Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, June 2021: 2334-2346

Research Article

An Analysis and Efficient Approach to Protect CR Networks

Dr. V. Rajmohan[1], Dr. T.Kavitha[2], Mr.V.Beslin Geo[3], Dr. V. R.Prakash[4]

Abstract

While launching wireless services the primary problem being encountered is Spectrum Scarcity problem. To rectify this problem Cognitive Radio (CR) network is used as a emerging and promising technology. To setup secured connection between the users of the network, CR network dynamically allocates free spectrum. The spectrum sensing performance is influenced by a threat which is known as Primary user emulation attack (PUEA). It reduces the spectrum access probability in the network. In out work, an approach is proposed to prevent this attack using Area Correlation based Localization Technique (ACLT). Malicious PUEA is effectively identified in this proposed method. The proposed approach provides a complete resist to the PUEA in the network and thereby averts the user from establishing any further communication. The proposed approach provides a considerable improvement in the overall network performance and spectrum utilization in a CR radio network.

Keywords: Cognitive radio network (CRN), Primary user emulation attack (PUEA), Area Correlation based Localization Technique (ACLT), Primary User (PU), Secondary User (SU).

I. INTRODUCTION

Cognitive Radio is an efficient approach to aid effective spectrum utilization. Cooperative networks which has inadequate radio resources is effectively modeled by Dynamic spectrum allocation. In a specified spectrum band, the primary users transmission probabilities is detected by spectrum sensing.

[1]Associate professor,Department of Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai. rajmohan.vijayan@gmail.com
[2]Professor, Department of Electronics and Communication Engineering Veltech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Tamilnadu, Chennai. drkavitha@veltech.edu.in
[3]Assistant professor, Department of Electronics and Communication Engineering, Hindustan Institute of Technology and Science,OMR,Padur, Chennai. vbeslin@hindustanuniv.ac.in
[4]Assistant professor, Department of Electronics and Communication Engineering, Hindustan Institute of Technology and Science,OMR,Padur, Chennai. vrprakash@hindustanuniv.ac.in

It is mandatory for the secondary users to identify the free spectrum holes. The secondary users have major threat in the form of Primary user emulation attack (PUEA). The secondary users inhibit their transmission possibilities by imitating the characteristics of the Primary Users. Spectrum utilization protocol states that the secondary users must immediately evacuate the spectrum bands once they detect the presence of primary transmissions. Since monitoring and

regulating the spectrum allocation is not efficient, it leads to many improper functions in the network. Denials of service (DoS) attacks, redundant discrepancies to the secondary users, discreetly hampering the possibilities of data transmissions attempts made by the secondary users in the network are some of the improper functions. PUEA exploits this criterion and emulates Primary User (PU) characteristics which are wrongly interpreted by the Good Secondary Users (SU) as the presence of actual primary users in the network. This leads to the swift evacuation of the spectrum bands by these Good secondary users. Then the malicious users occupy the complete white space for themselves. Such unethical DoS attack launched by the malicious secondary users on the good secondary users is termed as the Primary User Emulation Attack (PUEA) [1].

Various detection and preventive measures for PUEA have been proposed in [2], [3]. The authors have proved the efficiency in reducing the probability of PUEA in a network. The existing theories articulate widely about the Distance ratio test and Distance difference test which few decisive factor among the measures adapted to detect a PUEA. The authors have concluded that the success quotient of the Primary User Emulation Attack is maximum in the existing scenarios which were actually said to have been predicted to minimize the probability of a PUEA in both dynamic and Ad-hoc Cognitive radio networks [4].

The authors in [5] observed that realizing the Angle of Arrival (AoA) technique in differentiating a malicious attacker node from the authenticated primary user. The angle of transmitted signal is estimated by employing “Multiple Signal Classification” based AoA algorithm which correlates the antenna elements received data with that of the actual PU location (Angle) and discerns the attacker from the Primary user. The authors concluded that this technique was not very effective in accurately nailing down the attacker. Also the approach consumes more time and resource in the process.

In this work, an advanced “Localization Technique” is proposed and applied. This approach skillfully detects the PUEA attack by applying Area Correlation based Localization Technique (ACLT). This approach is evaluated with respect to the Time of Arrival (ToA) of a Signal from the SoI (System of Interest) and the Time Difference of Arrival (TDoA) of the signal. Apart from TDOA & TOA estimation, the signal strength is taken as the key parameter to assess the location of the transmitter. An accurate location of the transmitter decision is detected based on these parameters. Then the observed location of the transmitter is compared with the location of Actual primary user transmission recorded by the base station. Based on the results, decision is made whether the observed user is either an attacker or an authenticated Primary user. Finally if the PUEA was confirmed then the node responsible for PUEA is eliminated from the network to prevent it from establishing any further communication in the network.

The simulation results illustrate that the PUEA has been significantly detected and the users in the network have exceptionally exploited the spectrum utilization protocol.

The rest of the manuscript is organized as: Section II concentrates about various PUEA estimating techniques. Section III elaborates various Angle of Arrival estimating techniques available in the literature. Section IV, depicts the detection and prevention techniques of PUEA. Simulation results were discussed and depicted in section V. Section VI provides the conclusion of our work.

II. PUEA ESTIMATING TECHNIQUES

Every Primary User will be allocated by authorized frequency bands in the dynamic spectrum access environment. The Secondary Users utilize the spectrum bands only when the Primary User is void of using them. The signal of the authenticated primary user is diminished by the attacker. Then the attacker occupies the unused channels deliberately. This act will prevent other secondary users from accessing the vacant frequency bands thereby wasting the spectrum bands. This kind of attacks on CR networks give rise to a serious menace to the deployment in spectrum.

Based on the nature of the attack, there are two PUEA are observed so far. They are as:

1. Malicious Primary User Attack: This is also called as Denial of Service (DoS) attack. The attacker won't occupy the fallow bands. It prevents the other users to utilize the free bands.
2. Selfish Primary User Attack: The attacker occupies the complete free space for its own use. It aims at improving its chances of occupying the spectrum rather than sharing the free bands with the other good secondary users of the network.

CR network under PUEA is illustrated in the Fig.1. This shows the primary and secondary users' transmission in different frequencies. When an Emulation attack happens in the network, the secondary users are almost blind to the attack and tend to continuously loose the opportunities to access the free spectrum for a specific amount of time. The secondary users are not able to authenticate the primary users. Locating and authenticating to differentiate the primary users will be a major breakthrough. It can separate the Emulation attackers and PUEA probability can be reduced in a CR network. Various techniques were proposed in the literature to deploy in CR network to detect primary user emulation attack.

The authors in [6], used localization schemes alone to estimate and authenticate the location of Primary Users. But it is observed to be an inefficient approach since the model can be defeated by attacker by using Antenna arrays with different power levels. "RSSI based primary user localization" is one kind of procedure where the Decision on validating the primary user is made based on the signal strength received from all the receivers and finally by consolidating all the received sensing reports obtained at the Fusion centre. In case of an ideal primary user transmission, all RSSI values will be accurate with respect to the distance from each other.

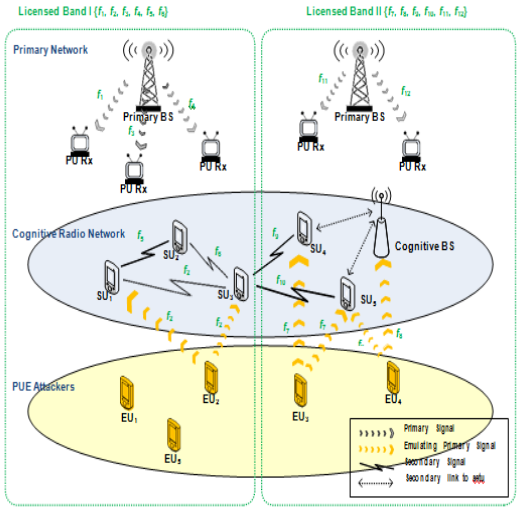

Fig. 1 .PUEA & Its impact on CR Networks

Nevertheless a detailed study concludes that this method is less reliable if used as the sole technique for nailing down an attack. The parameter comparison alone cannot provide an accurate result if the attacker is transmitting from a region nearer to the primary base station. RSS value might be of the same or nearer to a particular threshold which might lead to a vague result. Wireless link signatures can be enabled to detect primary user. Essential to this approach is a helper node, placed physically close to a primary user. This technique is very effective in terms of authenticating primary users which exploits the proximity of Helper node with a primary user [3]. But the major drawback in this technique is the predicament in authenticating wireless link signature of the helper node. If attackers are placed near helper nodes, then the detection of the primary user becomes feeble leading to external disturbances in the signal transmission.

The existing techniques fail to provide an exact estimate on the location of a PUEA and tender an in accurate approximation on the presence of the attacker in the network. Our proposed work therefore is a collaboration of both Localization and RSS technique which yields an accurate outcome and tends to protect the network from further emulation attacks launched by the same detected attacker thereby completely eliminating it from the network.

III. EXISTING TECHNIQUE TO DETECT PUEA

The technique widely used to detect PUEA is Angle of Arrival (AoA). When a signal is received from the transmitter, its AoA is estimated. Based on the estimation the secondary user can distinguish between malicious attacker and primary user [5]. All the secondary users are provided with Smart antenna which can estimate the arriving angles of all the received signals. The angle information of all the target primary users is shared with every secondary user. Upon estimating the AoA, the estimated information will be compared with the available data to identify whether the received signal is from the intended primary user or from the malicious attacker launching a hazardous attack in the network. This approach encounters some practical difficulties. The first one is, the probability of the missed detection is high in this approach. This

makes the approach time consuming and it become a cost expensive one. The next one is, when the malicious node is placed in close proximity of the primary user the secondary user will have erroneous interpretation. Therefore it leads to inaccuracy and the approach becomes inefficient.

A 3-element antenna array is shown in Fig.2. The three elements, secondary users, are displaced by the distance'd'. It is presumed that there is 'D' source signals will be received by each second user. It can be observed from the figure that at one point the angle of arrival at these three secondary users may be misinterpreted that the signal received is from the same source. Hence, in this AoA approach, to avoid misinterpretation the difference between angles of each signal sources should be greater than 1^o. And also the there should be minimum 6 antenna elements. To have better detection resolution more antenna elements should be used. Therefore to classify among multiple signal sources, the AoA of each and every signal source should be maintained with sufficiently large angles and the detectable angle difference should be atleast 1^o.

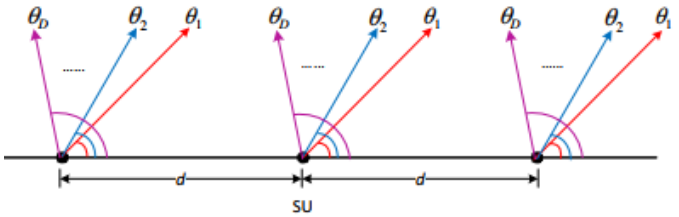

Fig.2 Geometry of a 3-element antenna array

From the above discussions it may be concluded that in AoA approach the accuracy in detecting the primary user might be lower due to receiver phase mismatch errors, multipath propagation of signals. Also to achieve better accuracy six-antenna strategy should be followed. This makes the AoA approach less cost effective one.

IV. PROPOSED TECHNIQUE TO DETECT AND PREVENT PUEA

In the CR network free spectrum is available. This free spectrum is not effectively utilized by the secondary users in the existing AoA approach. This is because in the CR network occurrence of PUEA is a predominant factor. Hence important thing to be considered in CR network is defense against PUEA. Area Correlation based Localization Technique (ACLT) is a better method to be applied in CR network. The probability of primary user emulation attack can be nullified in CR network with greater efficiency. In this approach the transmitter is localized so that the primary user emulation attack is eliminated. This is because the ACLT approach provides better iterative comparisons and better parameter estimations. ACLT can be categorized into 3 sub modules of implementation as follows:

A. Time of Arrival Estimation & Time Difference of Arrival calculation

The area over which the transmitter is lying can be effectively estimated by the "Time of Arrival" (TOA) of a transmitted. This is a crucial parameter. The spectrum sensing is performed round the clock using a pair of secondary users. The Authentic Node (AN) and Decision node (DN) make the pair of secondary nodes. The Authentic nodes are the set of authentic secondary users which performs spectrum sensing and report the spectrum occupancy status to the Decision node. The Decision node is the one which is responsible for taking decisions regarding the presence of primary transmission in the network with respect to the data obtained from the

Authentic Nodes [7]. The constant difference between time of arrival between the signals from the two authentic nodes estimates the area over which the transmitter is lying. The intersections of more than one such estimation projects two dimensional position area of the transmitter position. The TDOA measurement can be obtained as follows,

$$\Delta T_{(i,1)} = \frac{\sqrt{(ai-a)^2-(bi-b)^2} - \sqrt{(a1-a)^2-(b1-b)^2}}{C}$$

$\Delta T_{(i,1)}$ is the measured value of the Time Difference of Arrival which is deduced from the position of the transmitter (a,b), position of the authentic nodes (a_i,b_i) & position of the decision node (a_1, b_1). The values obtained are for 2 different times of arrival signals and for a pair of dedicated secondary authenticated nodes. For better accuracy 3 to 4 four such estimations can be obtained. The time delay is the critical factor since it may results in more energy consumption during both the transmitter localization process and spectrum sensing progression.

The coefficient of length between the transmitter and the authentic node can be expressed as, $L_i = \sqrt{(ai-a)^2-(bi-b)^2}$

Similarly, the coefficient of length between the transmitter and the Decision nodes can be expressed as, $L_1 = \sqrt{(a1-a)^2-(b1-b)^2}$

The measured TDOA value when multiplied with the speed of the signal gives the difference of the distances between the authentic nodes and the transmitter and the decision node and the transmitter. $L_{(i,1)} = C\{\Delta T_{(i,1)}\}$

The expression for the "Distance between the transmitter and the authentic node" is given by (L_i). Similarly the Distance between the transmitter and the Decision node is given by (L_1).

$$L_{(i,1)} = L_i - L_1$$

These coordinates is used to assess the area over which the transmitter is lying.

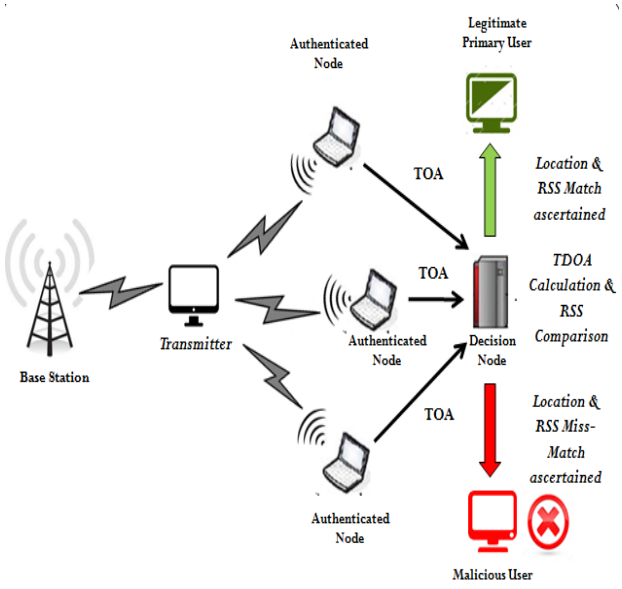

Fig.3 System Model of PUEA Detection Using Area Correlation based Localization Technique (ACLT)

The final conclusion over the calculated coordinates gives the exact estimation of the transmitter location and the area over which the transmitter is actually lying.

B. Receiver Signal Strength (RSS) estimation

With the assumption that the primary user is static all the estimations were obtained. Otherwise while estimating the transmitter positions the area correlation will be trivial. In this case RSS estimation should be considered as the factor to determine the transmitter position. The RSS is the secondary comparison factor in estimating the primary signal taking in to consideration the previously stored primary input telecast from the base station.

C. Transmitter Localization

The process of localizing the PUEA is illustrated in the flow chart depicted in Fig.3.

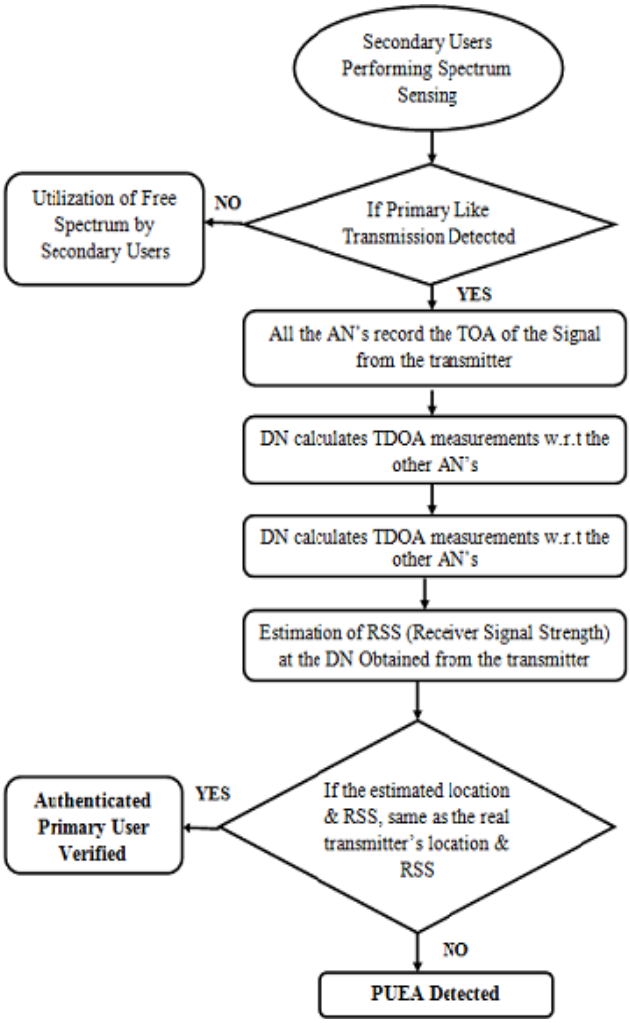

Fig.4 Flow chart of PUEA Detection Using Area Correlation based Localization Technique (ACLT)

The spectrum sensing is performed by the authentic node. If the empty spectrum indicates that the secondary users are on the process of sharing the spectrum among them and are utilizing the fallow bands. If a primary like transmission is detected the status is conveyed to the decision node of the network. Time of arrival of the transmitter signal by two or more authentic node is recorded. The decision node and the authentic node collaborate to calculate the Time Difference of Arrival. The Time Difference of Arrival is the actual estimation of the transmitter location. The RSS is calculated at the Decision Node for further confirmation of the transmitter's position.

The estimated transmitter position and RSS is compared with the known Primary user transmitter location & RSS. If the parameters match then the observed node is the primary node. If there is a mismatch, then the transmitter is concluded to be a primary user emulation attacker. Then the node responsible for causing the attack is eliminated from the network altogether making it impossible for the attacking node to launch any future attacks in the network. This systematic implementation procedure is represented as a flow chart in Fig.4. Since both RSS & transmitter position are verified, the accuracy in estimating the PUEA is considered higher.

V. RESULTS AND DISCUSSIONS

Various analyses have been done on Average time delay, Packet drop ratio, energy consumption rate, computation time, localization error against nodes. All these analysis is done with 30 nodes. Apart from this data rate measurement and delay measurement was also done. All the 30 nodes are considered as a set of secondary nodes or users. Among these 30 nodes two of them are assigned to be the authentic nodes.

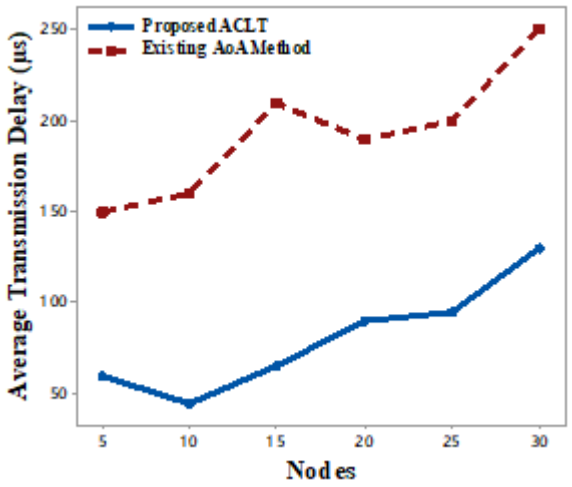

Fig.5 Transmission delay comparison between Existing and Proposed methodology

Fig. 5 compares the average transmission delay between the existing AoA approach and proposed ACLT approach. It is observed that the average transmission delay increases as the no. of nodes increased. However the existing AoA method has the maximum average delay of 255µs. Whereas the proposed ACLT approach has the average delay of 130µs. The minimum average delay for the existing AoA method is 150µs (for 5 nodes) is higher than the maximum average transmission delay of the proposed method (30 nodes). The average transmission delay is almost constant between 20 nodes and 25 nodes. It can be concluded that the proposed ACLT approach provides lesser average transmission delay compared to the existing AoA approach.

Fig. 6 shows Packet drop ratio comparison between the existing AoA method and proposed ACLT method. The spectrum sensing time is found to be very high for the existing system which is observed to be exceptionally minimized in case of the proposed ACL Technique. Localization error is therefore minimized to several degrees owing to the proposed techniques efficiency**.** The definite reason is due to the proposed algorithm implemented for localizing the transmitter with respect to minimum duration, due to which the packet drop ratio is considerably minimized with the present technique. The packet drop ratio is very les in the proposed approach. In the proposed approach, there is a slight increase in the packet drop ratio from nodes 5 to 15. Between nodes 15 to 20 the packet drop ratio is almost constant. Whereas for the existing AoA approach the packet drop ratio is constantly increasing almost in linear manner if the number of nodes is increased.

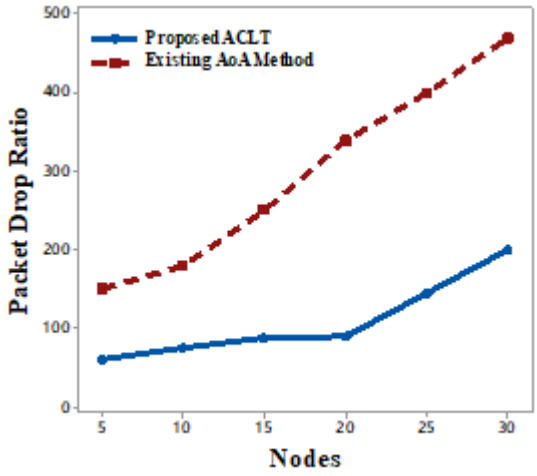

Fig.6 Packet Drop ratio comparison between Existing and Proposed methodology

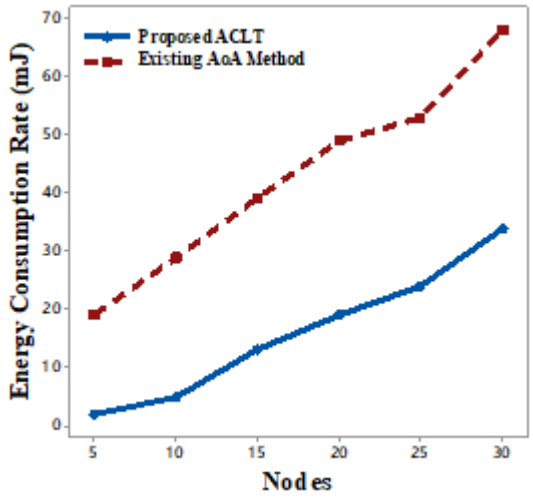

Fig.7 Energy Consumption Rate comparison between Existing and proposed methodology

Fig. 7 shows the comparison Energy Consumption rate between the existing AoA approach and the proposed ACLT approach. The energy consumption rate almost increases in linear manner for the increase of no. of nodes for both approaches. Energy efficiency is the most

important factor to be taken into account since the complete cognitive radio performance relies on this parameter. Spectrum sensing time increases the energy consumption exponentially. Proposed technique on the other hand is observed to have very minimum energy consumption due to the quick sensing performance. The simulated graph can be observed to have considerable variation in the energy consumption rate as shown in Fig.7.

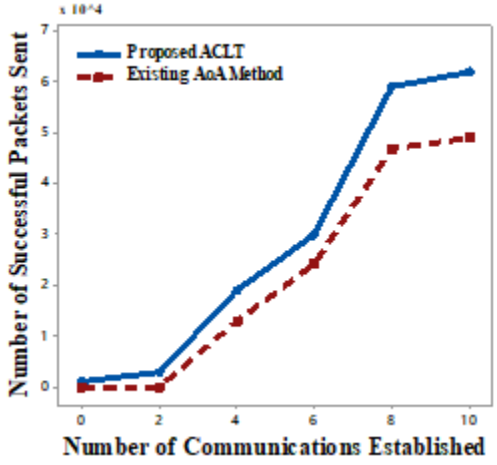

Fig.8 Throughput comparison between Existing and Proposed methodology

Throughput is another important parameter. Fig.8 illustrates the comparison of data transmission rate and the possible communication efficiency in both the existing AoA approach and proposed ACLT approach. The throughput in the proposed ACLT method is slightly higher than the existing AoA method. The throughput of the existing AoA approach is slightly reduced than the proposed method. This is due to the prolonged spectrum sensing time of the proposed ACLT approach

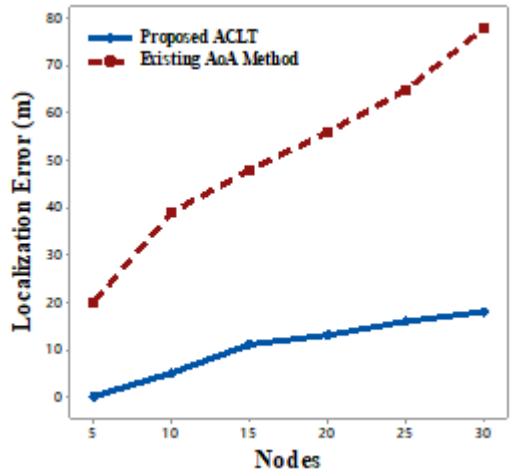

Fig.9 Localization Error estimation between Existing and Proposed methodology

Fig.9 compares the localization error encountered by the existing AoA approach and the proposed ACLT approach. The localization error is increasing in linear manner against the no. of nodes. This is due to the influence of receiver phase mismatch error and multipath propagation

effects which diminishes the chances of locating the transmitter with exact conviction. The proposed technique however is highly effective in localizing the transmitter over an area with greater accuracy, owing to the competent computation and iterative comparison techniques deployed.

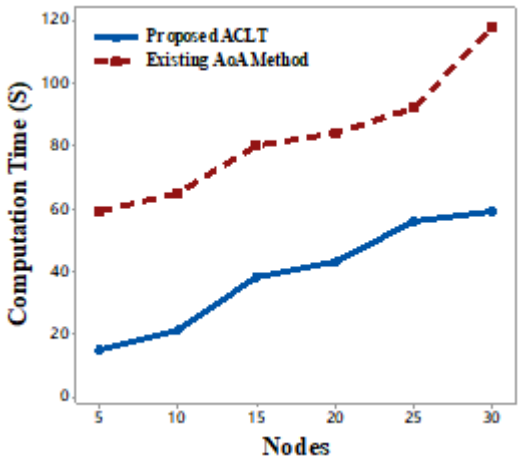

Fig.10 Computation Time between Existing and Proposed methodology

Fig. 10 compares the computation time between the existing AoA approach and the proposed ACLT approach. Detection of the Emulation attacker within nominal time duration is highly crucial. Because this parameter is vital in determining the performance efficiency of any algorithm implemented. The computation time is approximated to be high in case of the existing system, as the decision is to be made for ascertaining the transmitter's location based on the "Angle of Arrival" at all the antennas deployed in the network. Therefore a final conclusion is possible only after performing comparative analysis between the collective information procured at every smart antenna that has been positioned around the secondary users, which can be a tedious and time consuming task. The proposed technique is however much quicker compared to the existing method, which uses the "Time difference of arrival" between the obtained signals & the RSS guesstimate in nailing down the exact location of the transmitter with at most precision in nominal time duration. The performance metrics comparative analysis between the existing and proposed techniques, have made apparent the fact that the "Area Correlate based Localization Technique" is a competent procedure for both thwarting the multiple attacks and also in minimizing the probability of reoccurrences of PUEA in a cognitive radio network.

Fig. 11 shows the data rate comparison between the existing AoA approach and the proposed ACLT approach. The proposed technique is observed to have improved data rate since decision making capability of the proposed technique is proved to be quicker and much efficient. The result thus tends to analyze maximum trade off in terms of performance and is highly proactive in deducing the transmission bandwidth or spectrum availability.

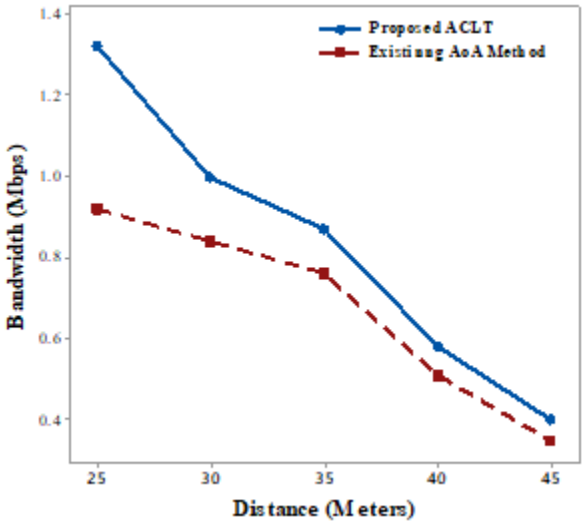

Fig.11 Data Rate Measurement

VI. CONCLUSION

It is observed from the above analysis that there are no. of proven methods available to detect the primary user emulation attack. But none of the method is so efficient to avoid the repeated PUEA occurrence in cognitive radio network. Also it is observed that tackling multiple attack is difficult in a dynamic cognitive radio environment. Hence an efficient spectrum utilization of the available spectrum hole is not viable, leading to spectrum wastage and reduction in both throughput and efficiency. Proposed system is deliberately avoiding the primary user emulation attack in the Cognitive Radio network by incorporating the ACL Technique. It is observed from the analysis that it minimizes the transmitter identification time and also thwarts multiple attacks and reoccurrence of such emulations by removing the attacking node from the network with much less complexity.

REFERENCES

[1] G. Jakimoski and K. P. Subbala,likshmi. Denial-of-service attacks on dynamic spectrum access networks, IEEE Cog.Nets Workshop, IEEE International Conference on Communications 2008, May. 2008.

[2] Yongcheng Li, Manxi Wang, Changdong Han, Lei Xie. A Primary User Emulation Attack Detection Scheme in Cognitive Radio Network with Mobile Secondary User, 2nd IEEE International Conference on Computer and Communications,- 2016.

[3] R. Chen, J. Park, and J. H. Reed. Defense against primary user emulation attacks in Cognitive Radio networks, IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 25-37-2008.

[4] Das, D., & Das, S. Adaptive resource allocation scheme for cognitive radio vehicular ad-hoc network in the presence of primary user emulation attack. IET Networks, 6(1), 5–13, 2017.

[5] Yanxiao Zhao , Jun Huang, Wei Wang and Rafida Zaman. Detection of Primary User's Signal in Cognitive Radio Networks: Angle of Arrival Based Approach, 978-1-4799-3512-3/14/-2014 IEEE.

[6] S. Lin, C. Wen and W. A. Sethares, "Two-Tier Device-Based Authentication Protocol Against PUEA Attacks for IoT Applications," in IEEE Transactions on Signal and Information Processing over Networks, vol. 4, no. 1, pp. 33-47, March 2018, doi: 10.1109/TSIPN.2017.2723761.

[7] V. Jayasree, R. Suganya. A Survey on Primary User Emulation Detection Mechanisms in Cognitive Radio Networks, International Journal of Computer Trends and Technology (IJCTT) – volume 14 number 2 – Aug 2014