Hindawi
Journal of Electrical and Computer Engineering
Volume 2023, Article ID 8920243, 13 pages
https://doi.org/10.1155/2023/8920243

Research Article

Enhance the Probability of Detection of Cooperative Spectrum Sensing in Cognitive Radio Networks Using Blockchain Technology

D. Balakumar and Nandakumar Sendrayan

School of Electronics Engineering, Department of Communication Engineering, Vellore Institute of Technology, Vellore 632014, India

Correspondence should be addressed to Nandakumar Sendrayan; snandakumar@vit.ac.in

Received 25 October 2023; Revised 24 November 2023; Accepted 9 December 2023; Published 18 December 2023

Academic Editor: Andrea Tani

Cognitive radio (CR) is the best way to improve the efficiency of spectrum consumption for wireless multimedia communications. Spectrum sensing, which allows legitimate secondary users (SU) to find vacant bands in the spectrum, plays a vital role in CR networks. When cooperative sensing is used in CR networks, spectrum availability must be taken into account. In many ways, the shared cooperative spectrum sensing (CSS) data among SU. The presence of a malicious user (MU) in the system and sending false sensing data can degrade the performance of cooperative CR. The sharp rise in mobile data traffic causes congestion in the licensed band for the transmission of signals. Handling this security issue in real time, on top of spectrum sharing, is a challenge in such networks. In order to manage the spectrum and identify MU, blockchain-based CSS is developed in this article. To gauge the efficiency of the proposed topology, performance metrics like sensitivity, node selection, throughput measurement, and energy efficiency are used. This work suggests a unique, easier-to-use CSS method with MU suppression that outperforms the current one. According to simulation studies, the suggested topology can increase the likelihood of MU detection by roughly 15% when 40% of system users are malicious.

1. Introduction

An intelligent network of wireless transceivers with reconfigurable settings is known as a cognitive radio network (CRN), that may change their configuration and communication characteristics on their own to meet the Quality of Service (QoS) standards or get used to the network environment shifting. The devices of CR are given as follows: (1). A software cognition module that allows for intelligent decision-making. (2). Enhanced dynamic spectrum access (DSA) capabilities at the radio level, allowing communication across several channels. (3). Low-bandwidth communication between normally nearby transceivers, allowing collaboration. The CRN nodes perceive the network environment on a local level.

A CR is a radio that can be dynamically designed and adjusted to use the finest wireless channels available in its immediate neighbourhood, avoiding user interference and traffic jam. Such a radio detects available channels in the wireless spectrum and adjusts its reception or transmission characteristics accordingly to allow more concurrent wireless communications in a given frequency band at a single place. This is an example of dynamic spectrum sensing in action.

One of the key issues in wireless communications is the rising demand for restricted spectrum resources. Due to the growing need for bandwidth applications, network operators must effectively meet expectations for more capacity and enhanced quality of service (QoS). Expanding spectrum use requires CR. Unlicensed users, or SUs, use the available spectrum in a CR network while the licensed user, or PU, is guaranteed to experience tolerable interference. Due to the authorization-based spectrum allocation plan, many bands are unused. Although it is believed that the radio spectrum is a limited resource, the problem with spectrum availability is not a lack of spectrum but rather an ineffective use of the spectrum. An essential resource on the path to fifth-generation (5G) and sixth-generation (6G) systems is the effective use of the radio spectrum.

There is a definite need for extra spectrum, and the constant rise in spectral efficiency is insufficient. The fixed allocation technique used in traditional radio spectrum management hinders the spectrum resources from being fully exploited. One SU can easily be changed while using spectrum sensing due to numerous circumstances, including multipath fading, shadow effects, etc.

Although CR networks are not widely available and channel availability is important for such crucial information sharing, broadcasting multimedia is more difficult than it is on conventional networks. Transmission of multimedia requires strict QoS criteria. Depending on the moment and place, the unused spectrum is made dynamically available. These circumstances have a significant impact on channel stability, or the channels' capacity to meet the specific SU QoS requirements. Cooperative multiuser spectrum sensing can help solve these problems.

Any signal type can be employed with the simple and uncomplicated energy detection (ED) technique, which does not require any prior knowledge of the signal that was really received. If SU are unaware of the characteristics of the PU signal, ED is the best approach with the least amount of complexity, and it has been extensively used in recent studies.

However, the performance of ED is usually hampered by channel fading, shadowing, or the signal-to-noise ratio (SNR) wall. To increase detection reliability, a multi-SU cooperative technique has been proposed. In a cooperative system, a large number of SU independently determine the spectrum's condition and report their findings to the cognitive users (CU) over a control channel. When determining if a signal of a particular bandwidth is present in a spectral region of interest, energy detection with a single antenna works poorly in low SNR regions. However, there are also potential risks, such as manipulation and malicious SU cooperation attacks.

Any type of computational gear, including computers and mobile phones, can function as clusters or consumers in a blockchain system. A block is a collection of events, and an assembly of units is created by the links joining the individual components. The process of adding a block to the network is called extraction. Hubs that do processing tasks are known as miners. Every new action is distributed to all locations inside the system, and each site generates its own block by compiling new occurrences and calculating the effort evidence for each problem. In addition to competing for the opportunity to construct a block, miners are in charge of verifying interactions and spreading activities. Miner workers who assist in building a new block receive payment.

Their contributions to the blockchain's management are acknowledged in this way. Miners work together to validate activities, publish the freshly built block, and verify the block in order to reach a consensus. Among all the competing participants in block formation, the first person to complete all complicated statistical estimates for a certain level of complexity is acknowledged for further transaction development and blockchain integration. The blockchain's architecture is shown in Figure 1.

The interference problem can be resolved with the use of CR, which enhances radio spectrum utilization. Three major tasks have been introduced by the CR, starting with radio-scene analysis. One can determine the first task associated with the availability of spectrum holes. Channel identification, which notifies the transmitter section of the channel's capacity availability, is the second function of CR. The transmission of power control and spectrum management is the CR's third job. The outcomes of the energy detector spectrum sensing approach have been enhanced for a range of SNR fluctuations, which is one of the critical elements for precise sensing.

The cyclostationary spectrum sensing approach incorporates the same cyclic properties and correlation techniques as the matched filter spectrum sensing methodology. Cyclostationary is a more complicated method than the others. When compared to an energy detector (ED), a matched filter approach is the most desirable one. The drawback of the matching filter approach is that it necessitates understanding the information contained in the PU signal. Other techniques use eigenvalues and wavelet analysis. The ED is the most pleasant of all the strategies because it requires no prior knowledge of the data and has a minimal processing cost and complexity. Cooperative sensing is the process by which the CR user provides the fusion center (FC) with the PU's information.

1.1. Contribution.

1.1. Contribution. This paper proposes a blockchain-based approach to enhance the cognitive radio network during cooperative spectrum sensing. The following is a summary of our proposed work's primary contributions:

(1) To convert every user, PU and SU, into blockchain-like blocks that come together to build a decentralized network

(2) The authentication of the cooperative users validates the energy detection method for spectrum sensing and its outcomes

(3) The use of digital signatures in blockchain technology to confirm the identity of PU and MU

(4) Energy detection, throughput, P_d, P_f, and SNR all impede the identification of a MU in individual sensing

(5) The thorough simulation findings that confirm our suggested mechanism's effectiveness

The purpose of this paper is to show that simple conditions might have MU. Provide extreme values, repeatedly signaling "always yes" or "always no." The information "always yes" will raise the false alarm probability, while the information "always no" will lower the chance of missing

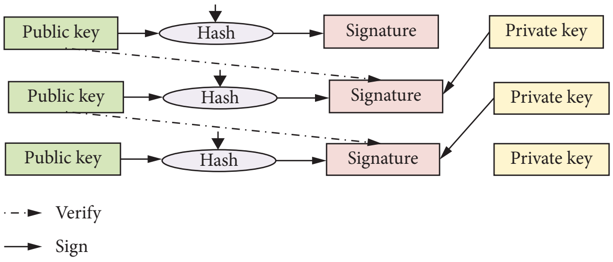

Figure 1: Architecture of blockchain technology.

a detection. To minimize the impact produced by MU, a novel cooperative detection technique is suggested. Two performance metrics, P_d and P_f, as well as a perceptual learning model, were used to investigate and evaluate cooperative spectrum sensing performance.

Techniques based on digital signal processing can be used to find SU and boost radio sensitivity. The detection of a MU in individual sensing is hindered by SNR, throughput, and energy detection. Results for a range of SNR variations show that one of the variables that are crucial to precise sensing has been improved for the energy detector spectrum sensing approach.

1.2. Organization. The remainder of the essay is structured as follows: Section 2 goes over the related work. Section 3 presents the scenario and methodology of the blockchain-enabled CR network and the ED of CR. The results are discussed in Section 4. The contributions and the possibilities of future research are discussed in Section 5. The abbreviations used in this article are listed in Table 1.

Table 1: List of abbreviations.

Acronyms	Description
5G	Fifth generation
6G	Sixth generation
AI	Artificial intelligence
AWGN	Additive white Gaussian noise
BE	Battlefield endpoints
CR	Cognitive radio
CRN	Cognitive radio networks
CSS	Cooperative spectrum sensing
CU	Central users
ED	Energy detection
ELM	Extreme learning machine
FC	Fusion center
FCFS	First come, first serve
IoT	Internet of things
IoV	Internet of vehicles
ML	Machine learning
MU	Malicious users
MWM	Maximum weight matching
PLO	Primary licensed operator
PoS	Proof of stake
PoW	Proof of work
PU	Prime users
QAM	Quadrature amplitude modulation
QoS	Quality of service
RF	Radio frequency
SNR	Signal-to-noise radio
SPASS	Spectrum sensing as a service
SSDF	Spectrum sharing data falsification
SU	Secondary users
SVM-RDA	Support vector machine-based red deer algorithm
TTBV	Two threshold-based voting

2. Related Work

Blockchain technology has the potential to effectively address these problems [1–5]. The addition of a reliable means to identify the fraudulent user thanks to the blockchain can increase network security [6]. The blockchain's decentralized structure raises security standards above those of traditional techniques. To allow the proper security measure alongside customer safety, the host's authentication connectivity regulation must be considered. Investigators have created several dangerous client detections that improve client privacy. Although this safety precaution has been utilized to protect client assets [7, 8], the techniques used are under the centralized control of a single authority.

The ProBLeSS protocol for proactive blockchain-based spectrum sharing is introduced. Successful traditions like PROLEMUS are used to implement learning power for better execution, and the absence of conventional Battlefield Endpoints (BE) validation is replaced by blockchain technology. Spectrum Sharing Data Falsification- (SSDF-) based assaults have the potential to seriously corrupt execution. These techniques must continue to handle the security risk even with reduced sharing. This necessitates the development of powerful CR engineering that can pinpoint the distinction between SU, which was made possible by social limit options in customs like PROLEMUS. ProBLeSS was put to the test on a virtual network using a clever SSDF attack. When compared to PROLEMUS under a comparable SSDF attack, this assault lowered the typical channel consumption by 2.74%, 8.3%, and 5.5% while identifying each delay [9].

Rajesh Babu and Amutha [10] introduced artificial intelligence- (AI-) based solutions for the blockchain-based spectrum of the CR network. This methodology is categorized into three stages, including limit detection, access via blockchain technology, and MU identification. The limit is first determined using the machine learning- (ML-) based extreme learning machine (ELM) approach. At that time, SUs had limited distribution options due to the blockchain approach. To ensure the effectiveness of the suggested model, a restructuring investigation was undertaken. The outcomes demonstrate that the proposed approach provides an improved implementation of various topologies. The study's findings showed that the introduced technique, in the presence of a SNR, obtained the most intense detection speed of about 0.68, while KNN showed a recognition speed of 0.58 and OR rules are about 0.5, respectively. Research on the sharing of spectrum across aerial/space networks and ground networks was summarized by Zhang et al. [11].

A brand-new design known as blockchain-based radio frequency (RF) has been introduced by Anh et al. [12]. Internet of Things (IoT) devices use RF-controlled backscatter CR discoveries to broadcast their diagnostic data to the subportal as bespoke transmitters on a computer. A blockchain network transmits the data acquired at the gateway for extra preparation, storage, and confirmation. In this way, the framework continuously improves the IoT framework while also increasing the energy economy and improving the usability of the range. In addition, information obtained from IoT devices is handled and verified independently. The susceptibility of IoT devices, the peculiar aspects of the blockchain environment and a continuous improvement issue for the gateway are required to achieve the goal.

The recommended handoff technique by Srivastava et al. utilizes a machine learning-based metaheuristic algorithm to address the handoff process of the spectrum mobility phase, which is a crucial aspect and one of CR networks distinguishing characteristics. SVM-RDA is predicated on prior environmental knowledge and shorter task execution times. That increased SUs practical use of the channel [13]. A proposed energy-efficient design for CRN by Bilibashi et al. allows each PU to select one SU as a relay node. PUs lease a portion of their assigned spectrum to the relay SUs in order to allow them to transmit data and promote the cooperative behavior of the SU [14]. According to Xu et al. secondary users with energy, harvesting capabilities can complete their information transmission task using their saved energy and the spectrum resources they have leased from the PU. For SUs, the act of leasing a spectrum resource results in a rise in costs [15].

The spectrum dollar, a blockchain-based computational value mechanism for secondary radio broadcasting, was introduced [16]. When Primary Licensed Operators (PLOs) get instructions and transfer restrictions, the usage of limitation currencies and noncash-oriented tailored restriction activities rises. The PLOs' fundamental sublimitation transition techniques describe the value of the limitation and the associated revenue portions.

Rathee et al. [17] created a blockchain for data rectification and a CRN-oriented Internet of Vehicles (IoV) from this MD, enabling unlawful and regulatory punishment of the company. It is known as the "order preference technique." It sends CRN to the IRV to find channels throughout distance identification as well as information transmission, showing its belief that CU would do so by asking questions about predefined ones. In addition, blockchain technology was employed to monitor every data transfer. On a test system, a fully acknowledged component from IoV was evaluated against a range of security metrics using different threshold detection and security constraints. For spectrum sensing and spectrum detection, a modified spider monkey optimization has been introduced [18].

To implement spectrum management and perform spectrum sensing, Khasawneh et al. [19] presented a routing method. They encoded the sensing data and created a metric to gauge the SUs' sensing behaviors to enhance the efficiency of power distribution and spectrum sensing.

The authors in [20] discusses the throughput performance of decision-based CSS systems for various networks and values of $\kappa - \mu$ fading parameters. The performance of energy detection-based wireless cognitive radio sensor networks is examined in relation to channel and network parameters. The ideal values for the number of CRSs and detection threshold are also obtained [21] for a number of other network parameters. Examines the CR wireless sensor network's throughput and energy efficiency in [22]. More specifically, conditions affecting the sensing (S) channels that involve both noise and α–μ fading are considered.

Tani et al. demonstrate that even in low-power scenarios, residual self-interference at mmWave wideband is a colored noise that significantly degrades detection performance. This approach reduces processing effort and accelerates the white noise case's predicted false alarm probability convergence. The theoretical analysis supporting the superior performance of the suggested whitening strategy over the offline-based approach, especially when applied to the sphericity test, is validated by numerical simulations [23].

The two most common problems with energy detection-noise uncertainty caused by not knowing the signal beforehand and the hidden node problem—are addressed in this work by the M-ary QAM technique employing blockchain. The suggested method yields more accurate results since it uses a 64-QAM signal in a cooperative technique rather than a 32-QAM and PSK signal [24].

The capabilities of full-duplex and cognitive radio systems were described by the author of [25]. For an urban UAV situation, an adaptive signal whitening solution based on the recursive least squares method is suggested to deal with the time-varying colored noise represented by the residual self-interference. We can see from numerical simulations that the adaptive whitening method performs better.

In a CRN, multiband CSS can give SU opportunistic spectrum access. The sensing work in multiband CSS is distributed among SUs according to their residual energy, capabilities, channel conditions, etc. However, in distributed CRNs, SU scheduling to detect a subset of channels is difficult primarily because there is no central entity and the network's conditions change when new SUs join the network.

To improve the system performance of distributed CRNs, they suggested a two-stage, multiband, multiuser CSS method. They developed two optimization problems: one to select a leader for each channel and another to choose associated cooperative SUs. An improved two-stage multiband, multiuser CSS approach was also suggested so that new SUs might participate in the CRN's sensing process by gaining knowledge from the experiences of the current SUs. For this, use the k-means classification technique; create an optimization problem to determine which joining SUs should be used to sense different channels [26].

In order to ensure that SU with similar information felt for the same channel are not picked and that the overall energy consumption is evenly spread among all channels, the authors [27] solve an optimization problem to choose the remaining cooperative SU.

The conclusion drawn from the extensive literature survey is that blockchain technology has recently been widely deployed in a wide range of applications, including

IoT, fog networks, ad hoc networks, cryptocurrencies, etc. [4]. It has peer-to-peer connectivity functionality, which is defined as a collection of units acting collectively to reduce the likelihood of single-point collapse [28, 29]. Distributed ledgers are used in blockchain systems to reduce costs and provide complete anonymity. A system of interconnected blocks stores transactions in a way similar to a traditional, accessible register. The parental unit and a previous block hash make up the unit header, as seen in Figure 1.

Every user of blockchain technology is an owner and has both a personal key and a set of public keys. The confidentiality of the personal key may not be guaranteed. For this reason, the adoption of the digital signature improves the confidentiality of the blockchain. The verification stage and the signing stage are the two phases of the digital signature system. It is entirely safe.

A hash is a distinct key produced by the SHA256 function. Each individual user has a distinct key that serves as their public key. The next user block is aware of this key. It is, in essence, a networked shared key. A crowd-sensing incentive system processes the sensing data that SUs upload using digital watermarking and calculates SU contributions to determine payout amounts [30].

Sun and Xiong [31] created "a consortium blockchain built on many lawfully operational local base stations that addressed the utilization of spectrum resources for transactions," which also offered a loan based payment method and provided a proper price structure. The two primary consensus algorithms, Proof of Stake (PoS) and Proof of Work (PoW), were examined and highlighted the importance of the consensus process in blockchain technology. By utilizing smart contracts, Bayhan et al. [32] presented the two threshold-based voting (TTBV) programme and the spectrum sensing as a service (SPASS) scheme concept. The algorithm can guarantee the exclusion of MU.

A consortium blockchain-based data transaction framework formulated by Chen et al. suggested a reiterative two-fold transaction process. The framework's goals are to get bids from buyers and sellers and to get them to decide how much and how many spectrum resources they wish to trade [33]. Kotobi and Bilen [34] created a blockchain corroboration topology that utilizes the first come, first serve (FCFS) transaction methodology for sales. They have initiated Specoins, a cryptocurrency intended to cover the costs associated with spectrum transfers. However, the aforementioned reports lack a practical selection mechanism and rarely take into account the possibility of MUs while the SU base station is choosing users [35–37]. An approach for assigning cooperative relays in CR networks that makes use of the maximum weight matching (MWM) method is discussed in depth by Cao et al. in their paper [38].

A high priority queuing model with discretion rule is suggested by Nandakumar et al. to manage effectively spectrum handoff in CRNs for priority-aware applications [39]. The authors of [40] propose a blockchain-based, safe information exchange method for edge IoT devices. This mechanism will enable intelligent edge IoT devices to finish challenging tasks. Girmay et al. suggested the LTE and 5G datasets for communication networks [41].

A two-phase method for heterogeneous SU scheduling that senses many channels using a multiband, multiuser CSS system. They take into account the varied channel information that is accessible, requiring up to 100 SU to be assigned in order to sense various channels, which makes this situation relevant to the Internet of Things [42].

Many academics have looked into how to identify harmful users in CR networks using a variety of conventional approaches. Because 5G and 6G systems connect enormous devices and produce more voluminous and dispersed data, managing spectrum data centrally is difficult after distinguishing MU in the spectrum-sensing phase. Attacks by malicious cognitive users and centralized FC design with single-factor failure are significant issues for managing the enormous volume of spectrum sensing data produced in the CR network. Security, privacy, concerns with trustworthiness, and attack vulnerability are just a few of the issues the centralized FC faces. An emerging technology that opens up new research horizons to solve this issue is the blockchain-enabled CR network.

The advantages and disadvantages of using blockchain are given, Immutability: not possible to erase or replace recorded data. Transparency: network members can verify data recorded in the blockchain. Censorship: there is no control at single party. Traceability: easy to tracing of changes on the network. The disadvantages are, Speed and performance: slower than normal traditional database. Implementation coast: high compare with traditional one. Data modification: not allow to easy modification of data once recorded.

The proposed work offers a secure CSS technique based on a blockchain-enabled CR network as well as ED while fighting against MU assaults to increase spectrum-sensing precision. The existing one, the sensing data is not stored in anywhere. Therefore, the SUs do not properly use the sensing data. While using this model, the unused spectrum details are available in the blockchain, and whenever the SUs need them, they can make use of the data and utilize the same. In this paper, the main contributions are the following:

(i) Formation of a blockchain-enabled CR network

(ii) Proposed flexible threshold spectrum ED method and MU detection

3. Scenario and Methodology

Each CR user does spectrum sensing to determine the status of the spectrum bands and provides the results to the blockchain network. Unfortunately, the spectrum sensing data obtained from MU does not provide the PU spectrum band's initial state. These MUs are harming the effectiveness of a CR network. Blockchain was utilized to record data on spectrum sensing, spectrum mining and bidding, spectrum auction outcomes, spectrum access history, and idle spectrum bands after getting findings from spectrum sensing. Blockchain offers a secure and trusted environment that guarantees the validity and integrity of data storage, enabling the cooperative administration of resources among various subjects.

In the proposed method, initially the blocks of SUs and PUs are created. Next, identify the spectrum using an energy detection technique. Thirdly, a blockchain is used to verify the participating nodes. Finally, MU is identified and distinguished as a trustworthy user. Below, these actions are described in Figure 2.

Block creation: PUs and SUs are transformed into blockchain blocks at the very beginning. A distributed ledger of nodes with information about PUs and SUs credentials is generated for this purpose. Both a public key and a private key will be present. Public key information includes details on shared data pertaining to various units in CR networks, such as the state of being SU or PU. While private keys hold node-specific information such as their location and authentication code.

ED: The main use of the energy detection method in spectrum sensing is here. We assume that the receiving signal's sampling rate is t and that there is a bandwidth of W Hz. We have two hypotheses: hypothesis 1 demonstrates that the signal is detected and is merely noise, while hypothesis 0 shows that the signal is detected and is a combination of noise and the signal transmitted by the PU.

MU Detection: Following completion of all processes required for spectrum detection among nodes, reliable users and MUs are found using the suggested mechanism, which uses digital signatures to confirm participating nodes based on public and private keys. There are two sorts of mistakes: miss detection and false alarm, which can result in errors in the detection of valid users and MU.

The proposed flexible threshold spectrum energy detection method enhances CSS network through the use of blockchain technology. Energy is identified when the CR network programme's units are constructed. After the nodes have finished the necessary spectral identification procedure, hostile as well as approved clients are separated. By verifying CSS units with digital signatures while accounting for combined confidential as well as accessible identities, the proposed technique allows customer authentication. There were two types of errors during the identification of a MU and valid users: false alarm and missed detections. The suggested morphology, spectral regulation, and CSS improve network performance.

3.1. Methodology. Three steps created from the suggested methodology serve as the foundation for all simulations.

(1) These methods assume that there are n SU, and one PU has been taken into account for convenience. Using blockchains, SU and PU are linked to one another in Step 1. Decentralized blocks are used to establish the connection between PU and SU. On the basis of their licensing, blocks of PUs and SUs are discriminated against. The user's service provider issues the licenses. When blocks are produced, the user's license is checked to see if they should be primary or secondary. If the PU detects the spectrum, the P block will be assigned; otherwise, the S block will be used.

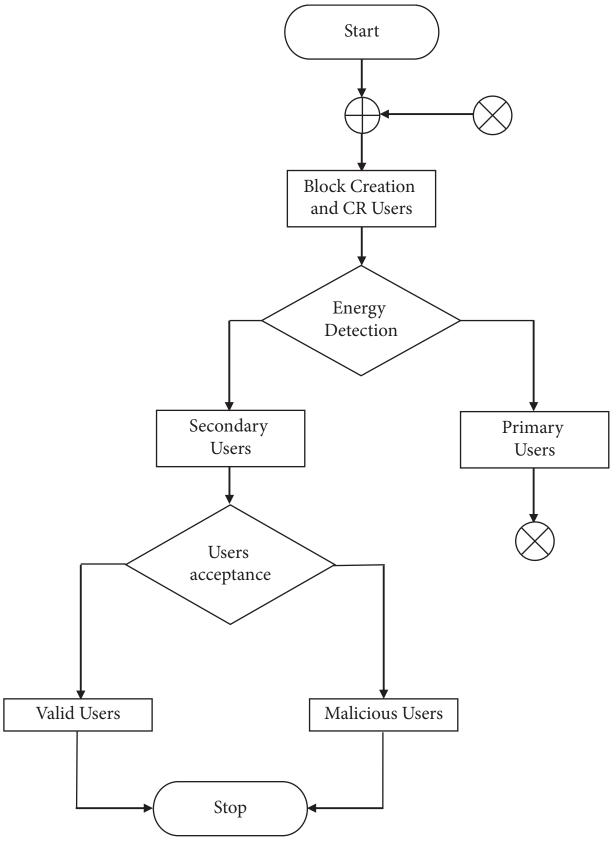

FIGURE 2: Flow diagram of proposed work.

(2) The energy detection method is used to sense the spectrum. SU will use the cooperative sensing method when attempting to access the spectrum. Every node will feel the spectrum and form two hypotheses in this scenario. When the spectrum is felt and the result is a noise signal, hypothesis 1 will be correct. When the output received is a combination of noise and an energy signal, hypothesis 0 will be true. Therefore, these two hypotheses will serve as the basis for the sensing output. If the first hypothesis is correct, then the mean channel is empty and the result of the spectrum sensing will be positive; otherwise, the channel is busy and the result of the sensing is negative. The next algorithm validates these sensing results.

(3) The results of each participating node's energy detection are then checked and verified. Verification of the user's digital signatures indicates that the transaction is valid users; otherwise, it is classified as MU. In this approach, the private key is validated after the public key, both of which help to reach a consensus regarding user validation. The equations described in the previous section are used to compute the probability of MU and to detect the valid users, miss detection, and false alarm.

3.2. Blockchain Formulation. The CR network in this proposed methodology uses the blockchain, and because the PU and SU are connected via peer-to-peer technology, the entire network is planned to be decentralized [43]. Only one PU and the number of SU are taken into consideration while analyzing the suggested technique. Figure 3 depicts the full architecture of the proposed blockchain-based spectrum sensing in CR networks.

The term "generic user" refers to CR networks, SU, and PU. The connection of all CR users is referred to as decentralized. The users have established a hash connection with one another. Each block in blockchain technology contains the following data:

Personal key: This is a block's unique identity key within the CR user. Only the private key is known to the CR user. A generated 16-bit key is used as a private key in the suggested process.

Sensing Outcome Hash (Public key): It is described as the block's data portion. It includes information on the specific outcomes of energy identification-based sensing. Hash it is described as a distinctive key produced by the SHA256 algorithm. Each user has their own special key, which is also known as their public key. The next block of the user is shown this key. This key may be distributed for the network's consideration.

Previous hash: It is described as the hash value's previous node. A peer-to-peer link is established as a result. Under these circumstances, complete nodes will take part in cooperative sensing.

The circled blocks, as shown in Figure 3, are generated by MU. These blocks are identified and removed from the current chain since the information present in these blocks are not correct.

The Algorithm 1 suggestion is implemented for the creation of blocks for CR users. The hashes that act as public keys are produced using the SHA256 method. It is a kind of cryptographic hash function that generates a key with a fixed size as an output from a variable-sized input. The current time of the machine is used to generate different keys. As a result, the block's time stamp is used to create each node's unique hash. The private key is also generated using a random function. The sensing output is stored in the block as a consequence of Algorithm 2 being applied to each participating node.

3.3. Energy Detection (ED).

The energy detection approach has been employed for reliable radio spectrum sensing. Basic sensing techniques like ED do not require any prior knowledge of the PU signal to operate. A specific region of the spectrum is measured by the energy received. To determine if the channel is open, the detector compares the observed energy to a threshold value. The extended sensing time required by this technology to improve the SNR results in increased power consumption, and the change in noise levels has a significant impact on detector performance. A CR must estimate the energy level in a spectrum band (or channel) for a specific amount of time in order to perform ED. In this topology, energy detection-based spectrum sensing is adopted. Figure 2 depicts the spectrum sensing topology.

The ED method develops a model that can be represented based on the statistical value of the signal energy that the cognitive user received.

$$Y(n) = \begin{cases} \omega(n), & \mathscr{H}_0, \\ s(n) + \omega(n), & \mathscr{H}_1, \end{cases} \tag{1}$$

where $s(n)$ is the PU signal, $\omega(n)$ is the noise, $Y(n)$ is the signal received at the cognitive node, $\mathscr{H}_0$ is the idle channel, and $\mathscr{H}_1$ is the channel occupied by the PU.

Spectrum is detected using the energy detection approach in Algorithm 2. SU will use the cooperative sensing method when attempting to access the spectrum. Every node will feel the spectrum and form two hypotheses in this scenario. When the spectrum is felt and the result is a noise signal, $\mathscr{H}_1$ will be correct. When the output received is a combination of noise and an energy signal, $\mathscr{H}_0$ will be true. Therefore, these two hypotheses will serve as the basis for the sensing output. If the first hypothesis is correct, then the mean channel is empty and the result of the spectrum sensing will be positive; otherwise, the channel is busy and the result of the sensing is negative. The results of the subsequent algorithms are then verified. The proposed flexible threshold spectrum energy detection algorithm is given below.

Thus, it is possible to assess the probabilities of miss detection of P_d and false alarm P_f utilizing

$$P_d = P\left(Y^1 > \wedge | \mathscr{H}_{1,}\right), \tag{2}$$

$$P_f = P\left(Y^1 > \wedge | \mathscr{H}_0\right), \tag{3}$$

where $\wedge$ is the decision threshold. P_f can be written as

$$P_f = \int_{\wedge}^{\infty} f_{Y\cdot}(y)\mathrm{d}y, \tag{4}$$

$$P_f = \frac{1}{\left(2^d\Gamma(d)\right)} \int_{\wedge}^{\infty} y^{d-1} e^{-(y/2)}\mathrm{d}y. \tag{5}$$

The above equation can be rewritten as

$$P_f = \frac{1}{2\Gamma(d)} \int_{\wedge}^{\infty} \left(\frac{y}{2}\right)^{d-1} e^{-(y/2)}\mathrm{d}y. \tag{6}$$

Substituting, $y/2 = t, \mathrm{d}y/2 = \mathrm{d}t$ and modifying the integration's bounds to $\wedge/2$ to ∞, the following is obtained

$$P_f = \frac{1}{2\Gamma(d)} \int_{\wedge/2}^{\infty} t^{d-1} e^{-(t)}\mathrm{d}t, \tag{7}$$

$$\begin{aligned} P_f &= \frac{\Gamma(d, (\wedge/2))}{\Gamma(d)} \\ &= P\left(Y^1 > \wedge | \mathscr{H}_0\right), \end{aligned} \tag{8}$$

where Γ (.) is the Gamma function. P_d can be written as

$$\begin{aligned} P_d &= 1 - F_{Y\cdot}(\wedge) \\ &= P\left(Y^1 < \wedge | \mathscr{H}_{1,}\right). \end{aligned} \tag{9}$$

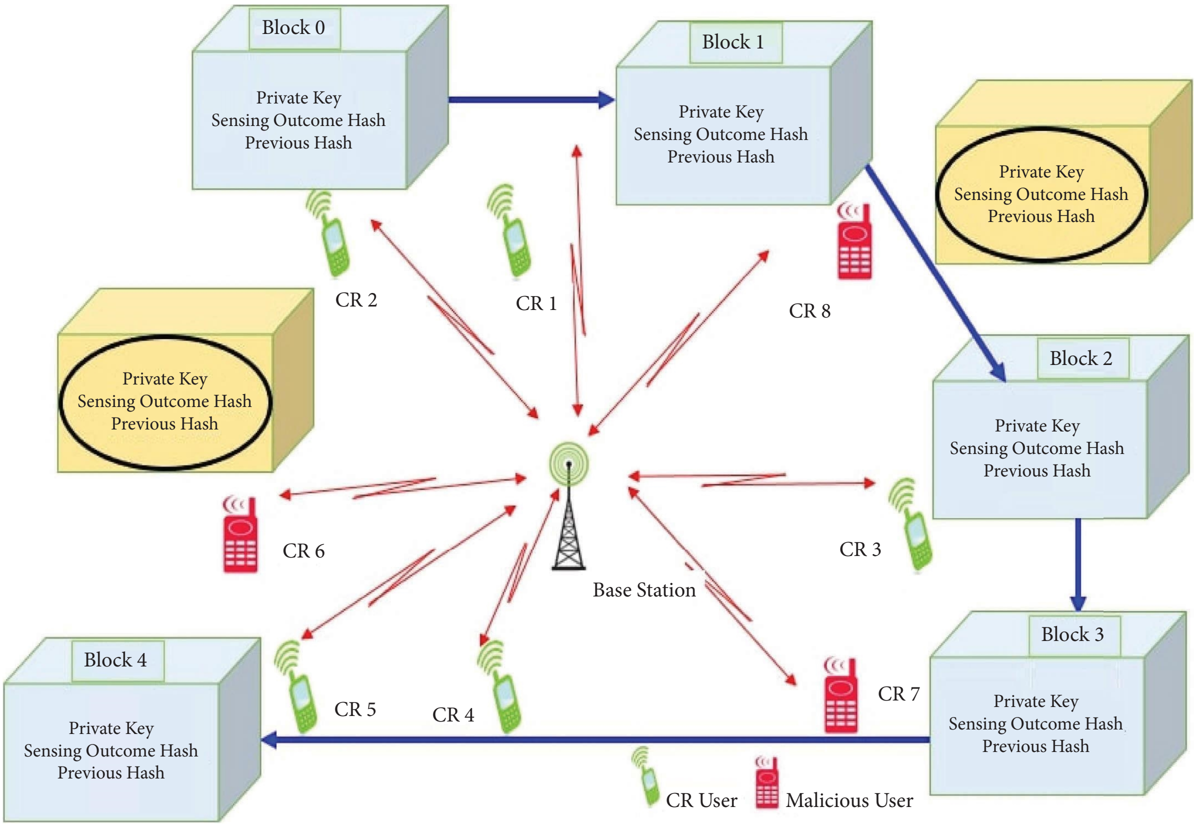

Figure 3: Architecture of the proposed blockchain-based spectrum sensing in CRN.

```
Input: A group of N primary node network.
Blockchain consists of One Primary Node P and $N-1$ secondary user node from $S_1$ to $S_{\{k-1\}}$.
Output: Blocks are formed on various nodes of the cognitive network.
for $j = 1$ to $N$
if authorized user then
    Primary block
else
    Secondary node $S_{\{k-2\}}$
end if
end for
```

Algorithm 1: Creation of blockchain on CR users.

```
Input: Think about the $N - 1$ secondary user spectrum and the primary user spectrum. Here, the PU and SU channel types are distinguished.
Output: A suggested flexible threshold spectrum energy detection algorithm helps to produce sensing outcomes. Channel Sense
if $y(n) = \omega(n)$, then
    Primary Users $\mathscr{H}_{0,}$
else
    $y(n) = s(n) + \omega(n)$, then
    Secondary Users $\mathscr{H}_{1,}$
end if
```

Algorithm 2: Proposed flexible threshold spectrum energy detection algorithm using blockchain.

```
Input: After energy detection, $N$ sets of $M - 1$ results and $y_{\{n-1\}}$ are received as input. Now, the results are validated using the
  public key and private key components of digital signatures.
Valid User and MU as Output
for the $y = 1$ to $n$ choice,
if public key is validated
  if the private key is confirmed.
    Valid User is discovered
  else
    MU is found
  end if
end if
end for
```

Algorithm 3: MU identification using digital signature verification.

Cumulative distribution function (CDF) can be depicted as

$$F_y(y) = 1 - Q_d(\sqrt{\lambda}, \sqrt{\wedge}). \tag{10}$$

In addition, $Q_d(x) = 1/2\pi \int_x^{\infty} e^{-t^2/2} dt$, is gaussian function, we assume that the system has $N(N < M)$ MU. Without losing generality, it can be imagined that SU, where $i = 1, 2, 3 \ldots N$, are evil and constantly give forth erroneous information with extreme values. The observed band's state, as suggested by the misleading information, is always the exact opposite of reality.

3.4. MU Detection. Energy is also recognized as the block that forms the CR network. MU and valid users are separated when the nodes have finished the necessary procedure of spectrum detection. With the aid of the suggested approach, user identification is accomplished by validating the nodes in the CR network using digital signatures, taking into consideration both public and private keys. During the identification of an authorized as well as a hostile customer, two sorts of errors occurred: false alarms and missed alerts.

Finally, in Algorithm 3, the ED result of each individual participating node is verified and validated. If the user's digital signatures are verified, it means it is a valid user; otherwise, it will be termed MU. In this algorithm, first the public key is verified and then the private key, which both contribute to the consensus on the validation of the user. Similarly, the probability of MU and valid user detection, miss detection, and false alarm are calculated by using the equations presented in the previous section.

The false alarm, missed detection, and authenticated user identification are discussed in depth below. A probability measurement shows the failure to distinguish between a legitimate and a malicious client. The possibility is determined by dividing the total iterations by the total number of missed detections. It can be expressed as shown in the following equation:

$$\begin{aligned} \mathrm{FA}(P) &= 1 - P^{\mathrm{MD}} \\ &= \frac{\theta^M}{\eta}, \end{aligned} \tag{11}$$

where FA(P) is the probability of false alarm, P^{MD} is the probability of malicious user identification, M is the no. of times to identify the authentic client, and η is the no. of iterations.

It is calculated to determine if the authenticated user was mistakenly identified and is represented mathematically as shown in the following equation:

$$\begin{aligned} MD(P) &= 1 - P^{AD} \\ &= \frac{\theta^A}{\eta}, \end{aligned} \tag{12}$$

where MD(P) is the probability of missed a detection, θ^A is the number of times to find an authenticated user, P^{AD} is the authenticated user probability.

It is characterized as the effective discovery of rogue nodes within the CR network community. The number of rouge nodes found divided by the number of iteration yields a probability of malicious user detection. It is formulated mathematically as follows:

$$P^{\mathrm{MD}} = \frac{\theta'^M}{\eta}. \tag{13}$$

It is defined as the CR network system correctly recognizing verified connections. The probability of authenticated user discovery is calculated by dividing the number of authorized sites found by the frequency of iteration. It is formulated mathematically as follows:

$$P^{\mathrm{AD}} = \frac{\theta'^A}{\eta}. \tag{14}$$

Relative trustworthiness for a user can be calculated as follows:

Table 2: Simulation parameter.

Parameter	Value/range
Size of the system	2000 m $*$ 2000 m
No. of primary user transmitter	1
No. of cognitive users	200
Number of samples	200 to 400
Primary user transmit power	−23 dBm to +5 dBm
Secondary user transmit power	10 dBm, 20 dBm
Frequency	470–790 MHz
Modulation coding scheme index	1–28
TDD uplink and downlink	1 : 1 [41]

$$a = \min\left(\frac{d_1}{d_2}, \frac{d_2}{d_1}\right). \tag{15}$$

Which can be derived as follows, the distance between users can be estimated using location coordinates. For simplification in calculating the distance between users, we consider the location in a (2-D) plane, where $(x_{\text{si}}, y_{\text{si}})$ are the x and y coordinates of the i^{th} secondary user, (x_p, y_p) are the x and y coordinates of an existing primary user and (x_m, y_m) are the x and y coordinates of the MU. The distance d_1 between the i^{th} SU and the PU is given by

$$d_1 = \sqrt{\left(x_{\text{si}} - x_P\right)^2 + \left(y_{\text{si}} - y_p\right)^2}, \quad i = 1, 2, 3 \ldots\ldots. N, \tag{16}$$

where i is the particular SU and the distance d_2 between the M^{th} MU and any good SU is also given by

$$d_2 = \sqrt{\left(x_m - x_{\text{si}}\right)^2 + \left(y_m - y_{\text{si}}\right)^2}, \quad i = 1, 2, 3 \ldots\ldots N. \tag{17}$$

The decision-making node can now use the estimated distance obtained using the coordinates to determine how trustworthy any of the SU in the system can be.

4. Results and Discussion

This section evaluates the suggested approach's performance based on ED and false alarms. When choosing the PU, the CSS network with a larger number of CRs may encounter significant delays. In order to determine how many ideal CRs are actually used to make the final decision, the enormous number must be optimized. The following research has been done to verify the presence of the anticipated blockchain-based security: The simulation of the proposed technique has been obtained by modelling the system and realizing it in the MATLAB 2014 environment. Table 2 lists the simulation transmitter specs for the suggested system.

P_d and P_f, acquired from 7500 detection rounds of simulation, are shown here under the specified average SNR and number of MUs. In the simulation, three algorithms—the noncooperative approach, the currently used MWM cooperative method, and the suggested flexible threshold spectrum energy detection method based on local decision results—are compared. First, we assume that the system has just $M = 5$ MU.

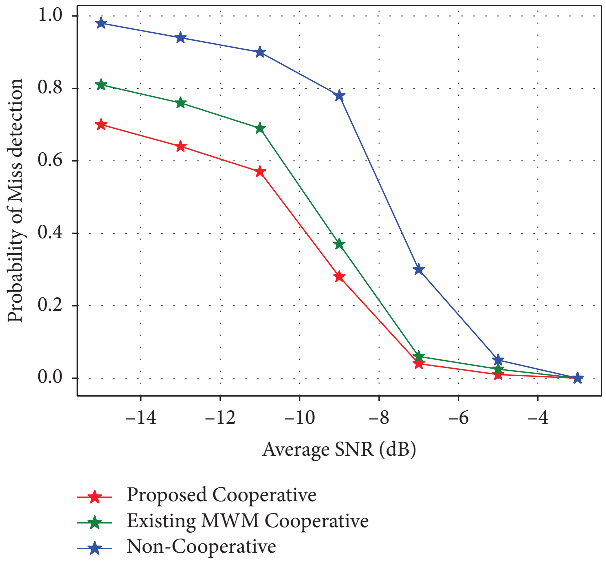

Figure 4: P_d vs SNR.

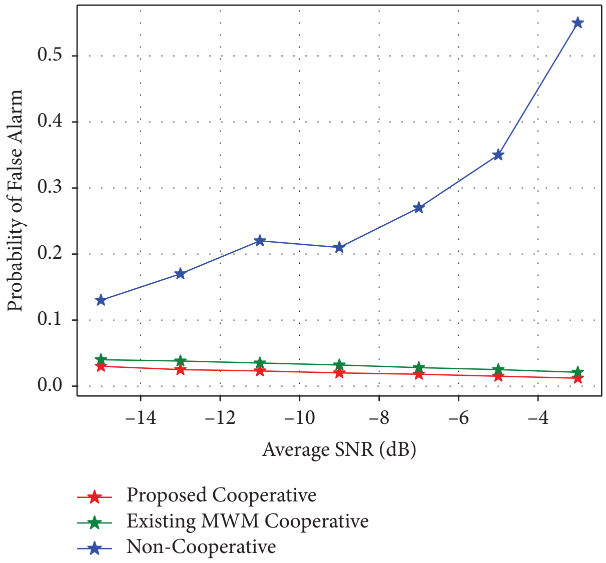

Figure 5: P_f vs SNR.

A CR network with $N = 200$ SUs, of which M are MU, and CU. A PU is present and may be sending out random QAM signals with a power of $\sigma_s^2 = 1$. Channels that connect SU and PU. With the same noise power $\sigma_n^2 = 1$, Rayleigh fading occurs. The range of average SNR values for various SUs is −15 dBm to −5 dBm, and they are all equal. SUs carry out energy detection, (2), and (3) offer accurate detection data that can be converted into quantified energy detection outcomes. Malicious SUs propagate erroneous information with extreme values on a constant basis. The system's highest permitted $P_f = 1\%$, which is uniformly quantized with $m = 16$ bits. The roll-off factors α and β are empirically determined at 0.5 and 0.95, respectively.

Figures 4 and 5 compare P_d and P_f side by side. In both pictures, the first curve represents system performance

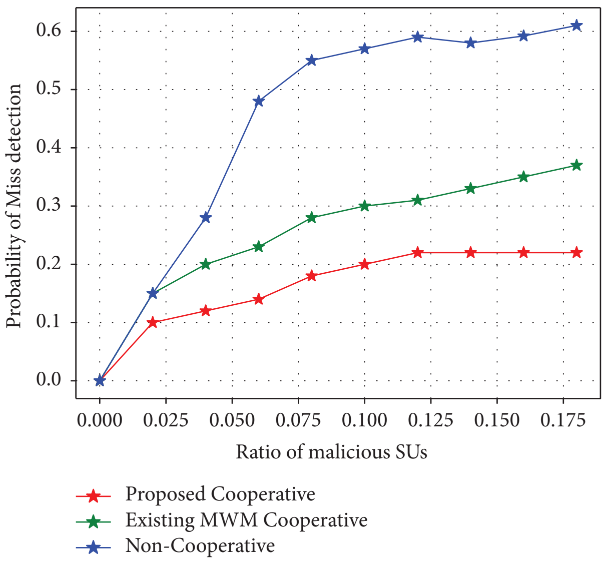

FIGURE 6: P_d vs malicious SU.

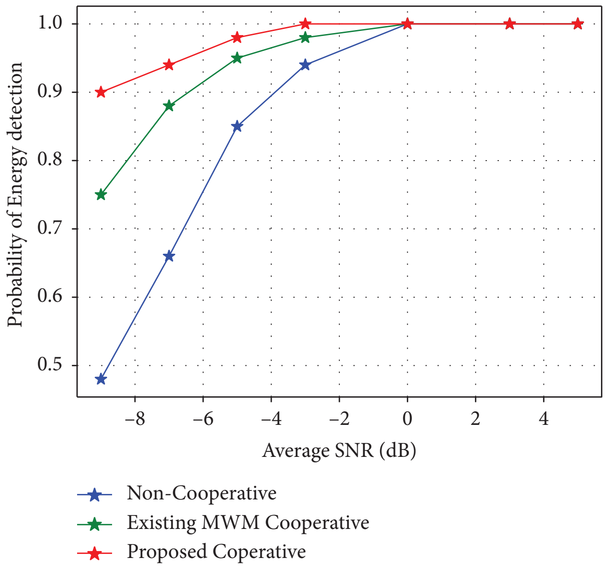

FIGURE 8: Probability of energy detection vs SNR.

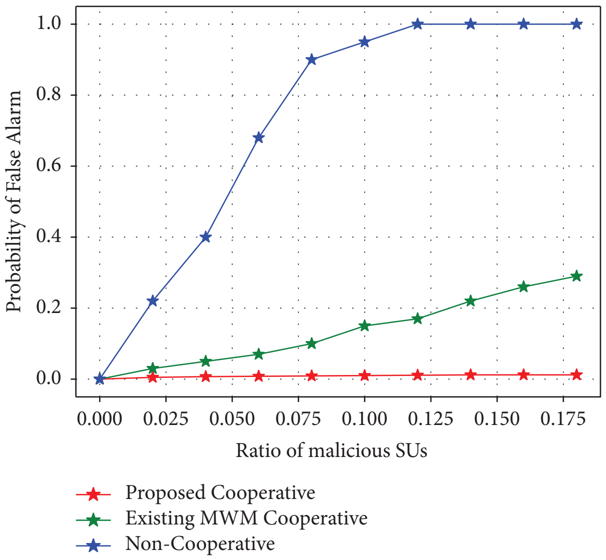

FIGURE 7: P_f vs malicious SU.

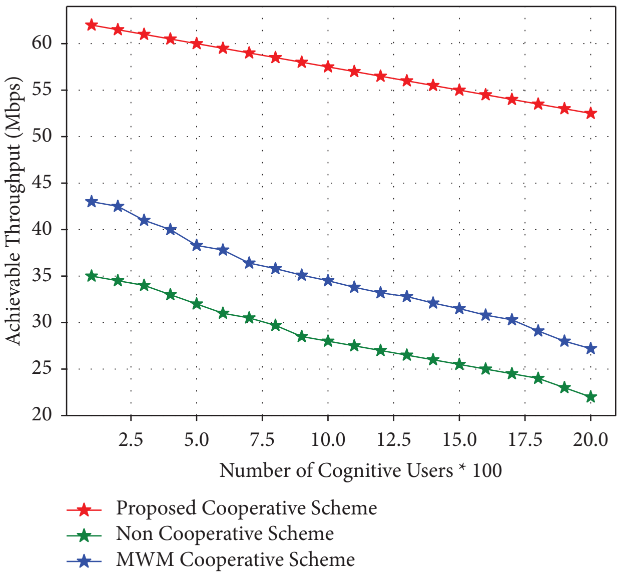

FIGURE 9: Achievable throughput of proposed cooperative scheme.

under ideal circumstances (i.e., when there is only one MU), and the second curve represents circumstances in which there are two harmful users. As can be seen, P_d and P_f suffer greatly when MU people are present. The third curves demonstrate that the proposed algorithms may greatly reduce incorrect information and enhance system performance to a level that is close to optimum.

When the average SNR is fixed at −10 dBm, the fixed ratio of the harmful user is compared with various methods of different parameters of P_d and P_f, as evaluated in (8) and (9) for varying ratios of malicious SUs, as shown in Figures 6 and 7. It can be clearly identified from the first curve in both graphs that system performance rapidly declines as the proportion of malicious SUs rises. The scatterplots in the figures represent the matching simulation findings. When the percentage of malicious users is up to 18%, P_d it is lowered by about 60% and P_f by more than 98% when compared to the noncooperative scenario without a MU. When techniques that inhibit MUs are utilized, performance decline can be successfully made up for. Comparing the proposed strategy to the current one, larger gains P_d can be made with less loss P_f.

Figure 8 shows the probability of ED in response to SNR. When compared to the signal, which is QAM, the ED method uses an additive white Gaussian noise (AWGN) channel. The availability of the spectrum is determined by the detection of noise and energy signals. If the energy value exceeds the threshold, indicating the use of a spectrum, the probability of detection is close to unity. On the other hand, the risk of a false alert predominates if its value goes below the threshold. This graph shows the likelihood of detecting energy in relation to the SNR for different sample counts. The graph clearly shows that as sample counts rise, the likelihood of detection gets closer to 1.

Figure 9 shows a comparison of the proposed cooperative scheme's throughput to that of a noncooperative scheme and the current MWM cooperative scheme. It has been discovered that the suggested strategy outperforms conventional methods for a larger number of cognitive users by a factor of 15%.

5. Conclusion

This research proposes a new CSS method for suppressing harmful users in CR systems. A method for managing spectrum sensing and identifying MU has been developed using a blockchain-based security enhancement system. The MU, who should be identified on the CR network, is completely collapsing the system's performance. In addition to spectrum sharing, the challenge in such networks is to manage this security issue in real-time. A strong CR architecture and protocol that can guarantee the integrity of the data transferred between SU for spectrum sensing is necessary for this. In the blockchain-enabled CR network, the proposed flexible threshold spectrum energy detection algorithm distinguishes between legitimate and fraudulent CR users with an accuracy of 63.5% compared to the traditional adaptive threshold spectrum energy detection technique. MU occasionally provides fake sensing data using the CR network, which reduces system performance. The CSS network has implemented blockchain-based security, enhancing system performance and spectrum sensing. According to a comparison analysis, the proposed strategy has produced the best spectrum management and security outcomes for the CR network. The suggested technique outperforms the current method in terms of missed detection probability with a minor loss in false alarm probability, according to theoretical analysis and simulation findings. In addition, the proposed method is less complex than the current one in terms of complexity, and a 15% throughput is increased.

Data Availability

Data sharing does not apply to this article as no datasets were generated or analysed during the current study.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Authors' Contributions

S. Nandakumar conceptualized the study, performed the visualization, supervised the study, and reviewed and edited the manuscript. D Balakumar performed formal analysis, performed investigation, proposed the methodology, performed the software analysis, validated the study, and prepared the original draft. All authors have read and agreed to the published version of the manuscript.

References

[1] Y. C. Liang, *Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence*, Springer Nature, Chengdu, China, 2020.

[2] X. Fan and Y. Huo, "Blockchain based dynamic spectrum access of non-real-time data in cyber-physical-social systems," *IEEE Access*, vol. 8, pp. 64486–64498, 2020.

[3] M. Grissa, A. A. Yavuz, B. Hamdaoui, and C. Tirupathi, "Anonymous dynamic spectrum access and sharing mechanisms for the CBRS band," *IEEE Access*, vol. 9, pp. 33860–33879, 2021.

[4] A. Sajid, B. Khalid, M. Ali, S. Mumtaz, U. Masud, and F. Qamar, "Securing cognitive radio networks using blockchains," *Future Generation Computer Systems*, vol. 108, pp. 816–826, 2020.

[5] B. Sarala, S. Rukmani Devi, and J. J. J. Sheela, "Spectrum energy detection in cognitive radio networks based on a novel adaptive threshold energy detection method," *Computer Communications*, vol. 152, pp. 1–7, 2020.

[6] G. Eappen and T. A Shankar, "Survey on soft computing techniques for spectrum sensing in a cognitive radio network," *SN Computer Science*, vol. 1, pp. 1–36, 2020.

[7] K. Rapetswa and L. Cheng, "Convergence of mobile broadband and broadcast services: a cognitive radio sensing and sharing perspective," *Intelligent and Converged Networks*, vol. 1, pp. 99–114, 2020.

[8] X. Fu, H. Wang, and P. Shi, "A survey of Blockchain consensus algorithms: mechanism, design and applications," *Science China Information Sciences*, vol. 64, no. 2, pp. 121101–121115, 2021.

[9] M. Patnaik, G. Prabhu, C. Rebeiro, V. Matyas, and K. Veezhinathan, "ProBLeSS: a proactive blockchain based spectrum sharing protocol against SSDF attacks in cognitive radio IoBT networks," *IEEE Networking Letters*, vol. 2, pp. 67–70, 2020.

[10] C. Rajesh Babu and B. Amutha, "Blockchain and extreme learning machine based spectrum management in cognitive radio networks," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 10, p. e4174, 2022.

[11] L. Zhang, Z. Wei, L. Wang, X. Yuan, H. Wu, and W. Xu, "Spectrum sharing in the sky and space: a survey," *Sensors*, vol. 23, no. 1, p. 342, 2022.

[12] T. T Anh, N. C Luong, Z. Xiong, D. Niyato, and D. I Kim, "Joint time scheduling and transaction fee selection in blockchain-based RF-powered backscatter cognitive radio network," 2020, https://arxiv.org/pdf/2001.03336.pdf.

[13] V. Srivastava, P. Singh, P. K. Malik et al., "Innovative spectrum handoff process using a machine learning-based metaheuristic algorithm," *Sensors*, vol. 23, no. 4, p. 2011, 2023.

[14] D. Bilibashi, E. M. Vitucci, V. Degli-Esposti, and A. Giorgetti, "An energy-efficient unselfish spectrum leasing scheme for cognitive radio networks," *Sensors*, vol. 20, no. 21, p. 6161, 2020.

[15] H. Xu, H. Gao, C. Zhou, R. Duan, and X. Zhou, "Resource allocation in cognitive radio wireless sensor networks with energy harvesting," *Sensors*, vol. 19, no. 23, p. 5115, 2019.

[16] M. A. Khan, M. M. Jamali, T. Maksymyuk, and J. Gazda, "A blockchain token-based trading model for secondary spectrum markets in future generation mobile networks," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 7975393, 12 pages, 2020.

[17] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BIoV: a cognitive radio technique for

blockchain- enabled internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4005–4015, 2021.

[18] G. Dinesh, P. Venkatakrishnan, and K. M. A. Jeyanthi, "Modified spider monkey optimization—an enhanced optimization of spectrum sharing in cognitive radio networks," *International Journal of Communication Systems*, vol. 34, no. 3, Article ID e4658, 2021.

[19] M. Khasawneh, A. Azab, and A. Agarwal, "Towards securing routing based on nodes behavior during spectrum sensing in cognitive radio networks," *IEEE Access*, vol. 8, pp. 171512–171527, 2020.

[20] S. Nallagonda, A. Bhowmick, and B. Prasad, "On selection of parameters for cooperative spectrum sensing schemes over $\kappa-\mu$ fading channels," *IETE Journal of Research*, pp. 1–11, 2022.

[21] S. Nallagonda, "Spectrum sensing performance of wireless cognitive radio sensor network with hard decision fusion over generalized$\alpha-\mu$fading channels," *International Journal of Communication Systems*, vol. 36, no. 10, Article ID e5498, 2023.

[22] S. Nallagonda, "Energy-efficiency performance of wireless cognitive radio sensor network with hard-decision fusion over generalized $$\alpha-\mu $$ fading channels," *Wireless Networks*, vol. 29, no. 6, pp. 2759–2771, 2023.

[23] A. Tani, D. Marabissi, and R. Fantacci, "Efficient real-time whitening for blind eigenvalue-based detection in mmWave full duplex cognitive radio," *IEEE Transactions on Wireless Communications*, vol. 22, no. 9, pp. 6213–6226, 2023.

[24] D. Balakumar and S. Nandakumar, "Cognitive radio spectrum sensing-based QAM technique using blockchain," *International Journal of Distributed Sensor Networks*, vol. 2023, Article ID 7225260, 16 pages, 2023.

[25] A. Tani and D. Marabissi, "Adaptive blind spectrum sensing for mmWave full duplex cognitive aerial BS," in *European Wireless 2023*, pp. 1–6, VDE, Frankfurt, Germany, 2023.

[26] A. Gharib, W. Ejaz, and I. Mohamed, "Distributed learning-based multi-band multi-user cooperative sensing in cognitive radio networks," in *Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, Abu Dhabi, UAE, October 2018.

[27] A. Gharib, W. Ejaz, and M. Ibnkahla, "Enhanced multiband multiuser cooperative spectrum sensing for distributed CRNs," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 256–270, 2020.

[28] M. Karimi, S. M. S. Sadough, and M. Torabi, "Improved joint spectrum sensing and power allocation for cognitive radio networks using probabilistic spectrum access," *IEEE Systems Journal*, vol. 13, no. 4, pp. 3716–3723, 2019.

[29] M. Hu and Q. Zhu, "Secondary user utility optimization algorithm on cooperative spectrum sensing," in *Proceedings of the 2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, pp. 463–467, Chengdu, China, December 2019.

[30] Y. He, M. Li, H. Li, L. Sun, and K. Xiao, "A blockchain based incentive mechanism for crowdsensing applications," *Journal of Computer Research and Development*, vol. 56, no. 3, pp. 544–554, 2019.

[31] J. Sun and G. Xiong, "Credit payment for radio resources transactions based on consortium blockchain in SCMA mMTC," *Acta Electonica Sinica*, vol. 47, no. 8, p. 1677, 2019.

[32] S. Bayhan, A. Zubow, and A. Wolisz, "Spass: spectrum sensing as a service via smart contracts," in *Proceedings of the 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pp. 1–10, Seoul, Korea (South), October 2018.

[33] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110–9121, 2019.

[34] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 32–39, 2018.

[35] D. Li, L. Qiu, J. Liu, and C. Xiao, "Analysis of behavioral economics in crowdsensing: a loss aversion cooperation model," *Scientific Programming*, vol. 2018, Article ID 4350183, 18 pages, 2018.

[36] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: applications, opportunities and challenges," *Journal of Network and Computer Applications*, vol. 177, Article ID 102857, 2021.

[37] X. Han, Y. Yuan, and F. Y. Wang, "Security problems on blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 45, no. 1, pp. 206–225, 2019.

[38] T. Cao, W. Xie, C. Wang, and Y. Xu, "A MWM relay assignment strategy based on spectrum availability for cognitive radio networks," in *Proceedings of the 2013 International Conference on Wireless Communications and Signal Processing*, pp. 1–6, Hangzhou, October 2013.

[39] S. Nandakumar, G. Sai Bharadwaj, and D. Srivastava, "Efficient spectrum handoff using hybrid priority queuing model in cognitive radio networks," *Wireless Personal Communications*, vol. 108, no. 1, pp. 203–212, 2019.

[40] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: a consortium blockchain-based efficient and incentive approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6367–6378, 2019.

[41] M. Girmay, V. Maglogiannis, D. Naudts, M. Aslam, A. Shahid, and I. Moerman, "Technology recognition and traffic characterization for wireless technologies in ITS band," *Vehicular Communications*, vol. 39, Article ID 100563, 2023.

[42] A. Gharib, W. Ejaz, and M. Ibnkahla, "Scalable learning-based heterogeneous multi-band multi-user cooperative spectrum sensing for distributed IoT systems," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1066–1083, 2020.

[43] A. Khanna, P. Rani, T. H. Sheikh, D. Gupta, V. Kansal, and J. Rodrigues, "Blockchain-based security enhancement and spectrum sensing in cognitive radio network," *Wireless Personal Communications*, vol. 127, no. 3, pp. 1899–1921, 2022.