Journal Pre-proof

Securing Cognitive Radio Networks using blockchains

Adnan Sajid, Bilal Khalid, Mudassar Ali, Shahid Mumtaz,
Usman Masud, Farhan Qamar

PII: S0167-739X(19)31599-7
DOI: https://doi.org/10.1016/j.future.2020.03.020
Reference: FUTURE 5525

To appear in: *Future Generation Computer Systems*

Received date : 16 June 2019
Revised date : 25 January 2020
Accepted date : 7 March 2020

Please cite this article as: A. Sajid, B. Khalid, M. Ali et al., Securing Cognitive Radio Networks using blockchains, *Future Generation Computer Systems* (2020), doi: https://doi.org/10.1016/j.future.2020.03.020.

Securing Cognitive Radio Networks using Blockchains

Adnan Sajid[1], Bilal Khalid[1], Mudassar Ali[1], Shahid Mumtaz[2], Usman Masud[1], Farhan Qamar[1]

***Abstract*—Due to the increase in industrial applications of Internet of Things (IoT), number of internet connected devices have been increased accordingly. This has resulted in big challenges in terms of accessibility, scalability, connectivity and adaptability. IoT is capable of creating connections between devices on wireless medium but the utilization of scarce spectrum in efficient manner for the establishment of these connections is the biggest concern. To accommodate spectrum allocation problem different radio technologies are being utilized. One of the most efficient technique being used is cognitive radio, which dynamically allocate the unlicensed spectrum for IoT applications. Spectrum sensing being the fundamental component of Cognitive Radio Network (CRN) is threatened by security attacks. Process of spectrum sensing is disturbed by the malicious user (MU) which attacks the primary signal detection and affects the accuracy of sensing outcome. The presence of such MU in system, sending false sensing data can degrade the performance of cognitive radios. Therefore, in this article a blockchain based method is proposed for the MU detection in network. By using this method an MU can easily be discriminated from a reliable user through cryptographic keys. The efficiency of the proposed mechanism is analyzed through proper simulations using MATLAB. Consequently, this mechanism can be deployed for the validation of participating users in the process of spectrum sensing in CRN for IoTs.**

***Keywords*—Spectrum Sensing, Cognitive Radio Networks, Blockchains, Malicious User Detection.**

I. Introduction

With the increase in number of communication devices, utilization of spectrum in efficient manner is the biggest challenge. Cognitive Radio Networks (CRN) consists of intelligent wireless devices which can efficiently sense the medium and effectively utilize the vacant or under-utilized spectrum. Secondary Users (SUs) are enabled by cognitive radios to opportunistically access the spectrum unused by the Primary Users (PUs). There are two basic objectives of Cognitive Radio Medium Access Control (CR MAC): controlling interference and avoiding collision between SUs. Medium Access Control (MAC) has an important role in several cognitive radio functions such as spectrum sensing, mobility, resource allocation and spectrum sharing [1]. MAC layer is used for the management and coordination of communication over wireless channels. In the presence of dynamic radio surroundings, the CRN access protocol shall create variety of choices in real time. These requirements makes realization of CRN a challenging task compared to standard access protocols in the present static spectrum policies. In recent decades, the thought of Opportunistic Spectrum Access (OSA) has emerged to considerably increase spectrum utilization [2]. For this, the SUs ought to have the flexibility of dynamically searching and utilizing the opportunities within the authorized spectrum in numerous dimensions like time, frequency, code, etc. Therefore, OSA protocol need to integrate spectrum sensing and access functionalities. In essence, spectrum sensing, spectrum allocation, spectrum access, spectrum sharing and spectrum quality determines the key parts for economical OSA protocol style. Cognitive radio has helped to improve spectrum scarcity [3]. Earlier, spectrum was allocated in fixed manner in which fixed users can only use licensed spectrum but with the concept of cognitive radio, SU can broadcast data on unlicensed spectrum without creating any interference with the operational licensed spectrum. This type of smart spectrum sensing enables the network to perform sensing in a secure manner. It can also efficiently avoid jamming attacks by malicious user (MU) using preemptive switching to higher quality channels. It utilizes power saving protocol by conversing low power when low bandwidth is required. This is an intelligent radio which improves the Quality of Service (QoS) by selecting frequency channels with a high rate of Signal to Noise Ratio (SNR).

Though cognitive radio has helped to improve spectrum scarcity, its implementation comes with certain challenges. Whenever CRN is implemented first problem is the decision making whether to use the distributed or centralized model. Similarly, another problem is learning mechanism in which the record of the previous decisions is maintained and utilized to improve its behaviour, which is a complex process. The problem which has attained the significant attention is the security of CRN [4]. This is due to the reason that various wireless devices are allowed to access the licensed spectrum used by PU, therefore they are prone to attack of MUs. CRN not only face security related issues like eavesdropping, tampering, forgery and non cooperation, etc., but also new security threats which directly relates to characteristics of cognitive radios, like denial of service attack, falsifying data, and emulation

1: Department of Telecommunication Engineering, University of Engineering and Technology, Taxila 2: Instituto de Telecomunicac oes - Polo de Aveiro, Portugal.

attack on PU. Therefore security problems in cognitive radios has become the hottest topic of ongoing research [5].

A. Contribution

In this article, a method is proposed to improve the security of cognitive radio network during spectrum sensing by utilizing the concept of blockchains. The main contributions of our proposed work are summarized as follows:

- We have converted all the users i.e., PUs and SUs in the forms of blocks similar to blockchain which combines to form a decentralized network.
- We have used energy detection method for spectrum sensing and its results are validated by authentication of the participating users.
- We have used the concept of digital signature in blockchains for the verification of malicious and authenticated user (AU).
- We have provided extensive simulation results which verify the efficiency of our proposed mechanism.

Rest of the paper is organized as follows: Section II gives brief overview of blockchains and cognitive radios network, section III outlines the previous related work on the issue, section IV presents the scenario and proposed mechanism along with the algorithms, section V discusses the results of the simulation run on the proposed model. Finally, the article is concluded in last section.

II. Blockchains and Cognitive Radios Networks

A. Overview of Blockchains

Blockchains have been adapted by many applications like cryptocurrencies, IoT, Cloud and Edge Computing, Fog Networks, Ad hoc Networks and others. This is due to its distinct property of peer to peer networking (having different nodes with same status to avoid risk of single point failure). Using the blockchain techniques and its distributed ledgers provide complete privacy and cost reduction. The initial and most renowned application of blockchains is bitcoin [6]. Bitcoin is a peer to peer system distributed over a time stamp server whose main task is to computationally proof the transactions in chronological order. Basically, a chain of digital signature is the electronic coin. Architecture of blockchain on basis of bitcoin is discussed in this section.

1) Architectural Background: Blockchain is a combination of blocks in sequence, which maintains a complete list of transaction records in the form of conventional public ledger. Figure 1 demonstrates an example of a blockchain. The block header which contains a previous block hash, whereas it has only one block which is parent block. It is worth noting that blocks belonging to uncle (block ancestors children) hashes would also be stored in ethereum blockchain [7]. The first block of a blockchain which is commonly used as genesis block has no parent block.

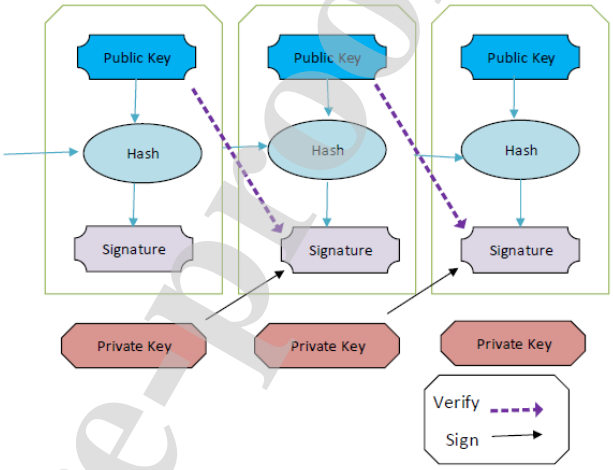

Fig. 1: Blockchain architecture

a) Block: A block is mainly consisted of the block header and body called block body as shown in Figure 1. In particular, the block header includes:

i) Block version: It indicates the set of rules for block validation to follow.
ii) Timestamps: Current time as seconds in Unix timestamp since Gregorian calendars first of January, YYYY.
iii) nBits: It targets the threshold of a valid and sound block hash.
iv) Nonce: Associated with 4-byte field, that typically starts with zero and will increase for each hash calculation.
v) Parent block hash: Associated as 256-bit hash price that points to the previously present block.

The body of block is consisted of a group counter for transactions. The most variety of group actions that a block will contain depends on the size of block and therefore the size of every transaction. Blockchain uses uneven cryptography mechanism which validates the authenticity of transactions [8]. Digital signature supported by uneven cryptography is employed in untrustworthy and dishonourable surroundings. Next we will try to shortly illustrate digital signature.

b) Digital Signature: Every user is owner of a combination of personal key and public key. The personal key that shall be unbroken in confidentiality is used to sign the transactions. Digitally signed transaction is broadcasted on whole network. The standard digital signature involves

two phases: signing phase and verification phase. As an example, a user Alice who desires to send a message to another user Bob.

i) Within the signing section, Alice protects her information by encrypting along with her personal key and sends encrypted data to Bob along with original information.
ii) Within the verification section, Bob validates the worth with Alices open (public) key. Therein method, Bob may simply check if the information has been sent is tampered or not.

This typical type of digital signature algorithmic rule, which is utilized in blockchains for protection of data is the elliptic curve digital signature algorithmic rule (ECDSA) [9]. Same method will be used in our proposed model but in a different scenario.

B. Cognitive Radio Networks

In order to apply blockchains in CRNs, We will provide a brief overview of CRNs.

1) Definition: Cognitive radio can be defined as a radio that can be programmed to access a dynamic spectrum by intelligently utilizing best wireless channel in order to avoid interference and congestion. There is a network of radios which tries to make connections among different nodes to avail the best available opportunity. There are two types of users, PUs and SUs, SUs avails the idle spectrum of PUs opportunistically. The process involves the steps like; spectrum access, spectrum sensing and spectrum mobility, etc. The fundamental step in opportunistic spectrum access is the spectrum sensing which is the main focus of in this article.

2) Spectrum Sensing: A major challenge in CRN is that the SUs are compelled to observe the presence of PUs in an exceedingly accredited spectrum and quit the band as early as possible, if the respective primary radio emerges so as to avoid interference caused in access to PUs [10]. This system is named as spectrum sensing. Spectrum sensing and its estimation is the opening and fundamental step to implement cognitive radio system [11]. Spectrum sensing techniques can be categorised as direct and indirect techniques. Direct techniques haver taken into account frequency domain, where the estimation is dispensed directly from signal by using correlation property. Whereas indirect technique is a time domain approach, where the estimation is performed by autocorrelation of the signal. Spectrum sensing may also be categorized as follows

- Primary transmitter detection: PUs are detected by performing access of the received signal at cognitive radio users. This type of approach includes detection using matched filter (MF), primarily based on energy detection, covariance based detection, waveform based detection, cyclostationary detection and detection using radio identification.
- Cooperative and Collaborative Detection: At first signals for spectrum vacancies are detected faithfully by cooperating or interacting with different users, and therefore the technique may be enforced as either central access to the spectrum with coordination by a spectrum server or decentralized mechanism in explicit by the formula of spectrum load smoothing or detection done externally.
- Interference Temperature Detection: In this approach, cognitive radios utilize ultra wide band (UWB) technology, the SUs are allowed to transmit at relatively low power and are restricted by the level of temperature of interference, therefore SUs do not cause harmful interference to PUs.

C. Implementations of Blockchains in Cognitive Radio Networks

Blockchains have a wide range of applications in different broadband cellular networks, cloud and fog networks as well as in IoTs. A limited number of research articles have been presented, related to blockchains in cognitive networks. Figure 2 shows the generalized concept of blockchain implementation in CRNs for spectrum sensing.

1) Dynamic Spectrum Access in CRNs using Blockchains: In the article [12], authors have proposed a blockchain based verification method for secure spectrum sharing in moving cognitive radios (CRs) in CRNs. They present a virtual money, Specoins, for instalment to get spectrum access. They have compared the power consumption of their proposed algorithms in presence of severe, moderate, slow and fast fading. Authors were successful in achieving advantage over previous methods of spectrum access in terms of scalability, quality of service while providing spectrum access to SUs and PUs. However the proposed model is compared with conventional Aloha which is very old technique of medium access and has now been outdated. MAC protocols like CSMA/CA are commonly used in cognitive radios.

2) Identity Management of CR Networks using Blockchains: In the article [13], the authors propose a security upgrading framework for CRNs using blockchains. The set-up permits network access using pseudonymous identities, which prevents the recreation of a subscriber's character identity. Authors of this article were successful in preventing unauthorized access to personal data by limiting the data exposure to non-authenticated users. The simulation results indicate that this approach reduces the access provisioning duration and decreases network signaling traffic, however, the scalability of CRNs has not been investigated by the authors.

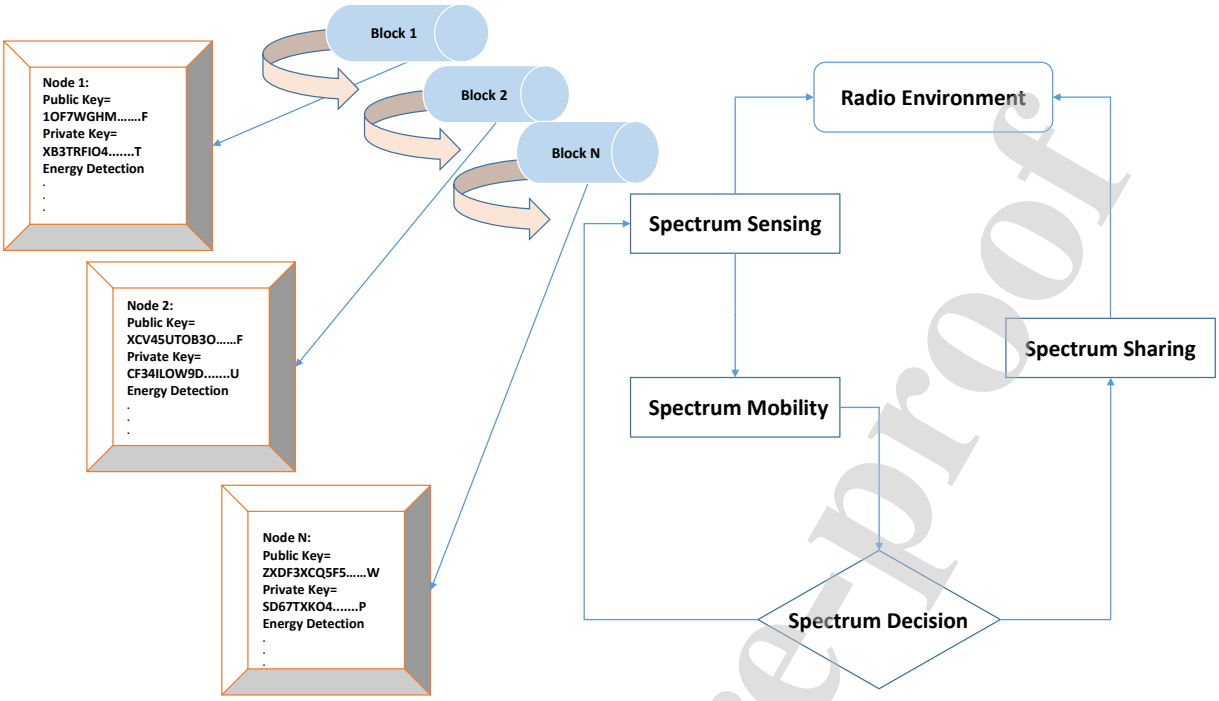

Fig. 2: Implementation of blockchain in cognitive radio environment

III. Related Work

Since the detection of malicious user is a conventional problem therefore different articles have been presented which investigate this area. In [14], a novel method is proposed for the identification of malicious user on the basis of outlier detection mechanism for cooperative spectrum sensing of cognitive radios. In the article [15], malicious user is detected and ex-pulsed in cooperative sensing, where a system is proposed which works independent of the malicious user present in network. In [16], a technique for cooperative detection and suppression of malicious user in cognitive radio system is presented. In [17], a decentralised system utilizes the spatial correlation of Received Signal Strength (RSS) in close premises of SU and outlier detection identifies the malicious user. A voting system is proposed which decides the presence of malicious user in neighbourhood of SUs. Similarly, another method is proposed in [18], where two Hidden Markov Model (HMM) are used to differentiate between malicious and honest user. This detection is achieved through the dissimilarity of respective HMM parameters. In another study [19], intelligent MUs and SUs are detected with high accuracy on the basis of proposed algorithm formulated on the concept of friend and foe detection method.

There are some methods which are proposed for the defence against Primary User Emulation (PUE) attack. In article [20], channel is chosen on the basis of dogfight method. A game based mechanism is proposed where the defender choose sensing channel by avoiding PUE attack. A localization based defence system is proposed in [21], where transmitter is verified by the location of transmitter and characteristics of transmitted signal. A cooperative scheme is proposed with the awareness on attacking capability in presence of PUE malicious attack. The probabilities of fake signal of PUE attack are estimated in the absence and presence of PUE attacks. Threshold is calculated in order to minimize total error probability [22].

In [23], a compromised sensor node is detected on the basis group voting scheme. A time based weight is assigned to each node. Quality of data transmission and weights combine to poll vote. Similarly in the article [24], compressed sensing technique is presented in which MU is removed while signal is being processed at fusion center. Low ranked matrix completion mechanism is applied for this purpose. In article [25], authors have presented a game theory based model which detects the intrusion attack in sensor network. A consensus mechanism is proposed in [26] by using a distributed network. Each SU selects neighbour after repetitive iterations to share sensing data. A reliable neighbour is selected by comparing the received reports against the local mean value. Results which deviates from reference local mean value are discarded. Detection scheme based on double sided abnormality is presented by the authors of [27] for cooperative spectrum sensing.

Referred Study	Description	Cooperative/ Non Cooperative Sensing	Defence against PUE Attack	Defence against SSDF Attack	Technique
[14]	MU Detection in Cognitive Radio Sensing Network	Cooperative	✓	✓	Detection Using Spatial Information
[15]	Expulsion of MU from Sensing in Cognitive Radio	Cooperative		✓	Received Signal Strength (RSS) Based Detection
[16]	Detection Technique with MU Suppression	Cooperative	✓	✓	Local Threshold Decision using detected energy and Weighted Coefficient (WC) Algorithm
[17]	Robust MU Detection Scheme	Cooperative		✓	Neighbourhood Majority Vote based on outlier-detection
[18]	MU Detection for Robust Collaborative Sensing	Cooperative		✓	Hidden Markov Model (HMM) Based Detection
[19]	Detection of Intelligent MU	Cooperative	✓	✓	Friend or Foe Detection
[20]	Combating PUE Attack	Both	✓		Game: Dog Figureht in Spectrum
[21]	Defence Against PUE Attack	Cooperative	✓		Transmitter Verification Scheme i.e. LocDef (localization-based defense)
[22]	Secure Cooperative Spectrum Sensing under PUE Attack	Cooperative	✓		Attack-aware threshold selection approach
[23]	Compromised Sensor Nodes Detection:	Cooperative			A quantitative approach based on weights
[24]	Compressive Sensing Technique for MU Detection	Cooperative		✓	Low-rank Matrix Completion based on adaptive outlier pursuit (AOP)
[25]	Intrusion detection in sensor networks: A non-cooperative game approach	Non Cooperative			Game theoretic framework and Nash equilibrium
[26]	Defence against SSDF Attack in Mobile Ad hoc Cognitive Networks	Cooperative		✓	Consensus Based Sensing Scheme
[27]	Catching attacker in collaborative sensing	Cooperative	✓		Abnormality Detection Approach
[28]	Malicious Attacker detection in Wireless Sensor network	Cooperative			spatial Correlation among the networking behaviors of sensors
[29]	Catchit: Detection of MUs in collaborative sensing	Cooperative	✓	✓	Onion-peeling Approach

TABLE I: Summary of Reference Work

This scheme do not require any advance information about attacker. Main idea is to utilize history of reports as a point in high dimension space for each SU. If points of SU are different at large scale then it is regarded as abnormal user. Cooperation among attacking nodes is not considered in this article. In [28], malicious sensors are identified by simple majority vote. Decision are made as 1 or 0. If more than half votes are in favour of malicious status of sensor then it is deemed as outlier. This mechanism has a shortcoming for not being operate-able in small sensor networks. In [29], onion peeling mechanism is presented for the defence of compromising users. A threshold is defined which determines the status of MU. If the current value is higher than threshold then reports of that user are discarded. This process continues until each MU is detected and removed. The authors in [30], propose a blockchain based secure information sharing mechanism in edge IoT devices, this information sharing mechanism will lead to complete complex task in intelligent edge IoT devices. The authors in [31], formulate an optimization problem with an objective to maximize energy efficiency in CRN, with constraints on outage probability and CR transmission. They propose a low complexity linear search algorithmto solve the problem. The authors in [32], propose a cognitive network virtualization resource configuration in order to improve the security of information centric networks. The authors in [33] discuss conventional physical layer security mechanism for wireless communication systems.

The research articles discussed in the section II and III lead to the idea of using blockchain for enhancement of security of CRNs. In this article, a method is proposed to detect the MUs during spectrum sensing in CRNs by utilizing the concept of blockchains.

IV. Scenario and Proposed Mechanism

A. Scenario

Before moving towards the model scenario of the system, consider Figure 3 and Figure 4, which show the centralized and decentralized network of users connected to the base station. These are the topologies in which users can access the cognitive base station. Consider a

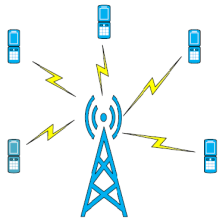

Fig. 3: Centralised topology

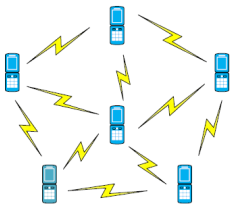

Fig. 4: Decentralized topology

network of cognitive radios in which there are multiple number of PUs and SUs. Figure 5 shows that PUs are present far away from the SUs but they are in range of its effective transmission range. This is a cooperative sensing mechanism in which all the nodes participate to get outcome. Sensing period start at the beginning of spectrum sensing and concludes at the time when consensus outcome is achieved that the user is malicious or authenticated. We are going to implement blockchains on CRN, therefore, our network is totally decentralized where PUs and SUs are connected in peer-to-peer topology. For convenience, we take only one PU and N number of SUs. Figure 6 clearly shows the blockchain implementation for the spectrum sensing in CRNs. PUs and SUs are named as CR users in general. All the CR users are connected with each other in a decentralized manner. Hash to hash connection has been created among them. Each block of CR user contains four type of information which are explained below:

a) Hash: Hash is unique key which is generated by sha256 function [34]. Every user has its unique key which act as a public key of that particular user. This key is known to the next block of user. In short it is a shared key on network.

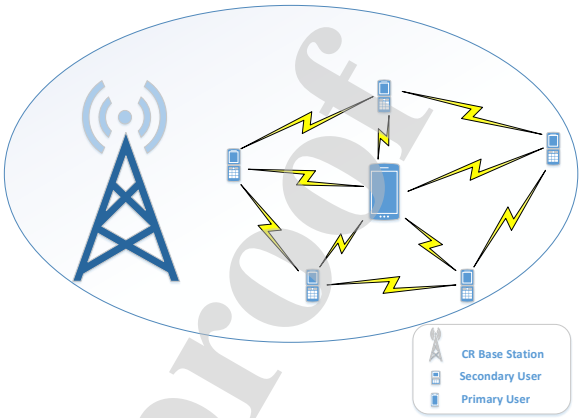

Fig. 5: Model scenario without blockchains and MU

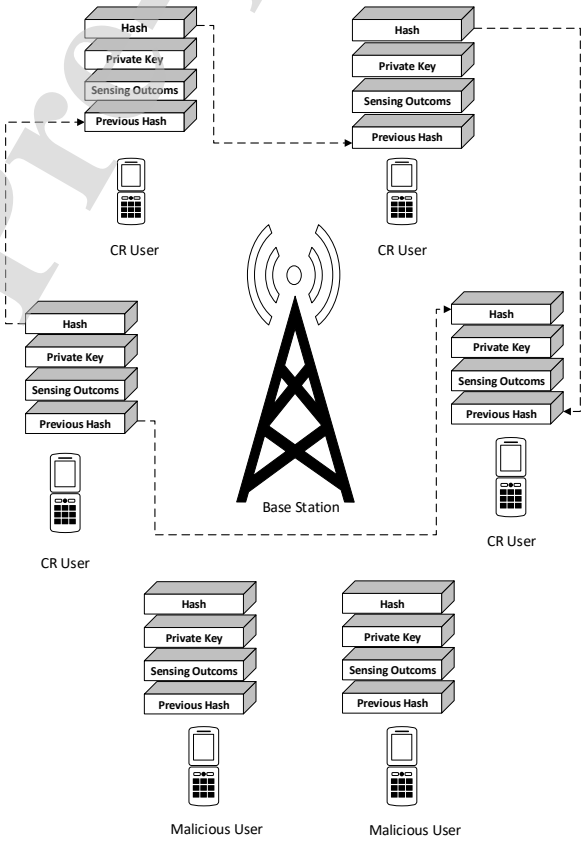

Fig. 6: Model scenario with blockchains and MU

b) Sense Outcome: This is the data part of the block. It contains the information of final outcome of sensing

on the basis of energy detection method. This method is explained further in next section.

c) Private Key: This is the unique identity key of each block which is only known to the CR user itself. In our proposed method 16 bit key is generated which act as private key.

d) Previous Hash: It contains the hash value of previous node. Hence a peer to peer connection is established. In this scenario, all the nodes will participate for cooperative sensing.

B. Proposed Mechanism

Figure 7 shows the flow chart of the proposed mechanism. Firstly, we will create blocks of SUs and PUs. Secondly, we will sense the spectrum using energy detection method. Thirdly, the participating nodes are validated using blockchain. Finally, MU is detected and discriminated from reliable user. These steps are elaborated in detail below.

1) Creation of Blocks: At the very first stage, PUs and SUs are converted into blocks of blockchains. For this purpose a distributed ledgers of nodes having information of PUs and SUs credentials is created. There will be a public key and private key. Public key contains information related to common data related to different units in CRNs like status of being SU or PU. Whereas, private keys contain secret data of nodes like their location, authentication code, etc.

2) Energy Detection: This is the main part of the spectrum sensing in which we are using energy detection method. We consider that there is a bandwidth W Hz and the sampling rate of receiving signal is t. We have created two hypothesis, Hypothesis 1 which detects the signal and concludes that it only consists of noise whereas, Hypothesis 0 shows that detected signal is combination of noise and signal sent by PU. It is shown in equations given below:

$$f(x) = \begin{cases} 1, & \text{n(t)} \\ 0, & \text{s(t)+n(t).} \end{cases} \tag{1}$$

where

$$n(t) \not\Rightarrow AWGN\ Noise \not\Rightarrow H_1$$

$$n(t) + s(t) \not\Rightarrow AWGNNoise\ +\ Signal \not\Rightarrow H_0$$

and

$$H_1 \not\Rightarrow Idle\ Channel$$

$$H_0 \not\Rightarrow Busy\ Channel$$

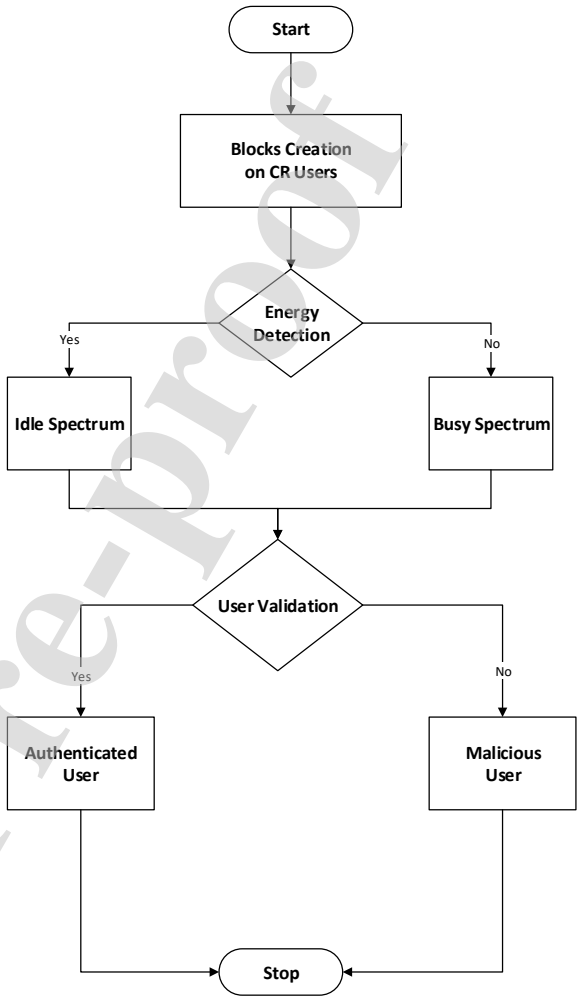

Fig. 7: Flow chart of proposed mechanism

3) Malicious User Detection: After performing all necessary steps for spectrum detection among the nodes, reliable users and MUs are detected using proposed mechanism in which digital signatures are used to verify participating nodes on the basis of public and private key. There are two types of errors according to binary hypothesis test presented in [35]; miss detection and false alarm which can cause error in detection of AU and MU. Probability of detection, miss detection and false alarm are given below:

i) Probability of AU Detection: It means the successful iterations which leads to the verification of AU. When Θ_a number of times AU is detected for η number of iterations give us probability of AU detection (P_{ad}).

$$P_{ad} = \frac{\Theta_a}{\eta}$$

ii) Probability of MU Detection: It means the successful

Algorithm 1 Creation of Blocks on Cognitive Radio Networks

$INPUT:$ *A set of N nodes in current network. A blockchain consist of one Primary Node P and* $N-1$ *secondary user nodes from* $S1$ *to* $Sn-1$
$OUTPUT:$ *Blocks are created on different nodes of cognitive network.*
$for\ i = 1\ to\ n$
if *licensed user* **then**
  create a node P
else
  create a node S_{i-2}
end if

iterations which leads to the verification of MU. Probability of MU detection (P_{md}) is given by the ratio of Θ_m number of times MU is detected by η number of iterations .

$$P_{md} = \frac{\Theta_m}{\eta}$$

iii) Probability of Miss Detection: It shows the unsuccessful iterations which leads to the detection of AU. When Θ'_a number of times AU is not detected for η number of iterations gives us probability of miss detection (P_m).

$$P_m = 1 - P_{ad} = \frac{\Theta'_a}{\eta}$$

iv) Probability of False Alarm: This probability shows the miss detection of MU which leads to false alarm. Probability of false alarm (P_f) is given by the ratio of Θ'_m number of times MU was unable to be detected by η number of iterations .

$$P_f = 1 - P_{md} = \frac{\Theta'_m}{\eta}$$

4) Outcome: In this step, outcome is obtained on the basis of above mentioned steps that whether spectrum sensing is done reliably or attacked by MU.

C. Proposed Algorithms

All the simulations are performed on the basis of three algorithms which are designed from the proposed mechanism. In these algorithms we assume that there are N number of SUs and for convenience we have considered a single PU. In the Algorithm 1, SUs and PU are connected with each other using blockchains. Connection between PU and SUs is established in the form of decentralized blocks. Blocks of PU and SUs are discriminated on the basis of there license. License are issued by the service provider of the user. When blocks are created, their status of being primary or secondary is decided by verifying the license of the user. If the spectrum is being sensed by the PU then it will be allocated P block otherwise S block is allocated. In Algorithm 2, spectrum is sensed by using energy detection method. When SUs try to access the spectrum, they will participate in cooperative sensing method. In which all nodes will sense the spectrum and make two hypothesises. Hypothesis 1 will be true when the spectrum is sensed and outcome received is a noise signal. Hypothesis 0 will be true when output received is combination of noise and energy signal. Hence, output of sensing will be made on these two hypothesises. If result of first hypothesis is true then its mean channel is vacant and spectrum sensing result will be positive otherwise channel is busy and sensing outcome is negative. These sensing outcomes are then verified by next algorithms. Finally in Algorithm 3, energy detection result of individual participating node is verified and validated. If the user's digital signatures are verified it means it is AU otherwise it will be termed as MU. In this

Algorithm 2 Energy Detection on Block Network

$INPUT:$ *A set of* $N-1$ *nodes of secondary Users 'S' participate in sensing the Primary User P's spectrum. There are two hypothesis* H_1 *for idle channel and* H_0 *for busy channel*
$OUTPUT:$ *Sensing outcome is obtained using energy detection method in variable* Y
Sense channel X :
if $X = n(t)$ **then**
  $Y = H_1$
else
  if $X = n(t) + s(t)$ **then**
    $Y = H_0$
  end if
end if

Algorithm 3 Detection of MU using Verification of Digital Signature

$INPUT:$ *A set of* $N-1$ *outcomes* Y_{n-1} *are received after energy detection. Now result are verified on basis of digital signature i.e Public and Private Keys*
$OUTPUT:$ *Reliable and Malicious Users are detected.*
$for\ Decision\ Y = 1\ to\ n$
if *Public Key is verified* **then**
  if *Private Key is verified* **then**
    Authenticated User Detected
  else
    Malicious User Detected
  end if
end if

algorithm firstly public key is verified and then private key which both contribute to make consensus on validation of user. Similarly, probability of MU and AU detection, miss detection and false alarm are calculated by using equations presented in previous section.

D. Complexity of MU Detection

For the computation of the complexity involved in the detection of MU, number of participating nodes plays an important role. In the present scenario there are three type of nodes i.e., primary nodes (N_p), secondary nodes (N_s) and malicious nodes (N_m). It is clear from the proposed mechanism and algorithms, that the process of detection of AU and MU depends on the participating nodes N which participates in the validation process. Clearly from the proposed algorithms:

$$N = N_p + N_s$$

Therefore, complexity involved in detection of MU can be represented as $O(N^2)$.

E. Performance Metrics

Performance of the proposed mechanism of securing cognitive mechanism is analyzed in terms throughput, frame loss and response time.

1) Response Time: Response time (T_r) is the total time utilized for the validation of secure nodes, which means time required for the data stream to travel among the participating nodes which includes connection establishment, verification of public key, verification of private key and authentication of nodes to be malicious or reliable. T_r is calculated as the time interval between the moment when blocks are created on the participating and the moment when status of node to be malicious or reliable is determined. The obtained numerical values are measured in seconds.

2) Frame Loss: Frame loss (FL) is the measure of data which is lost through the transmission of data. There can be different reasons for the loss of data like fading and noise, etc. FL is given as:

$$FL\% = \frac{DL - TP_{DL}}{DL}$$

where $FL\%$ is percentage frame loss, DL is the total data load and TP_{DL} is throughput across data load DL. While, throughput (TP) is total number of data (bits or bytes) traveled over a network in processing time (sec). TP can be shown as:

$$TP = \frac{D}{T_l(B_x) - T_f(B_x)}$$

where, D is the total amount of data exchanged among the participating nodes N. $T_l(B_x)$ and $T_f(B_x)$ shows the last and first data packet sent per unit time using blockchain based securing protocol B_x.

V. Experimental Results

Experimental results are obtained by carrying simulations on proposed approach to identify the MU and AU present in spectrum sensing network.

A. Simulation Setup

Proposed method is simulated using MATLAB. For all the simulations cognitive radio network similar to setup [36] is considered. Low range of SNR is considered i.e., -8 dB to 4 dB for the AWGN channel. While, Quadrature Phase Shift Keying (QPSK) modulation is used for the test therefore modulation index 4 of Phase Shift Keying (PSK) modulator is used. Energy detection of the signal is analyzed at 500, 700 and 1000 number of samples. Whereas flat Rayleigh fading is applied on channel for the comparison of results. All the base station and cognitive radio users i.e., PUs and SUs are uniformly distributed.

B. Results and Discussion

For the creations of blocks on CR users as proposed in Algorithm 1 is implemented. SHA 256 function [34] is used for the creation of hash which act as a public key [34]. It is a cryptographic hash function which generates

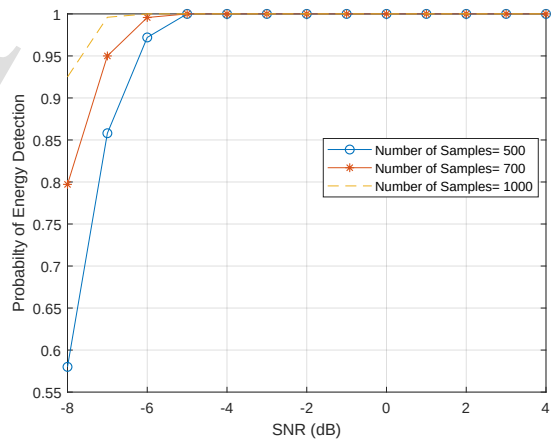

Fig. 8: Energy detection at different number of samples

a key of fixed size as an output with input of variable size. Current time of the system is utilized to create different keys. Hence, time stamp of the block involves in the creation of unique hash of each node. Similarly, private key is also generated by a random function. Sensing outcome is stored in the block from the results of Algorithm 2 executed for each participating node. Figure 8 shows the probability of energy detection with respect to SNR. A GPSK modulated signal is used in the energy detection mechanism whereas AWGN channel is used. Spectrum availability is determined by the detection of noise and

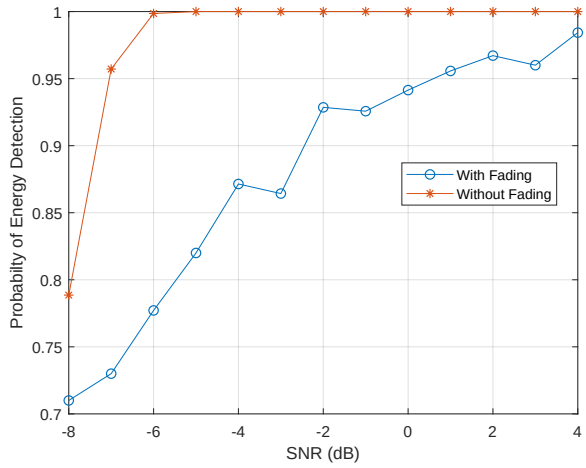

Fig. 9: Energy detection with/without fading channel

energy signal. If the value of energy is greater than the threshold it means that spectrum is being used and probability of detection is close to unity. Whereas if its value is less than the threshold probability of false alarm is dominant. This figure shows probability of energy detection at different number of samples with respect to SNR. It is clear from the figure that with increase in number of samples probability of detection approaches to unity. Figure 9 shows the comparison of energy detection for

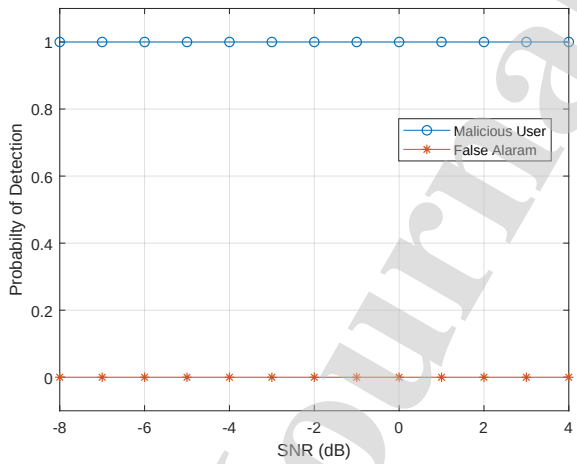

Fig. 10: Probability of MU detection and false alarm across different values of SNR.

different channel impairments. Two type of channels are considered i.e., with fading and without fading channels. Rayleigh fading and AWGN channels are used for the simulations respectively. Figure 10 and 11 show the result

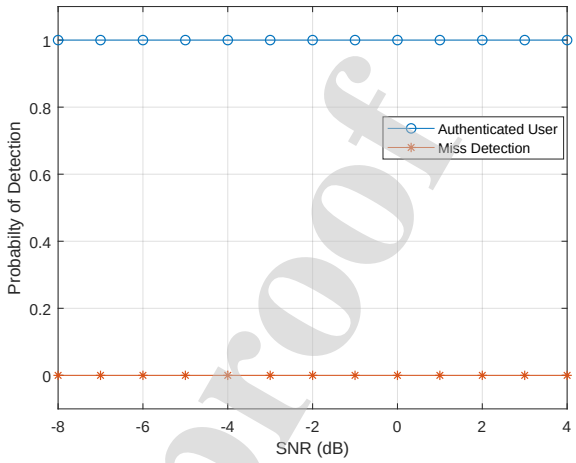

Fig. 11: Probability of authenticated user detection and miss detection across different values of SNR

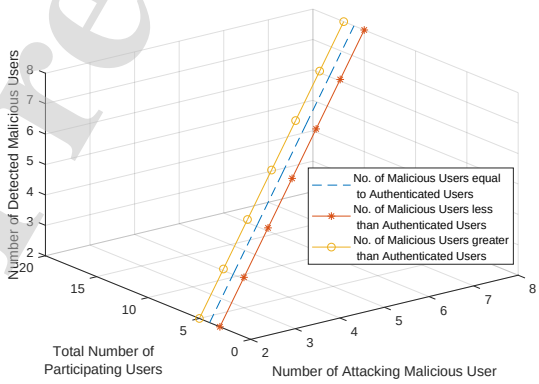

Fig. 12: Number of detected MU vs number of attacking MU across load of different participating nodes.

of detection of AU and MU. Probabilities of MU detection, false alarm, licensed alarm and miss detection of licensed user. After receiving the sensing decision implemented through Algorithm 2, private and public keys which are the digital signature of the authenticated nodes. If the digital signature of the participating node matches with the blockchain based users in CRN it is termed as AU otherwise MU. The results shows the 100 percent detection of MU and reliable user. While, probability of false alarm and miss detection is zero. Figure. 12 shows the accuracy of MU detection in presence of different user load. Results are analyzed in different ratios of MUs and AUs. Figure 13 shows the comparison of time consumption with and without fading channel. It is clear from the figure that fading channel consumes more time for the detection of MU.

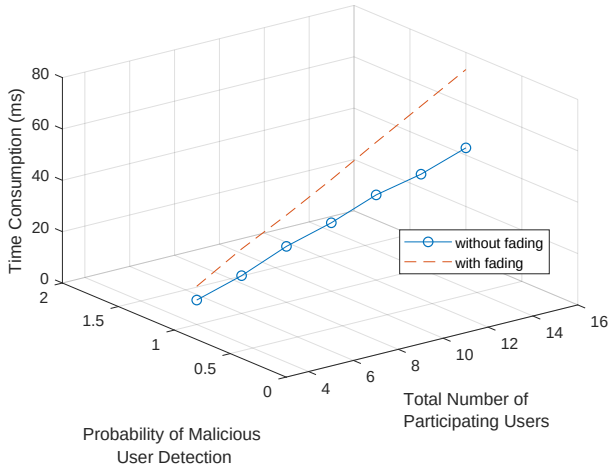

Fig. 13: Comparison of time consumption in milliseconds for fading channel

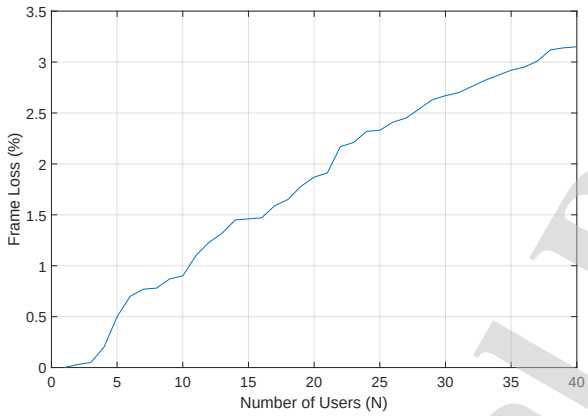

Fig. 14: Frame loss% across load of users

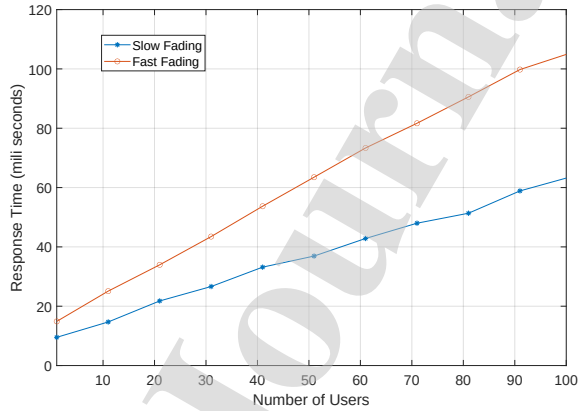

Fig. 15: Comparison of response time for two fading channels

Performance of the blockchain based design is analyzed by mainly two factors i.e., response time (T_r) and frame loss (FL%). Figure 14 shows the FL% across different number of users. With increase of number of users FL% increases. For the evaluation of FL, we have considered the mean throughput because the size of the packets of the public and private keys are variable. Figure 15 shows the comparison of response time for slow fading and fast fading channel. It is clear from the results that validation and identification of nodes are more efficient in slow fading channel whereas response time is higher in case of fast fading.

VI. Conclusion

In this article, spectrum sensing phase of cognitive radio networks is investigated under the presence of MUs. A new mechanism is proposed using the concept of blockchains. An appropriate recognition strategy is utilized which identifies the AU and MU successfully with hundred percent efficiency by validating the digital signature of the blockchain based nodes present in cognitive radio network. Results have shown that all the attacking MU are detected. Hence, the energy detection outcome of MU is not considered for the spectrum sensing in CRN. The MU is permanently blocked for any further process and cannot participate in spectrum sensing any further. Moreover, the complexity of blockchain based model is very low as compared existing models.

References

[1] J. Xiang, Y. Zhang, and T. Skeie, "Medium access control protocols in cognitive radio networks," *Wireless Communications and Mobile Computing*, vol. 10, no. 1, pp. 31–49, 2010.

[2] C. Santivanez, R. Ramanathan, C. Partridge, R. Krishnan, M. Condell, and S. Polit, "Opportunistic spectrum access: Challenges, architecture, protocols," in *Proceedings of the 2nd annual international workshop on Wireless internet*. ACM, 2006, p. 13.

[3] Z. Tabakovic, "A survey of cognitive radio systems," *Croatian post and electronic communications agency*, 2013.

[4] A. S. Hamood and S. B. Sadkhan, "Cognitive radio network security status and challenges," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*. IEEE, 2017, pp. 1–6.

[5] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks survey of security issues in cognitive radio networks," *Journal of Internet Technology*, vol. 12, 03 2011.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[7] G. Peters, E. Panayi, and A. Chapelle, "Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective," 2015.

[8] NRI, "Survey on blockchain technologies and related services," http://www.meti.go.jp/english/press/ 2016/pdf/0531 01f.pdf, 2015.

[9] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," *International journal of information security*, vol. 1, no. 1, pp. 36–63, 2001.

[10] E. Hossain, D. Niyato, and Z. Han, "Dynamic spectrum access in cognitive radio networks," *Dynamic Spectrum Access and Management in Cognitive Radio Networks*, 01 2009.

[11] D. B. Rawat and G. Yan, "Signal processing techniques for spectrum sensing in cognitive radio systems: Challenges and perspectives," pp. 1 – 5, 12 2009.

[12] K. Kotobi and S. G. Biln, "Secure blockchains for dynamic spectrum access," *IEEE vehicular technology conference*, 2018.

[13] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, and J. S. Deogun, "Identity management using blockchain for cognitive cellular networks," pp. 1–6, 05 2017.

[14] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2488–2497, 2010.

[15] S. Yadav and M. J. Nene, "Rss based detection and expulsion of malicious users from cooperative sensing in cognitive radios," in *2013 3rd IEEE International Advance Computing Conference (IACC)*. IEEE, 2013, pp. 181–184.

[16] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in *2009 IEEE International Conference on Communications*. IEEE, 2009, pp. 1–5.

[17] C. Chen, M. Song, C. Xin, and M. Alam, "A robust malicious user detection scheme in cooperative spectrum sensing," in *2012 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2012, pp. 4856–4861.

[18] X. He, H. Dai, and P. Ning, "Hmm-based malicious user detection for robust collaborative spectrum sensing," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11, pp. 2196–2208, 2013.

[19] S. R. Sabuj, M. Hamamura, and S. Kuwamura, "Detection of intelligent malicious user in cognitive radio network by using friend or foe (fof) detection technique," in *2015 International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, 2015, pp. 155–160.

[20] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3566–3577, 2010.

[21] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on selected areas in communications*, vol. 26, no. 1, pp. 25–37, 2008.

[22] A. A. Sharifi, M. Sharifi, and M. J. M. Niya, "Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach," *AEU-International Journal of Electronics and Communications*, vol. 70, no. 1, pp. 95–104, 2016.

[23] T. Li, M. Song, and M. Alam, "Compromised sensor nodes detection: A quantitative approach," in *2008 The 28th International Conference on Distributed Computing Systems Workshops*. IEEE, 2008, pp. 352–357.

[24] Z. Qin, Y. Gao, M. D. Plumbley, C. G. Parini, and L. G. Cuthbert, "Low-rank matrix completion based malicious user detection in cooperative spectrum sensing," in *2013 IEEE Global Conference on Signal and Information Processing*. IEEE, 2013, pp. 1186–1189.

[25] A. Agah, S. K. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach," in *Third IEEE International Symposium on Network Computing and Applications, 2004.(NCA 2004). Proceedings*. IEEE, 2004, pp. 343–346.

[26] F. R. Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *MILCOM 2009-2009 IEEE Military Communications Conference*. IEEE, 2009, pp. 1–7.

[27] H. Li and Z. Han, "Catching attacker (s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," in *2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN)*. IEEE, 2010, pp. 1–12.

[28] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*. IEEE, 2007, pp. 1937–1945.

[29] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: Detect malicious nodes in collaborative spectrum sensing," in *GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*. IEEE, 2009, pp. 1–6.

[30] 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, Dec 2019.

[31] L. Zhang, M. Xiao, G. Wu, S. Li, and Y. Liang, "Energy-efficient cognitive transmission with imperfect spectrum sensing," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1320–1335, May 2016.

[32] J. Wu, M. Dong, K. Ota, J. Li, W. Yang, and M. Wang, "Fog-computing-enabled cognitive network function virtualization for an information-centric future internet," *IEEE Communications Magazine*, vol. 57, no. 7, pp. 48–54, July 2019.

[33] B. Dai, Z. Ma, M. Xiao, X. Tang, and P. Fan, "Secure communication over finite state multiple-access wiretap channel with delayed feedback," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 723–736, April 2018.

[34] N. Courtois, M. Grajek, and R. Naik, "Optimizing sha256 in bitcoin mining," vol. 448, 09 2014, pp. 131–144.

[35] T. Tran and H.-Y. Kong, "An analysis of combining methods in cooperative spectrum sensing over rayleigh fading channel," *Journal of electromagnetic engineering and science*, vol. 10, 09 2010.

[36] K. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proceedings of the IEEE*, vol. 97, pp. 878 – 893, 06 2009.

Highlights

- In this article, a blockchain based method is proposed to detect the malicious users in cognitive radio networks to improve the security.
- The results shows the 100% detection of malicious users.

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Adnan Sajid is currently pursuing his Bachelor's degree in Telecommunication Engineering from University of Engineering and Technology, Taxila, Pakistan. His research interests includes Blockchains, Wireless Sensor Networks, Cognitive Radio Networks, Internet of Things and Antenna Designs for future applications.

Bilal Khalid is currently enrolled in final year at BS Telecommunications Engineering in University of Engineering and Technology. Taxila, Pakistan. His research interests are Wireless Communication, Cognitive Radio Networks and Internet of Things.

Mudassar Ali (mudassar.ali@hotmail.com) received his PhD degree from School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Pakistan, in 2017. He received his B.S. in Computer Engineering and M.S. in Telecom Engineering in the year 2006 and 2010 respectively, from University of Engineering and Technology, Taxila, Pakistan, with a major in wireless communication. From 2006 to 2007 he worked as Network Performance Engineer with Mobilink (An Orascom Telecom Company). From 2008 to 2012 he worked as Senior Engineer Radio Access Network Optimization with Zong (A China Mobile Company). Since 2012, he is an Assistant Professor at Telecom Engineering Department, University of Engineering and Technology, Taxila, Pakistan. His research interests include 5G wireless systems, heterogeneous networks, interference coordination and energy efficiency in 5G green heterogeneous networks.

Shahid Mumtaz (smumtaz@av.it.pt) received his M.Sc. degree from the Blekinge Institute of Technology, Sweden and his Ph.D. degree from University of Aveiro, Portugal. He is now a senior research engineer at the Instituto de Telecomunicac¸ ˜oes - P´olo de Aveiro, Portugal, working in EU funded projects. His research interests include MIMO techniques, multi-hop relaying communication, cooperative techniques, cognitive radios, game theory, energy efficient framework for 4G, position information assisted communication, joint PHY and MAC layer optimization in LTE standard. He is the author of several conferences, journals and books publications