IMPROVED SECURITY MECHANISM FOR SPECTRUM HANDOFF IN COOPERATIVE WIRELESS NETWORKS

[1]ANAND RANJAN, [2]O.P. SINGH, [3]HIMANSHU KATIYAR

[1]Department of Electrical and Electronics Engineering, Amity School of Engineering and Technology, AMITY University, Lucknow Campus, Uttar Pradesh, India.

[2]Department of Electronics Engineering, Rajkiya Engineering College, Sonbhadra, Uttar Pradesh, India.

[1*]anandranjan@live.com, opsingh@amity.edu,grmishra@amity.edu,katiyarhimanshu@gmail.com

ABSTRACT

Cooperative wireless communication (CWC)is emerging as a cutting-edge technology with the goal of making opportunistic and dynamic use of unused spectrum bands. Fixed spectrum allotment by highly secure entities are results in challenging utilization of resources. In this paper, we present a unique cognitive user emulation attack (CUEA) in cooperative communication networks (CCN) that can employ during spectrum handoff to detect intruders. We next provide a safe handoff mechanism which can effectively counter quite an assault by providing a coordinating cognitive user that evaluates individual cognitive user's levels of trust predicated on its behavioral attributes. The coordinating cognitive user can effectively recognize malicious individual's users by perusing trust factors. MATLAB simulations are used to verify the suggested mechanism's performance. The simulation results demonstrate the suggested mechanism's utility in terms of wrong authentication recognition likelihood, detection level, throughput level, and transmission time.

Keywords: *CCN, CWC, CUEA, Spectrum Handoff.*

1. INTRODUCTION:

Only an available portion of the spectrum can be assigned to a relay node inside the CCN system. As a result, the relay node must detect the spectrum ranges, keep the information, as well as determine the white spaces. The three primary categories of spectrum sensing methods are as follows:

- **Primary Transmitter Detection**

The essential concept behind such method is to detect the primary transmitter's signals, but it is quite weak. Spatial monitoring is used to do this. The strategies for identifying the transmitters are as follows:

a. **Matched Filter Detection:** Matched filter is an effective method at static Gaussian noise where the main signal from the customer information is well-known relay node operator. Since spectral correlation qualities of the signals are typically dissimilar, any signal that would be obscured in interference as well as noise can be recognized employing a matched filter.

b. **Energy Detection:** When the primary signal information is uncertain, energy detection is a better alternative. An energy detector determines the energy acquired on a primary band throughout an evaluation period, and then if the examined energy is lower than pre-defined criteria, a spectrum hole is confirmed. Energy detectors frequently trigger false alarms as a result of its ability to discriminate between different signal categories [6].Explains how to perform a threshold optimization as well as lower the likelihood of error.

c. **Feature Detection:** Any modulated signal is generally characterized by built-in periodicity or otherwise cyclostationarity.This property might be distinguished using a spectral correlation function [10].The resilience of features recognition toward noise power fluctuation is their major benefit. It is, nevertheless, technologically challenging as well as needs extended observational times.

- **Primary Receiver Detection**

The primary receiver detection goal is to locate users who are the primary recipient's information inside relay node contact region. In the primary receiver identification, leakage power is used to determine existence the principal recipient. It will required added hardware, such as a sensor system that supports the region's principal receivers. It is presently only relevant to the identification of receivers, yet being the most efficient method for finding spectrum gaps.

- **Interference Based Detection**

For interference measurements, the FCC has created a framework. This model shows how the signal of a radio station is designed toward work in a region in which input power hits noise level. As more interfering signals appear at various points around the operating zone, the noise level grows. By selecting a specific thresholds, which would be the greatest amount of distortion that the reception can endure, the interference temperatures model regulates interference observed at the reception.Because cognitive users can't tell the difference among PU signals versus interference, this model's issue is measuring the interference temperatures accurately.

Recent work has simulated on the MatLab Software by following the international standards used for co-operative spectrum sensing. A safe handoff mechanism to counter quite assault by malicious users are tackled through machine learning approach using fuzzy logic. The fuzzy logic is simple and fast decision scheme that do not require any high level hardware complexity like other algebraic methods but the limitations that are associated with fuzzy inference system is the optimum decision of appropriate membership function (MF),type of MF and MF parameters and number of MF assigned to each input and output variable. In this article the limitation is existing because of large time taken in exploring best out of multiple combinations of aforementioned attributes related to fuzzy membership function.

2. RELATED WORK:

Jiang Zhu(2017) [11] In the medical field, wireless sensor networks are used to collect multimedia content from a variety of sources, like as video streaming, pictures, voice, cardiac, as well as pulse rate data, which necessitates a larger bandwidth and much more usable spectrum. In contrast, today's modern radio spectrum is extremely congested because of rapidly growing popularity of many wireless services. As a result, cognitive wireless sensor networks (CWSN), which take utilization of the benefits of cognitive radio technologies, are a possible solution to the spectrum shortage problem. One of most difficult aspects of the CWSN is maximizing network longevity with suitable power control mechanisms. The power management technique based on game theory depending on Hidden Markov Model (HMM) presented to handle grid connected control concerns in CWSNs with incomplete input, based on the diversity as well as independence of spectrum sensing findings between subscribers of cognitive wireless sensor networks (CWSNs). CWSNs may employ HMM to estimate if or not their contenders are playing game, improving the data consistency and resulting in efficient transmitted power.

Arsany Guirguis, (2018) [12] described a conventional routing protocols within cognitive radio networks restrict areas that are heavily overloaded with main users, allowing just a tiny portion of usable links enabling secondary route creation. Furthermore, wireless communications are susceptible to channels impairments like multipath fading, causing the strength of usable links to fluctuate greatly. They introduced an undercover: multi-hop connectivity system besides cognitive radio networks that combines collaborative beam forming using layer 3 routing. The protocol, in particular, revisits basic assumption made by region routing algorithms for overlaying cognitive radio networks: that intermediate Consumers are unable to access range while main users are utilizing this. They permit collection number of customers, every one having particular antenna, to work together as well as broadcast in areas where principal consumers are active in undercover. This is accomplished by using beam forming to null out signal at primary receivers. Furthermore, whenever feasible, the goal is to increase transmission dependability at auxiliary locations. It makes the system interference-aware and allows for the high levels of disturbance that cooperative communications often cause. As a result, cooperative communications are penalized based on the number of secondary rows that are adversely impacted.

Yihang Du,(2019) [13] focused on transmission delay reduction and increased energy effectiveness as two major issues in multi-hop systems, where topologies as well as spectrum information are difficult to achieve. As a result, this paper proposes the cross-layer routing algorithm dependent as of quasi-cooperation multi-agent knowledge. To begin, a standardized utility feature is created to construct a suitable tradeoff among the two metrics by captivating into account both end-to-end delay as well as power consumption. The joint development issue is then described along with a Stochastic theory as well as quasi-cooperative multi-agent understanding technique for solving the challenges that only requires information sharing with preceding nodes, is proposed. To improve performance even more, it required to crack links but also reduce version variation, experiences replaying is used to update speculation assumption. Simulation findings display that the suggested scheme outperforms in terms of latency, packet drop, and energy economy, coming near to the performances of an ideal system. The author of this study created ERT-CMAQL, multi-hop CRN-based quasi-cooperative multi-agent learner system.

Dingde Jiang, (2016) [14] discussed that due to wireless networking with cognitive capabilities, node coordination exists significant difficulty. The collaborative multi-hop navigation through cognitive systems is subject of this research. Cognitive networks with multiple hops; they offer a new approach for constructing collaborative routing. The Interference between terminals includes both primary as well as secondary user into account by this method. Through multi-hop cognitive wireless systems using several main and auxiliary consumers, clustering as well as collaboration is used to increase collaborative routing efficiency. They introduced a novel clustering-based constructive multi-hop cognitive networking method towards improve system throughput by considering optimum propagation length, telecommunication, broadcast controlling as well as energy management, including channel estimation. The strategy is both possible and effective, according to simulated data.

3. METHODOLOGY:

A CCU provides each user's authentication as well as security through the handoff process by analyzing and regulating their actions by recognizing as well as estimating actual antenna relying on communication behavior. The vitality of the subscriber in the networks, the packet transmission ratio of destination node, as well as the number of cluster heads available in the system all affect the identification and eradication of handoff issues. The suggested security technique is provided in two scenarios: 1) when a novel user (NU) is identified as a main user (PU), 2) when NU is identified such as a CU or HCU. That whenever a CU (cooperative network user) wishes to change its existing transmission towards another available channel mostly with entrance of the PU via packet transmission by retrieving prior key functions, then spectrum handoff is launched (i.e., spectrum sensing, spectrum decision, and spectrum sharing). MUs (malicious users) can compromise the CU during spectrum handoff, allowing them to launch numerous malicious activities in the cooperative network architecture. The MU takes advantage of the time it takes to depart the current channel and acquire newly unoccupied channels throughout the spectrum handoff operates like true PU or CU.

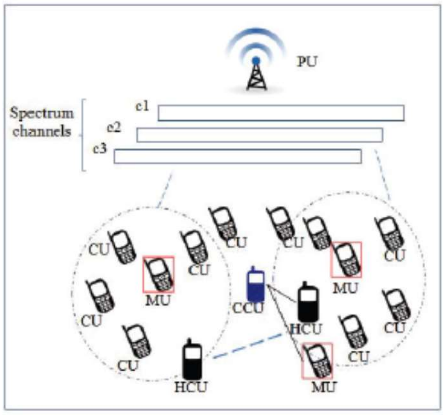

Fig. 1: A Typical CU Handoff Mechanism For Cooperative Network

3.2.1 System Model:

Applying CCU to estimate trust value (TV) of every CUs, recommended security mechanism intends to identify as well as resolve the newly revealed security danger inside the cooperative network, dubbed CUEA. The suggested mechanism's systems model is shown in Fig. 1. It includes an HCU, CCU, PU, as well as n numbers of CUs in a centralized cooperative network setting. When a PU arrives, the HCU asks additional route from the CCU, and it includes n CUs that use the PU's idle channels of communications. Fig. 2 depicts the flowchart of the recommended system, in which specific CUs are designated as PU, MU, or HCU out of a total of n. Primarily, the CCU identifies the type of customer (PU, HCU, or CU) by detecting its communication parameters, as well as when the PU is identified, all communication is terminated. Furthermore, when user is CU, CCU permits five original transmissions to study the user's trust value (behavior) by storing each operation in its databases. CCU certifies the legality of CU as 1 or 0 after a predetermined number of transmissions; if TV is recognized as 1, the user is MU as well as will be continuously prohibited by CCU. Likewise, if the user is HCU, there is a risk of MU intrusion if the HCU's genuine location is faked. The CCU checks the legitimacy of the HCU by looking up its ST inside lookup table. If the harmful user's trust value is more than the trust value of HCU as well as ST of valid CU, the user is allowed to continue communicating; else, the user is labeled malicious in the cooperative network.

During the system's preliminary setup, all nodes are presumed to be legitimate and reliable. As a result, the network is regarded as reliable and optimal at the time of installation. In a cooperative networks, the security enhances as the communication exchanges between nodes expands. The trust values dispersed at arbitrary at first and single node chosen as the CCU to check the legitimacy of HCUs as well as NU. However, because every node's trust value might rise or fall based on that's own communication behavior, CCU nodes may dynamically switch to node with greater trust value. A CCU is chosen from among n CUs based on its survival time (ST) as well as energy capacity to ensure because it possesses enough energy to allow communication between CUs. The PU transmitter's transmission range is considered to include the entire CR network, i.e. CRN cells (CRNC). To evaluate CUEA, a MU is placed at arbitrary near a particular HCU throughout communication (between (HCU as well as CCU) or (NU as well asCCU)) to push HCU/NU to quit the cooperative network's allocated channel. The MU's objective is to harm system efficiency by preventing trusted CUs from obtaining inactive spectrum channel. The energy-sensing technology Ei is used to detect the unoccupied spectrum band.

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

where X(ij) is the j-th sample of i-th CU's acquired signal, is a specified threshold value, M is i-th CU's total number of samples The CCU is chosen depending on the CRNC's appropriate energy level as well as CU's survival timing. The CU with the most energy as well as the longest ST is chosen as the coordinators, who build a look-up table with each user's CCU ID, CU ID, CU address, TV ID, as well asST. The user's ST represents entire amount of time the user was active in the network. Predetermining numerous threshold levels for the purpose of analyses authenticity of communication nodes validates proposed technique in both an ideal and malevolent environment. Between 10% as well as 30% of the baseline energy remained at the nodes is the threshold value at which a node is defined susceptible. Any cooperative networks node with a value less as this value is not authorized to transmit or receive data packets. Half of the measured characteristics acquired by studying their communication behavior is used as the preset threshold value.

The databases used in this article to associate the communication in between the user are synthetically generated by binary sequence generator algorithms. However the real world data is noisy and has different features and characteristics. In synthetic database when associated with simulation is not cast parallel performance to real world. The assumption of malicious user is also randomly assigned but it may be difficult to access the malicious user prototype during development phase of algorithm. These threats for validating this work may remove by using the data records of telecommunication available on lab repository available for research and analysis purpose. The data must contain the user records and activities saved during several experiments in lab and external environment using wireless sensor nodes.

3.2.2 User Identification

CCU recognizes both authorized and malicious CU behavior by evaluating TV for each CU based on some features such as user liveliness as well as packet/data delivery ratio (DDR) as stated in [42], storing an intervention history for all CUs based on their own TV, and acting appropriately within the cooperative system. The CCU's first responsibility when a NU joins the network is to determine as to if the NU comprises CU or PU. This is accomplished by determining their behavioral features, like least threshold of the PU signals detected by CCU, using hypothesis testing. In order to establish safe communication mechanism across various CUs, CCU must determine legality of CU, HCU, as well as PU. There are three possibilities in a cooperative network: (1) NU is defined as PU, (2) NU is recognized for HCU, as well as (3) NU is classed as CU. The specifics of each case are provided below.

3.2.2.1 Case 1:

NU is discovered to be a PU. Within PU broadcast range, CCU disables all communications. To initiate transmission, the communication CU finds out a suitable idle route.

3.2.2.2 Case 2:

NU is recognized like HCU, before restarting transmission on a new unoccupied channel, the CCU double-checks the HCU's authenticity. There are two possibilities when a NU is classified as a CU: NU is an HCU or NU is a CU. The option of CUEA exists if NU is HCU. During the CU handoff, a MU may appear at any time and pretend to be a legal HCU, requesting that the idle channel be assigned to it by CCU. The CCU looks up the CU's ID and ST in the lookup table in this situation. The valid HCU has a longer ST than the MU, as well as internal transmissions T. As a result, the CCU may evaluate if the client is a genuine CU as well as allocate the idle channels towards the HCU in the following manner**:**

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

The TV of the CUs is calculated by taking into account the user's behavioral traits such as liveliness, DDR, as well as TV. By counting the amount of broadcasts request forwarded to CCU, the user's liveliness is used to determine harmful conduct. It determines the network's level of activity. The number of communications/interactions performed by a CU in system could be utilized to evaluate its engagement. It can be used to identify malicious networks that send out a lot of requests in order to lure adjacent nodes for spectrum occupancy or to transmit/forward packages in cheapest route possible. MU forwarded request towards the CCU for use of the spectrum channel (guessed to be greater than 10 requests per millisecond like threshold number). Furthermore, because MU frequently impacts network security by rejecting incoming data transfers or merely rerouting data to a different route, DDR is seen as a crucial measure for detecting malicious user activity. Each user's TV would be assigned a number between one and zero. The TV is a 1 if the liveliness as well as DDR features reach a predetermined given threshold, else it is a 0.

3.2.2.3 Case 3: NU is taken for CU.

The CCU permits beginning transmissions as well as continues to monitor the NU's activity in its own look-up table. As soon as a NU is considered as a novel CU, following scenarios are available:

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

When a NU joins the network, its ST is significantly lower than that of the CUs currently there. As a result, the CCU firstly allows five broadcasts to the NU in order to determine NU's validity. The behavior of its communicative activity in the network is measured using an arbitrary transmission time. If NU is CU,TV of CU will be higher than predetermined number. If the NU is MU, on the alternative hand, the TV will be less than the predetermined threshold ratio of zero. CCU keeps track of CU transmission data in its look-up table as well as verifies NU's TV after a certain period of transmissions.

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

If the NU's TV is 1, the NU is considered a trustworthy CU, as well as continued transmission is permitted. However, the NU is treated as a MU, and subsequent transmission remains disabled. This developed mechanism's flowchart, as shown in Fig. 2, is further elaborated using various methods.

4. RESULTS AND DISCUSSIONS:

In this project, a cooperative network is developed having two different area with some primary users PU and multiple cooperative networkusers (CU). In figure 3 it can be observed that the proposed CRN has 25 nodes having random initial positions and they are moving in different direction and displacements.

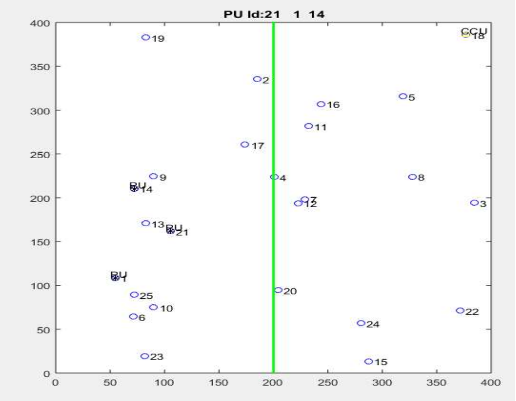

Figure 3: Distribution Of Nodes In Crn

Figure 3 shows the initial coordinates of all the nodes distrusted randomly in Area 1 and 2.The position f nodes is changing with uneven displacements. The nodes which lie at the boundary of Area1 and 2 are taken as passing through the handoff process.

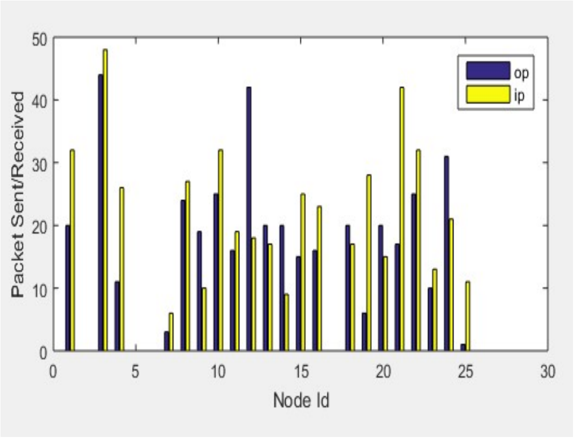

Figure 4: Packet Sent And Received By Different Nodes

Figure 4 shows the value of data input and output at each node respectively at a specific round in the cooperative network. The blue bar shows the plot of data sent by each node and yellow bar represent data received by each node. In this case total 25 nodes are only considered.

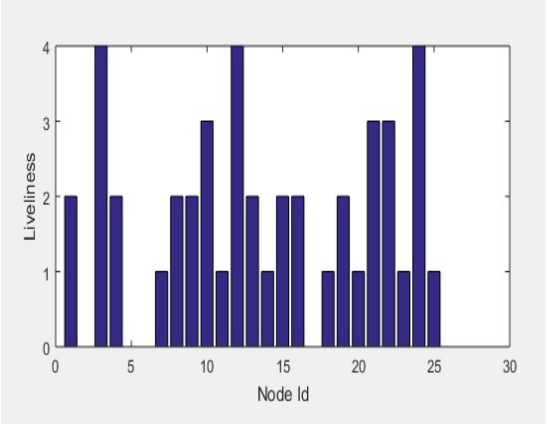

Figure 5: Liveliness Value Of Each Node.

Figure 5 shows the value of the liveliness of each node respectively at a specific round. The blue bar shows the plot of liveliness value each node. In this case total 25 nodes are only considered.Liveliness is decides as per the count of total time a node is get active for performing the data transmission task.

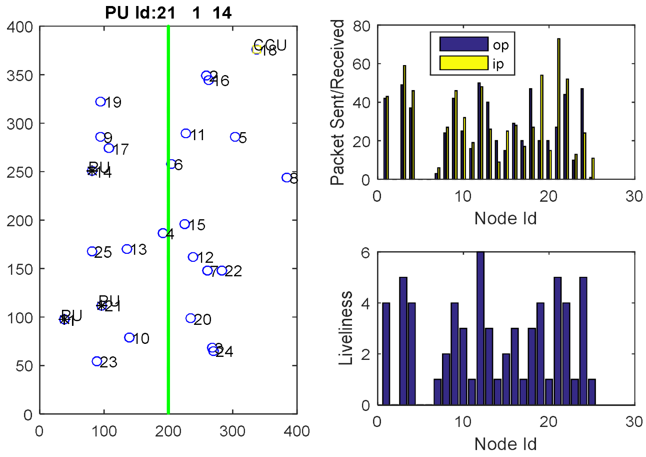

Figure 6: Network Nodes Position(Left),I/P And O/P Data And Liveliness At Round 15.

In figure 6 (left) the cooperative networkis shown having two different area with primary users PU and CU. In figure 5 it can be observed that the status of nodes is shown for 25 nodes moving in different direction and displacements.In this figure 6 the top right subplot shows the value of data input and output at each node respectively at round.15 The blue bar shows the plot of data sent by each node and yellow bar represent data received by each node. In this case total 25 nodes are only considered.The bottom right subplot shows the value of the liveliness of each node respectively at a 15th round. The liveliness is decides as per the count of total time a node is get active for performing the data transmission task.In the similar manner in each round the figure values are updated for respective nodes.

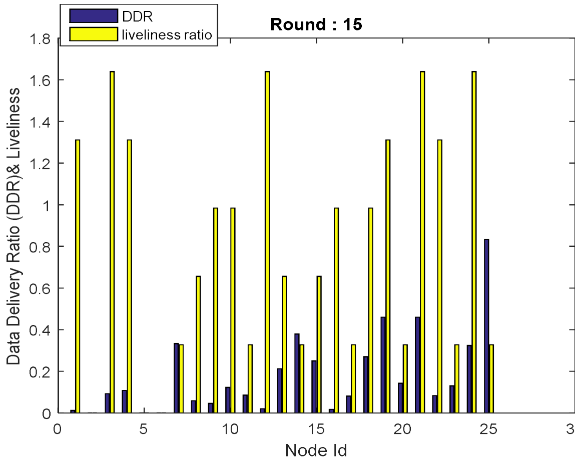

Figure 7: Data Delivery Ration And Liveliness At Round 15.

In this figure 7 the bar plot shows the value of data delivery ratio (DDR) along with the value of liveliness at each node respectively at round.15 The blue bar shows the plot of data delivery ration by each node and yellow bar represent liveliness each node. In this case total 25 nodes are only considered.

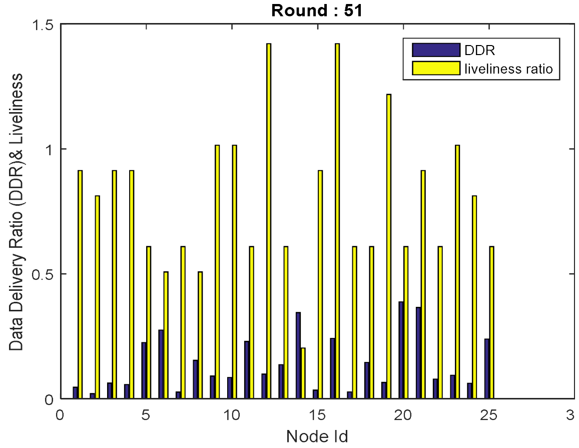

Figure 8: Data Delivery Ration And Liveliness At Round 51.

In this figure 8 the bar plot shows the value of data delivery ratio (DDR) along with the value of liveliness at each node respectively at round.51 The blue bar shows the plot of data delivery ration by each node and yellow bar represent liveliness each node. In this case total 25 nodes are only considered.It may be observed that as the rounds are increasing the value of DDR and liveliness are changing.

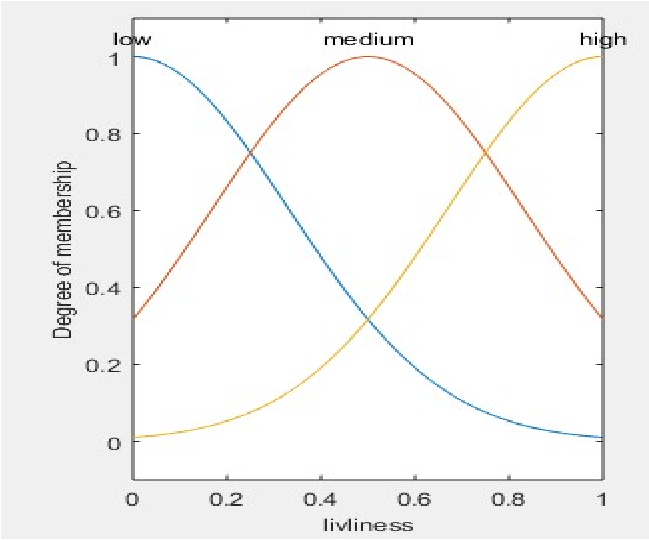

Figure 9: Fuzzy Membership Function For Input Variable As Liveliness

The figure 9 displays the value of fuzzy membership function portion for the DDR as the input 1.The y axis is the membership value lies between 0 to 1.The x axis is the DDR value and it varying prom 0 to 1.The DDR as an input variable is divide into three membership functions.

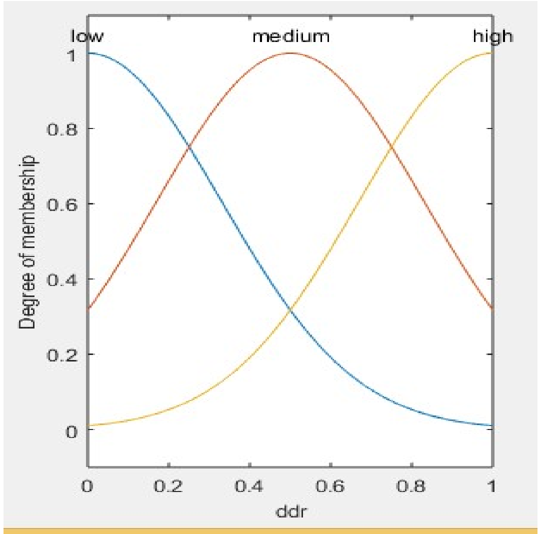

Figure 10: Fuzzy Membership Function For Input Variable As Liveliness

The figure 10 displays the value of fuzzy membership function portion for the liveliness as the input 2.The y axis is the membership value lies between 0 to 1.The x axis is the liveliness value and it varying prom 0 to 1. The liveliness is an input variable is divided into three membership functions. 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 the trust value.

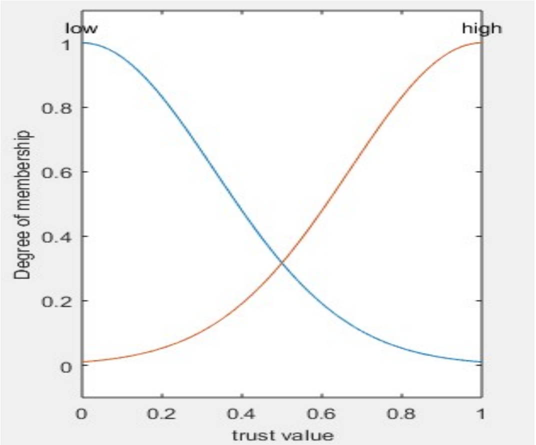

Figure 11: Fuzzy Membership Function For Output Variable As Trust Value

The figure 11 displays the value of fuzzy membership function portion for the trust value of node as the output. The y axis is the membership value lies between 0 to 1.The x axis is the trust value and it varying prom 0 to 1.The trust is an output variable is divided into two membership functions.

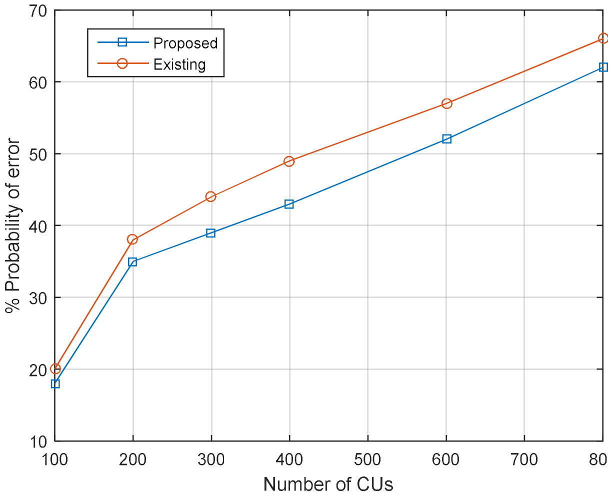

Figure 12: Percent Probability Of Errors With Respect To Different Numbers Of Cognitive Users

In the figure 12 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 cooperative network of specific area. The plots shows that as the number of CUs is improved 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.

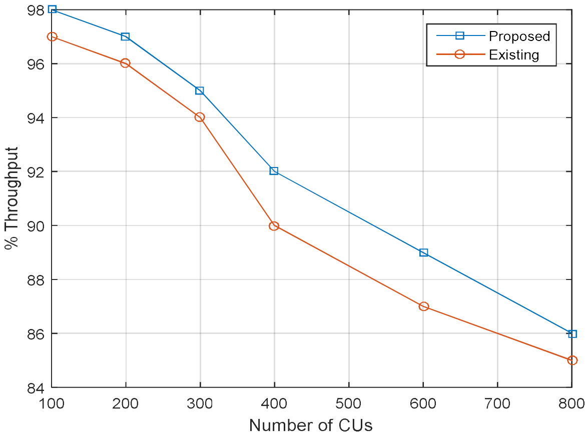

Figure 13: Percent Throughput With Respect To Different Numbers Of Cognitive Users

In the figure 13 shows the percent throughput of the cooperative network 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 cooperative networkof specific area. The graphs illustrate that the Percentage throughput drops as the number of CUs grows. 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 862%. It may be easily observed that the percentage throughput in transmission over the cooperative network is increased in the fuzzy based decision approach.

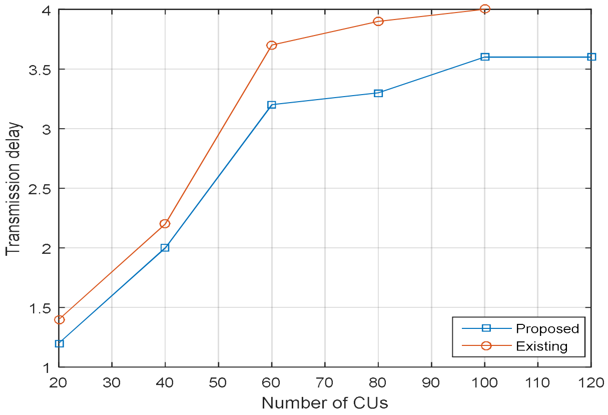

Figure 14: Transmission Delay With Respect To Different Numbers Of Cognitive Users

The figure 14 displays the transmission delay in seconds of the cooperative network 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 cooperative network of specific area. The plots shows that as the number of CUs is improved 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 cooperative network is decreased in the fuzzy based decision approach.

Table 2: Percent Throughput At Different Area In M²

Area in sqr m	Percent Probability of error	
	Existing	Proposed
500	97	98
1000	96.5	98.2
1500	96	98.1
2000	95	96.3
2500	91	94
3000	89	90

Table 3: Percent Throughput At Different Area In M²

Area in sqr m	Percent Probability of error	
	Existing	Proposed
500	1.4	1.2
1000	1.5	1.3
1500	1.8	1.7
2000	2.1	2
2500	2.4	2.3
3000	2.6	2.54

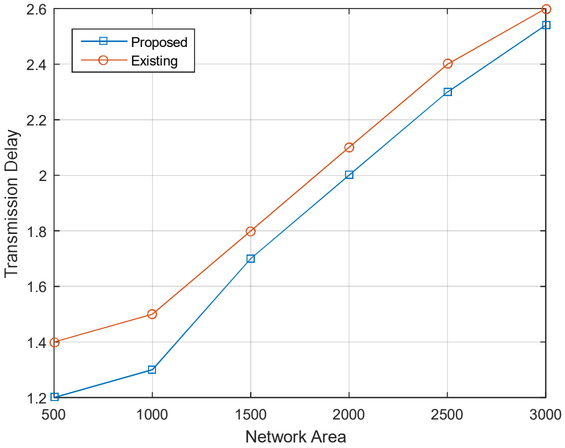

Figure 15: Transmission Delay With Respect To Different Network Area In M².

The performance in this article is shown in terms of results generated on calculating the throughput and transmission delay. The results of proposed work are compared with existing protocol. The on average percent throughput is 94% on using the fuzzy logic based detection of malicious user during handoff while the existing approaches gives highest on average throughput as 95.7%.The increment in the throughput is 1.7%.Since the existing methods already have high throughput hence significant boost in proposed scheme are not observed. However there are still option to reduce the probability of error by including advanced error detection methods on the sacrifice of transmission delay and computational complexity.

5. CONCLUSION:

The probability of error as well as throughput among various numbers of CUs is studied in the cooperative system to determine the scalability with the suggested method. The probability of error grows as the range of CUs improves, as seen in the data. While overall number of CUs increases, the throughput automatically falls. Furthermore, the aforementioned conclusion is backed by an examination of the message modification, in which the incoming CUs alter the information that was sent it throughout node's authentication method in an effort to boost the node's chances of transmission. Even with a huge number of CUs, the suggested fuzzy logic-based approach outperforms the thresholding approach. The performance gain is due to the concept that each node's/trust CU's value is generated to more correctly determine each node's actual behavior. The node's TV rises as it becomes increasingly involved inside each modification activity. In future different available modern machine learning methods may associate in learning to decide the label of user type during handoffs. ANFIS/SVM/ANN like methods may also used to check out the detection efficiency in terms of accuracy, complexity and delay. Biologically inspired algorithms are still a choice that may opt to discover. Presently genetic algorithm, particle swarm optimization, ant colony optimization are simple, robust and efficient search methods that may minimize the task of manual searching of parameters and rules used for developing the fuzzy inference system.

REFERENCES:

[1] Ian F. Akyildiz, “Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey,” I.F. Akyildiz et al. / Computer Networks 50 (2006) 2127–2159

[2] DipankarRaychaudhuri, “CogNet - An Architectural Foundation for Experimental Cognitive Radio Networks within the Future Internet,” MobiArch’06, December 1, 2006, San Francisco, CA, USA. Copyright 2006 ACM 1-59593-566-5/06/0012

[3] Manuj Sharma, “Channel Selection under Interference Temperature Model in Multi-hop Cognitive Mesh Networks,” Advanced Numerical Research and Analysis Group, DRDO, Hyderabad, India, 2007 [4] Guo-Mei Zhu, “STOD-RP: A Spectrum-Tree Based On-Demand Routing Protocol for Multi-Hop Cognitive Radio Networks,” * 3National Chengchi University, Taipei, Taiwan Email: {guomei, ian}@ece.gatech.edu, gskuo@ieee.org This work was conducted during her stay at BWN Lab in 2007-2008.

[5] Muhammad Zeeshan , “Backup Channel and Cooperative Channel Switching On-Demand Routing Protocol for Multi-Hop Cognitive Radio Ad Hoc Networks (BCCCS),” 2010 6th International Conference on Emerging Technologies (ICET)

[6] Lei Ding, “Distributed Routing, Relay Selection, and Spectrum Allocation in Cognitive and Cooperative Ad Hoc Networks,” This material is based upon work supported by the US Air Force Research Laboratory under Award No. 45790. Approved for Public Release; Distribution Unlimited: 88ABW-2010-0959 dtd 9 Mar 10.

[7] Jang-Ping Sheu, “Cooperative Routing Protocol in Cognitive Radio Ad- Hoc Networks,” 2012 IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks

[8] DongyueXue, “Cross-Layer Scheduling for Cooperative Multi-Hop Cognitive Radio Networks,” arXiv:1106.0735v1 [cs.NI] 3 Jun 2011

[9] Lei Ding, “Distributed resource allocation in cognitive and cooperative ad hoc networks through joint routing, relay selection and spectrum allocation,” L. Ding et al. / Computer Networks xxx (2015) xxx–xxx

[10] Jianhui Huang, “Big Data Routing in D2D Communications with Cognitive Radio Capability,” IEEE Wireless Communications • August 2016 1536-1284/16/$25.00 © 2016 IEEE

[11] Jiang Zhu , “A game-theoretic power control mechanism based on hidden Markov model in cognitive wireless sensor network with imperfect information,” J. Zhuetal./Neurocomputing220(2017)76–83

[12] ArsanyGuirguis, “Cooperation-based Multi-hop Routing Protocol for Cognitive Radio Networks,” Preprint submitted to Elsevier March 10, 2018

[13] Yihang Du, “A Cross-Layer Routing Protocol Based on Quasi-Cooperative Multi-Agent Learning for Multi-Hop Cognitive Radio Networks,” Sensors 2019, 19, 151; doi:10.3390/s19010151 www.mdpi.com/journal/sensors

[14] Dingde Jiang, “Collaborative Multi-hop Routing in Cognitive Wireless Networks,”

Wireless PersCommun (2016) 86:901–923 DOI 10.1007/s11277-015-2961-6

[15] 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

[16] J. I. Mitola, “Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio Dissertation,” Dissertation Royal Institute of Technology Sweden, vol. 294, no. 3, pp. 66–73, 2000.

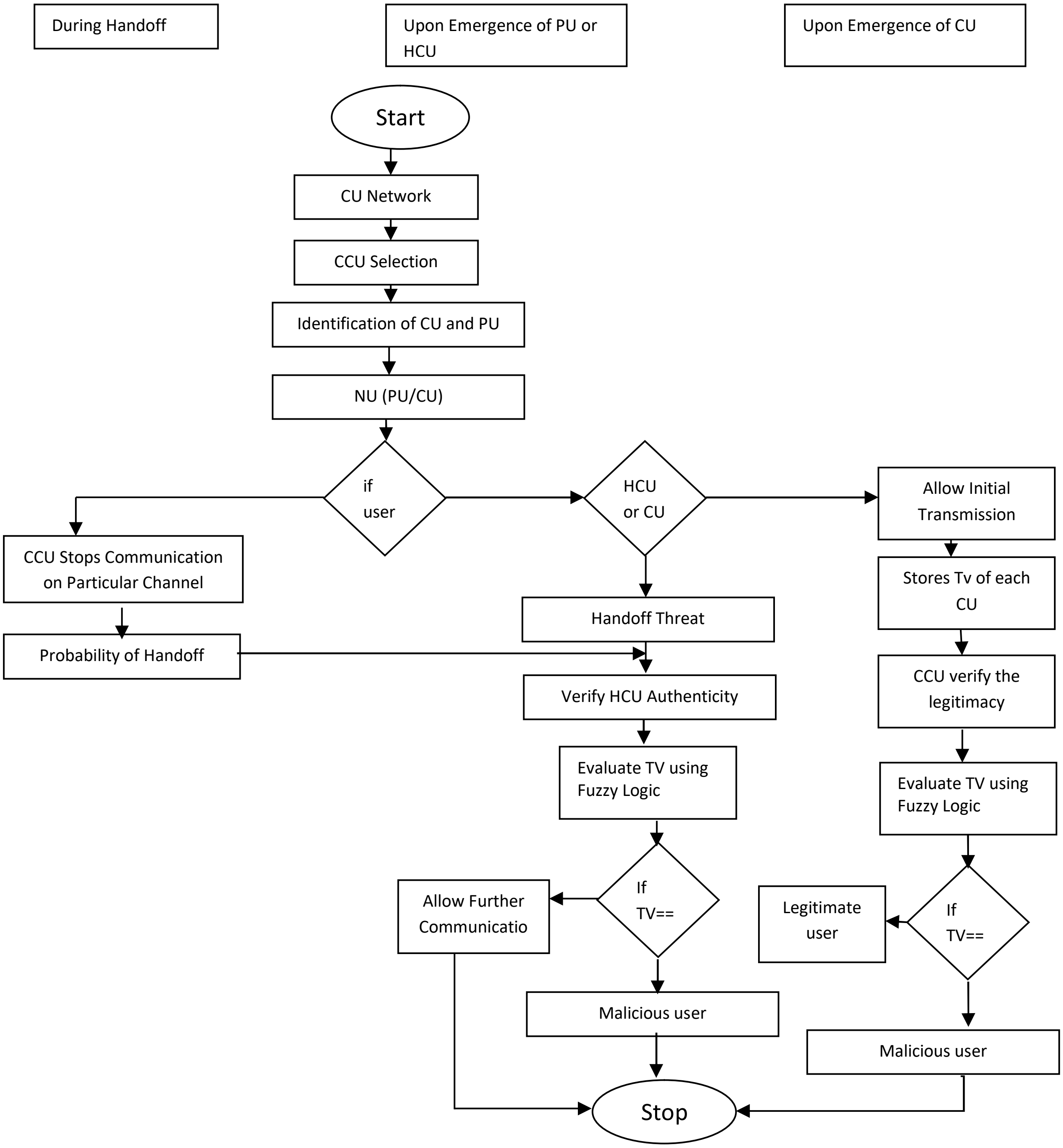
During Handoff
Upon Emergence of PU or HCU
Upon Emergence of CU
Start
CU Network
CCU Selection
Identification of CU and PU
NU (PU/CU)
if user
HCU or CU
Allow Initial Transmission
CCU Stops Communication on Particular Channel
Stores Tv of each CU
Handoff Threat
Probability of Handoff
CCU verify the legitimacy
Verify HCU Authenticity
Evaluate TV using Fuzzy Logic
Evaluate TV using Fuzzy Logic
Allow Further Communicatio
If TV==
Legitimate user
If TV==
Malicious user
Malicious user
Stop

Fig. 2: Flowchart Of The Suggested Cognitive Radio Network Cell Spectrum Handoff