Security Threats in Cognitive Radio Networks

Abdul Hameed Ansari[1], Shreyas Kumawat[2]
[1,2]*Department of Electronics and Telecommunication Engineering, Pravara Rural Engineering College, Loni, Ahmednagar, M.S. India*

Abstract **- A cognitive radio system has the ability to observe and learn from the environment, adapt to the environmental conditions, and use the radio spectrum more efficiently. These Radios are used all over the world in numerous wireless communication networks due their incredible features and ability to operate dynamically. In last couple of decades, lots of improvements has been done in cognitive radio environment to improve the system and end user experience. Many efficient models and algorithms were proposed by various researchers for spectrum sensing in cognitive radios. But still there are lots of security threats affecting the network. Many different attacks are performed on the cognitive radio networks which intends to harm the communication causing various problems and issues for the user and the system. In this paper, we review many different security threats and solutions for them based on the Open Systems Interconnection(OSI) layers of the cognitive radio network. Also, we discuss about the prevention of network from malicious users and later we express blockchain based security methods for spectrum sensing in cognitive radio network.**

Index Terms **- Cognitive Radios, Security, Spectrum sensing, jammer, blockchain.**

INTRODUCTION

There has been a huge increase in wireless communication systems in recent decade. Many communication sectors are using cognitive radio systems in their network. For such networks, fixed spectrum policy is implemented, i.e, only authorized users(primary users) can use the spectrum for very long time. This creates spectrum scarcity due to increase in demand. To tackle such problem, dynamic spectrum management is used. In this case the secondary users(unlicensed users) can use the spectrum whenever the spectrum is idle or not used by the primary user. This creates an efficient system which fulfills every users demand. To build such system, numerous algorithms and models have been proposed these past years which can perform faster, efficient and cause less errors in the spectrum sensing. Even with better spectrum sensing algorithms, these networks are vulnerable to various security threats, few general examples such as jamming, spectrum sensing data falsification attack (SSDF), Primary user emulation attack (PUE) and many other related to the transceiver or the layers of the cognitive radio network. These security threats creates interference in the network which results in communication loss, transmission of data of users, faults and error in the spectrum sensing and missed detection of spectrum holes, etc[18-19].

These attacks are carried out on the layers(Physical, Link, Network, transport and Application layer) of the cognitive radio network. Malicious users/attackers perform these attacks with an intent to harm the network and create disturbance. Every attack has its own specific method, feature and use. These attacks create disturbance to the legitimate user which on other hands benefits the attackers in their own desired way or aim. These attacks can be performed on the transceiver, primary and secondary users, on the communication network, on specific nodes in the network and the cognitive radio itself. In further chapters we will see detailed classification and information of these attacks.

To fightback these attacks, the cognitive radio system should [18-19] detect that there is a malicious attempt getting performed in the network and tackle the problem with specific methods related to the type of attack. Many different methods has been modelled and presented by researchers to solve such problems, we will discuss those in further chapters.

In this paper, we review some of the latest advancements in security and protection for cognitive radio networks. We discuss the different types of attacks, solutions presented by many researchers and future scope. We also review some methods and research done to detect malicious users in the cognitive radio environment. Along with that we

mention some blockchain based methods used in spectrum sensing environment.

literature survey

F. Slimeni, Z. Chtourou and A. B. Amor [1] proposed, "Reinforcement Learning Based Anti-Jamming Cognitive Radio Channel Selection". In this work, author mentions the problems created by jamming in cognitive radio networks. They propose a model based on Q-learning approach and Markov Decision process. Their method avoids any channel in the cognitive radio network which is jammed, allowing the network work smooth and without any problem.

A. Krayani, M. Farrukh, M. Baydoun, L. Marcenaro, Y. Gao and C. S.Regazzoni [2] proposed, "Jammer detection in M-QAM-OFDM by learning a Dynamic Bayesian Model for the Cognitive Radio". In this paper, the author describes recent trends in IoT devices which works in cognitive networks. They mentions problems associated with the network about jamming attacks. To detect the problems , they proposed couple of methods, single and bank parallel methods. These methods are based on Dynamic Bayesian Network and works in OFDM.

Furqan, H.M., Aygül, M.A., Nazzal, M. et al. [3] presented, “Primary user emulation and jamming attack detection in cognitive radio via sparse coding”. In this research, the author mentions the Primary user emulation attack which decreases the utilization of spectrum in cognitive radio. They propose a method based on sparse coding which detects the jamming attack and displays difference in real primary user, the jammer node and the blank spectrum space.

TYPES OF ATTACKS

Cognitive radios are highly vulnerable to security threats. We can see the Open Systems Interconnection (OSI) layers of cognitive radio network in figure 1.

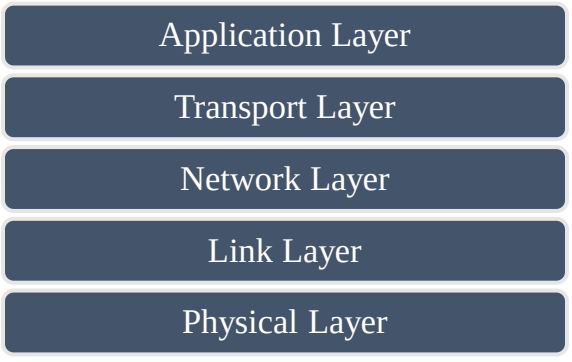

Figure 1. OSI Layers in Cognitive Radio Network

Over the past couple of decades, lots of threats and attack types have be designed and upgraded as per the advances in security upgrades have been made in the cognitive radio networks. Each attack model has specific features such as frequency range, mobility, ability to jam multiple nodes, ability cooperate with other jammers, phase and time, etc. These threats are divided into different categories based on their targeted layer. Classification these are given in figure 2. [5,6,7]

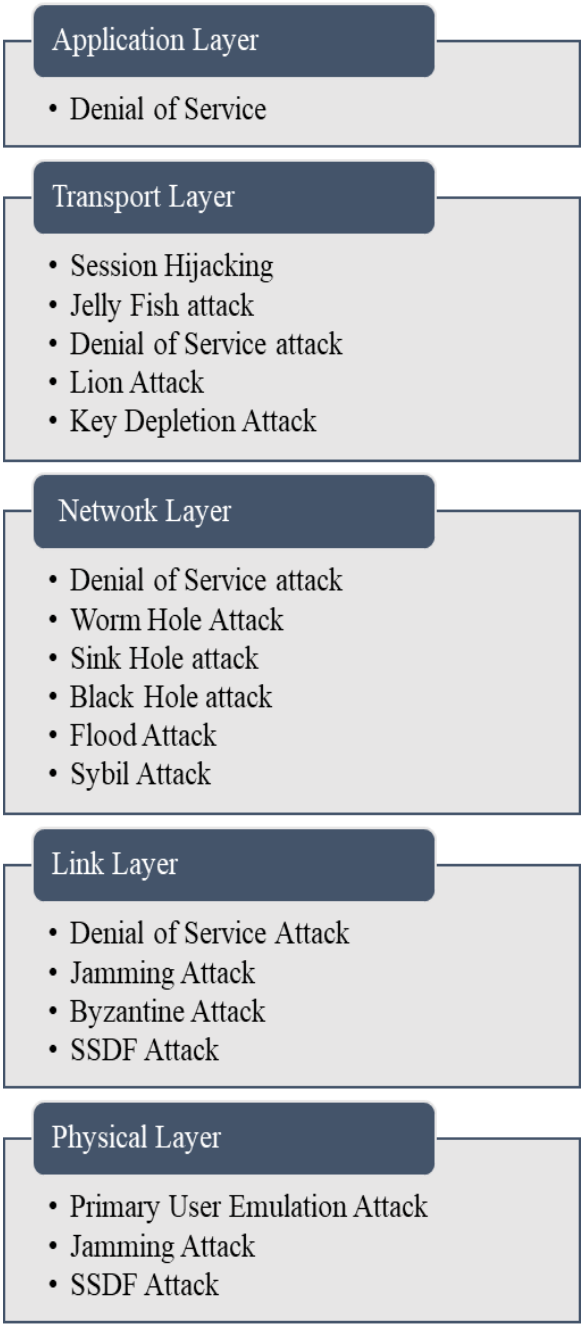

Figure 2. Attacks Performed on different OSI layers in Cognitive Radio Network

EFFECTS OF ATTACKS AND SOLUTIONS TO THEM

1. Application Layer:

A. Denial of Service attack:
In this attack the licensed Primary user and secondary users detects that the channel is in use, but it is occupied by the malicious user. This attack creates high false detection in the cognitive radio spectrum sensing. This attack can be solved by using trust metrics and dynamic path identifiers.

2. Transport Layer:

A. Session Hijacking:
In this attack, the attacker hijacks the session between two nodes. Which causes the session to pause. This attack can be solved by using encryption and ciphering of the packets sent.

B. Jelly Fish Attack:
This attack captures the closed loops and generate false delay in the communication. Due to this there is less throughput occurred in the network. This attack can be avoided by creating cluster-based routing.

C. Lion Attack:
This attack is triggered by the Primary User Emulation attack which creates distortion in the TCP. This results in high packet timeout which causes packet loss and delay. This attack can be tackled by using encryption and ciphering.

D. Key Depletion Attack:
The attacker creates huge number of session keys which breaks the cipher system due to repetition of one of the keys. This attack can be avoided using cryptography and key management.

3. Network Layer:

A. Worm Hole Attack:
In this attack the attacker tunnels the messages and packets and sends them to some far away part of the network, later replying to those messages causing disturbance in the network. This attack can be tackled using authentication in routing for the network.

B. Sink Hole Attack:
The attacker disguises as the fastest route to the base station for the nodes. This causes all the closest nodes to route through the attackers device which increases the control of network in attackers hands. This attack can be repelled by applying in delay in every hop.

C. Black Hole Attack:
This attack simply creates hindrance in the transmission or communication of users, nodes and the radio itself. It can be tackled by using authentication in the routing for the network.

D. Flood Attack:
In this attack, the attacker broadcasts it's message on all the nodes in a specific part of the network which creates confusion to other nodes thinking that the attacker is in nearby nodes but in reality, it is far away. This makes the anti-security methods to confuse and hard to tackle the problem. Still this attack can be tackled using many different cooperative algorithms.

E. Sybil Attack:
This attack is designed to restrict the access of licensed user to use the spectrum. The attacker creates fake identities which sends information to the network creating a smokescreen in front of network. This attack can be repelled by using Radio Resource testing and Random Key Predistribution.

4. Link Layer:

A. Jamming Attack:
Jamming is a vast concept, it has lots of types, effects, purposes and methods. Generally, a jammer device stops the licensed user(primary user) from using the channel and on the other hand the attacker uses the spectrum. This also makes secondary user unable to user the channel which is allotted to the primary user.

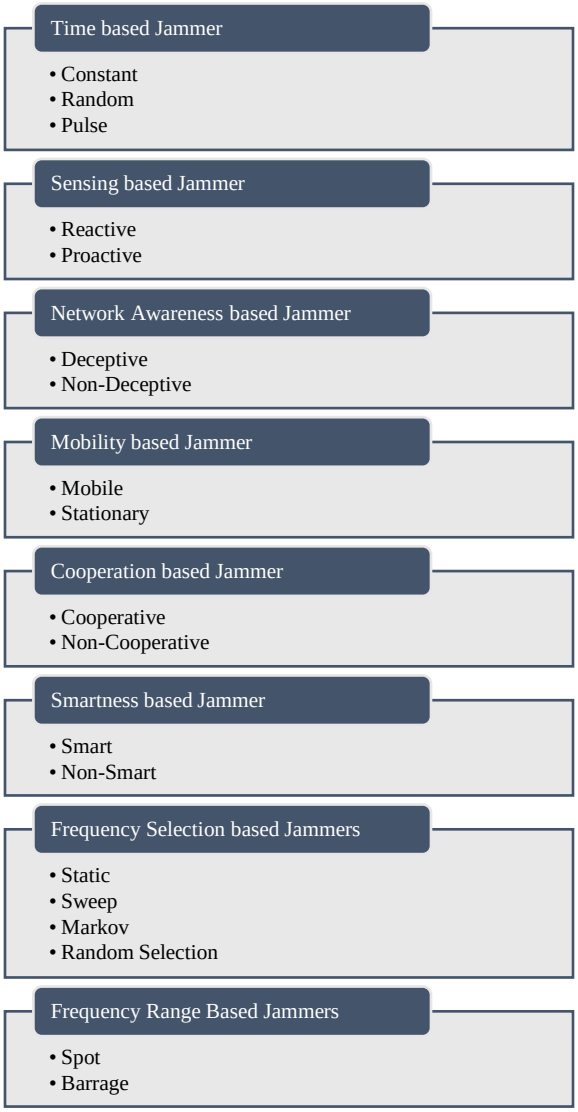

Figure 3. Types of Jammers in Cognitive Radio Network.

Figure 3. displays different types of jamming attacks based on the features of attack models [4]. These jammers creates lots of problems in the cognitive network such as preventing users from using the spectrum, denial of service, malicious use of spectrum by the attacker, halt in the communication and transmission in the network, etc.

Before tackling a jammer, it is necessary to detect it. Each jammer type has different of jamming methods which leads to different anti-jamming methods in detecting, solving and tackling the attack as well. Most of the anti-jamming algorithms are based on Q-learning approach but varies according to the attack.

B. Byzantine Attack:

Byzantine attack is a type of Spectrum Sensing Data Falsification (SSDF) attack. It sends false reports to the fusion center creating a great degade in spectrum sensing operation. This attack can be avoided or fixed by using homogenous and heterogenous algorithms.

C. Spectrum Sensing Data Falsification (SSDF) Attack:

This attack is pretty general and popular in case of cognitive radio networks. In this, the attacker sends false information to the cognitive radio which in turn disturbs the spectrum sensing process and further causes inefficiency in the spectrum due to inability of licensed users to use the spectrum. This attack can be repelled by various types collaborative spectrum sensing techniques. These techinques are improved since many years and varies according to the type of attack.

5. Physical Layer:

A. Primary User Emulation (EUA) Attack:

In this attack, a malicious user is disguised as primary or secondary user by emulating the signal. This user gains access to the spectrum which causes interference in the communication of legitimate licensed users as well as secondary users. This attack can be avoided by using End-to-End authentication in communication network and using trust metrics.

1.Malicious user detection

Detecting a malicious user is one of the initial steps of security in the cognitive radio network. There has been a lot of research developed for this topic to tackle these types of users. Figure 4 displays general cognitive radio network with malicious user. In [10], the authors proposed an approach based on physical layer coding and Friend-or-Foe detection. They worked on this method to tackle the malicious user which impersonates the secondary user. Their method was able to detect the malicious user with very high success rate and less false alarms.

In [11], the researchers used Fastprobe method to detect the malicious user. In this method, the base station keeps learning the transmission information of legitimate secondary users which creates a trust in between base station and secondary user. Due to this,

a difference is observed in between a malicious user and secondary user as the values available in the base station fails to meet for the malicious user. They consider metrices such as pathloss and power level of the transmission for detection.

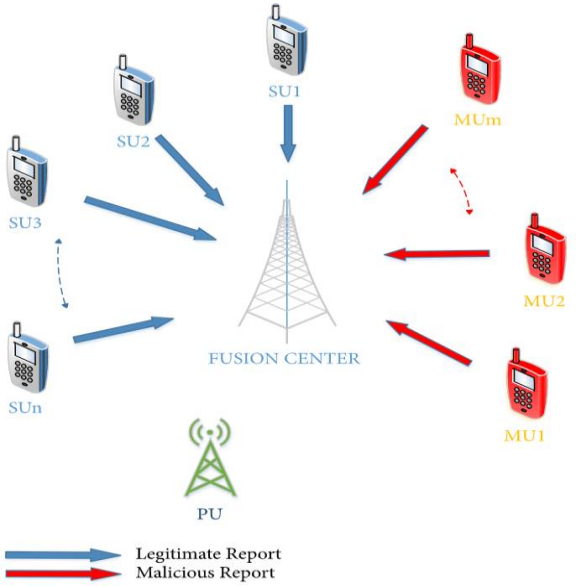

Figure 4: A network with legitimate and malicious users.

In [12] the authors presented a machine learning based approach to detect malicious users. They user support vector machine which is an effective machine learning algorithm that checks data from different mediums. They took fading and non-fading channel network to test their method. Their method allows the fusion center to learn the spectrum sensing result and based on that it takes decision if the user is legit or malicious. The results they displayed showed an incredible performance with perfect detection and classification of both types of users(secondary and malicious).

The work done in [13] proposes a defense against SSDF attack using density based malicious user detection in a wide-band environment. Their proposed method is implemented on compressive sensing matrix in compressive sensing and density clustering in machine learning. This algorithm allows the fusion center to distinguish between legitimate user and malicious user. Their result shows that the performance of the system with detection of malicious user works great with the help of legitimate user.

In [14], the researchers use a double adaptive threshold approach to distinguish between a legitimate user and malicious user. Their method works by measuring the weights of metrices by using maximal ratio combining. They assign fixed weights to the legitimate secondary users due to which the fusion center is able to understand the difference between the secondary user and the malicious user. Their method also detects a doubtful user which is in between the fixed weights and the malicious users weights. They displayed the results by comparing with various other methods in terms of probability of detection and probability of false alarm. Their method outstands every method they compared with.

2.Blockchain Technology in Cognitive Radios

The spread of Blockchain technology has increased with very high speed in recent few years. Due to the incredible concept of decentralization of any network and transaction between two or more peers has increased the popularity and usage of this technology. The best use of this technology can be seen in cryptocurrencies. There has been countless number of cryptocurrencies built on the concept of blockchain. Figure 5 shows a centralized and decentralized network.

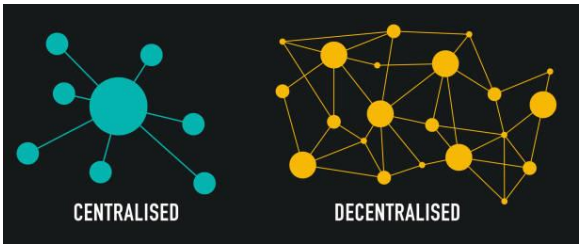

Figure 5. Centralized and Decentralized communication network.

The blockchain technology is highly secure due to its decentralization and cryptography. Blockchain is a a Distributed Ledger Technology (DLT). All the distributed ledgers in a blockchain network cannot be changed or altered. As well as all the hashes and transaction in between the ledgers are transparent. The distributed ledger is connected to the chain through nodes. These nodes are nothing but devices in any network which holds the information copy of blockchain. All these nodes are needed to verify any new block is added in a blockchain which creates a trusted and highly secure network.

A general blockchain consists of elements such as:

A. Ledger:

A ledger is a data stored on a node. It has information about the node, transactions and transfer of any data. Ledger can be accessed by the node and any changes

made in the ledger are synchronized and verified by all other nodes in the blockchain. Malicious attacks are reduced by the use of decentralized ledger.

B. Hash:

A hash is fixed mathematical string which is unique for every block and it is impossible to find or guess the hash value due to its highly secure hashing algorithm. A general blockchain uses SHA-256 algorithm.

C. Node:

A node is any electronic device which holds the copy of blockchain. Node validates, accept, reject and interact with any transaction or communication in the blockchain.

D. Keys:

There are two types of keys in blockchain, 1. Public key and 2. Private Key. These keys allow to communicate with other nodes. They are a part of Public-Key-Cryptography algorithm.

In cognitive radios, blockchain technology can create a very secure spectrum sensing environment. Such as in this work [8], the author explains a helper node-based spectrum sensing environment in cognitive radio network. In this, when a secondary user is trying to find a vacant space in spectrum, the nearby nodes will also help the user to achieve faster and more accurate detection with less false alarms. They used smart contract(a digital transaction used in blockchain) based on Ethereum blockchain which improves the trust in between helpers nodes and the secondary user. The method they proposed also helped the system to identify malicious users and malicious nodes due the failure of these users to meet the criteria denoted in the smart contract.

In [9], the researchers propose a blockchain based cooperative spectrum sensing method on a smart contract. There method allows the smart contract to execute requests and data transmission of secondary user automatically along with that they apply asymmetric encryption which blocks the malicious user to impersonate as secondary user, generally an SSDF attack. As the secondary user starts sensing data, it will generate a hash value which will be within the blockchain and can only be identified by the base stations. Their results displayed a good performance in terms of detection probability even in an environment of malicious users.

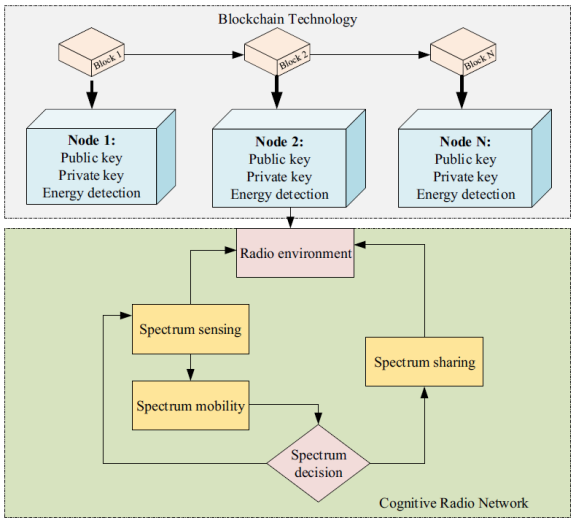

Figure 6: A Blockchain based spectrum sensing inside a cognitive radio network.

In [15], the authors have presented a spectrum sensing algorithm based on blockchain technology. Their algorithm is also able to detect malicious user. They converted the primary and secondary users as blocks in the chain. They allotted ledgers to each node. The public and private keys are given which contains information about PU, SU, location, etc. For spectrum sensing they used a popular method: Energy detection. And for detecting the malicious user, the digital signatures are used with the help of public key and private key. When the malicious user fails the verification in the blockchain, the user gets discarded and refused to access the spectrum.

An another blockchain based approach has been proposed in [16], the authors proposed a cooperative sensing mechanism along with integration of blockchain in the network. They assigned hash values and blocks to both primary and secondary users. Each transaction between these users will be done by verifying the keys and hash value. They have demonstrated a peer-to-peer connection in between these users. During the spectrum sensing, they have used energy detection method along with adaptive threshold. For the detection of malicious user, the energy and the blocks generated by the blockchain helps identifying the legitimate user and a malicious user. They displayed their result with a good performance by comparing their method to other methods. Their method was more stable, has high detection levels and low false alarm probability compared to other methods(FOF and TTA). Their method also performed good in terms of efficiency,

throughput, error probability and frame loss when the number of users increased.

For effectively identifying the vacant spaces in spectrum, there are helper nodes which helps users, but this causes more energy wastage. To solve this problem, researchers in [17] have proposed a smart contract-based spectrum sensing as a service method. In their method, they deploy a smart contract in the network for the user and helpers, if the helpers detect the vacant space accurately, then it will get the payment. They also present a two-threshold based voting method to detect helpers which are fraud or malicious and the algorithm discards them from the network. Their method displayed a good performance in terms of detection and false alarm for legitimate primary users in a malicious user environment for OR, Majority and logic. Also, their result showed a probability for malicious helper node.

CONCLUSION

In this review paper, we described various types of security threats in different OSI layers of cognitive radio networks. These threats create heavy damage to the network and the experience of users in many different ways. We discussed many different types of attacks and their impacts on the network. We also displayed numerous jamming attacks based on their features. Also, we given general solutions for many security threats with review of methods which helps detection of malicious users. We also reviewed some of the blockchain technology-based methods for spectrum sensing which provides good security and protection for the cognitive radios.

FUTURE SCOPE

The cognitive radio network is vast concept which holds major importance and need in our life. These networks are powerful and highly useful for networking. But they suffer from lots of security threats. Even with these threats, much different research has been done and methods has been proposed to take down these problems. Every new spectrum sensing algorithm introduced in the networks brings a new challenge to protect the network from malicious attacks. There are many areas in the field of protection of cognitive radio networks which can be improved and fixed in best possible way. Also, with the increase of new unique technologies such as blockchain, there are numerous possibilities which can help not only cognitive radio networks but as well as every wireless network.

REFERENCE

[1] F. Slimeni, Z. Chtourou and A. B. Amor, "Reinforcement Learning Based Anti-Jamming Cognitive Radio Channel Selection," 2020 4th International Conference on Advanced Systems and Emergent Technologies (IC_ASET), 2020, pp. 431-435, doi: 10.1109/IC_ASET49463.2020.9318287.

[2] A.Krayani, M. Farrukh, M. Baydoun, L. Marcenaro, Y. Gao and C. S.Regazzoni, "Jammer detection in M-QAM-OFDM by learning a Dynamic Bayesian Model for the Cognitive Radio," 2019 27th European Signal Processing Conference (EUSIPCO), 2019, pp. 1-5, doi: 10.23919/EUSIPCO.2019.8902495.

[3] Furqan, H.M., Aygül, M.A., Nazzal, M. et al. Primary user emulation and jamming attack detection in cognitive radio via sparse coding. J Wireless Com Network 2020, 141 (2020). https://doi.org/10.1186/s13638-020-01736-y

[4] Aref, M.A., Jayaweera, S.K. and Yepez, E. (2020), Survey on cognitive anti-jamming communications. IET Commun., 14: 3110-3127. https://doi.org/10.1049/iet-com.2020.0024

[5] R. Dubey, S. Sharma and L. Chouhan, "Secure and trusted algorithm for cognitive radio network," 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), 2012, pp. 1-7, doi: 10.1109/WOCN.2012.6331887.

[6] M. W. Akram, M. Salman, M. A. Shah and M. M. Ahmed, "A review: Security challenges in cognitive radio networks," 2017 23rd International Conference on Automation and Computing (ICAC), 2017, pp. 1-6, doi: 10.23919/IConAC.2017.8082089.

[7] Hlavacek, Deanna and J. Morris Chang. “A layered approach to cognitive radio network security: A survey.” Comput. Networks 75 (2014): 414-436.

[8] Suzan Bayhan, Anatolij Zubow, and Adam Wolisz. 2018. Spass: Spectrum Sensing as a Service via Smart Contracts. In 2018 IEEE

International Symposium on Dynamic Spectrum Access Networks (DySPAN).IEEEPress,1–10. https://doi.org/10.1109/DySPAN.2018.8610483

[9] Ji, Chu & Zhu, Qi. (2021). Smart contract-based secure cooperative spectrum sensing algorithm. International Journal of Distributed Sensor Networks. 17. 155014772110586. 10.1177/ 15501477211058673.

[10] S. Rahman Sabuj, M. Hamamura and S. Kuwamura, "Detection of intelligent malicious user in cognitive radio network by using friend or foe (FoF) detection technique," 2015 International Telecommunication Networks and Applications Conference (ITNAC), 2015, pp. 155-160, doi: 10.1109/ATNAC.2015.7366805.

[11] Jithesh M and Harish Kumar C H, 'Malicious user detection in cogntive radio networks. International Journal of Science and Research 2015. ISSN: 2319-7064.

[12] Md Shamim Hossain, Md Sipon Miah, Machine learning-based malicious user detection for reliable cooperative radio spectrum sensing in Cognitive Radio-Internet of Things, Machine Learning with Applications, 2021, 100052, ISSN: 2666-8270, https://doi.org/10.1016/j.mlwa. 2021. 100052.

[13] Hongxing Wu, Xuekang Sun, Caili Guo and Shiyu Ren, "Malicious user detection for wide-band cognitive radio networks," 2016 Asia-Pacific Microwave Conference (APMC), 2016, pp. 1-4, doi: 10.1109/APMC.2016.7931291.

[14] Muhammad Sajjad Khan, Muhammad Jibran, Insoo Koo, Su Min Kim, Junsu Kim, "A Double Adaptive Approach to Tackle Malicious Users in Cognitive Radio Networks", Wireless Communications and Mobile Computing, vol. 2019, Article ID 2350694, 9 pages, 2019. https://doi.org/10.1155/2019/2350694.

[15] Adnan Sajid, Bilal Khalid, Mudassar Ali, Shahid Mumtaz, Usman Masud, Farhan Qamar, Securing Cognitive Radio Networks using blockchains, Future Generation Computer Systems, Volume 108, 2020, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.03.020.

[16] Khanna, A., Rani, P., Sheikh, T.H. et al. Blockchain-Based Security Enhancement and Spectrum Sensing in Cognitive Radio Network. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-08729-0.

[17] S. Bayhan, A. Zubow and A. Wolisz, "Spass: Spectrum Sensing as a Service via Smart Contracts," 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), 2018, pp. 1-10, doi: 10.1109 /DySPAN.2018.8610483.

[18] A.H. Ansari, S. M. Gulhane and Pachore N. M., "Signal detection over fading channels in presence of correlated noise," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016, pp. 1186-1192, doi:10.1109/ICACDOT.2016.7877773.

[19] H. Ansari and S. M. Gulhane, "Cyclostationary method-based spectrum sensing and analysis using different windowing method," 2015 International Conference on Energy Systems and Applications, 2015, pp. 684-688, doi: 10.1109/ICESA.2015.7503437.