IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 17, Issue 1, Ser. I (Jen. – Feb. 2022), PP 14-23
www.iosrjournals.org

Enhanced Spectrum Handoff Security Mechanism In Cognitive Radio Network

Ranajeet Kumar, Dr. Rakesh Kumar Singh
Dept. Of Electronics Engineering, KNIT Sultanpur

Abstract: *Cognitive radio (CR) is a trend setting innovation fully intent on using the spectrum groups which are unused in an astute and dynamic manner. The portions of range or spectrum groups which are not utilized, are classified "range openings (spectrum holes)" or "blank areas (white space)". Process of range or spectrum allocation is for minimizing any possibility of interference between secondary and primary users. But CR technology faces various challenges because of the varying nature of the range available, and also the different quality of service requirements of various services. So in this work we introduce a cognitive user emulation attack (CUEA) in a cognitive radio network (CRN), which can be exploited by intruders during spectrum handoff. Then, we propose an enhanced spectrum handoff security mechanism based on fuzzy logic that can successfully counter such an attack by introducing a coordinating cognitive user that computes the level of trust of each cognitive user based on its behavioural characteristics and users can be effectively identified as malicious or not by looking up the trust values. MATLAB simulation is used to measure the performance of proposed mechanism. The simulation results show that the utility of the proposed mechanism in terms of its probability error in correctly identifying users, throughput rate, and transmission delay.*

Keywords: *Cognitive Radio Network, Spectrum Handoff Security, Fuzzy Logic, Data Delivery Ratio and Liveness, Probability of Error, Throughput rate, Transmission Delay.*

Date of Submission: 12-01-2022 Date of Acceptance: 27-01-2022

I. Introduction

Today increasing usage of internet-connected devices and services needs more spectrum band for transmission [1]. Hence cognitive radio technology is used to make spectrum for maximum utilization. Specifically, the CR allows unlicensed or cognitive users (CU) to utilize the idle bands of the primary users (PU). There are four key functions to use the idle spectrum which are spectrum sensing, spectrum decision, spectrum sharing (access), and spectrum handoff (or spectrum mobility) [3], [4]. In the first three key functions, the CU senses the network environment and selects an idle channel among the available idle bands. Then, the CU makes a transmission channel on the selected band and taking as avoiding interference with other users [5], [6]. In the last key function, the CU switch its current transmission channel to other available channel [7]-[9]. During the spectrum handoff, it is possible that a malicious user (MU) send request for transmission which increases the transmission delay and degrading the network performance. Thus, the HCU needs to be distinguished from the MU in order to conduct a trusted spectrum handoff [37].

Therefore, in this paper, we commence a new security threat in the CRN during handoff, called a cognitive user emulation attack (CUEA). Next, we explain how this attack can be mitigated by a coordinating cognitive user (CCU) by calculating the trust factor/value (TF/TV) of CUs using fuzzy logic. The CCU is the control node of CRNC responsible for verifying the legitimacy of HCU or new incoming users in the system. The behaviour of each CU is also regularly analysed and monitored by the CCU during the handoff mechanism, with the intention of identifying any malicious behaviour [37].

The rest of the paper is structured as follows. In Section 2, survey of the related literature on CRN spectrum handoff. In Section 3, our proposed mechanism is presented. In Section 4, the performance of the proposed mechanism is demonstrated under various attack scenarios in comparison with other existing mechanisms. In Section 5, the conclusion of the paper is provided [37].

II. Literature Review

As spectrum handoff is an integral function of the CRN, designing a handoff mechanism is a topic of ongoing interest. Conventional spectrum handoff schemes can be divided into proactive and reactive strategies. For example, Wu et al. [22] projected a proactive spectrum handoff where a common optimal communication with a proactive spectrum handoff (OTPH) scheme is presented. The OTPH and dynamic programming methods are used to overcome the problem of packet transmission within a predefined deadline. Their simulation results

show that it is possible to achieve a high data rate at a low cost. Wang et al. [23] proposed a reactive spectrum handoff scheme where the preemptive resume priority queuing system is used to leverage channel availability. Its performance was analyzed in terms of traffic survival rates and transmission latency. There are many other mechanisms in this direction [24]-[29].

Afsana et al. [30] presented a trusted and energy-aware cluster modelling in which a cluster head is selected based on the normalized distance to improve the successful data transmission and to reduce the power needed for transmission. Their simulation results suggest a possibility of efficiently utilizing the average spectrum handoff delay and network throughput. A suboptimal greedy mechanism for target channel sequence selection is proposed in [31]. Other more recent mechanisms in this direction are proposed in [32], [33]. A dynamic weight adjustment mechanism to enhance the effectiveness of data transmission during spectrum handoff is proposed in [32]. The channel is assigned based on a weight adjustment algorithm that takes into account the channel bandwidth availability, transmission power, fading aspect, etc. Further, a two-server authentication protocol is proposed in [33] to prevent password forging attacks. Here, each client's password is divided and stored in two independent servers to increase the reliability of the password [37].

Although there are several primary user emulation attack (PUEA) methods [34] countering and spectrum handoff mechanisms, ensuring security during spectrum handoff is still not well investigated. With the arrival of a PU transmitter, the CU required to vacate the occupied channel before searching for a new unused channel. Preventing other nodes from occupying the channel is a type of jamming attack specific to PUEA and CUEA. During the spectrum handoff mechanism, the amount of delay incurred while vacating and occupying another unused channel may be exploited to degrade the network performance. For example, an MU can behaving like a legitimate PU and can prevent an HCU from occupying a channel [37].

Cryptographic techniques can be used to secure the spectrum handoff process [35], [36]. However, these techniques need key management and generate high computational and communication overheads. Therefore, a new spectrum handoff technique that can achieve security without high overheads is needed. Further, a number of authors have proposed various security schemes in other communication networks such as cloud, sensors, mesh and crowdsourcing [37].

A trust-based spectrum handoff mechanism is in [37]. Where threshold method is an approach to decide the trust value on the behaviour of CU which is not appropriate for taking decision. Therefore I proposed fuzzy logic based mechanism to make decision and identification that can effectively resolved the discussed security attack.

III. Proposed Handoff Security Mechanism

The identification of each CU during the handoff mechanism is provided by a CCU by computing their TVs from their communication behaviour using fuzzy logic. The finding and removal of handoff threats depend upon the liveliness of the CU, data delivery ratio of intermediate nodes, and the number of nodes present in the network. The spectrum handoff is initiated whenever a CU desires to switch its ongoing transmission to another accessible channel with the arrival of the PU through the packet transmission by recalling the previous key functions (i.e., spectrum sensing, spectrum decision, and spectrum sharing). During the spectrum handoff, the CU can be compromised by MUs that can introduce various malicious attacks in the CRNC environment as in Figure 1. The MU exploits the delay needed to vacate the present channel and occupy a new unused channel during the spectrum handoff to behave as a legitimate PU or CU. Table 1 provides the list of symbols and abbreviations used in this manuscript [37].

Table 1: List of Symbols and Abbreviations

Symbol	Description
MU	Malicious User
NU	New User
PU	Primary User
SU	Secondary User
CR	Cognitive Radio
CCU	Coordinating Cognitive User
CRN	Cognitive Radio Network
CRNC	Cognitive Radio Network Cell
CU	Cognitive User
CUEA	Cognitive User Emulation Attack
CFSR	Channel Filtering Sender Receiver
CCC	Common Control Channel
DDR	Data Delivery Ratio
HCU	Handoff Cognitive User
ID	Identity
ST	Survival Time

TF/TV	Trust Factor/Trust Value
M	Total Number of Samples
Xi,j	j-th Sample of i-th CU
Ei	Energy sensing technique of ith CU
γ	Predefined Threshold Value

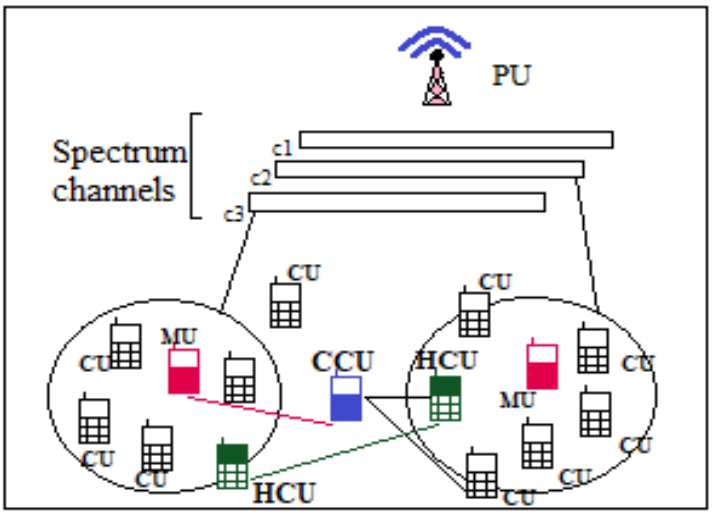

Figure 1: A typical CU handoff mechanism for CRNC.

3.2 Model of proposed mechanism

The proposed security mechanism based on fuzzy logic intends to distinguish and resolve the recently uncovered security threat in the CRN, called CUEA, by computing of the TF/TV of all the CUs. The model of the proposed mechanism is shown in Figure 1. It includes a unified CR environment, including a HCU, CCU, PU, and n number of CUs. The HCU requests for another channel from the CCU upon arrival of a PU and contains n number of CUs which utilize the idle channels of the PU for communication. Figure 2 presents the flowchart of the proposed framework where among n number of CUs, some are selected as PU, MU, and HCU. Initially, the CCU analyzes the type of users by identifying their communication characteristics.

Initially, all nodes are assumed to be trusted. Hence, the network is also deemed to be trusted and ideal. So the trust values are initially distributed randomly and one of the nodes is elected as CCU for verifying the legitimacy NU. However, as the trust value of each node can increase or decrease depending on its communication behavior the CCU node can dynamically change to a node having a higher trust value. Among n CUs, a CCU is elected based also on the survival time (ST) and energy level to make sure that it has sufficient energy to provide communication among the CUs. The communication range of the PU transmitter is assumed to cover the whole CR network, i.e. CRN cell (CRNC). In order to consider the CUEA, an MU is randomly deployed near a target HCU during the communication between HCU and CCU or NU and CCU in order to force the HCU/NU to leave the occupied channel. The goal of the MU is to degrade the performance of the system by limiting the trusted CUs from accessing the idle spectrum channel. For sensing the vacant spectrum band, the energy sensing technique Ei is used where

$$Ei = \sum_{j=1}^{M} |X_{(i,j)}|^2 = \begin{cases} if\ Ei \geq \gamma, then\ user\ is\ present, \\ if\ Ei \leq \gamma, then\ user\ is\ absent. \end{cases}$$

where X(ij) is the j-th sample of the i-th CUs received signal, γ is a predefined threshold value and M is the total number of samples of the i-th CU. The CCU is selected based on the sufficient energy level and survival timing of CU in the CRNC. The CU having sufficient energy level and the longest ST would be elected as the coordinator that creates a look-up table which includes CCU ID, CU ID, CU address, TV, and ST of each user. The ST of the user is the total time period for which the user remained alive in the network. In order to analyze the legitimacy of communicating nodes, the proposed mechanism is validated against an ideal and malicious environment [37] by fuzzy membership function based on the input variables DDR and Liveness.

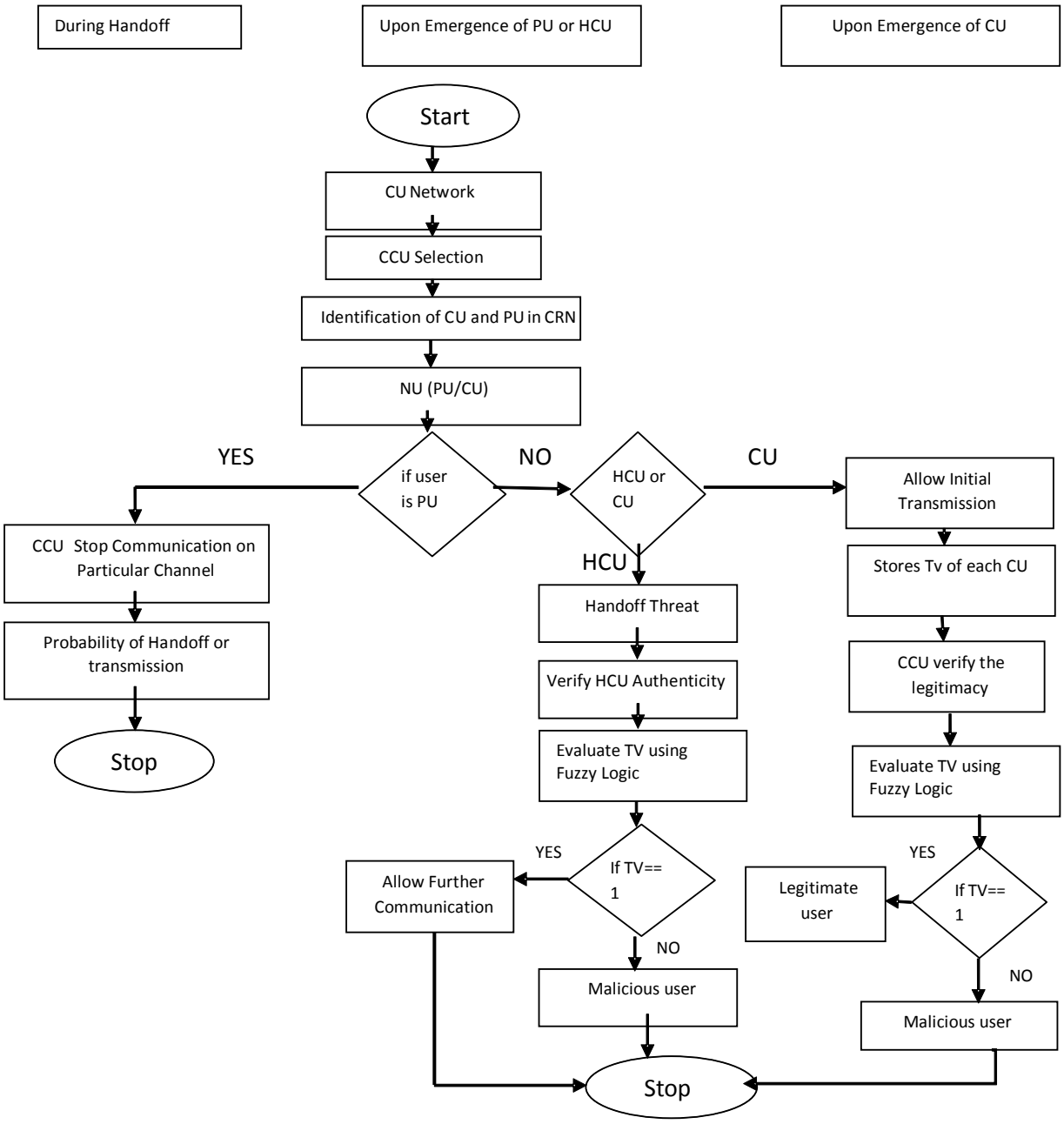

Figure 2: Flowchart of the proposed spectrum handoff of CRN cell.

3.3 Identification of user

The legitimate and malicious behaviour of CU is identified by CCU that computes TV of each CU by using certain characteristics such as the liveliness of user and packet/data delivery ratio (DDR) described in [19] and keeps the action record of all CUs depending on their TV and acts accordingly. Whenever an NU enters in the network, the first step of the CCU is to identify whether the NU is CU or PU. This is done by measuring its behavioural characteristics such as the minimum threshold of the PU signals identified by CCU employing hypothesis testing. In order to ensure a secure communication process among different CUs, CCU needs to identify the legitimacy of CU, HCU, and PU. There are three possible cases: (1) NU is identified as PU, (2) NU is identified as HCU, and (3) NU is identified as CU. The details of each case are presented below [37].

1: NU is identified as a PU

NU is recognized as a PU. The CCU shuts down all the correspondence inside the PU transmitter range. The conveying CU looks for a new idle channel in the network to continue its transmission.

2: NU is identified as HCU

The CCU verifies the legitimacy of the HCU before resuming the transmission on a different vacant channel. Whenever an NU is identified as a CU, there are two possibilities: NU is HCU or NU is CU. If NU is HCU, then there is the possibility of CUEA. During the handoff of CU, an MU may enter randomly and behave like a legitimate HCU, and request the CCU to assign the idle channel to it. In this case, the CCU checks the lookup table in order to verify the CUs ID along with its ST. The legitimate HCU has a longer
ST compared to that of the MU and may also have some transmissions T inside the network. Therefore, the CCU can verify whether or not the user is a legitimate CU and can accordingly allocate the idle channel to the HCU as follows.

$$HCU = \begin{cases} CU\colon\ ST_{CU}ST_{MU}\ have\ some\ transmission\ T, \\ CU\colon\ ST_{CU}ST_{MU}\ have\ no\ transmission\ T. \end{cases}$$

The CUs' TV is computed by measuring the behavioural characteristics of the user such as liveliness, DDR, and TV . The liveliness of the user measures the malicious behaviour by checking the number of broadcast requests sent to the CCU. It measures the level of activeness of nodes in the network. The activeness can be determined by the number of communications/interactions done by the CU in the network. It can be used to detect the malicious nodes that often excessively broadcast request messages to attract neighbouring nodes for spectrum occupation or transmit/forward packets through the shortest path. The MU sends request messages (assumed to be more than 10 requests per millisecond as a threshold value) to the CCU for using the spectrum channel. Further, DDR is considered to be an important parameter for measuring the malicious behaviour of the users because MU often degrades the network performance by dropping incoming data transmissions or simply rerouting the data to another path. The TV of each user would be computed to be either 1 or 0 [37].

3: NU is identified as CU

The CCU allows the initial transmissions and keeps recording the behaviour of the NU into its look-up table. When the NU is identified as a new CU, the possible cases are:

$$NU = \begin{cases} CU, \\ MU. \end{cases}$$

When an NU enters the network, its ST is relatively shorter than the ones of CUs already residing in the network. Therefore, to identify the legitimacy of NU, the CCU initially allows five transmissions to the NU. Random transmission time is chosen for measuring the behaviour of its communicating process in the network. If the NU is CU then the TV of CU would be 1. On the other hand, if the NU is MU, the TV would be 0. The CCU stores the record of transmission information of CUs in its look-up table and checks the TV of NU after the specified number of transmissions.

$$NU = \begin{cases} TV == 1, \quad then\ CU, \\ TV == 0, \ \ then\ MU. \end{cases}$$

If the TV of the NU is 1, then the NU is identified as a trusted CU and further transmission is allowed. Otherwise, the NU is considered to be a MU and further transmission is blocked. The flowchart of the proposed mechanism as illustrated in Figure 2 [37].

IV. Performance Evaluation

4.1 Simulation Setting

In order to evaluate the proposed mechanism, the simulation environment is created using MATLAB and the performance is validated on a network having a simulation area of 400 m × 400 m and 25 IoT devices and 500 round. These devices are identified using unique numbers, which are assigned during the initialization phase in the system. We simulate the performance of the proposed mechanism in terms of throughput (bps) and the handoff status of the CU. Figure 3 shows the considered CRN scenario. In the proposed scenario, whenever a new user enters the CRNC, its legitimacy is validated by the CCU based on the TV. The CCU assigns the TV (0 or 1) to the entered user based on its initial behaviour such as liveliness and DDR. The parameters for the network simulation are depicted in Table 2.

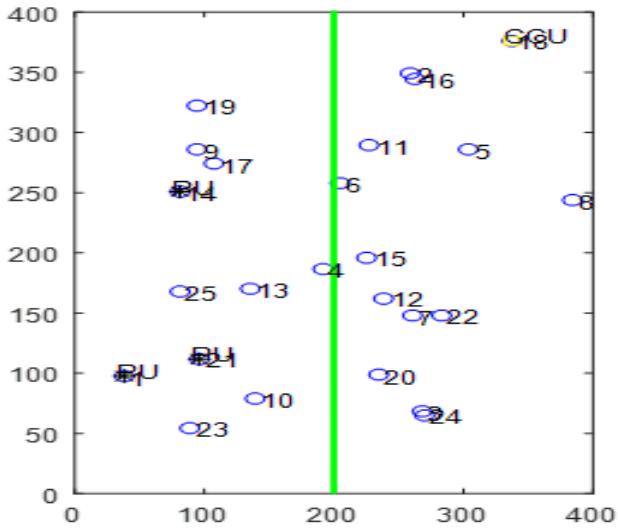

Figure 3: Distribution of nodes in CRN

Table 2: Simulation parameters

Parameters	Size
Network Area	400 m×400 m
Number of Users	25
MAC Protocol	IEEE 802.22
Routing Protocol	AODV
Simulation Round	500
Traffic Source	CBR
Packet Size	512 bytes
Antenna	Omni-Directional

4.2 Data delivery ratio (DDR) And Liveness

DDR is the ratio of data sent and received by the node in CRN and Liveliness is decides as per the count of total time a node is get active for performing the data transmission task. DDR and Liveness as input variable of fuzzy logic system is shown in Figure 4.

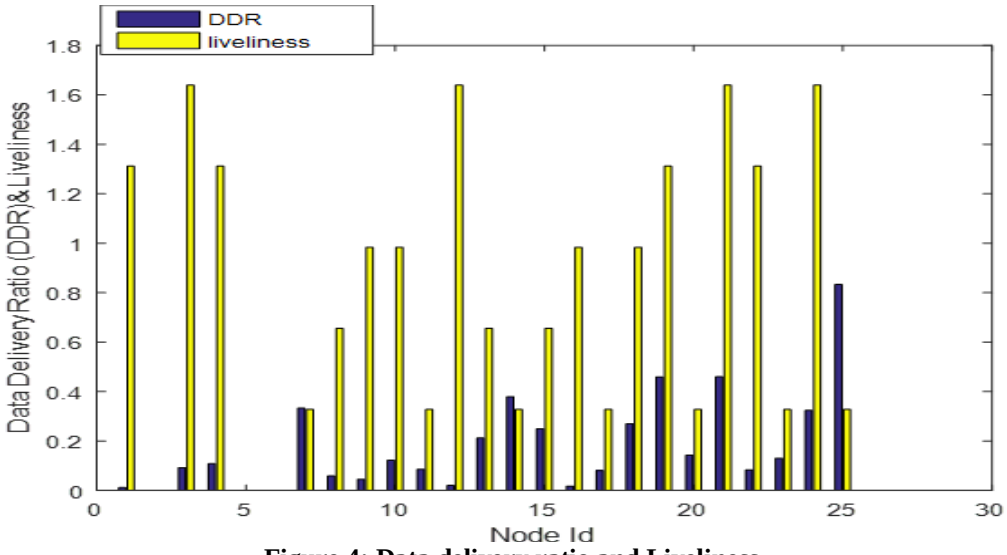

Figure 4: Data delivery ratio and Liveliness.

4.3 Fuzzy logic membership function for input variable and output variable

In fuzzy logic input variables are DDR and Liveness and output variable is Trust Value. All the membership values lies between 0 to 1. Both of the input variables i.e. DDR and liveliness will be passed through the fuzzy

logic model and the degree of membership in respective low, medium and high range will be decided to evaluate trust value as shown in Figure 5.

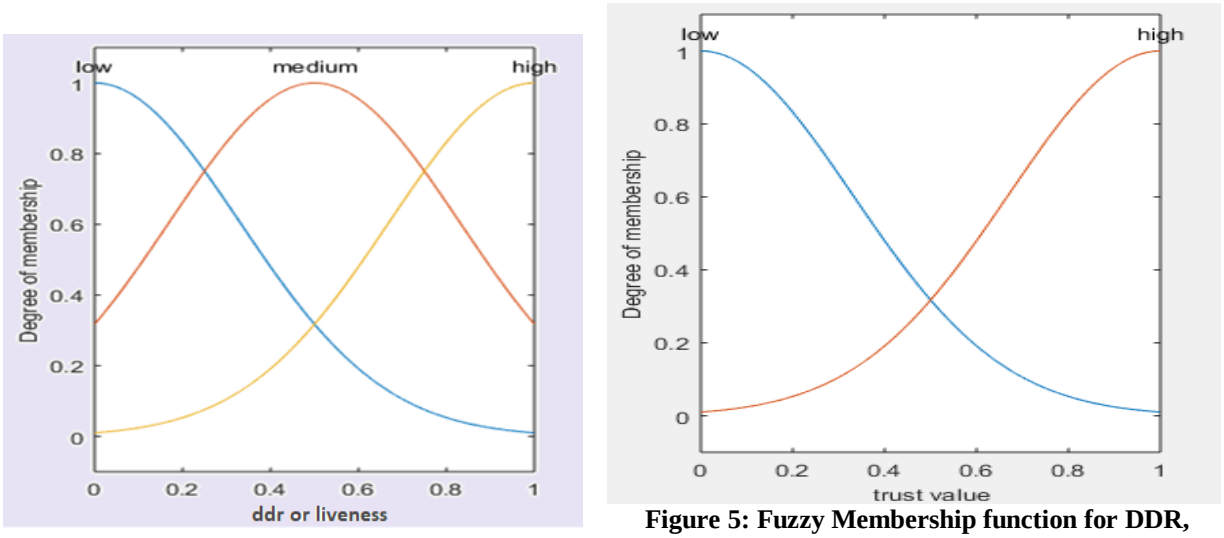

Figure 5: Fuzzy Membership function for DDR, Liveness and Trust Value.

4.4 Impact on probability of error

In the Figure 6 shows the percent probability of error. It is shown in the figure along the y axis .Since it is the percentage hence lies in between 0 to 100 %.The x axis is showing the number of cognitive users considered within a CRN of specific area. The plots shows that as the number of CUs is increased the percent probability of error increases. The minimum percentage of error is 20% for existing thresholding approach and the proposed fuzzy based decision approach has percentage probability of error is 18%. The maximum percentage of error is 65% for existing thresholding approach and the proposed fuzzy based decision approach has percentage probability of error is 62%.It may be easily observed that the percentage the probability of error in determining the malicious user is reduced in the fuzzy based decision approach.

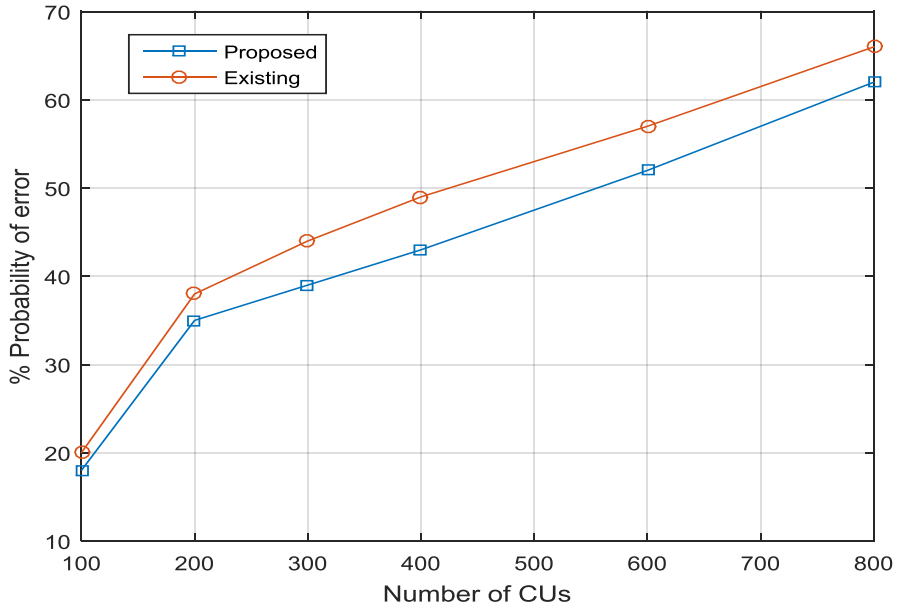

Figure 6: Percent probability of errors with respect to numbers of cognitive users.

4.5 Impact on throughput

In the Figure 7 shows the percent throughput of the CRN is shown in the figure along the y axis .Since it is the percentage hence lies in between 0 to 100 %.The x axis is showing the number of cognitive users considered within a CRN of specific area. The plots shows that as the number of CUs is increased the percent throughput decreases. The maximum percentage of throughput is 96% for existing thresholding approach and

the proposed fuzzy based decision approach has percentage of throughput is 98%. The minimum percentage of throughput is 85% for existing thresholding approach and the proposed fuzzy based decision approach has percentage throughput is 86%. It may be easily observed that the percentage throughput in transmission over the CRN is increased in the fuzzy based decision approach.

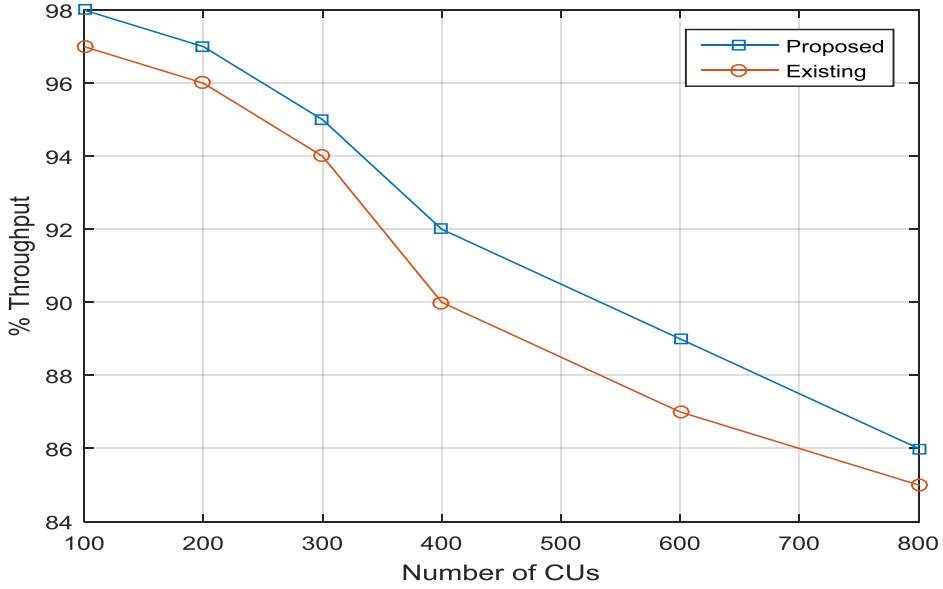

Figure 7: Throughput with respect to numbers of cognitive users.

4.6 Impact on transmission delay

In the Figure 8 shows the transmission delay in seconds of the CRN is shown in the figure along the y axis .Since it is the delay observed on running the process on 100 rounds hence it lies in between 1 to 4 seconds. The x axis is showing the number of cognitive users considered within a CRN of specific area. The plots shows that as the number of CUs is increased the transmission delay increases. The maximum transmission delay is 4 seconds for existing thresholding approach and the proposed fuzzy based decision approach has transmission delay is 3.5 seconds (approx.). The minimum transmission delay is 1.3 seconds for existing thresholding approach and the proposed fuzzy based decision approach has transmission delay is 1.2 seconds. It may be easily observed that the transmission delay in transmission over the CRN is decreased in the fuzzy based decision approach.

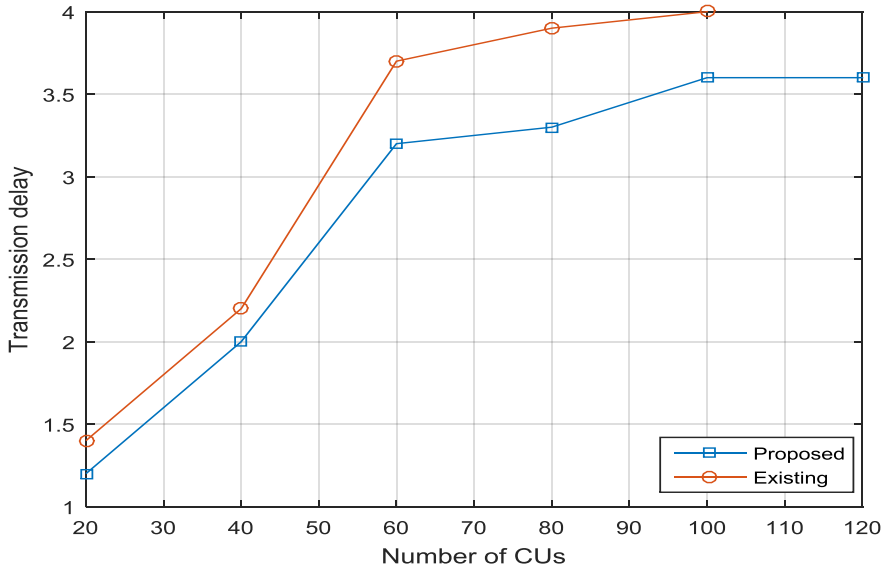

Figure 8: Transmission delay with respect to numbers of cognitive users.

4.7 Comparison with existing mechanism

As in the earlier approaches, the spectrum handoff security in CRN is not explored in fast performance term, and hence, proposed security mechanism is sharply verified the performance of CRN by analyzing the behaviour of cognitive users based on fuzzy logic artificial intelligence system. In threshold decision based method the trust value is due to approximate value of threshold which sometimes make inaccurate decision but it is depicted in proposed mechanism. The proposed handoff mechanism is designed to provide accurate channel sensing by reducing the handoff delay, transmission delay, and energy consumption. Also, a probabilistic system model is used to analyze the trust-based security under various transmission delays, probability of attack strength, and the probability of error during CU mobility. Figures 6, 7 and 8 illustrate the gain of the proposed mechanism because this trust-based security scheme using fuzzy logic validates each handoff of CUs before allowing it to resume its transmission process on another vacant channel [37]. Following table 3 shows the comparative performance enhancement of proposed mechanism.

Table 3: Summary of results for comparison of existing and proposed algorithm

Percent Probability of error		**Percent throughput**		**Transmission delay**	
Existing	**Proposed**	**Existing**	**Proposed**	**Existing**	**Proposed**
25.21	21.75	94.08	95.76	1.96	1.84
High	Low	Low	High	High	Low
	Better		Better		Better

V. Conclusion

The demand for highly efficient spectrum utilization scheme is getting more pronounced in the recent increasing digitalized application at high definition. But, this has also introduced multiple type of new threats over the security. In this work, I have introduced a smart cognitive user based attack emulation scheme for the cognitive radio network (CRN), that helps to exploits the intruders attack during the process of the handoff. I have also proposed and developed a simulation model on MatLab software having a highly secure handoff process that helps to counter the attack successfully introduced by malicious user through the supervision of coordinating cognitive user that evaluates the trust value level using the fuzzy logic algebra for cognitive user going through the handoff process based on its behavioural characteristics. To assess the adaptability of the proposed mechanism, the throughput for various number of CUs is thought of. As portrayed in outcomes the likelihood of mistake increments as the number of CUs augments. The throughput normally diminishes as the number of CUs increased. In expansion, the above outcome is additionally upheld by examining the message modification process, where the new CUs alters the sent message during the node's validation in an attempt to expand its shot at transmissions. The proposed fuzzy logic based mechanism still performs better than that of thresholding approach with an enormous number of CUs. The performance gain comes from the way that the trust esteem of each node. CU is processed to all the more precisely choose the actual conduct of each node. The TV of the node increases as the node is associated with the alteration process more. And the performance of proposed fuzzy logic based mechanism is noticed better compared to that of thresholding approach with the different network region in CRN.

Acknowledgement

I express my deepest sense of gratitude towards my supervisor Prof. Rakesh Kumar Singh, Department of Electronics Engineering of Kamla Nehru Institute of Technology, Sultanpur, for their patience, inspiration, guidance, constant encouragement, moral support, keen interest, and valuable suggestion during preparation of this research paper.

References

[1]. E. Hill and H. Sun, "Double threshold spectrum sensing methods in spectrum-scarce vehicular communications," IEEE Trans. On Indus. Info., vol. 14, no. 9, pp. 4072–4080, 2018.

[2]. B. Zheng, M. Wen, S. Lin, W. Wu, F. Chen, S. Mumtaz, F. Ji, and H. Yu, "Design of multi-carrier lbt for laa&wifi coexistence in unlicensed spectrum," IEEE Network, 2019. doi:10.1109/MNET.2019.1900172.

[3]. A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Cooperative spectrum sensing in multiple antenna based cognitive radio network using an improved energy detector," IEEE Communications letters, vol. 16, no. 1, pp. 64–67, 2011.

[4]. S. K. Haider, A. Jiang, M. A. Jamshed, H. Pervaiz, and S. Mumtaz, "Performance enhancement in P300 ERP single trial by machine learning adaptive denoising mechanism," IEEE Netw. Letters, vol. 1, no. 1, pp. 26–29, 2018.

[5]. E. Meshkova, Z. Wang, K. Rerkrai, J. Ansari, J. Nasreddine, D. Denkovski, T. Farnham, J. Riihij¨arvi, L. Gavrilovska, and P. M¨ah¨onen, "Designing a self-optimization system for cognitive wireless home networks," IEEE Trans. on Cognitive Commun. And Netw., vol. 3, no. 4, pp. 684–702, 2017.

[6]. B. Van Nguyen, H. Jung, D. Har, and K. Kim, "Performance analysis of a cognitive radio network with an energy harvesting secondary transmitter under nakagami fading," IEEE Access, vol. 6, pp. 4135–4144, 2018.

[7]. K. Kumar, A. Prakash, and R. Tripathi, "Spectrum handoff in cognitive radio networks: A classification and comprehensive survey," Journal of Net. and Comp. App., vol. 61, pp. 161–188, 2016.

[8]. A. Koushik, J. D. Matyjas, F. Hu, and S. Kumar, "Channel/beam handoff control in multi-beam antenna based cognitive radio networks," IEEE Trans. on Cognitive Commun. and Netw., vol. 4, no. 1, pp. 30–42, 2017.

[9]. B. Zheng, M. Wen, S. Lin, W. Wu, F. Chen, S. Mumtaz, F. Ji, and H. Yu, "Design of multi-carrier LBT for LAA & WiFi coexistence in unlicensed spectrum," IEEE Network, 2019. doi:10.1109/MNET.2019.1900172.

[10]. Y. Wu, F. Hu, Y. Zhu, and S. Kumar, "Optimal spectrum handoff control for CRN based on hybrid priority queuing and multiteacher apprentice learning," IEEE Trans. on Veh. Technol., vol. 66, no. 3, pp. 2630–2642, 2016.

[11]. Y. Zhao, Z. Hong, Y. Luo, G. Wang, and L. Pu, "Prediction-based spectrum management in cognitive radio networks," IEEE Sys. Journal, vol. 12, no. 4, pp. 3303–3314, 2017.

[12]. M. Kashif, Z. Ullah, M. Iqbal, L. Musavian, S. Sarwar, X. Wang, S. Mumtaz, Z. Ul-Qayyum, and H. M. Safyan, "Multiuser detection using hybrid arq with incremental redundancy in overloaded mimo systems (workshop paper)," in International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 642–653, Springer, 2019.

[13]. P. M. Rodriguez, A. Lizeaga, M. Mendicute, and I. Val, "Spectrum handoff strategy for cognitive radio-based MAC for real-time industrial wireless sensor and actuator networks," Comp. Netw., vol. 152, pp. 186–198, 2019.

[14]. J. Qi, F. Hu, X. Li, A. Koushik, L. Hu, and S. Kumar, "CR based video communication testbed with robust spectrum sensing/ handoff," in Info. Technol.: New Generations, pp. 59–70, Springer, 2016.

[15]. M. E. Bayrakdar and A. Calhan, "Improving spectrum handoff utilization for prioritized cognitive radio users by exploiting channel bonding with starvation mitigation," AEU-Int. Journal of Elec. And Commun., vol. 71, pp. 181–191, 2017.

[16]. M. Aggarwal, T. Velmurugans, M. Karuppiah, M. M. Hassan, A. Almogren, and W. N. Ismail, "Probability-based centralized device for spectrum handoff in cognitive radio networks," IEEE Access, vol. 7, pp. 26731–26739, 2019.

[17]. R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," IEEE Commun. Surveys & Tuts, vol. 17, no. 2, pp. 1023–1043, 2014.

[18]. Z. Zheng, T. Wang, J. Wen, S. Mumtaz, A. K. Bashir, and S. H. Chauhdary, "Differentially private high-dimensional data publication in internet of things," IEEE Int. of Things Journal, 2019. doi:10.1109/JIOT.2019.2955503.

[19]. G. Rathee, P. Thakur, G. Singh, and H. Saini, "Aspects of secure communication during spectrum handoff in cognitive radio networks," in 2016 International Conference on Signal Processing and Communication (ICSC), pp. 64–69, IEEE, 2016.

[20]. M. Patnaik, V. Kamakoti, V. Matya´sˇ, and V. Rˇ eha´k, "PROLEMus: A proactive learning based mac protocol against PUEA and SSDF attacks in energy constrained cognitive radio networks," IEEE Trans. on Cognitive Commun. and Netw., 2019. doi:10.1109/TCCN.2019.2913397.

[21]. S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A. Y. Zomaya, and R. Ranjan, "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks," IEEE Trans. on Netw and Service Management, vol. 16, no. 3, pp. 924–935, 2019.

[22]. Y. Wu, Q. Yang, X. Liu, and K. S. Kwak, "Delay-constrained optimal transmission with proactive spectrum handoff in cognitive radio networks," IEEE Tran. on Commun., vol. 64, no. 7, pp. 2767– 2779, 2016.

[23]. C.-W. Wang and L.-C. Wang, "Analysis of reactive spectrum handoff in cognitive radio networks," IEEE Journal on selected areas in commun., vol. 30, no. 10, pp. 2016–2028, 2012.

[24]. A. F. Tayel, S. I. Rabia, and Y. Abouelseoud, "An optimized hybrid approach for spectrum handoff in cognitive radio networks with non-identical channels," IEEE Trans. on commun., vol. 64, no. 11, pp. 4487–4496, 2016.

[25]. L. Zhang, T. Song, M. Wu, X. Bao, J. Guo, and J. Hu, "Trafficadaptive proactive spectrum handoff strategy for graded secondary users in cognitive radio networks," Chinese Journal of Electronics, vol. 24, no. 4, pp. 844–851, 2015.

[26]. M. Mehrnoush, R. Fathi, and V. T. Vakili, "Proactive spectrum handoff protocol for cognitive radio ad hoc network and analytical evaluation," IET Commun., vol. 9, no. 15, pp. 1877–1884, 2015.

[27]. F. Liu, Y. Ma, H. Zhao, and K. Ding, "Evolution handoff strategy for real-time video transmission over practical cognitive radio networks," China Commun., vol. 12, no. 2, pp. 141–154, 2015.

[28]. C. Pan, X. Zhang, and K. Yan, "Efficient spectrum handoff scheme in cognitive radio," in 2015 5th International Conference on Information Science and Technology (ICIST), pp. 40–45, IEEE, 2015.

[29]. D.-J. Lee and W.-Y. Yeo, "Channel availability analysis of spectrum handoff in cognitive radio networks," IEEE Commun. Letters, vol. 19, no. 3, pp. 435–438, 2015.

[30]. F. Afsana, N. Jahan, F. A. Sunny, M. Kaiser, and S. Mamun, "Trust and energy aware cluster modeling and spectrum handoff for cognitive radio ad-hoc network," in 2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), pp. 1–6, IEEE, 2015.

[31]. A. Y. Zakariya, A. F. Tayel, and S. I. Rabia, "Comments on optimal target channel sequence design for multiple spectrum handoffs in cognitive radio networks," IEEE Trans. on Commun., vol. 63, no. 8, pp. 3021–3024, 2015.

[32]. Z. Zhi-jin, Z. Lu-ping, and W. Hai-quan, "Spectrum handoff based on adaptive weights adjustment," IET Commun., vol. 9, no. 5, pp. 674–680, 2015.

[33]. X. Yi, F.-Y. Rao, Z. Tari, F. Hao, E. Bertino, I. Khalil, and A. Y. Zomaya, "ID2S password-authenticated key exchange protocols," IEEE Trans. on Computers, vol. 65, no. 12, pp. 3687–3701, 2016.

[34]. D.-T. Ta, N. Nguyen-Thanh, P. Maill´e, and V.-T. Nguyen, "Strategic surveillance against primary user emulation attacks in cognitive radio networks," IEEE Trans. on Cognitive Commun. and Netw., vol. 4, no. 3, pp. 582–596, 2018.

[35]. 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.

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

[37]. G. Rathee, N. Jaglan, S. Garg, B. J. Choi, and K.K. R. Choo, "A Secure Spectrum Handoff Mechanism in Cognitive Radio Networks," IEEE Trans. on Cognitive Communications and Networking.,2019. doi: 10.1109/TCCN.2020.2971703.

Ranajeet Kumar, et. al. "Enhanced Spectrum Handoff Security Mechanism In Cognitive Radio Network." *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)* 17(1), (2022): pp 14-23.