I.J. Wireless and Microwave Technologies, **2023, 6, 32-38**
Published Online on December 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.06.04

Mitigation of Byzantine attack using LSP algorithm in CR Networks through Blockchain Technology

Amith K S*
Visveswaraya Technological University of Karnataka, India “A J Institute of Engineering and Technology”/ Department of Computer Science, Mangaluru, 575006, India
E-mail: freekash@gmail.com
ORCID iD: https://orcid.org/0009-0006-8555-7298
*Corresponding Author

Yerriswamy T
Visveswaraya Technological University of Karnataka, India “K L E Institute of Technology”/ Department of computer Science, Hubbali
E-mail: swamy1976ty@gmail.com
ORCID iD: https://orcid.org/0000-0001-9790-402X

Received: 03 March, 2023; Revised: 12 April, 2023; Accepted: 16 May, 2023; Published: 08 December, 2023

Abstract: In the past couple of years, the research on the Byzantine attack and its defense strategies has gained the worldwide increasing attention. In this paper, we present a secure protocol to escape from the Byzantine attack in the cognitive radio networks. This protocol is implemented using the Lamport-Shostak-Pease algorithm and blockchain technology. A reliable distributed computing system must be able to handle the faulty components to deliver the error less performance. These faulty components send the conflicting information to the other parts of the system. As a result, it creates a problem which is similar to the Byzantine Generals Problem (BGP). In order to design a reliable system, it is necessary to identify and overlook such faulty components.

In the cognitive radio networks, there are the two types of users i.e. primary and secondary users. The primary users hold the licensed spectrum whereas the secondary users hold the leased spectrum. In these CR networks, there can be a similar problem like BGP while allocating the spectrum to the secondary users. Also, it requires all the users to agree on a common value, even with some faulty users in the network. This is called as the Byzantine Agreement. Here we have addressed this Byzantine General problem to develop a reliable and secure spectrum allocation using the Lamport-Shostak-Pease algorithm. It can solve the BGP for $n \geq 3m+1$ users in the presence of ‘m’ faulters. In this implementation, the blockchain technology is used as the efficient decentralized database which records all the transactions of the users, like exchanging currency, mining, updating the blockchain and auctioning the spectrum for lease.

Index Terms: Blockchain Technology, Byzantine attack, Security, Lamport-Shostak-Pease Algorithm, Secure Blockchains and Cognitive Radio.

1. Introduction and Related Work

In the distributed system design [1], the reliability is an important parameter to be considered. This parameter tells the ability of the system to work efficiently even in case of failures in the different parts of the system. There are different types of failures in the components. One of them is the crash failures in which the failed component has no response. And in some other failures, they send out the conflicting messages. These failures create a situation that is like the Byzantine Generals Problem [2, 3, 4].

In this digital era, the demand for wireless technology has been increased tremendously with an increase in the number of wireless devices and services. This has resulted into the scarcity of spectrum to serve the needs of wireless communication devices. In order to solve this problem and to utilize maximum spectrum resources, the cognitive radio technology [5, 6, 7] has been proposed. In this technology there are the two types of users, those are the primary and secondary users. Initially, the secondary user senses the spectrum to access it. The concept of cooperative spectrum sensing has been introduced to reduce the drawbacks like noise, path loss, shadowing, and fading. In some cases, the secondary users participating in the cooperative spectrum sensing process may report the false information which results into the wrong decision-making. Such scenario of malicious falsification is similar to Byzantine attack. From a decade, a plenty of research has been carried out in this field to defense/mitigate the problem of Byzantine Attack. But according to the survey, still there is a requirement to be fulfilled for the efficient spectrum sensing, allotment, and utilization. Also, in terms of mitigation of Byzantine General attack problem and it's defense techniques.

Let us discuss more in detail about the Byzantine Generals attack problem in the context of Cognitive Radio Networks and cooperative spectrum sensing and allotment. Imagine, for example, there is one primary user (PU) and two secondary users (SU_1 and SU_2) in a particular CR network. Primary user is the licensed user of the spectrum whereas the secondary users will access the spectrum on lease. Assume that the primary user is the only faulter as shown in Fig.1, which gives conflicting information to the half of the secondary users that the value of their order is 0 (no spectrum allocation), and the other half that their value is 1 (spectrum allocation). After receiving the order, the secondary users should send the received information to each other. Upon collecting the information from SU_2 then the SU_1 understands that there is the conflicting information from the PU and SU_2. Similarly, the same analysis will be made by the SU_1. Finally, it is very difficult to make a decision. This situation is similar to the Byzantine Generals Problem in terms of spectrum allocation and the cognitive radio networks.

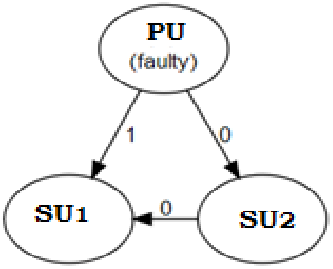


Fig.1. Byzantine Generals Problem: Primary user is faulty

Consider in another case in which SU_2 is malicious and sends the wrong information to the other secondary user SU_1 as shown in Fig. 2. In this case, the secondary user SU_1 receives conflicting information from the primary user and the secondary user SU_2. Finally, it will be difficult to take the decision for the secondary user SU_1. The similar situation happens for the SU_2 when the SU_1 is malicious. These three scenarios are very similar to the Byzantine Generals Problem in the spectrum allotment of cognitive radio networks.

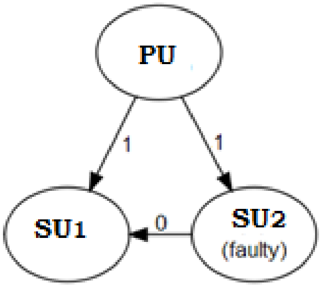


Fig.2. Byzantine Generals Problem: Secondary user SU2 is faulty

One of the possible solutions is to send oral messages (which are forgeable). In this solution to cope-up with m-traitors, it must be needed with a minimum of (3m+1) generals. Following assumptions are to be considered to use the oral messages.

Assumption 1: Every message is delivered correctly.

Assumption 2: The receiver can identify the sender upon reception of every message.

Assumption 3: The receiver can detect if there is no message.

The first two assumptions assure that there is no interference from a traitor. Assumption 3 will foil a traitor who is silent. In this method, also there is a possibility that the traitor can lie which makes the solution to be very difficult. To overcome this, we have another solution which is to use un-forgeable (signed) messages. In this method in addition to the above three assumptions, we have two more assumptions:

Assumption 4: Signature is not forgeable.

Assumption 5: Everyone can verify the signature whether it is authentic or not.

In this approach, the Primary user (PU) sends a signed message to all the secondary users (SUs). Then the SU adds his signature and sends it to the other secondary users. This solution is possible for any number of generals and possible faulters.

Data is the most valuable asset of any business. Large amount of data will be captured by the intelligent devices like automatic vending machines, IoT based security systems. With the help of big data analysis technology, the processing of large amount of data has become very easy. Also, there should be a necessary platform to access and exchange the data with high security and at a low cost. The blockchain technology [8, 9] can provide the above features at a low cost. It is a new technology which integrates decentralization, distributed computation, asymmetric encryption, timestamp, consensus algorithm. Recently, the attention has been increased towards this technology due to its security, anonymity and data integrity without involving any third party. In an application of any currency transaction, the traditional technology is often centralized and controlled by the third-party organization and all information is controlled by it. However, Blockchain technology can solve this issue efficiently.

Nowadays, the blockchain technology [10] is most widely used for enabling and securing spectrum sharing in cognitive radio networks (CRNs). The spectrum sharing mechanisms have the more importance due to the needs related to increasing spectrum usage. This protocol is also widely used in virtual currency transactions. In such applications, it is necessary to provide the secure and reliable spectrum sharing mechanism. Here, blockchain is considered as the decentralized database technology in which the owner of the data maintains control. As a general-purpose database technology, it can be applied to virtually any business context. But it cannot be a cost-effective solution in all types of businesses. Following features are to be considered as the requirements before applying it to the any business application--decentralization, transparency, immutability, availability, and security.

2. Review of Previous Studies

In the paper [11], by Jun Du, Xiang et al., the problem of cooperative spectrum sensing (CSS) in censoring-enabled CRNs is explained in detail. An optimization problem has been formulated to improve the performance of cooperative spectrum sensing in the censoring-enabled the Cognitive Radio Networks and developed an expectation maximization-based algorithm to solve it, where the presences of primary user and the reliabilities of each secondary user can be jointly estimated. The proposed robust CSS scheme performs better than the previous reputation-based approaches.

In the paper [12], Byzantine Agreement model for Intrusion Detection, Prevention & Counter-measure Systems (IPS) has been proposed by C. Fernando. The current IPSs have the drawbacks like inability to survive failures and malicious attacks. A Secure Architecture and Fault-Resilient Engine (SAFE) is developed to solve the Byzantine General's Problem. Byzantine Agreement Protocols will be used to achieve consensus about which nodes have been compromised or failed, with a series of synchronized, secure rounds of message exchanges. Once a consensus has been reached, the offending nodes can be isolated and counter-measure actions can be initiated by the system.

The Byzantine attack in CSS is called as the spectrum sensing data falsification (SSDF) attack. It is one of the major drawbacks in CRNs. In the paper [13], a tutorial on the recent advances in the Byzantine attack and defence for CSS has been provided. The existing Byzantine attack behaviours and its attack parameters have been discussed. The spear-and-shield relation has been proposed for the Byzantine attack and defence model.

In the paper [14], in order to improve the spectrum utilization, Collaborative (or distributed) spectrum sensing model is proposed for the CRNs. The data fusion technique is adopted in the collaborative spectrum sensing. Also analysed the problem of Byzantine attacks in CRNs, where malicious users send false sensing data to the fusion center (FC) leading to an increased probability of spectrum sensing error. In this method, FC will identify the malicious attackers and remove from the data fusion scheme. From the results and analysis, this model proves as robust against Byzantine attacks and removes them from CRN.

In the paper [15], it has been proposed that a defence scheme which exploits the cognitive process of spectrum sensing and spectrum access. Also, the proposed model by author is more reliable and highly robust over the other state-of-the-art model. It is because of its capability in spectrum sensing performance and identification of malicious users. In this paper the optimal cooperative spectrum sensing scheme is designed. Also, the proposed model can exploit the information of falsified reports to improve the global sensing performance. From the numerical simulations, it can be verified that the proposed scheme’s performance even in the critical cases of a greater number of malicious users.

In the paper [16] by Juan Sheng et al., a novel attacker-identification algorithm with dynamic attack probability is proposed. This model can enhance the overall detection probability effectively to reduce the false alarm probability. Also, a weight coefficient is explored for energy detection to make a robust system. Simulation results show that the proposed algorithm performs better than the previous works.

Many of the existing schemes are focussed on how to mitigate the negative effect of Byzantine attack under some assumptions like attackers are in minority and/or a trusted node exists for data fusion. Without depending on these assumptions, the authors [17] have analysed the integrated model of Byzantine attack and FC. A generic Byzantine attack model is designed by analysing sophisticated malicious behaviours. In this model the author has derived the condition which makes the FC blind because of malicious users. Also, an optimal attack strategy is proposed to maximize Baye’s risk. In addition to this, an estimation algorithm is proposed to have the knowledge of the attack. In this model, we have adopted the optimal fusion rule.

In the paper [18], two new counter-attacks are proposed which integrates the Byzantine coalition head attack and the CSS.

First counter-attack model: The probability of attack and selection formula for coalition head are derived from the exchanged SNR values.

Second counter-attack model: In this model, counter-attack for multi-channel Byzantine attack and the probability of available channel detection in the presence of Byzantine attackers is derived. Integration of these two counter-attack models can eliminate Byzantine attackers in the CRNs.

In the paper [19], the author has described the problem of Byzantine Attack in secure network communication. Also the network security assumptions and its Byzantine attacks are discussed. Then a secure random network coding model was proposed for resisting the Byzantine attacks. In this model, the Cipher Block Chaining technology is combined with random network coding. The correctness and security is proved with the results. Finally a safety code is realized.

3. Implementation

The proposed model consists of two types of users i.e., the primary and secondary users. In the cognitive radio networks, primary users are the licensed users of spectrum. They can lease their allotted spectrum to the secondary users. There are the M number of primary users. They work as the half duplex transceivers. And the spectrum is divided into K orthogonal channels. These channels are symmetric with an assumption error free communication. Also the time is divided into T_2,..T_n equal length slots and T_1 represents overhead. A common control channel is used for the transmission of control information. The MAC frame is shown in the Fig. 3 It used for information exchange over the allotted time slots.

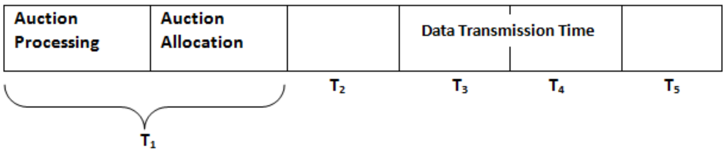


Fig. 3. MAC frame time slots to access a spectrum

A CR which has the processing power to update the blockchain will be rewarded with cryptocurrency. Primary users can lease their allotted spectrum using these cryptocurrencies. This protocol can convert a real currency into cryptocurrency and vice versa. Also, the secondary user with limited processing power can obtain these cryptocurrencies in lieu of updating the blockchain. It happens in two approaches i.e., simulation and practical. In the simulation approach, a CR can transmit the data by earning enough coins of cryptocurrency in the blockchain. In the practical approach, a CR can transmit the data only if it has enough processing power, battery, and time. Blockchain is a database which records all the transactions of the users, like exchanging currency, mining, updating the blockchain and auctioning the spectrum for lease.

Spectrum Access using Lamport-Shostak-Pease Algorithm

In this paper, we have extended the application of the Lamport-Shostak- Pease (LSP) algorithm to solve the Byzantine General's Problem in accessing the spectrum of a cognitive radio network. Following is the terminology to be considered in this algorithm. A commanding general is considered as the primary user.

A primary user (PU) must send an order to his n-1 secondary users (SUs) such that:

IC 1: All loyal secondary users obey the same command.

IC 2: If the primary user is loyal, then every loyal secondary user obeys the command that he sends.

Here, IC 1 and IC 2 are known as the interactive consistency conditions. According to the scientists Lamport, Shostak, and Pease, the Byzantine Generals problem can be solved by using the Oral Messages algorithm (Unsigned messages).

Unsigned Messages algorithm (UM)

This algorithm is designed for one primary user with (n-1) secondary users-based model. It is the recursive algorithm with m-number of traitors/faulters where m is the non-negative integer.

Whenever the primary user sends a message, the value **I** will be received by the secondary user. Require default value $\mathbf{I_{def}}$ if traitorous primary user does not send a message. Here, if the value of **I** is '1' then it represents to access the spectrum of a cognitive radio network. If the value of **I** is '0' then no spectrum access in that particular CRN. As and when the secondary user is assigned with a channel of a spectrum, user releases the coins of cryptocurrency to the primary user. The entire database of the transaction will be updated in the blockchain.

Define function **majority**$(\mathbf{I_1,...,I_{n-1}}) = \mathbf{I}$ if a majority of the values $\mathbf{I_i} = \mathbf{I}$.

Algorithm UM(n, 0):

Step1: The PU sends **I** to all the secondary users.

Step2: All SUs use the value **I** received from the PU or the value $\mathbf{I_{def}}$ if nothing is received.

Algorithm UM(n, m), m>0:

Step1: The primary user(PU) sends value **I** to all the secondary users(SUs).

Step2: For each SU_i, the PU sends value $\mathbf{I_i}$ to the SU_i. In case of no message from the PU the value '$\mathbf{I_{def}}$' is considered. Now SU_i acts as the new PU to perform UM(m-1) with (n-2) remaining SUs.

Step3: For each i & each j≠i,

let $\mathbf{I_j}$ = value SU_i received from SU_j in step (2) or $\mathbf{I_{def}}$ if no value received. Now each SU computes the majority values from $\mathbf{(I_1,....., I_{(n-1)})}$ to take the decision.

4. Results

In our simulation, LSP and Pease algorithm has been used to access the channel of a spectrum in the CRN by solving the Byzantine Attack Problem. Consider n=4 with 1-traitor the following results can be obtained with UM(4,1).

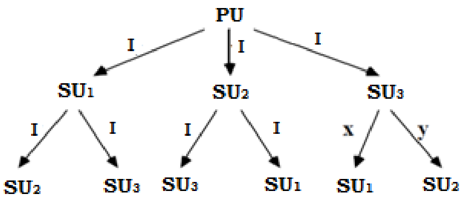
Here, PU→ Primary User of the spectrum in a CRN and

SU→ Secondary User.

Case I: Secondary User (SU_3) is a traitor

Stage1 results:

SU_1: $I_1 = I$
SU_2: $I_2 = I$
SU_3: $I_3 = I$



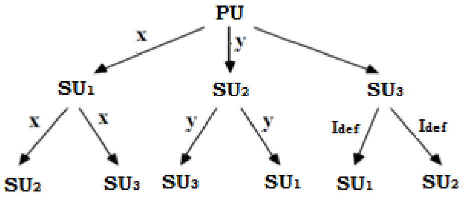
Stage2 results:

SU_1: $I_1 = I, I_2 = I, I_3 = x$
SU_2: $I_1 = I, I_2 = I, I_3 = y$
SU_3: $I_1 = I, I_2 = I, I_3 = I$

Majority calculation results:

SU_1: Majority(I, I, x)=I
SU_2: Majority(I, I, y)=I
SU_3: Majority(I, I, I)=I

Case II: Primary User (PU) is a traitor



Stage1 results:

SU_1: $I_1 = x$
SU_2: $I_2 = y$
SU_3: $I_3 = I_{def}$

Stage2 results:

SU_1: $I_1 = x, I_2 = y, I_3 = I_{def}$
SU_2: $I_1 = x, I_2 = y, I_3 = I_{def}$
SU_3: $I_1 = x, I_2 = y, I_3 = I_{def}$

All the three secondary users will receive the same value i.e. majority (x, y, I_{def}).

Byzantine Attack Problem will be solved in the above-mentioned manner in both the cases so that a secure channel of the CRN will be released upon the agreement and availability of funds and resources.

The proposed algorithm performance is better than the conventional algorithms in terms of data transmission. Fig. 4 shows the performance comparison of different systems in which the proposed system performance is better than the other conventional systems. We can increase the throughput at a cost of high-power consumption. So therefore, there's a trade-off between the expensive spectrum and the power storage. The same points are valid for the worse fading condition in Fig. 5 Here, the improvement of throughput does not start as more CRs join the network. With the more secondary users participating in this system can perform better than the random-access nature of a conventional multiple-access system.

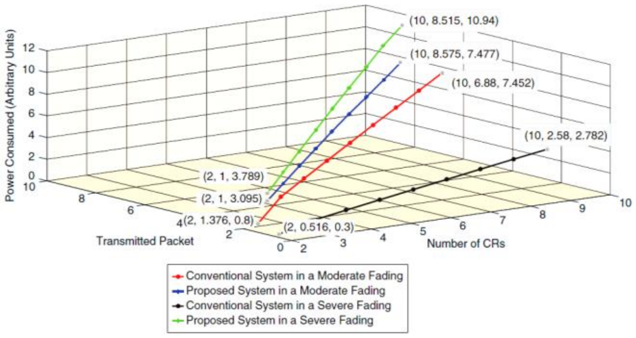


Fig. 4. Power consumption performance (w.r.t. number of CRs) of the conventional and proposed system

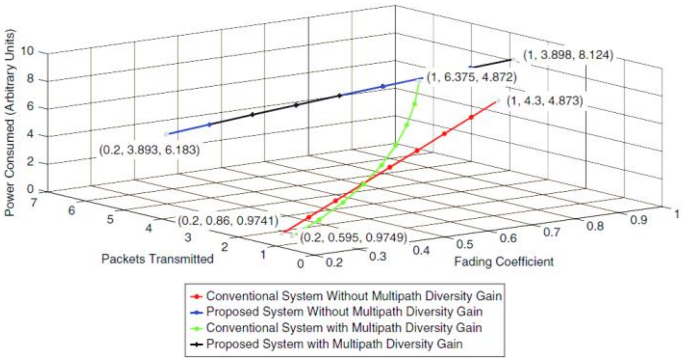


Fig. 5. Power consumption performance (w.r.t. fading coefficients) of the conventional and proposed system

5. Conclusion

In this paper, we have described the Byzantine Generals problem. Also, we have defined the conditions for the solution of this problem. The solution to this problem has been presented using Lamport-Shostak and Pease algorithm. In the CR networks, there can be a same kind of problem like BGP while allocating the spectrum to the secondary users. Here, we have addressed this Byzantine General problem and developed a reliable and secure spectrum allocation using the the Lamport-Shostak and Pease algorithm has been used to access the channel of a spectrum in the CRN by solving the Byzantine Attack Problem. The implemented design solves the Byzantine Generals problem for $n \geq 3m+1$ users in the presence of m faulters. Finally, the proposed algorithm can mitigate the Byzantine attack effectively and efficiently in the CRNs with the help of blockchain technology.

References

[1] S. Parshutina, Bogatyrev, "Models to support design of highly reliable distributed computer systems with redundant processes of data transmission and handling, " *IEEE, International Conference Quality Management, Transport and Information Security, Information Technologies "*, June 2017, volume 01, p. p. 096 - 099.

[2] P. Anand, et al., "Collaborative spectrum sensing in the presence of Byzantine attacks in Cognitive Radio Networks, " *IEEE, second International Conference on COMmunication System & NETworks*, April 2010, volume 01, p. p. 01 - 09.

[3] M. Kim, *et al*., "On counteracting Byzantine attacks in network coded peer – to - peer networks, " in *IEEE Journal on Selected Areas in Communications*, volume 028, no. 05, volume 01, p. p. 0692 - 0702, June 2010.

[4] V. K. Garg and J. Bridgman, "The Weighted Byzantine Agreement Problem, " *IEEE International Parallel and Distributed Processing Symposium,* May 2011, volume 11, p. p. 0524 - 0531.

[5] J. Ren, Zhang, et. al., "Exploiting Secure and Energy-Efficient Collaborative Spectrum Sensing for Cognitive Radio Sensor Networks, " in *IEEE Transactions on Wireless Communications*, volume 14, no. 10, p. p. 06813 - 06827, Dec-16.

[6] A. Sivakumaran, Alfa and Maharaj, "An Empirical Analysis of the Effect of Malicious Users in Decentralized Cognitive Radio Networks," *IEEE 89th Vehicular Technology Conference*, Aug 2019, volume 021, p. p. 01 - 05.

[7] J. Kelly, Ashdown, "Spectrum Sensing Falsification Detection in Dense Cognitive Radio Networks using a Greedy Method, " NAECON - 2018, *IEEE National Aerospace & Electronics Conference*, May 2018, volume 31, p. p. 0144 - 0151.

[8] M. B. H. Weiss, et al., "On the Application of Blockchains to Spectrum Management, " in *IEEE Transactions on Cognitive Communications & Networking*, volume 5, no. 2, p. p. 0193 - 0205, Mar 2019.

[9] N. C. Luong, , et al., "Joint Transaction Transmission and Channel Selection in Cognitive Radio Based Blockchain Networks: A Deep Reinforcement Learning Approach, " *IEEE International Conference on Acoustics, Speech and Signal Processing*, Mar 2019, volume 13, p. p. 08409 - 08413.

[10] K. Kotobi and Bilén, "Blockchain-enabled spectrum access in cognitive radio networks, " *IEEE Wireless Telecommunications Symposium*, May 2017, volume 02, p. p. 01 - 06.

[11] J. Du, *et al*., "A byzantine attack defender for censoring-enabled cognitive radio networks, " *International Conference on Wireless Communications and Signal Processing*, Jun 2015, volume 14, p. p. 01 - 06.

[12] Fernando C, "Using Byzantine Agreement in the Design Of IPS Systems," *IEEE International Performance, Computing, & Communications Conference*, Jun 2007, p. p. 0528 - 0537.

[13] Linyuan Zhang, Guoru Ding, et al., "Byzantine Attack and Defense in Cognitive Radio Networks: A Survey, " in *IEEE Communications Surveys and Tutorials*, volume. 017, no. 03, p. p. 01342 - 01363, Dec 2015.

[14] Ankit S. Rawat, Priyanka Anand, Chen and Varshne, "Countering byzantine attacks in CRNs, " *IEEE International Conference on Acoustics, Speech and Signal Processing*, Dallas, 2010, volume 15, p.p. 03098 - 03101.

[15] L. Zhang, et al., "Defending Against Byzantine Attack in Cooperative Spectrum Sensing: Defense Reference and Performance Analysis, " in *IEEE Access*, volume 04, p.p. 04011 - 04024, Apr 2016.

[16] Fulai Liu, et al., "Dynamic attack probability based Spectrum Sensing against Byzantine attack in Cognitive Radio," *2nd IEEE International Conference on Computer & Communications*, 2016, p. p. 01494 - 01498.

[17] Jun Wu et al., "Generalized Byzantine Attack and Defense in Cooperative Spectrum Sensing for CRNs, " in *IEEE Access*, volume 06, p. p. 53272 - 53286, Mar 2018.

[18] B. Kasirii, et al., "Secure cooperative multi-channel spectrum sensing in CRNs, " *Military Communications Conference*, Baltimor, May 2011, volume 18, p. p. 0272 - 0276

[19] F. Tao, et al., "Security Random Network Coding Model against Byzantine Attack Based on CBC," *4th International Conference on Intelligent Computation Technology & Automation*, Mar 2011, volume 17, p.p. 01178 - 01181

Authors' Profiles

Amith K S, Assistant Professor, Department of Computer Science & Engineering, A J Institute of Engineering and Technology, Visveswaraya Technological University, Belavagi, Karnataka, India.

Major interests: Cognitive radio networks, 5 G Networks, Blockchain Technology, design of fault-tolerant distributed computing systems; network topological organization.

Professor Yerriswamy T, Department of Computer Science & Engineering, K L E Institute of technology, Hubbali, Visveswaraya Technological University, Karnataka, India

Major interests: High-performance computer systems and networks: Mathematical Model using graph theory, design of radar system, Blockchain technology, Machine and Deep learning Model network.

How to cite this paper: Amith K S, Yerriswamy T, "Mitigation of Byzantine attack using LSP algorithm in CR Networks through Blockchain Technology", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.6, pp. 32-38, 2023. DOI:10.5815/ijwmt.2023.06.04