International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218645

Preventing Cognitive User Emulation Attack in Cognitive Radio Network by Calculating Trust Values Using Fuzzy Logic

Spriha Pandey*, Ashawani Kumar
Department of Electronics and Communication Engineering, Babu Banarasi Das University, Lucknow, India

Article Info
Volume 8, Issue 6
Page Number : 239-250

Publication Issue :
November-December-2021

Article History
Accepted : 15 Dec 2021
Published: 24 Dec 2021

ABSTRACT

Cognitive radio has proved to be an efficient and promising technology for the future of wireless networks. Its major and fundamental aim is to utilize the spectrum bands which are not efficiently exercised. These bands can be accessed using Opportunistic Spectrum Access (OSA), by a secondary user only when primary user is not transmitting over the channel. Cognitive radio manages spectrum through its cognitive radio cycle, which performs a set of management functions such as, spectrum sensing, spectrum assignment, spectrum sharing and spectrum mobility/handoff. During this cycle, at several stages, cognitive radio is very much vulnerable to security attacks. This is also due to the exposed nature of cognitive radio architecture. One such security attack which has not been much explored and can cause serious security issues is Cognitive User Emulation Attack (CUEA). This attack is expected to occur at the time of spectrum handoff. In this article the reason of occurrence of CUEA is explained along with counter measures to prevent this threat in the network by implementing trust mechanism using fuzzy logic. The proposed system is simulated and analyzed using MATLAB tool.

Keywords: Cognitive User Emulation Attack (CUEA), Cognitive Radio Network (CRN), Spectrum Handoff, Trust Value/Factor (TV/TF), Fuzzy Logic.

I. INTRODUCTION

In today's scenario the demand to access any wireless communication network, at a personal level, has increased drastically and the number of users per network has increased manifolds. Hence, more or less each and every functioning network working as per the current technology is highly saturated, demanding a break through either in technology or in the approach of accessing these networks. This is where Cognitive radio comes into picture, proving itself a milestone for the efficient utilization of spectrum bands.

Cognitive radio (CR) was the term coined and proposed by Joseph Mitola III in [1], [2]. This was an entirely novel concept in the field of wireless communication wherein the network is deemed to be intelligent and adaptive to its surrounding in order to provide the most appropriate service to its users. The fundamental concept behind this technology is to exploit the available resources efficiently by allowing secondary or unlicensed users to utilize the available bands in a network when the primary or licensed user has not occupied them, in order to prevent its under-utilization in the era of scarce radio resources. Licensed user having the authority to use their allotted bands at any time, is always given priority and secondary users will have to vacate the channel on the arrival of primary user. Cognitive radio performs its objectives by maintaining a cognitive radio cycle which performs the functions: spectrum sensing, spectrum assignment, spectrum sharing and spectrum handoff/mobility which are well explained in [3], [4].

Cognitive radio network is more exposed to its environment as compared to conventional wireless network because of its fundamental behaviour (adaptability, awareness, learning and memory). This means that CRN is very much prone to security threats and attacks. These attacks may be possible in two ways [5], [6]: selfish attack and malicious attack. These attacks are possible in cognitive radio at different stages [7], [8] of its cognitive cycle and in different layers of network architecture. Here, we are discussing about one such attack that occurs during handoff phase in cognitive radio network.

During Spectrum handoff the entire cognitive cycle is repeated as the user will have to search for a new idle channel in the network and then perform channel allocation. Meanwhile, PU will occupy its licensed channel and begin its transmission. Now this entire process might involve some delay which could be exploited by the malicious user (MU). Malicious user might act like a legitimate user of that network to occupy a channel or is very likely to imitate the handoff user (HU) by forging its id to access any available channel. This kind of attack is termed as Cognitive User Emulation Attack (CUEA) [9].

CUEA is not much explored as a possible security attack in CRN. In [9], [10] authors have tried to explain its occurrence, cause and prevention using trust based mechanism. In this article we have proposed the extension to their work by using fuzzy logic. Fuzzy logic is a mathematical tool used to remove fuzziness or indefiniteness depending on the inputs at hands are sceptical or imprecise as in case of Cognitive Radio Architecture. Hence, fuzzy logic being multi-valued helps in accurate calculation of trust value (TV) as compared to bi-valued result (0 or 1).

This paper explains how we can prevent CUEA attack in cognitive network by calculating trust value using fuzzy logic. Trust value of a node will depend on its behaviour in the network. If any malicious activity is identified by Centralized Cognitive User (CCU), which is a part of the network, then the node will be declared as malicious and the decision will be taken by CCU.

The paper is divided into different sections to explain the functioning and implementation of this model. Firstly, literature review is given to introduce the studies and researches performed related to this work. Secondly, system model has been discussed giving detail of how the work is implemented to prevent CUEA. Further, the performance of the system is evaluated using MATLAB tool to attain improved results by the use of fuzzy logic in the model.

II. RELATED WORK

Cognitive radio has been defined by different authors in different ways in [1]-[3], [12]. The concept of cognitive radio was evolved on the basis of Software Defined Radio (SDR). SDR helps us in achieving an adaptive intelligent radio which serves the purpose of

cognitive radio [13]-[15]. Cognitive radio performs its spectrum management functions by maintaining cognitive radio cycle which is elaborated in [16]-[19]. As per the literature cognitive radio is very much vulnerable to security attacks as compared to the conventional wireless network. In [20], the authors have explained the possible attacks in CRN along with the specification of phases in which the attack can occur.

Similarly, articles [21], [22] explains how CR is exposed several security attacks and how these attacks occur at different network layers in Cognitive radio architecture. For example, Jamming attacks and PUEA can occur at the physical layer, Control Channel Saturation and SSDF (Spectrum Sensing Falsification Attack) can occur at data link layer, Hello and Sinkhole attack can occur at network and so on. Further, the article [23], [24] gives a survey on all the attacks specific to CRN and a comparison of attacks with the traditional wireless network. They also thoroughly explains the preventive measures that should be taken to control threats in CRN.

One such threat which has recently gained acknowledgement and is not much explored is Cognitive User Emulation Attack (CUEA). This attack was introduced by Geetanjali Rathee in article [9] and further extended and elaborated in [10]. CUEA is expected to occur at the time of spectrum handoff. Spectrum handoff is very likely to take place whenever a primary user (PU) arrives for transmission in its licensed band [21]. Researches in articles [22]-[24] explains the type of handoff proposed and drawbacks associated with each one of them. There is some amount of delay in every handoff case which drives the conclusion that CUEA is very much prone in cognitive radio. Hence, to develop a secure, robust and reliable network we need to take measures in order prevent threats in the system.

Several mechanisms have been proposed and applied from encryption to cryptographic techniques and secure routing to data aggregation in order to prevent different types of attack [25]-[28]. But these techniques focuses on specific vulnerabilities and are considered conventional method of preventing threats as they increase computational load on the system due to high power and memory requirement. Many researchers today are relying on Trust based mechanism [29]-[34] the authors have also used the same mechanism to prevent CUEA, which has been further extended in our work by using fuzzy logic (to decide final trust value). In order to understand how fuzzy logic works and its application articles [35]-[40] has been studied.

III. PROPOSED MECHANISM FOR SECURE HANDOFF

In this work, we are trying to build a system that ensures security during spectrum handoff as it is considered as the utmost vulnerable phase as per the researches. In Cognitive User Emulation Attack (CUEA), a Malicious User (MU) takes advantage of the delay introduced in the network during handoff because of processes like spectrum sensing, arrival of primary user and allocation of channel to current CR user. MU will imitate like a legitimate cognitive user (CU) and thus a legitimate CU can be defaced by a MU in the cognitive radio network.

In the work shown we have used trust based mechanism for detection of a malicious node in the network. Further to improve the Trust value decision (0 or 1) fuzzy logic has been implemented to explore possibility between 0 and 1(yes, no, possibly yes, possibly no etc.). In Fig. 1 flowchart of the proposed model is represented.

As per the system design, we will have 50 Iot devices in a network. These devices will be randomly located in a given area and communicate to each other by transmitting packets. During handoff a malicious user (MU) can try to enter into the system by forging id of a handoff user (HU). The task of identification of a user and its legitimacy within the network is handled

by Centralized cognitive user (CCU). Whenever a user enters into the network it will be CCU's responsibility to firstly identify the type of user (PU, CU or MU). There will be different criteria set for identification of each user inside the network by the CCU.

The given model is proposed for attacks in two types of case: a) When the user entering the network is a primary user (PU), b) When the user entering the network is cognitive user (CU) or handoff user (HU). Hence, CCU will have to check a user's legitimacy by determining its type and then checking their behaviour in terms of Liveliness and Data Delivery Ratio (DDR) along with their previous performance.

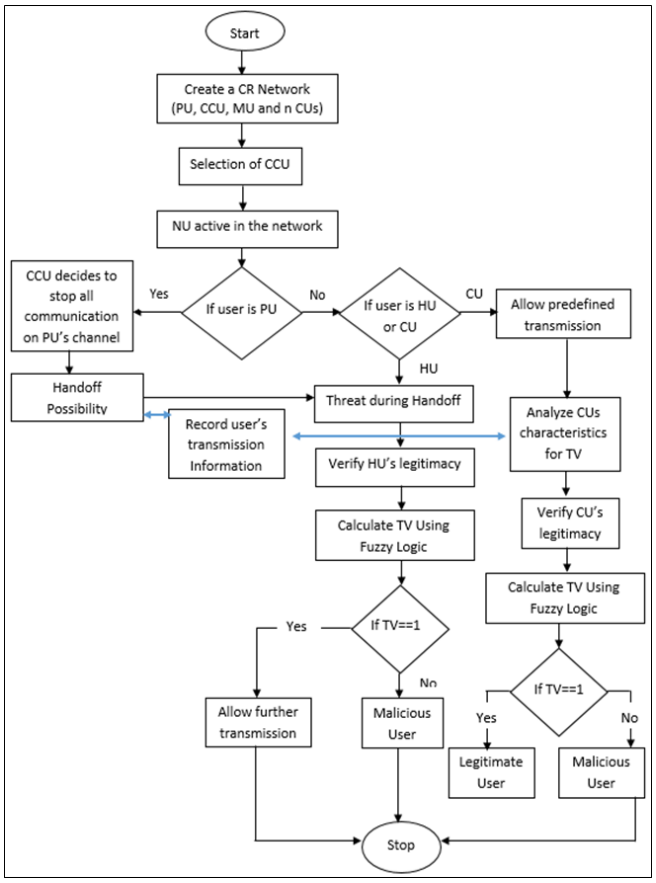

Figure 1: Flowchart of the proposed mechanism

A. System Model

The network must contain n number of cognitive users among them some are selected as PU, CU, HU and a CCU. The identification of node is based on their behavioural characteristics. Centralized Cognitive User (CCU) will be responsible to control the entire network functioning along with identification of a user's legitimacy.

CCU Selection: The node which initially has the highest trust value (initially randomly distributed) will be selected as the CCU. But the dynamics changes after every round of execution. After each round of performance the node with highest trust value and longest viability period (VP) is selected as the CCU. Here, viability period means the time for which node was active in the network. Any new user entering the network should be tested and identified by the CCU. A new user (NU) can enter in the network with three possible ways: PU, CU or NU. Identification of each user type is same as explained in [10].

In the designed system all the nodes are deemed to be non-static or mobile which helps us in getting closer to the real time environment. The entire network area is divided into two zones i.e. zone 1 and zone 2. Any user shifting from one zone to another will be termed as the handoff user (HU). Fig. 2 depicts the system model showing possibility of CUEA.

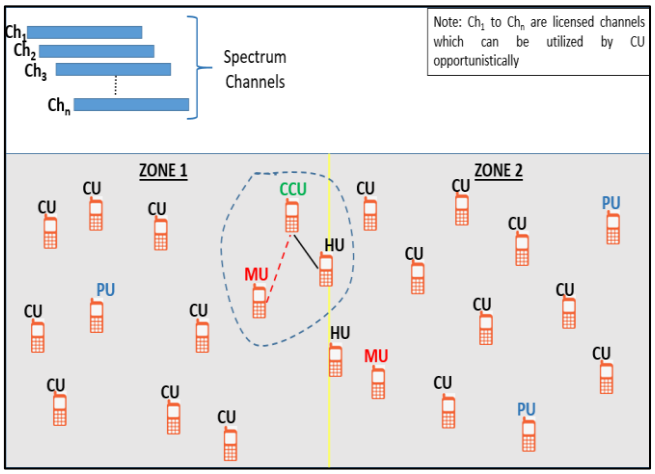

Figure 2: Possibility of CUEA occurrence

Handoff in the system can occur in two cases: a) when the user moves from one zone to another, b) when a PU arrives and CU will have to move to a new channel. In both these cases the HU will have to request CCU for allotment of a new channel to

continue its transmission. This might involve some delay and provide a chance for the malicious user (MU) to enter into the network by forging the id of handoff user. Therefore before assigning a channel the CCU checks the legitimacy of HU from its past performance and interactions inside the network.

Initially, in the network all nodes are considered trustworthy, reliable and genuine. Hence all the nodes get equal opportunity of transmission. Also, at the time of network establishment all nodes are randomly assigned trust value ranging from 0 to 1 based on SITO algorithm [35]. As nodes spend more time in the network their activeness, survival and transmission loyalty helps in determining their trust value.

If the trust value is 1, node is legitimate else if trust value is 0 node is considered malicious. As the nodes continues their transmission in the network their trust values can change (increases or decreases) depending on their nature in the network. Trust value in our model depends on liveliness and data delivery ratio of each node. It is further explained under section 3.2.

B. Calculation of Trust Values

Trust value helps in determining legitimacy of a node. It depicts the height of loyalty a node has for the network it exists in. Thus, accurate calculation of trust value is an important factor for a secure and threat free system. Trust value in our proposed model basically depends on two behaviour of node: Liveliness and Data Delivery Ratio (DDR).

1. Liveliness: It is defined as the parameter that determines how active a node remains in the network. A malicious node might always try to attract more and more packets towards it by sending several broadcast message and luring them to provide shortest or least cost destination path and thus having high liveliness (more than the threshold).

2. Data Delivery Ratio (DDR): It is defined as a measure to check the amount of messages received and send by a node. The affected node lures the neighboring nodes to send their data packets and once received this node tends to drop the packets on their way. Thus the ratio of data forwarding would be reduced very low even lowering the overall network throughput.

3. Trust Value: So the parameters liveliness and data delivery ratio are input for the calculation of trust value. In this work instead of simplify deciding value as 0 or 1 we use fuzzy logic. Liveliness and DDR are fed as input to the fuzzy controller which further depending on the fuzzy rule set determines the final trust value. Algorithm for calculation of trust value is explained below:

Algorithm 1: Calculating Trust Value (TV)

Input*: *Liveliness and DDR
Set Degree of Membership
Set Rules for Fuzzy Logic
Input to Fuzzifier (Liveliness and DDR)
Output Trust Value

C. Implementation of Fuzzy Logic

Fuzzy logic helps in evaluating possibilities between a yes and a no rather than just having true or false value. A fuzzy set is defined as a set deprived of any sharp and crisp boundaries. It deals with elements which are defined on the basis of degree of membership. In this model the nodes loyalty is determined through its behaviour i.e. Liveliness and Data Delivery Ratio (DDR).

These two acts as input to the fuzzy controller which after fuzzification gives result which is trust value of that node. The fuzzification is performed on the basis of rules which are set using the MATLAB Fuzzy Inference System Toolkit. These rules helps in deciding the multi-valued output which is a feature of fuzzy logic. Fig. 3 explains the role the fuzzy logic in calculating trust value.

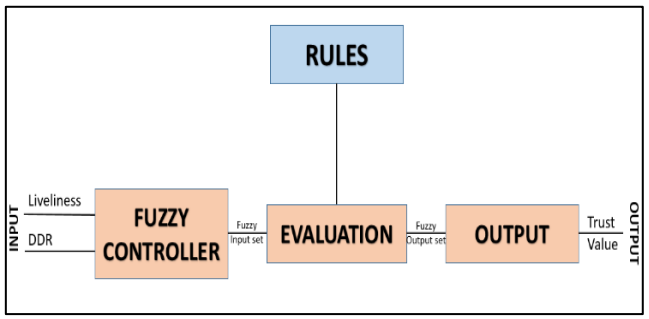

Figure 3: A representation of trust value calculation using fuzzy logic

A membership function defines how every value of the input set is plotted to some value of membership or degree of membership. The graph obtained represents membership functions. The membership function used in our model in fuzzy logic implementation is as below in Fig. 4.

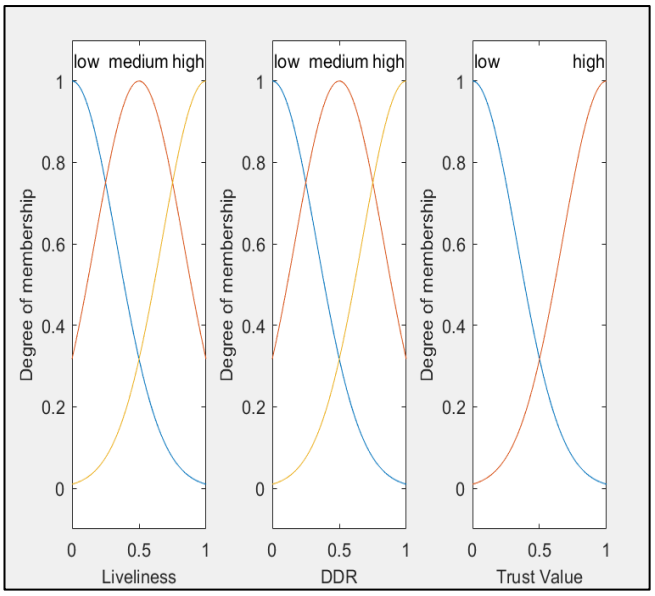

Figure 4 : Degree of membership for input and output variable

The main function of fuzzy logic is to map the input space to an output space which is primarily done by implementing if-then logic which is called rules. The rules are defined in our system to calculate trust value depending on input liveliness and DDR.

In the above table shown Liveliness and DDR are the two input variables. Low, Medium and High are the membership functions (MFs) for the fuzzy set. The combination of these MFs at different input points results in output (Low or High) which is decided on this rule. There could be max nine (3x3 = 9) rules for this fuzzy set. The rules mentioned above can be explained as:

- If (Liveliness is low) and (DDR is low) then (trust value is low)
- If (Liveliness is medium) and (DDR is low) then (trust value is low)
- If (Liveliness is high) and (DDR is medium) then (trust value is high) and so on.

Thus, use of fuzzy logic helps in better evaluation of trust value of each node and therefore in efficiently recognizing the malicious node, if any, in the network.

Table 1: Rules for calculating Trust Value

Liveliness / DDR	Low	Medium	High
Low	Low	Low	Low
Medium	High	Low	High
High	High	High	High

IV. PERFORMANCE ANALYSIS

Security is a principal issue in any wireless network. Considering cognitive radio and its vulnerability a new type of threat has been explored in [10] which is termed as CUEA. In this paper we have tried to prevent such attack using fuzzy logic in the system. Hence the model shows that the attack strategies that can be possible is during:

- During emergence of NU
- During emergence of HU (during handoff)

CUEA might firstly occur when a new user arrives and the user is detected as PU, so any CU communicating on that channel will switch to another channel. Secondly when the there is any handoff due to movement of CU from one zone to another. To give the complete analysis of system

performance we need to check the throughput the system produces.

To calculate throughput the formula used is:

$$R_{HU} = \mu_1 * log_2(1 + SNR_{CU}) + \mu_3 * log_2\left(1 + \frac{SNR_{CU}}{1 + SNR_{MU}}\right) \quad (1)$$

where, SNR_{CU} and SNR_{MU} signifies signal to noise ratio because of transmission caused by CU and MU respectively at HU receiver. Throughput, in general, is specified as the amount of data sent from the received data in a given period of time or in other words it is explained as the maximum transmitted data rate by a wireless system in a given time interval. In order to present improved result than [10] we have used the same parameters for performance evaluation. The states μ1 and μ3 are the ones in which there is possibility of MU's presence therefore we are calculating throughput against these states. In the given model analysis will be based on four different states of CU and MU existence:

$$\begin{aligned} W_{s0} &= neither\ CU\ nor\ MU \\ W_{s1} &= only\ CU\ no\ MU \\ W_{s2} &= no\ CU\ only\ MU \\ W_{s3} &= both\ CU\ and\ MU \end{aligned} \quad (2)$$

Here, W_{s0} represent the case when both CU and MU is absent at CCU. W_{s1} represent the case when CU is performing handoff and requests CCU for a new channel. W_{s2} represents the case when MU is trying to prove its legitimacy to CCU and act as a legitimate CU. W_{s3} represents the case when both CU and MU are present which means both are trying to prove their trustworthiness to CCU.

Let us say there are two hypothesis, C_0 and C_1, where C_0 means absence of CU and C_1 means presence of CU at CCU. Similarly hypothesis M_0 and M_1 means absence and presence of MU at CCU respectively. Therefore, representing the states W_{sk} as μ_k, from these hypothesis we can define the states mentioned in Eq. (3) as:

$$\begin{aligned} \mu_0 &= P(W_{s0}) = P(C_0, M_0) = P(M_0/C_0)P(C_0) \\ \mu_1 &= P(W_{s1}) = P(C_1, M_1) = P(M_1/C_1)P(C_1) \\ \mu_2 &= P(W_{s2}) = P(C_2, M_2) = P(M_2/C_2)P(C_2) \\ \mu_3 &= P(W_{s3}) = P(C_3, M_3) = P(M_3/C_3)P(C_3) \end{aligned} \quad (3)$$

In order to check the performance we need to analyze the probability of error that can occur in the system. Analyzing the parameters we will see how probability of error is affected by probability of false authentication and probability of miss detection.

Now, let us say that Pfa represents the probability of false authentication of occurrence of MU at CCU i.e. MU is absent but CCU detects it as MU's presence. Similarly, Pmd represents probability of miss detection which means CCU detects MU's presence as its absence. Both these functions can be equated as $P_{fa} = P(Q_1|M_0)$ and $P_{md} = P(Q_0|M_1)$, where, Q_1 denotes decision of CCU to detect MU's presence and Q_0 as CCU's decision to detect MU's absence. The performance of the system will be affected when the CCU decision will lead to error in the result. Probability of error can be denoted as:

$$\begin{aligned} P_e &= P(M_1, Q_0) + P(M_0, Q_1) \\ P_e &= P(Q_0|M_1)\,P(M_1) + P(Q_1|M_0)\,P(M_0) \\ P_e &= P_{md}P(M_1) + P_{fa}\,P(M_0) \end{aligned} \quad (4)$$

V. RESULTS AND DISCUSSION

In order to check the performance of the proposed system, we need to simulate the entire process. For simulation we have used MATLAB tool and the analysis is performed on a network with simulation area of 400 m × 400 m and 50 IoT devices. Each of these devices is assigned a unique identification number at the time of initialization. After the initialization phase, as the nodes are mobile they are allowed to move within the network area and handoff users are identified. Then user's legitimacy is tested and throughput is calculated to evaluate the network performance.

Initially all users are given random TV so if any user approaching CCU has TV 0, it will be declared as a malicious node. If in case a malicious node tries to imitate a legitimate HU then the system performance will decrease and hence the throughput. This will be

because the malicious nodes will drop the packets, thus decreasing DDR. Therefore, any HU approaching CCU will first have to prove its reliability to CCU. Fig. 5 shows the network topology obtained through simulation.

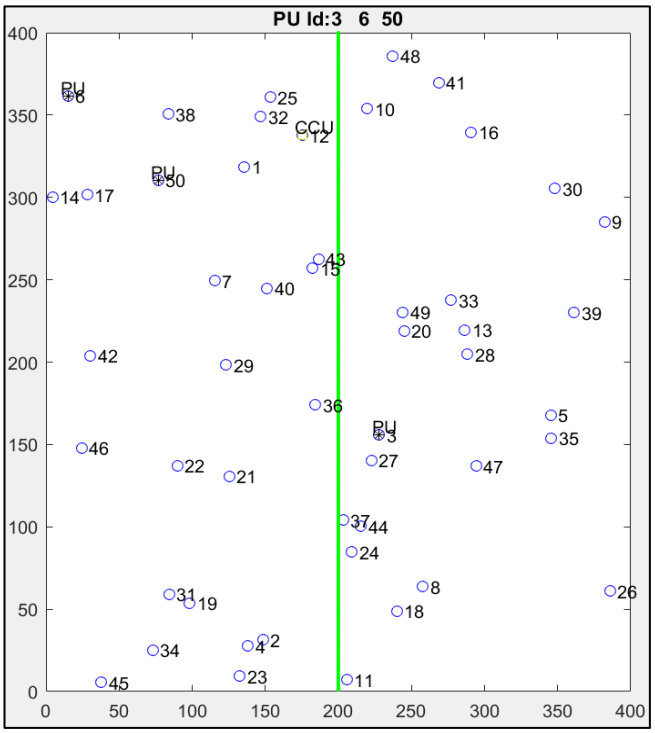

Figure 5: Network Topology

The comparative analysis of TV calculation by using only trust based mechanism and by using fuzzy logic along with trust based mechanism is shown. The proposed approach of calculating trust value using fuzzy logic to check legitimacy of any node has proved to be better as compared to the existing approach. Using the probabilistic model the results shown in [10] proves that along with reduction in error probability of malicious node identification, the approach had also reduced the delay in transmission during handoff and improved the throughput of the system when compared to earlier existing approaches which are also based on probability modeling.

The study based on our proposed model has proved to effectively improve the results of [10]. The analysis was based on same parameters i.e. transmission delay, throughput and probability of error for comparison. The results given in Fig. 6 shows that the use of fuzzy logic has improved the throughput of the system due to more accurate identification of malicious node.

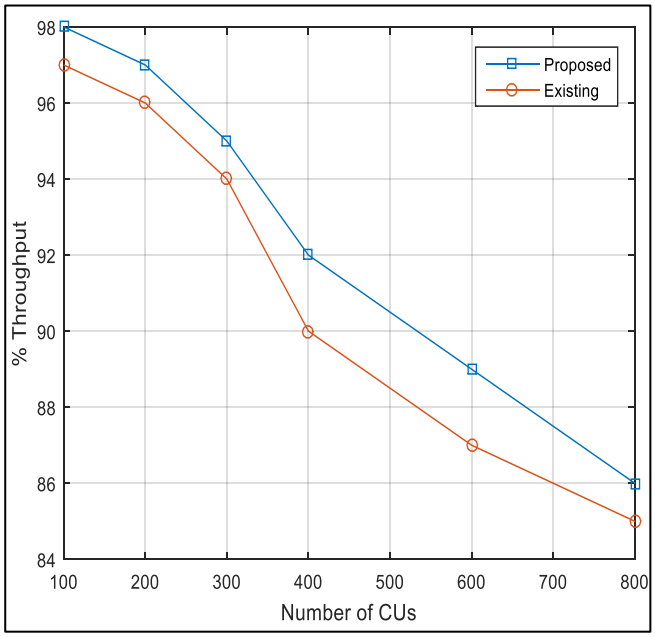

Figure 6: Number of CUs vs Throughput

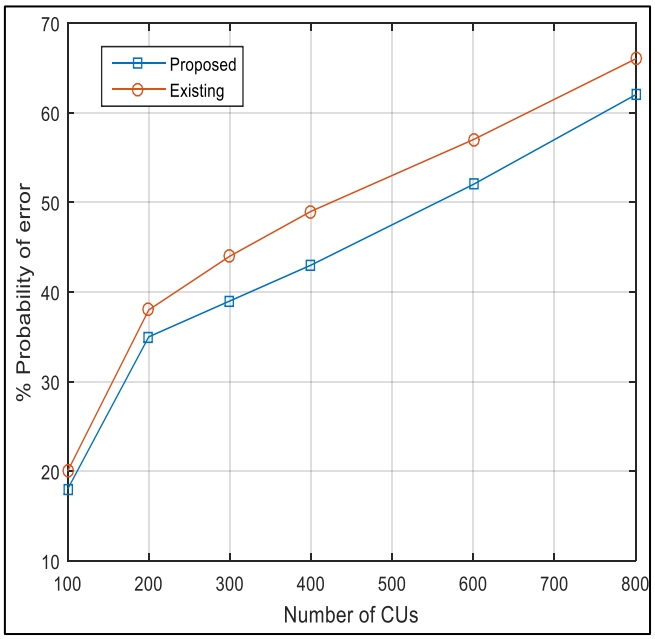

Figure 7: Number of CUs vs Probability of error

The probability of error in Fig. 7 has also been seen to be decreased thus improving the performance of the model proposed for prevention of CUEA. In terms of spectrum handoff the transmission delay in the system also reduces as shown in Fig. 8 since the nodes

are accurately identified and hence there is less probability of a node to block the transmission of a CU thus adding delay.

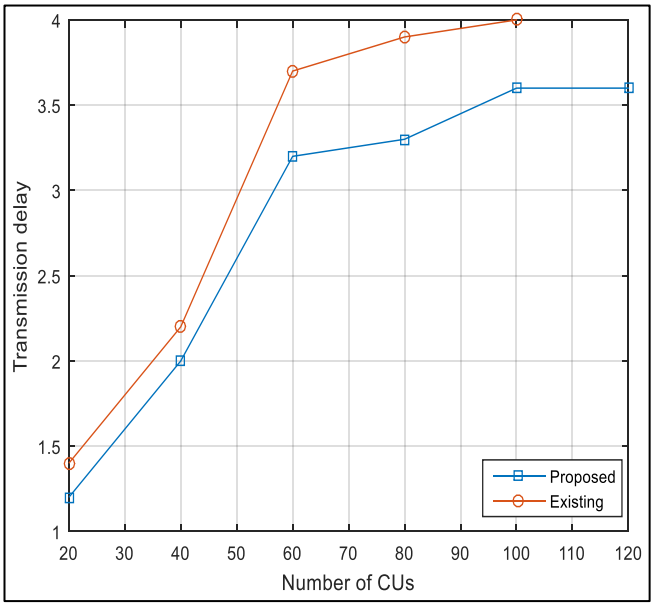

Figure 8: Number of CUs vs Transmission delay

The parameters are analysed depending on the number of CUs in the system which also helps us in evaluating the scalability of the proposed system. It is seen that as the number of CUs increases the throughput of the system decreases. Also, with the rise in number of CUs the probability of error also rises.

VI. CONCLUSION AND FUTURE SCOPE

In this paper, we have tried to secure the process of spectrum handoff by working on a newly introduced security attack CUEA which occurs during spectrum handoff. In order to mitigate this attack effectively we have used fuzzy logic to calculate trust values of each node which helps in accurately determining whether a node is trustworthy or not. A centralized node called CCU is elected among the cognitive nodes which exploits the behavioral characteristics of other node to decide their TV. Depending on these characteristics values (low, medium or high) and a set of rules, fuzzy controller decides the TV (low or high). Fuzzy logic helps in finalizing the trust value efficiently as it analyses all possibilities in between 0 to 1. Thus improving the overall system throughput, transmission delay and probability of error. The future scope might include extending this work to encompass other types of jamming attacks in the system and trying to prevent them with similar technique as it has proved effective against other probabilistic models.

VII. REFERENCES

[1] I.F. Akyildiz, L. Won-Yeol, C.V. Mehmet and M. Shantidev, “Next generation/dynamic spectrum access/ cognitive radio wireless networks; a survey”, Computer Networks, 50(2); 2127-2159, 2006.

[2] J. Mitola III, “Cognitive radio: An integrated agent architecture for software defined radio.” PhD thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, May 2000.

[3] John A. Stine and David L. Portigal, "Spectrum 101: An Introduction to Spectrum Management", March 2004, MITRE TECHNICAL REPORT

[4] Spriha Pandey and Ashawani Kumar, “A Review on Modern Spectrum Sensing and Assignment Techniques In CRN”, International Journal of Scientific Research in Science, Engineering and Technology, Vol. 8, issue 2, pg. 171-181, 2021.

[5] Yingkun Wen, Yan Huo, Liran Mao, Tao Jing and Qinghe Gao, "A Scheme for Trustworthy Friendly Jammer Selection in Cooperative Cognitive Radio Networks", 2019, 2895639, IEEE Transactions on Vehicular Technology.

[6] Mee Hong Ling, Kok-Lim Alvin Yau, Junaid Qadir and Qiang Ni, "A Reinforcement Learning-based Trust Model for Cluster Size Adjustment Scheme in Distributed Cognitive Radio Networks", 2018,2881135, IEEE

Transactions on Cognitive Communications and Networking.

[7] Yenumula B. Reddy, "Security Issues and Threats in Cognitive Radio Networks" AICT 2013 : The Ninth Advanced International Conference on Telecommunications, 978-1-61208-279-0

[8] D. Ganesh and T. Pavan Kumar, "A Survey on advances in security threats and its countermeasures in cognitive radio networks" International Journal of Engineering & Technology, Vol 7, issue 2.8, 2018, 372-378

[9] Geetanjali Rathee, Prabhat Thakur, G Singh and Hemraj Saini, "Aspects of Secure Communication during Spectrum Handoff in Cognitive Radio Networks", IEEE, 2016, 978-1-5090-2684-5

[10] Geetanjali Rathee, Naveen Jaglan, Sahil Garg, Bong Jun Choi, and Kim-Kwang Raymond Choo, "A Secure Spectrum Handoff Mechanism in Cognitive Radio Networks", IEEE Transactions, 2020 2971703

[11] L. Giupponi and Ana I. Pérez-Neira, "Fuzzy-based Spectrum Handoff in Cognitive Radio Networks", 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), 15-17 May 2008.

[12] S.Haykin, "Cognitive radio: brain-empowered wireless communications," vol. 23, no.2, pp. 201{220, February 2005

[13] J. Mitola III and G. Maguire Jr, "Cognitive radio: making software radios more personal," Personal Communications, IEEE, vol. 6, no. 4, pp. 13–18, 1999

[14] F. K. Jondarl, "Software-defined radio: basics and evolution to cognitive radio," EURASIP J. Wirel. Commun. Netw., vol 2005, no. 3, pp. 275{283, 2005.

[15] V. Bose, "A software driven approach to SDR design," COTS Journal, Jan. 2004.

[16] Monisha Devi, Nityananda Sarma and Sanjib Kumar Deka, "A General Framework for Spectrum Assignment in Cognitive Radio Networks" Springer, Advanced Computing and Communication Technologies vol.702, 2019, pp 163-172.

[17] Q. Zhao et al., "Decentralized Cognitive MAC for Opportunistic Spectrum Access in Ad Hoc Networks: A POMDP Framework," IEEE JSAC, vol. 25, no. 3, Apr. 2007, pp. 589–99.

[18] R. Menon, R. M. Buehrer, and J. H. Reed, "Outage Probability Based Comparison of Underlay and Overlay Spectrum Sharing Techniques," Proc. IEEE DySPAN 2005, Nov. 2005, pp. 101–9.

[19] Senhua Huang, Xin Liu, and Zhi Ding, "Opportunistic Spectrum Access in Cognitive Radio Networks" IEEE Communications., The 27th Conference on Computer Communications.

[20] Wajdi Alhakami, Ali Mansour and Ghazanfar A. Safdar, "Spectrum Sharing Security and Attacks in CRNs: a Review", International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014

[21] Wang C-W and Wang L-C. "Analysis of reactive spectrum handoff in cognitive radio networks", IEEE Journal on Selected Areas in Communications Volume: 30, Issue: 10, November 2012

[22] Krishan Kumar , Arun Prakash and Rajeev Tripathi, "Spectrum handoff in cognitive radio networks: A classification and comprehensive survey", Journal of Network and Computer Applications, Oct 2015, 1084-8045

[23] Prince Semba Yawada and Mai Trung Dong, "Intelligent Process of Spectrum Handoff/Mobility in Cognitive Radio Networks", Journal of Electrical and Computer Engineering, Mar 2019, Article ID 7692630

[24] Julie Thomas and Prasanth P Menon, "A Survey on Spectrum Handoff in Cognitive Radio Networks", Internantional Conference on Innovations in Information Embedded and Communication Systems, Mar 2017

[25] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey", Journal of Network and Computer Applications, 2012, vol. 35, pp. 1691–1708

[26] J. Xiong, D. Ma, H. Zhao, and F. Gu, "Secure multicast communications in cognitive satellite-terrestrial networks," IEEE Commun. Letters, vol. 23, no. 4, pp. 632–635, 2019.

[27] Y. Wang, X. Tang, and T. Wang, "A unified QoS and security provisioning framework for wiretap cognitive radio networks: Astatistical queueing analysis approach," IEEE Trans. on Wireless Commun., vol. 18, no. 3, pp. 1548–1565, 2019.

[28] A.G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks", IEEE Communications Surveys & Tutorials, 2013, vol. 15, issue: 1 , pp. 428 -445.

[29] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," 1996. [Online]. Available: http://citeseer.ist.psu.edu/blaze96decentralized.html

[30] V. Oleshchuk, "Trust-based framework for security enhancement of wireless sensor networks," in Intelligent Data Acquisition and Advanced 347Computing Systems: Technology and Applications, IDAACS, 4th IEEE Workshop on, 2007, pp. 623–627.

[31] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," SIGMOBILE Mob. Comput. Commun. Rev., vol. 13, no. 2, pp. 86–95, Sep. 2009.

[32] W. Wang, H. Li, Y. Sun, and Z. Han, "Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks," EURASIP J. Adv. Signal Process, vol. 2010, pp. 4:4–4:4, Jan. 2010.

[33] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in Wireless Communications and Networking Conference (WCNC), 2011 IEEE, 2011, pp. 599–604.

[34] Yingkun Wen, Yan Huo, Liran Mao, Tao Jing and Qinghe Gao, "A Scheme for Trustworthy Friendly Jammer Selection in Cooperative Cognitive Radio Networks", 2019, 2895639, IEEE Transactions on Vehicular Technology.

[35] L. Giupponi and Ana I. Pérez-Neira, "Fuzzy-based Spectrum Handoff in Cognitive Radio Networks", 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), 15-17 May 2008.

[36] Aruna Bajpai and Virendra Singh Kushwah, "Importance of Fuzzy Logic and Application Areas in Engineering Research", International Journal of Recent Technology and Engineering (IJRTE), Volume-7 Issue-6, March 2019.

[37] Vinod Kumar and R.R.Joshi, "Hybrid Controller based Intelligent Speed Control of Induction Motor", Journal of Theoretical and Applied Information Technology, 2005.

[38] Padmalaya Nayak, and Anurag Devulapalli, "A Fuzzy Logic-Based Clustering Algorithm for WSN to Extend the Network Lifetime", IEEE SENSORS JOURNAL, VOL. 16, NO. 1, JANUARY 1, 2016

[39] Rabia Aziz, C.K. Verma, Namita Srivastava, "A fuzzy based feature selection from independent component subspace for machine learning classification of microarray data", genomic data 8 (2016) 4-15, 2016 elsevier inc.

[40] Mohsen Bakhshi, Mohammad Hosein Holakooie, Abbas Rabiee, “Fuzzy based damping controller for TCSC using local measurements to enhance transient stability of power systems”, Electrical Power and Energy Systems 85 (2017) 12–21

[41] Martin Maca’s and Lenka Lhotsk’a, "Social Impact Theory Based Optimizer", ECAL 2007, LNAI 4648, pp. 635–644, 2007, Springer-Verlag Berlin Heidelberg 2007.

Cite this article as :

Spriha Pandey, Ashawani Kumar, "Preventing Cognitive User Emulation Attack in Cognitive Radio Network by Calculating Trust Values Using Fuzzy Logic", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 6, pp. 239-250, November-December 2021. Available at doi : https://doi.org/10.32628/IJSRSET218645
Journal URL : https://ijsrset.com/IJSRSET218645