; and the range is 0.6–1 when the probability is 10%. From Figure 9a, we can intuitively find that the correction value is at a high level when the probability of malicious behavior is 30% and 10%, and is at a low level when the probability is 80%. Meanwhile, it can be seen that when the node's probability of malicious behavior changes, the correction value level can change rapidly, and then adjust the node weight quickly.

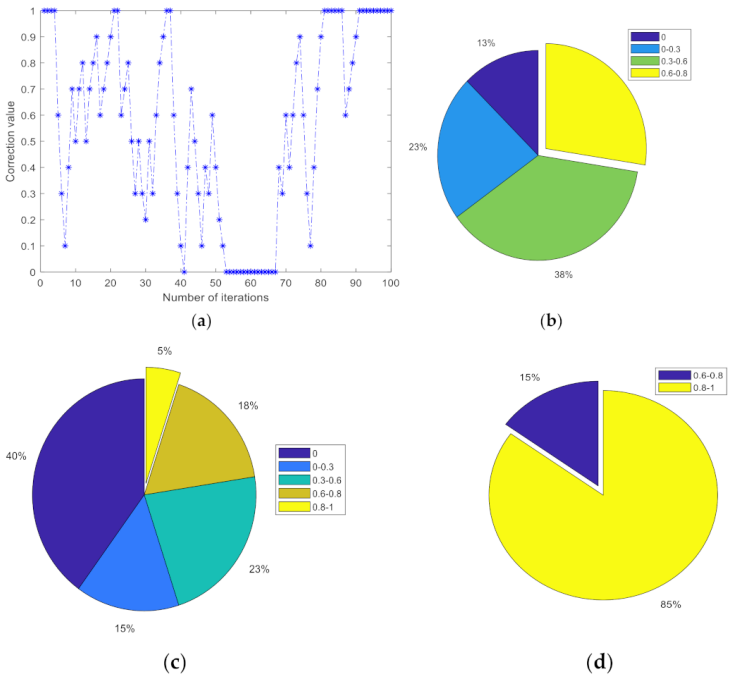

Figure 9. (**a**) The change of recent reputation correction values under different probability of malicious behavior; (**b**) numerical distribution when the probability of malicious behavior is 30%; (**c**) numerical distribution when the probability of malicious behavior is 80%; (**d**) numerical distribution when the probability of malicious behavior is 10%.

Figure 10 describes the weight distribution of all nodes when there are different numbers of malicious nodes among 20 sensing users. When the number of MUs is three, the first three nodes in the sequence are malicious nodes, and the weight of which is close to zero in the ideal case. The subsequent nodes maintain a higher sensing weight, where some of the individual nodes' sensing weights are slightly lower due to performance differences and other factors. When the number of MUs is six, the first six nodes in the sequence are malicious nodes, and the weight of these malicious nodes is significantly lower than that of honest nodes. It can be seen from the seventh and eighth node that the weight of the pseudo honest node is larger than that of the malicious node, but much lower than that of the honest node. The comparison of the two curves in Figure 10 shows that with an increase of the number of MUs, the sensing weight of MUs will gradually increase. However, it can be effectively suppressed by using the proposed APR_SWSS algorithm.

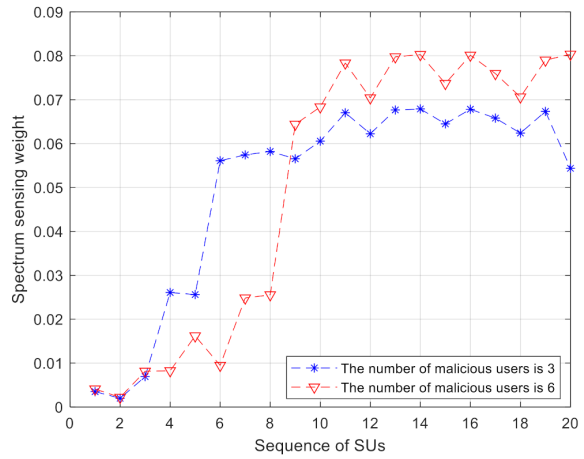

Figure 10. Weight distributions of nodes with different number of malicious nodes.

To further verify the performance of the proposed APR_SWSS algorithm, the equal-gain combination (EGC) algorithm and the beta reputation based weight (BRBW) algorithm [48] are chosen for comparison. The EGC algorithm combines the uploaded results of each sensing node with equal probability, and the BRBW algorithm adjusts the node weight based on the historical data sensed by the node. As shown in Figure 11a, the detection probability decreases with the increasing number of malicious nodes. When the number of malicious nodes is 10, which is half of the total number of sensing nodes, the detection probability of the traditional EGC algorithm fluctuates around 0.5, and its performance is seriously affected. However, the APR_SWSS algorithm can maintain the detection probability above 0.7. Compared with the BRBW algorithm, when the number of malicious nodes is more than half of the total number of nodes, the APR_SWSS algorithm can still play a certain role in resisting SSDF attacks, and its detection probability is above 0.6.

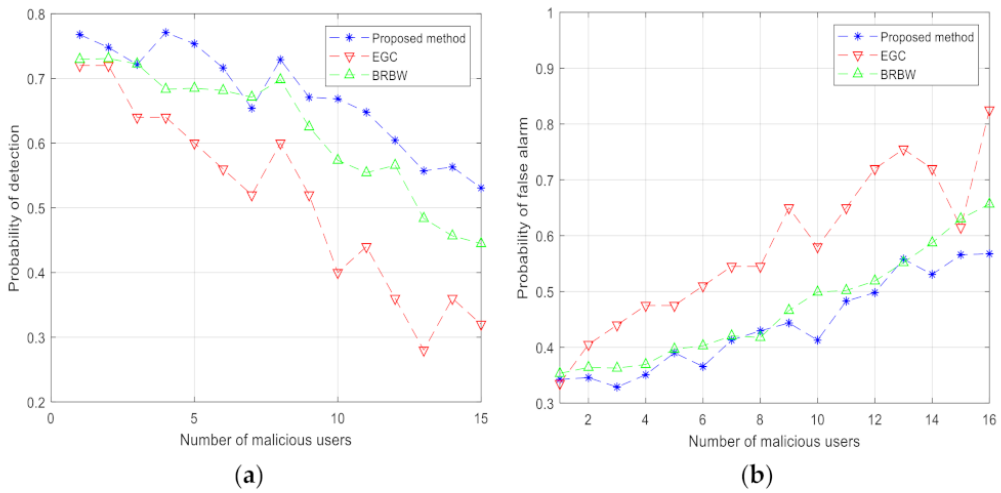

Figure 11. (**a**) The change of detection probability with the increase of malicious nodes for three different algorithms; (**b**) the change of false alarm probability with the increase of malicious nodes for three different algorithms.

Figure 11b shows that the false alarm probability increases with the increasing number of malicious nodes. When the malicious nodes account for half of the total number of nodes, the EGC algorithm is greatly affected, while the APR_SWSS algorithm can limit the false alarm probability to a lower level. Compared with the two algorithms, the proposed APR_SWSS algorithm has better performance even in the case of high number of malicious nodes.

Figure 12 shows the change of the detection probability of three algorithms under different number of assistants. Under the K-N criterion, when the number of assistants is eight, the detection probability of the APR_SWSS algorithm is about 95%, which is better and more stable than that of the EGC and BRBW algorithm. Therefore, under the K-N criterion, compared with the EGC algorithm and the BRBW algorithm, the APR_SWSS algorithm can achieve more stable and accurate joint spectrum sensing result in CR network with fewer assistants.

Figure 13 illustrates the receiver performance under different compression ratios when SNR = 4, the number of MUs is 5, and the probability of SSDF attack is 80%. It can be seen that the performance of EGC algorithm drops sharply when the malicious node carries out SSDF attack. Compared with the BRBW algorithm, the APR_SWSS algorithm can resist SSDF attack more effectively, have better performance under lower compression ratio, and achieve more accurate spectrum sensing with lower cost.

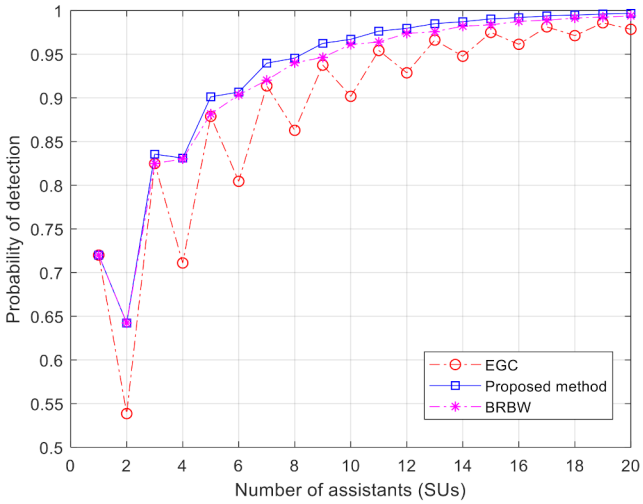

Figure 12. The change of detection probability under different number of assistants for three different algorithms.

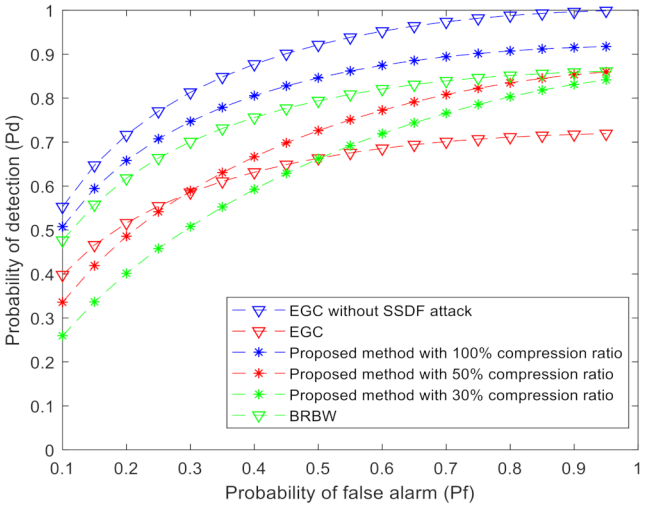

Figure 13. Comparison of spectrum sensing performance under different compression ratio (SNR = 4, MUs no. = 5, probability of SSDF attack = 80%).

The above simulation results show that the modified value of the recent historical reputation based on the historical sensing records of the blockchain can accurately reflect the recent sensing performance of the node. The proposed APR_SWSS algorithm can reduce the intention of malicious behavior of the node by increasing the cost of malicious attack, and set the ASR of the node, which can be combined with the PSR to realize the reasonable weight allocation. Compared with the traditional EGC algorithm and BRBW algorithm, the proposed APR_SWSS algorithm can effectively reduce the sampling cost of the system, effectively resist SSDF attacks, obtain more accurate sensing results, and achieve more stable and secure CSS.

4. Discussion

Since the proposed scheme uses blockchain as a decentralized database, it takes a long time to reach consensus among nodes and block propagation, which makes blockchain system almost impossible to achieve low latency. Meanwhile, a large amount of computing power will be consumed through the POW formula mechanism. On the premise of ensuring sufficient security, optimizing the consensus mechanism can be a solution to realize a blockchain system with low computing power consumption and low latency. In

addition, the proposed scheme can also be combined with intelligent contract. Therefore, the distributed sensing decision algorithm and intelligent contracts for spectrum sharing application scenarios will be our future research directions.

5. Conclusions

In the CSS network, to solve the problem that the sensing performance is significantly reduced when SSDF attacks were launched by malicious nodes, a blockchain-based APR_SWSS algorithm was proposed. It adjusted the weight through the active and passive reputations. Firstly, a blockchain-based cooperative spectrum sensing model containing malicious nodes was established. Then, the sensing process of the system model was described in detail, where the blockchain is used as the medium of database and data exchange to realize a trust-free spectrum sensing environment. Subsequently, we divided the reputation of a single node into the ASR and the PSR. By comprehensively considering both reputation values, all nodes in the current sensing task were dynamically allocated weights, and more accurate sensing results were obtained through fusion judgment. The simulation results showed that the algorithm proposed in this paper can effectively reflect the performance of the recent sensing nodes according to the data on the blockchain, and realize the reasonable weights allocation through the reputation value under low computing power requirements. When the malicious nodes to honest nodes ratio is set to about 1/7 and the pseudo honest node to honest nodes ratio is set to about 1/3, using K-N joint sensing judgment, the proposed algorithm can obtain reliable sensing results with fewer assistants. In particular, when the number of assistants is 10, the stable and accurate sensing results can be obtained. Meanwhile, compared with traditional algorithms, it can achieve low compression ratio sampling, and can effectively resist SSDF attacks, ensuring the security of cooperative spectrum sensing and the stability of sensing performance.

Author Contributions: Conceptualization, X.X. and Z.H.; methodology, X.X. and Z.H.; software, X.X.; validation, Y.Z., X.X. and Z.H.; formal analysis, X.X. and Z.H.; investigation, X.X.; resources, Z.H. and Y.B.; data curation, X.X.; writing—original draft preparation, X.X., Z.H., Y.Z., M.C. and Y.B.; writing—review and editing, X.X., M.C. and Z.H.; visualization, X.X.; supervision, Z.H.; project administration, Z.H.; funding acquisition, Z.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant No. 61963012, and in part by the Hainan Provincial Natural Science Foundation of China under Grant No. 620RC564.

Acknowledgments: The authors would like to thank the editors and the reviewers for their valuable time and constructive comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mitola, J.; Maguire, G.Q. Cognitive radio: Making software radios more personal. *IEEE Pers. Commun.* **1999**, *6*, 13–18. [CrossRef]
2. Wang, B.; Liu, K.R. Advances in cognitive radio networks: A survey. *IEEE J. Sel. Top. Signal Process.* **2010**, *5*, 5–23. [CrossRef]
3. Li, A.; Hamouda, W. Advances on spectrum sensing for cognitive radio networks: Theory and applications. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 1277–1304.
4. Yucek, T.; Arslan, H. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 116–130. [CrossRef]
5. Zhang, L.; Xiao, M.; Wu, G.; Alam, M.; Liang, Y.C.; Li, S. A survey of advanced techniques for spectrum sharing in 5G networks. *IEEE Wirel. Commun.* **2017**, *24*, 44–51. [CrossRef]
6. Hu, Z.; Bai, Y.; Zhao, Y.; Shen, C.; Xie, M. Adaptive and blind wideband spectrum sensing scheme using singular value decomposition. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 3279452. [CrossRef]
7. Sun, H.; Nallanathan, A.; Cui, S.; Wang, C.X. Cooperative wideband spectrum sensing over fading channels. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1382–1394. [CrossRef]
8. Hu, Z.; Bai, Y.; Huang, M.; Xie, M.; Zhao, Y. A self-adaptive progressive support selection scheme for collaborative wideband spectrum sensing. *Sensors* **2018**, *18*, 3011. [CrossRef]

9. Qin, Z.; Gao, Y.; Plumbley, M.D.; Parini, C.G. Wideband spectrum sensing on real-time signals at sub-Nyquist sampling rates in single and cooperative multiple nodes. *IEEE Trans. Signal Process.* **2015**, *64*, 3106–3117. [CrossRef]
10. Liang, W.J.; Chien, T.H.; Lu, C.S. Theoretical stopping criteria guided greedy algorithm for compressive cooperative spectrum sensing. *Comput. Commun.* **2017**, *111*, 165–175. [CrossRef]
11. Chen, L.; Wang, J.; Li, S. An adaptive cooperative spectrum sensing scheme based on the optimal data fusion rule. In Proceedings of the 2007 4th International Symposium on Wireless Communication Systems, Trondheim, Norway, 17–19 October 2007; pp. 582–586.
12. Li, J.; Li, B.; Liu, M. Performance analysis of cooperative spectrum sensing over large and small scale fading channels. *AEU Int. J. Electron. Commun.* **2017**, *78*, 90–97. [CrossRef]
13. Qin, Z.; Gao, Y.; Plumbley, M.D. Malicious user detection based on low-rank matrix completion in wideband spectrum sensing. *IEEE Trans. Signal Process.* **2017**, *66*, 5–17. [CrossRef]
14. Zhang, L.; Ding, G.; Wu, Q.; Zou, Y.; Han, Z.; Wang, J. Byzantine attack and defense in cognitive radio networks: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1342–1363. [CrossRef]
15. Chen, C.; Song, M.; Xin, C.; Alam, M. A robust malicious user detection scheme in cooperative spectrum sensing. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 4856–4861.
16. Gul, N.; Khan, M.S.; Kim, S.M.; Kim, J.; Elahi, A.; Khalil, Z. Boosted Trees Algorithm as Reliable Spectrum Sensing Scheme in the Presence of Malicious Users. *Electronics* **2020**, *9*, 1038. [CrossRef]
17. Gray, M.L.; Suri, S.; Ali, S.S.; Kulkarni, D. The crowd is a collaborative network. In Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, San Francisco, CA, USA, 27 February–2 March 2016; pp. 134–147.
18. Zhang, B.; Hu, K.; Zhu, Y. Spectrum allocation in cognitive radio networks using swarm intelligence. In Proceedings of the 2010 Second International Conference on Communication Software and Networks, Singapore, 26–28 February 2010; pp. 8–12.
19. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Manubot* **2019**. Available online: https://git.dhimmel.com/bitcoin-whitepaper/ (accessed on 6 May 2021).
20. Battah, A.; Iraqi, Y.; Damiani, E. Blockchain-Based Reputation Systems: Implementation Challenges and Mitigation. *Electronics* **2021**, *10*, 289. [CrossRef]
21. Fernández-Caramès, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
22. Kearney, J.J.; Perez-Delgado, C.A. Vulnerability of Blockchain Technologies to Quantum Attacks. *Array* **2021**, *10*, 100065. [CrossRef]
23. Ikeda, K. Security and privacy of blockchain and quantum computation. *Adv. Comput.* **2018**, *111*, 199–228.
24. Ikeda, K. qBitcoin: A peer-to-peer quantum cash system. In *Science and Information Conference*; Springer: Cham, Switzerland, 2018; pp. 763–771.
25. Gao, Y.L.; Chen, X.B.; Xu, G.; Yuan, K.G.; Liu, W.; Yang, Y.X. A novel quantum blockchain scheme base on quantum entanglement and DPoS. *Quantum Inf. Process.* **2020**, *19*, 1–15. [CrossRef]
26. Kiktenko, E.O.; Pozhar, N.O.; Anufriev, M.N.; Trushechkin, A.S.; Yunusov, R.R.; Kurochkin, Y.V.; Lvovsky, A.I.; Fedorov, A.K. Quantum-secured blockchain. *Quantum Sci. Technol.* **2018**, *3*, 035004. [CrossRef]
27. Rodrigues, L.A.; Júnior, J.F.R.; do Amaral, A.R. Social tagging for e-learning: An approach based on the triplet of learners, learning objects and tags. In *International Workshop on Learning Technology for Education in Cloud*; Springer: Cham, Switzerland, 2015.
28. Chaer, A.; Salah, K.; Lima, C.; Ray, P.P.; Sheltami, T. Blockchain for 5G: Opportunities and challenges. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
29. Manogaran, G.; Rawal, B.S.; Saravanan, V.; Kumar, P.M.; Martínez, O.S.; Crespo, R.G.; Montenegro-Marin, C.E.; Krishnamoorthy, S. Blockchain based integrated security measure for reliable service delegation in 6G communication environment. *Comput. Commun.* **2020**, *161*, 248–256. [CrossRef]
30. Xu, H.; Klaine, P.V.; Onireti, O.; Cao, B.; Imran, M.; Zhang, L. Blockchain-enabled resource management and sharing for 6G communications. *Digit. Commun. Netw.* **2020**, *6*, 261–269. [CrossRef]
31. Bayhan, S.; Zubow, A.; Wolisz, A. Spass: Spectrum sensing as a service via smart contracts. In Proceedings of the 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Korea, 22–25 October 2018; pp. 1–10.
32. Zhou, Z.; Chen, X.; Zhang, Y.; Mumtaz, S. Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks. *IEEE Netw.* **2020**, *34*, 24–31. [CrossRef]
33. Lv, P.; Zhao, H.; Zhang, J. Blockchain Based Spectrum Sensing: A Game-Driven Behavior Strategy. In Proceedings of the 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 11–13 December 2020; Volume 9, pp. 899–904.
34. Ariyarathna, T.; Harankahadeniya, P.; Isthikar, S.; Pathirana, N.; Bandara, H.D.; Madanayake, A. Dynamic spectrum access via smart contracts on blockchain. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6.
35. Kotobi, K.; Bilén, S.G. Blockchain-enabled spectrum access in cognitive radio networks. In Proceedings of the 2017 Wireless Telecommunications Symposium (WTS), Chicago, IL, USA, 26–28 April 2017; pp. 1–6.
36. Kotobi, K.; Bilen, S.G. Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access. *IEEE Veh. Technol. Mag.* **2018**, *13*, 32–39. [CrossRef]

37. Rawat, D.B.; Alshaikhi, A. Leveraging distributed blockchain-based scheme for wireless network virtualization with security and QoS constraints. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 332–336.
38. Careem, M.A.A.; Dutta, A. Sensechain: Blockchain based reputation system for distributed spectrum enforcement. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11–14 November 2019; pp. 1–10.
39. Bayhan, S.; Zubow, A.; Gawłowicz, P.; Wolisz, A. Smart contracts for spectrum sensing as a service. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 648–660. [CrossRef]
40. Pei, Q.; Ma, L.; Li, H.; Li, Z.; Yan, D.; Li, Z. Reputation-based coalitional games for spectrum allocation in distributed cognitive radio networks. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7269–7274.
41. Ye, F.; Zhang, X.; Li, Y. Comprehensive reputation-based security mechanism against dynamic SSDF attack in cognitive radio networks. *Symmetry* **2016**, *8*, 147. [CrossRef]
42. Pei, Y.; Hu, S.; Zhong, F.; Niyato, D.; Liang, Y.C. Blockchain-enabled dynamic spectrum access: Cooperative spectrum sensing, access and mining. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
43. Patnaik, M.; Prabhu, G.; Rebeiro, C.; Matyas, V.; Veezhinathan, K. ProBLeSS: A proactive blockchain based spectrum sharing protocol against SSDF attacks in cognitive radio IoBT networks. *IEEE Netw. Lett.* **2020**, *2*, 67–70. [CrossRef]
44. Zhang, G. Research on Cognitive Radio Spectrum Sensing Security Mechanism Based on Blockchain. *J. Phys. Conf. Ser.* **2020**, *1578*, 012045. [CrossRef]
45. Zhang, Y.; Fang, Z. Dynamic Double Threshold Spectrum Sensing Algorithm Based on Block Chain. In Proceedings of the 2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE), Xiamen, China, 18–20 October 2019.
46. Tangsen, H.; Li, X.; Ying, X. A Blockchain-Based Node Selection Algorithm in Cognitive Wireless Networks. *IEEE Access* **2020**, *8*, 207156–207166. [CrossRef]
47. Hu, Z.; Bai, Y.; Cao, L.; Huang, M.; Xie, M. A sequential compressed spectrum sensing algorithm against SSDH attack in cognitive radio networks. *J. Electr. Comput. Eng.* **2018**, *2018*, 4782718. [CrossRef]
48. Bai, P.; Zhang, X.; Ye, F. Reputation-based Beta reputation system against SSDF attack in cognitive radio networks. In Proceedings of the 2017 Progress in Electromagnetics Research Symposium-Fall (PIERS-FALL), Singapore, 19–22 November 2017; pp. 792–799.