IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

Blockchain-Enabled Security for Cognitive Radio Networks

Savita[1] and Ms. Meenakshi Arora[2]
[1]Research Scholar, Department of CSE, Sat Kabir Institute of Technology & Management, Bahadurgarh
[2]Assistant Professor, Department of CSE, Sat Kabir Institute of Technology & Management, Bahadurgarh

Abstract: *This abstract discusses the pressing issue of spectrum scarcity in wireless communication and presents Cognitive Radio (CR) as a promising solution. With the proliferation of wireless applications, the demand for spectrum has intensified, leading to inefficiencies in spectrum allocation. CR technology enables unlicensed secondary users to share licensed spectrum bands with primary users without causing interference, thus optimizing spectrum utilization. This abstract highlights the potential of Cognitive Radio Networks (CRNs) in enhancing communication efficiency and addressing spectrum redundancy. However, it also underscores the limited research on the security aspects of CRNs, emphasizing their vulnerability to attacks compared to wired networks. The abstract introduces a proposed methodology for improving spectrum allocation algorithms, demonstrating superior detection probabilities and maximum interaction times compared to existing algorithms. These findings suggest the effectiveness of the proposed approach in optimizing spectrum utilization and enhancing network performance in CRNs*

Keywords: Blockchain, CRN Security, Error Rate, NES Algorithm

I. INTRODUCTION

A blockchain constitutes an expanding series of interconnected blocks, encompassing encrypted documents representing transactions. It functions as a decentralized ledger technology, incorporating cryptographic hashing, timestamps, and transactional data within each block. Prior to inclusion in a block's hash, transactional data must demonstrate existence at the block's issuance. Furthermore, the hash of a block is integral to the hash of transactional data. As blocks are linked, they form a chain wherein each subsequent block enriches the accumulated knowledge. Data integrity within each block is paramount, ensuring retroactive alterations to any block necessitate corresponding modifications to all subsequent blocks, thus safeguarding against tampering.

It is crucial to emphasize that many of the advances discussed will not be relevant for some years, if not decades, after they have occurred. No, we are not implying that everything will unfold exactly as we have described it — simply that the technology exists to make it feasible. As a result, it is not a call to action, but rather a call to raise awareness about the issue. Some areas of blockchain may leave you with more questions than you started with, but we hope that once you have a basic understanding of the technology, you will be in a better position to consider how it may impact the social, commercial, and societal elements that are most important to you and your organization.

A key component of Bitcoin's construction is the blockchain technology, which serves as the crypto currency's shared ledger. In this case, consider blockchain to in the same vein as Microsoft Windows or Apple MacOS, with bitcoin representing simply a single of the many apps that may be run on it, as opposed to other operating systems. While blockchain does provide an easy way to record Bitcoin transactions (through the use of an openly accessible shared ledger), it also provides a way to record transactions involving any other asset, whether it is physical (such as gold), intangible (such as cash), or digital (such as digital currency). With the help of this shared ledger, it is possible to record any transaction and track the movement of any asset at any time. regardless of whether the object is physical or intangible, or if it is digital. The settlement of securities, for example, may be completed in minutes rather than days thanks to block-chain technology. As well as assisting companies in controlling the It may be used to allow manufacturers to exchange production data with original equipment manufacturers, as well as to track the flow of products and associated payments (OEMs) and regulatory authorities in order to reduce the number of product recalls.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

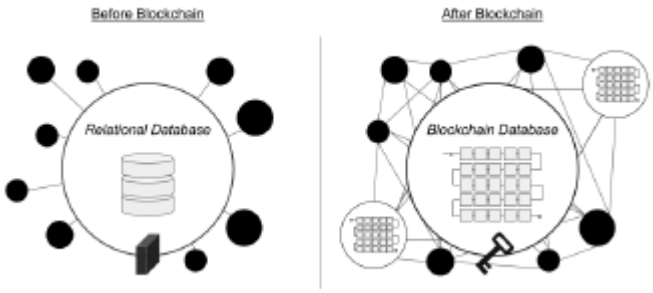

Figure 1.1: Business networks before and after blockchain.

Traditional methods of recording transactions and monitoring assets necessitate the maintenance of individual ledgers and other records by members of a network, as shown on the left in Figure 1.1. Because it necessitates the use of intermediaries who charge fees for their services, this traditional method may prove to be too expensive. There are several reasons why this system is inefficient, including delays in the implementation of in addition to other issues, there are issues with agreements and the duplication of labour necessary to maintain several ledgers. As a consequence of fraud or hacking, or even by making a simple error, the whole company network is put at risk, including the entire financial system, put at risk of being compromised as well.

II. LITERATURE SURVEY

Pei *et al.* (2012) have proposed C.R been viewed as the mostly encouraging strategy to eliminate the issues of spectral utility. C.R could examine the spectral bands& recognize free channelling that would be utilized by cognitives clients without any interference to essential (primary) clients. Because of the different dynamic attributes of C.R.Ns, adjustment & secured interaction are of more prominent approaches than different wireless systems. These papers proposed a dependent trust administration mechanism in terms of cognitive cycles, that could refer framework BER adequately & making out spectral distribution more sensible and secure. The final, simulated o/ps defined that the given schemes had the benefits of solid adjustment &least error rating.

Wang-Ji and Ray-Chen (2014) had proposed C.R organizations being applied methodology for range constraints. S.Uget detecting instrument to taken-out in the fundamental customer's accessibility. This stir develops a trusted-based data gathering way to deal with adjust dangerous SU attack in range identification of the intellectual radio frameworks. The given planning joined the immediate & recycled identifying affirmation to guarantee the overall execution & gets a constant redirection models to keep away from dangerous SUs from detailing counterfeit acknowledgment boundaries.

Pei et.al (2012) told a trusted the executives modelling via the entire psychological cycling for concentrated C.R.Ns to tackle the securities dangers buying via conniving elements, for example, egotistical, malevolent, and perfect hubs, yet they didn't show how range dynamic happens in a range sharing component. The range dividing component among the essential and optional organizations in a C.R.N needs S.Us submit to the pioneering accessingrules out. Self-centered & pernicious clients might send bogus information or adulterate the detecting information, or might need to utilize a PU's range and neglect to clear the range, regardless of whether the PU needs to recover its own range. These are named delicate security dangers. In this way, PUs should be given a trusted ensuredvia S.Us to permit themselves to utilize such ranges. In any case, like a trusted limits sharing system hadn’t being given in the writing to defeat the delicate securities dangers in C.R.Ns. To sum up the issue, there was no approach proposing in the writing that range could be partaken in a safe manner in C.R.Ns. To conquer the above issue, a Trusted techniques for Securing and dynamic range accessing in CRNs is proposed.

Zou *et al.* (2013) have proposed Cognitive Radio (CR) as a promising innovation for future remote range designation to enhance the utilization of the authorized groups. In any case, CR remote systems are vulnerable to different assaults and can't offer proficient security. Primary User Emulation (PUE) is a standout amongst the most genuine assaults for CR systems, which can altogether expand the spectral receiving fault probability. Here, a defense procedure against the PUE assault is proposed in CR systems utilizing conviction propagation, which maintains a strategic distance from the arrangement of extra sensor systems and costly equipment in the systems utilized as a part of the current literature. In

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

this proposed approach, every secondary client figures the nearby local functionality and the similarity work, processes the messages, trades messages with the neighboring clients, and computes the advantages until merging. At that point, the PUE assailant will be identified, and all the secondary clients in the system will be identified in a communicate route about the behavior of the attackers signal. Thus, all SUs can keep away the PUE attackers essential (primary) emulation signal later on. Simulation comes about to demonstrate that the proposed approach delivers rapidly, and it was more reliable to identify the PUE attacker.

The optional gadgets inside reach will consider an essential client is dynamic, and will don't communicate information over channel. The literature discuses different algorithms to identify the Primary User Emulation attack, but noneof the method showed how to mitigate the attack in Cognitive Radio Network. So it is aimed to provide a solution to identify and remove the Primary User Emulation Attack (PUEA) in CRN, by means of which a Secured communication can be established in Cognitive Radio Networks.

As indicated by CRN design, the key hubs (León et al. 2010) produce and store the entirety of the significant information, for example, the distinctive keys that are utilized to convey in the arrange and play out the significant responsibilities regarding keeping up with the security of the organization. There isn't a lot of work in the writing which chooses a hub as the vital job to work with framework security.

Notwithstanding, it is conceivable that pernicious hubs might assault the vital hubs of the CRN, compelling the entire organization to perform at a corrupted level or even take it disconnected. In the event that aggressors assault the organization with the end goal of debasing the framework execution, the framework accessibility and dependability will fall in an emotional manner and the entire organization will implode. Be that as it may, there is no approach presently proposed for accessibility upgrade in CRNs for smooth and strong correspondence. Additionally, it is seen that different specialists have proposed various methods for deciding the degree of certainty and utilizing it to keep up with secure correspondence between hubs in various regions. In any case, none of them give a total strategy which addresses and models every one of the perspectives needed for setting up secure correspondence. There are still holes in the exploration on approaches which gauge and keep up with security in CRNs communication. The main issue occurs when CR systems are continuously isolated into un-predictable segments due to node mobility and distinctive Spectrum accessibility model. More often, these segments are randomly associated; subsequently, secure as well as reliable routing gets to be real issue for these sorts of system. Thus it is aimed to defeat these issues.

WeifengMou*et al.* (2017) has investigated the security performance of multiple relaying CRN with collaborative distributed beam forming scheme against passive eavesdropping attacks. El-Hajj (2011) have proposed Cognitive Radio (CR) as a novel innovation that guarantees to resolve the spectral issue by permitting secondary clients to exist together with essential clients without making impedance to their correspondence.

Here, a brief diagram of the CR innovation is given as a point by point investigation of the security assaults focusing on Cognitive Radio Networks (CRNs) together with the related mitigation methods. The assaults as for the layer they target beginning from the physical layer and traveling to the vehicle layer is classified. An estimation of the proposed countermeasures is displayed together to different arrangements thus it increases to accomplish a protected and trusted CRN.

From the literature it was found that secrecy capacity is a standout among the most essential physical layer security parameters for Cognitive Radio systems. But none of the approach proposed a light weight scheduling scheme for Physical layer securities in CRNs when the users are in mobility hence its is aimed to propose a Secure Scheduling Scheme for Physical layer securities in CRNs.

III. PROPOSED ALGORITHM

It is essential to treat the hub trust esteem as a major file in order to take an interest in helpful identifying if one is interested in improving the safety of intellectually distant businesses. Therefore, the combination of hub trust worth and essential framework design may match the detecting accuracy requirements while simultaneously reducing the amount of energy that is used.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

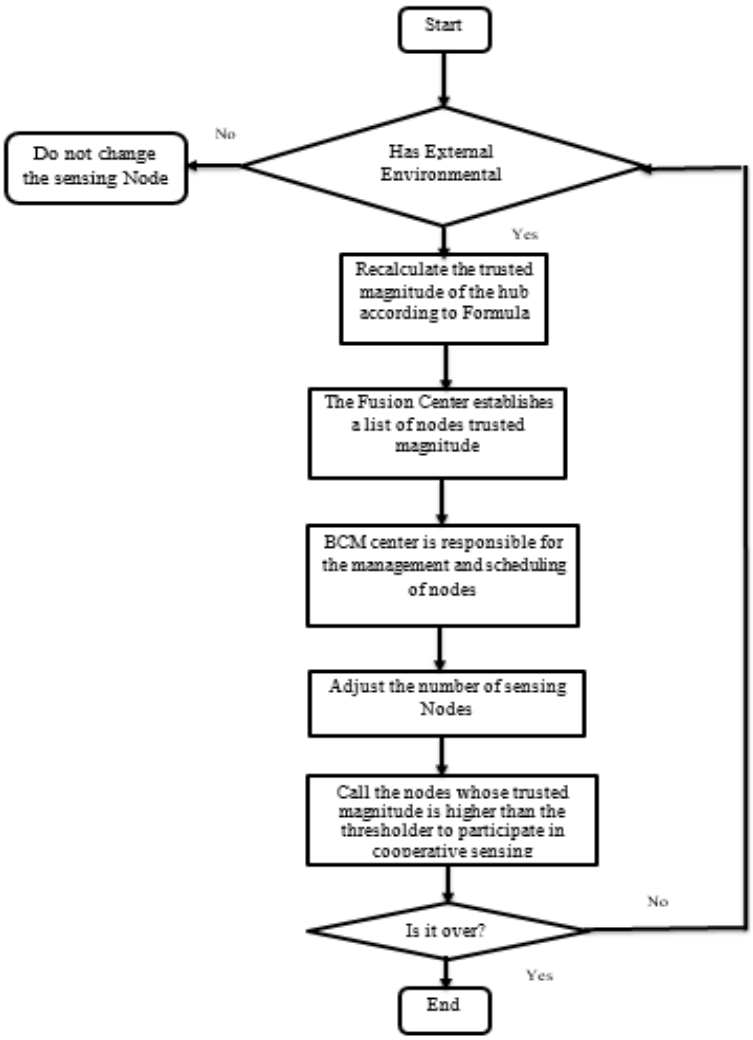

Figure 3.1NES Technique Flow Chart

It may be possible for the blockchain community on the board to be more effective in preventing information chaos. Further development of the detecting execution of psychological distant organizations is possible with the use of an integrated weighing device that is reliant on stand-out [27]. In the first step of the computation, the unchanging quality of each hub in the framework is evaluated. The reliability of this analysis is dependent on the genuine and insightful data. Whenever a suspicious node is found, it swiftly decides on a particular option for the hub's finding knowledge, and this decision is implemented immediately. The computation takes into account the power of the structure but also takes into account the additional energy consumption; however, the influence of natural changes on the real hub is not taken into consideration. In point of fact, the radio environment is constantly changing, and a change in the functioning status of the essential client would likewise influence the detecting of hubs. As a result, it is essential to construct an ongoing evaluation system for hubs in order to keep up with any changes that may occur in the current environment. It is possible for it to cease detecting work on schedule at the point in time when the hub execution begins to fail, and then when the hub execution begins to improve, it is possible for it to be relocated to the work on schedule position. This study establishes a hub assessment computation and hubs determination tool to make the evaluation and selection of hubs more accurate and efficient. Figure 3.1 depicts the hubs determination calculation stream graph for your viewing pleasure.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

Design of Algorithm

The assessment objects of proposed scheme is 2-times affirmation issue bet[n]the square tied I.o.T device and mental far off association mix center.

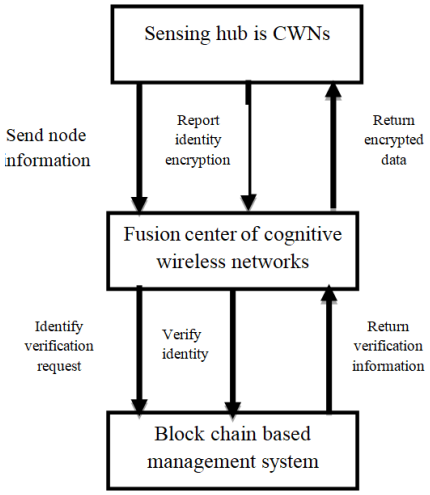

Figure 3.2 Security calculation construction of intellectual remote organization

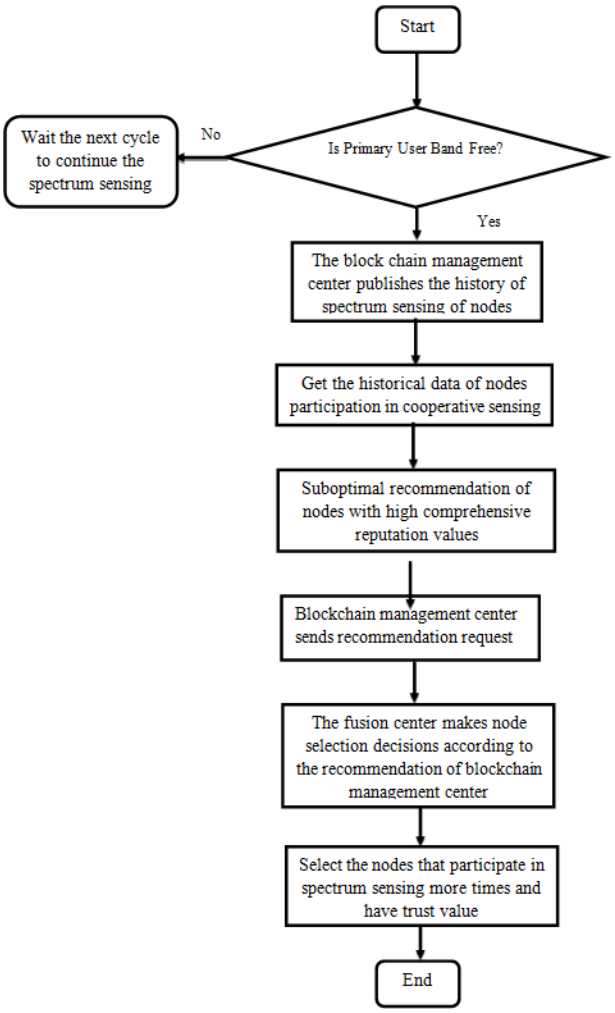

Figure 3.3 Proposed Technique for Block chain based CWN

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

Hence, the design in proposed method is essentially made from the block-chain structure, the mental distant association blend center, and the square fastening IoT device. Customers talk by means of the square binding system through the blend place.

The specific development is shown in Fig-3.3

The internet of things contraption sent-out center information to the blend places, and the mix local area requests the block chain system for the presence of its center information, and subsequently the center point sending the data supported through the secretly keying to the mix place, and checks at whatever point the identifying center has related secretly key-out matched signature it. Expecting these are, forwarding the center point's sales to the square fastening structure, & forwarded the responses of the square affixed design back-to the distinguishing center point. The information supported by the distinguishing center point could confirming the personality of participated in range identifying, & could moreover ensured that its-data had n't being modified or created.

IV. RESULT ANALYSIS

This portion, we need to talk about the outcome examination of Block-chain innovation in C.R.Ns. The reenactment boundary is talked about in the table 4.1

Table 4.1 Simulation Parameter

Sr. No.	Parameter	Value
1	Simulation Area Setting	A Circular area with a radius of m
2	Primary User	Place a primary user anywhere on the edge of circular area
3	Working Parameters of primary user	BPSK signal with power of 100 MW and bandwidth of 100 kHz.
4	Number of Nodes	Randomly place 15 nodes (5 nodes with SNR = -18 dB and -14 dB respectively)
5	Noise Settings	AWGN
6	Average Detection Times	10000
7	Auxiliary Node	3
8	Spectrum Detection Method of Node Front End	Energy Detection

The round region with sweep m is characterize as recreation space of the organization. The essential clients are set anyplace on the edge of roundabout region. The signal powers is 100.00 Mega Watt & data transfer capacity of 100.00k.Hertz. Likewise, 15-hubs are set in-the framework. Past these S.N.R of such hub is– 18.00 dB & - 14.00 dB individually. The commotion utilized in given framework is A.W.G.N. The normal recognition period & assistant hubs are 10000.000 & 3.00 separately. Energies recognition technique is utilized as range location.

C.R.N Topology is characterized in the fig 4.1. The diverse no. of essential & auxiliary clients is put specifically math. The scope of organization lies between - 500 to 500 m. There is one essential client and numerous optional clients. The essential client is situated at the focal point of region while auxiliary clients are situating around the essential clients with the particular example.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

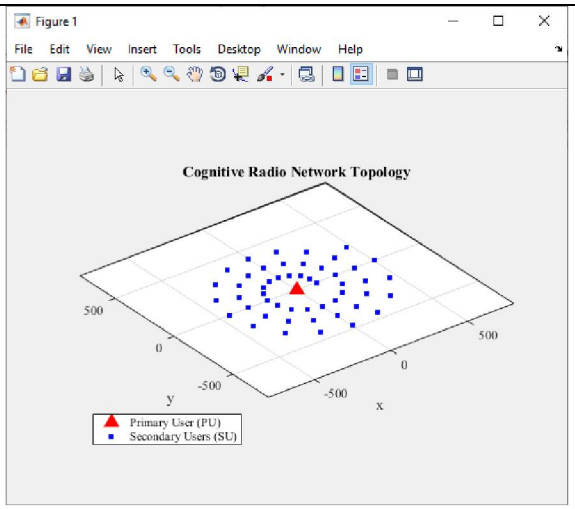

Fig 4.1 Cognitive Radio Topology

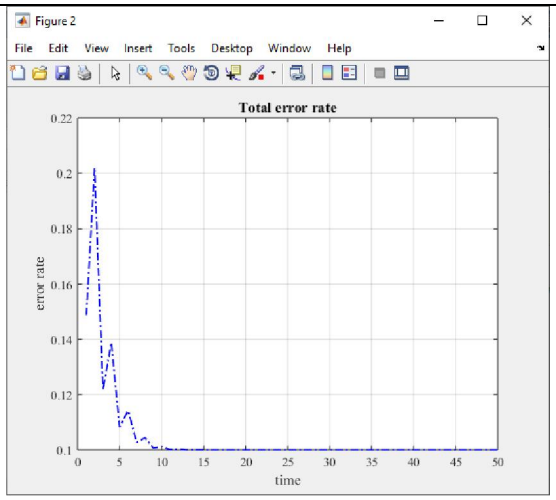

Fig 4.2 Total Error Rate

The Total mistake rate is displayed in the fig 4.2. The absolute blunder rate is start 15 % for 1 sec. As the diagram shows that all out detection-probabilities to 20.05 % via the time-span of 2 sec. Unexpectedly, the all out blunder speed is reduction to 10.00 %. The consistent states mistake is 10.00 %.

Similarly, fig 4.3 shows the results of a simulation comparing the sensing performance of various N.E.S and suggested methodologies. This paper's location probability calculation is more accurate than the standard calculation under the same fake caution likelihood because of four harmful nodes in psychologically distant organization.

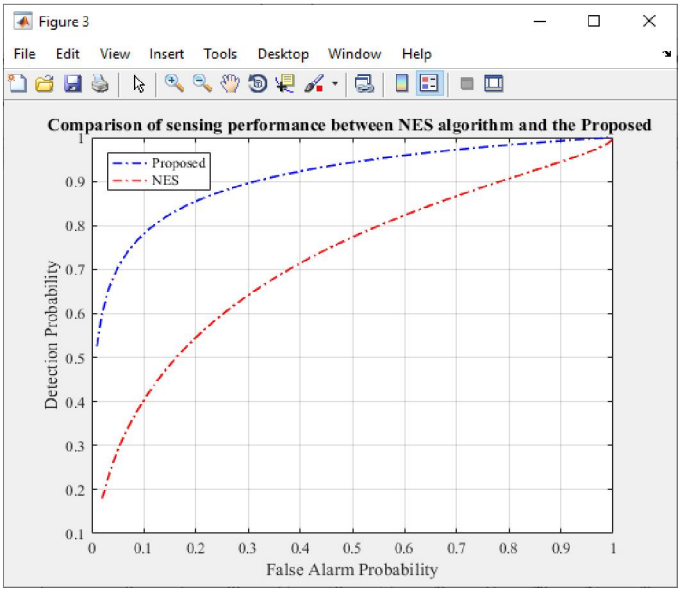

Fig 4.3 Analysis of the Similarities and Differences in the Sensing Capabilities of the Proposed and N.E.S Algorithms

V. CONCLUSION

The detection probability increases with the rise in false alarm probability, with a maximum probability capped at 1. In the NES Algorithm, the detection probabilities range from 0.813 to 0.931 for false alarm probabilities of 0.6 to 0.9, respectively. Conversely, in the proposed Algorithm, the detection probabilities range from 0.973 to 0.999 for the same false alarm probability range. The maximum interaction time for the NES + SSB Algorithm and the Proposed Algorithm is recorded at 274.1583 and 476.7970, respectively, at a safety index value of 120.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

REFERENCES

[1]. Abbas, Sana-e-Zainab, S & Wajahat 2010, 'An Efficient Algorithm for Secure & Fair Dynamic Spectrum Access in Cognitive Radio Networks', Canadian Journal on Multimedia and Wireless Networks, vol. 1, no. 3, pp. 173-177.

[2]. Amarnathprabhakaran, A & Manikandan, A 2013, 'An Efficient Communication and Security for Cognitive Radio Networks', International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 2, issue 4, pp. 1689-1696.

[3]. Anand Z Jin & Subbalakshmi, KP 2008, 'An analytical model for primary user emulation attacks in cognitive radio networks', DySPAN 2008, 3rd IEEE Symposium, IEEE, pp. 1-6.

[4]. Atta & Alireza 2012, 'A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Direction', Proceeding of IEEE, pp. 3172-3186.

[5]. Bhattacharjee, Suchismita & Ningrinla Marchang 2015, 'AttackResistant Trust-Based Weighted Majority Game Rule for Spectrum Sensing in Cognitive Radio Networks', International Conference on Information Systems Security, Springer, pp. 441-460.

[6]. Bhattacharya, PP, Khandelwal, R, Gera, R & Anjali Agarwal 2011, 'Smart radio Spectrum management for Cognitive radio', International journal of Distributed and parallel systems, vol. 2, no. 4, pp. 12-24.

[7]. Cabric Danijela M Mishra & Brodersen, RW 2004, 'Implementation issues in specrtum sensing for cognitive radios. Signal Systems and Computers', Conference record of 38th Asilomer Conference, IEEE, vol. 1, pp. 772-776.

[8]. Chen, R, Park, J & Reed, JH 2008, 'Toward secure distributed spectrum sensing in cognitive radio networks', Communications Magazine, IEEE, vol. 46, no. 4, , pp. 50-55.

[9]. Dubey Rajni, Sanjeev Sharma & Lokesh Chouhan 2012, 'Secure and trusted algorithm for cognitive radio network', Ninth International Conference on Wireless and Optical Communications Networks (WOCN), IEEE, pp. 1-7.

[10]. Etkin, R, Parekh, A & Tse, D 2005, 'Spectrum sharing for unlicensed bands', Proc. IEEEDySPAN 2005, IEEE, pp. 251–258.

[11]. FCC 2003, 'Notice for Proposed Rulemaking (NPRM 03-322)', Facilitating Opportunities for flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies. ET Docket, pp. 03- 108.

[12]. Feng Lin, Robert C Qiu, Zhen Hu, Shujie Hou, Lily Liy, James P Browningz & Michael C Wicks 2012, 'Cognitive Radio Network as Sensors: Low Signal-to-Noise Ratio Collaborative Spectrum Sensing', Proceedings of Aerospace and Electronics Conference (NAECON), IEEE, pp. 978-985.

[13]. Harish Ganapathy, Constantine Caramanis & Lei Ying 2010, 'Limited Feedback for Cognitive Radio Networks Using Compressed Sensing', IEEE 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton), IEEE, p. 10901097.

[14]. Haykin & Simon 2005, 'Cognitive radio: brain-empowered wireless Communication. Selected Areas in Communications', IEEE Journalon, vol. 23, no. 2, pp. 201–220.

[15]. Haykin & Simon 2010, 'Cognitive radio: brain-empowered wireless communications', IEEE Journal of Selected Areas of Communication, vol. 2, pp. 201-220.

[16]. Ian F Akyildiz, Won-Yeol Lee & Kaushik R Chowdhury 2006, 'Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey', Computer networks, vol. 50, no. 13, pp. 2127- 2159.

[17]. Januszkiewicz & Lukasz 2010, 'Simplified human body models for interference analysis in the cognitive radio for medical body area networks', 8th International conference on Medical Information and Communication Technology, IEEE, pp. 15-24.

[18]. Juebo & Long Tang 2012, 'Research and Analysis on Cognitive Radio Network Security', Wireless Sensor Network, vol. 4, pp. 120-126.

[19]. Khuong Ho-Van & Thiem Do-Dac 2018, 'Reliability-Security Tradeoff analysis of Cognitive Radio Networks with jamming and licensed interfernce', Wireless Communication and Mobile Computing, Hinadwi, vol. 2018, pp. 1-15.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 8, April 2024

[20]. Kwang Cheng Chen, Peng-Yu Chen, Neeli Prasad, Ying-Chang Liang & Sumei Sun 2009, 'Trusted cognitive radio networking. Wireless Communications and Mobile Computing'.

[21]. León, Olga, Juan Hernández-Serrano & Miguel Soriano 2010, 'Securing cognitive radio networks', International journal of communication systems no. 5, pp. 633-652.

[22]. León, Olga, Juan Hernández-Serrano & Miguel Soriano 2010, 'Securing cognitive radio networks', International Journal of Communication Systems, vol. 23, issue 5, pp. 633-652.

[23]. Mao, Huaqing & Li Zhu 2011, 'An investigation on security of cognitive radio networks', International Conference on Management and Service Science (MASS), IEE, pp. 1-4.

[24]. Matteo Cesana, Francesca Cuomo & Eylem Ekici 2010, 'Routing in cognitive radio networks: Challenges and solutions', Ad Hoc Networks, Elsevier., pp. 18-39.

[25]. McLoone, Safdar, GA & O'Neillne, M 2009, 'Common Control Channel Security Framework for Cognitive Radio Networks', IEEE 69th, Vehicular Technology Conference, VTC Spring 2009, IEEE, pp. 26-29.

[26]. Meng, T 2015, 'Spatial Reusability-Aware Routing in Multi-Hop Wireless Networks', IEEE TMC, DOI 10.1109/TC.2015.2417543 .

[27]. Mitola, J & Maguire, GQ 1999, 'Cognitive Radio: Making software radios more personal', IEEE personal Communications, vol. 6, no. 4 , pp. 13-18.

[28]. Muhammad Ayzed Mirza, Mudassar Ahmad, Muhammad Asif Habib,Nasir Mahmood, Nadeem Faisal, CM & Usman Ahmad 2018, 'CDSS:Cluster-based distributed cooperative spectrum sensing model against primary user emulation cyber attack', The Journal of Supercomputing, Springer, Available Online, pp. 1-17.

[29]. Parvin Sazia & Farookh Khadeer Hussain 2012, 'Trust-based security for community-based cognitive radio networks', IEEE 26th International Conference on Advanced Information Networking and Applications, IEEE, pp. 518-525.

[30]. Parvin, Sazia & Farookh Khadeer Hussain 2011, 'Digital signature based secure communication in cognitive radio networks', Broadband and Wireless Computing, Communication and Applications (BWCCA), IEEE, pp. 230-235.