



Investigations on detection and prevention of primary user emulation attack in cognitive radio networks using extreme machine learning algorithm

N. Sureka¹ · K. Gunaseelan¹

Received: 14 December 2020 / Accepted: 2 March 2021

© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2021

Abstract

Cognitive radio is a competent technology which resolves the spectrum scarcity crisis in a network by allocating free spectrum dynamically and establishes coexistence between the users of the network, without interfering with the incumbent transmission. Primary user emulation attack (PUEA) is one of the major threats to the spectrum sensing performance that decreases the spectrum access probability of the unlicensed users of the network. In this paper Detection and prevention of PUEA is realized proficiently using Time-Distance with signal Strength Evaluation (TDSE) and Extreme Machine Learning (EML) algorithm. TDSE implementation makes it feasible to identify the malicious PUE attacker under mobile user stipulation and EML algorithm provides a swift comparative decision regarding the malicious attack. The technique is also proven to improve the sensing ability, energy efficiency and brings down the overall delay of the system, illustrating a considerable improvement in the overall network performance and spectrum utilization in a cognitive radio network.

Keywords Cognitive radio network (CRN) · Primary user emulation attack (PUEA) · Receiver signal strength (RSS) · Time–distance and signal strength evaluation (TDSE) and extreme machine learning (EML) algorithm

1 Introduction

Dynamic spectrum allocation is crucial in modeling cooperative network which intellectually exploits the inadequate radio resources. Cognitive radio is one such intelligent device that assists in effective spectrum utilization and exterminates spectrum wastage in a wireless communication network. The accurate estimation of the PU's transmission probability is mandatory for the Secondary User's (SU's) to identify the free spectrum holes. Spectrum utilization protocol states that the SU's must immediately evacuate the spectrum bands once they detect the presence of a primary transmission. Primary User Emulation Attack (PUEA) poses major threat to the secondary users and hinders their transmission rate by emulating the characteristics of PU's

(Fragkiadakis et al. 2013). Primary user emulation attackers are a set of secondary users which are also termed as Malicious User's (MU's), that imitates the PU's characteristics, which is erroneously interpreted by the Good SU's as the presence of actual PU's in the network, leading to an instant evacuation of the spectrum bands unnecessarily by the Good SU's. The MU's thus occupy the complete white space for themselves, creating redundant discrepancies to the SU's and discreetly hampering the data transmissions attempts made by these good SU's in the network. Such unethical Denial of service (DoS) attacks launched by the MU's on the good SU's, is termed as the PUEA (Jakimoski and Subbalakshmi 2008). This unethical spectrum exploitation by the MU's has raised concern on the network defense and unwanted spectrum wastage in a dynamic cognitive radio networks.

With many PUEA detection and prevention measures devised so far (Singh and Sharma 2014), there are few proven techniques to eternally thwart the PUEA effect from the network. The existing theories articulate extensively about the techniques like the 'Distance Ratio Test' and 'Distance Difference Test' encapsulating very less vital factor adapted to detect and eliminate PUEA effect altogether from the network. Our study so far has lead to a

✉ N. Sureka
sureka.ns05@gmail.com

K. Gunaseelan
guna_2012@yahoo.co.in

¹ College of Engineering Guindy, Anna University, Chennai, India

conclusion that the real time feasible model for eradicating the PUEA has not yet been devised successfully and the probability of repeated attacks are found to be maximum in the existing scenarios which actually claim to minimize the probability of a PUEA in both dynamic and Ad-hoc Cognitive radio networks (Das and Das 2017).

We present an advanced “Detection technique” to proficiently detect the PUEA by applying Time distance and receiver signal strength evaluation (TDSE) based Localization Technique with respect to the Extreme Machine Learning (EML) algorithm. The reference for the existing TDOA work was obtained from the work proposed by the authors (Chen et al. 2008). The important factor that is to be considered here is that, apart from Time distance estimation the signal strength of the receiver is also taken as the key parameter to assess the location of the transmitter. A collaborative decision based on all these three parameters tend to provide an accurate decision on the location of the transmitter which is compared with the location of Actual primary user transmission recorded by the base station and concluded as either an attacker or an authenticated Primary user even under mobile secondary user (Li et al. 2016). 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 exemplify accurate detection of the PUEA and the exceptional exploitation of the spectrum utilization etiquette by the proposed technique.

1.1 Contributions

- a. Time distance and receiver signal Strength evaluation (TDSE).
- b. Implementation of extreme learning in collaborative conclusion of PUEA in mobile SU's.
- c. Eliminating the emulating transmitter from the network in order to eradicate the probability of future attacks from the same malicious secondary user.

The rest of the manuscript is systematized as follows. In Sect. 2 the various aspects of PUEA has been elaborate, touching upon the relevant assumptions that have been performed in our analysis. Section 3 elaborates on the algorithms of existing technique. Section 4 makes evident of the proposed detection procedures adapted to perceive and thwart a potential PUEA, with the tabulated analysis and the necessary Numerical evidences. Illustration of simulation results using NS2 is depicted in Sect. 5. Section 6 gives a brief insight on the conclusion drawn from the investigations performed so far.

2 Primary user emulation attack estimating techniques

In a Cognitive radio system, the electromagnetic environment is sensed to adapt the functionalities and dynamically vary its radio operating parameters with the varying atmosphere (Dasari and Venkatram 2021). Though the dynamic spectrum allocation is a perceptive standard to minimize spectrum wastage, it also paves way for numerous security threats, one among which is the PUEA (Jin et al. 2012). The Primary Users (PU'S) are the authenticated users of the frequency bands, and the Secondary Users (SUs) are allocated with the free bands provided the PU remains idle. Therefore it is highly crucial that the spectrum sensing performed by the SU's is extremely accurate. The PUEA mitigates the PU signal characteristics, deliberately confusing the SU's and preventing them from accessing the vacant frequency bands. There is a high probability that the SU's either evacuate the spectrum band which they are currently deployed with or simply they might wait for ages to get allocated with the free spectrum band.

There are two variants of PUEA studied so far, based upon the motive behind the attack launched,

1. *Malicious primary user attack* The primary motive behind the attack is to thwart the possibility of a good secondary user from utilizing the fallow bands rather than the attacker occupying the fallow bands for its own benefit. They do not try to occupy the bands but deploy attack mechanism to prevent the usage of free bands from being utilized by other users of the network. This attack is also termed as the Denial of Service (DoS) attack (Kshirsagar and Kumar 2021).
2. *Selfish primary user attack* The attacker tends to utilize the complete free space for its own use, aiming at improving its chances of occupying the spectrum rather than sharing the free bands with the other good secondary users of the network.

Cognitive radio under PUEA is illustrated in the Fig. 1. The figure shows the PU's and SU's transmission at various frequency rages. When the network comes under Emulation attack by the Emulation user of the network (EU) the secondary users are almost blind to the attack and tend to continuously loose an opportunity to access the free spectrum for a considerable amount of time.

One of the reasons deduced to eradicate PUEA is that the secondary user's inability to authenticate the primary users. This way of locating primary users will be a major breakthrough in differentiating & separating the Emulation attackers and avoid PUEA probability in a CR

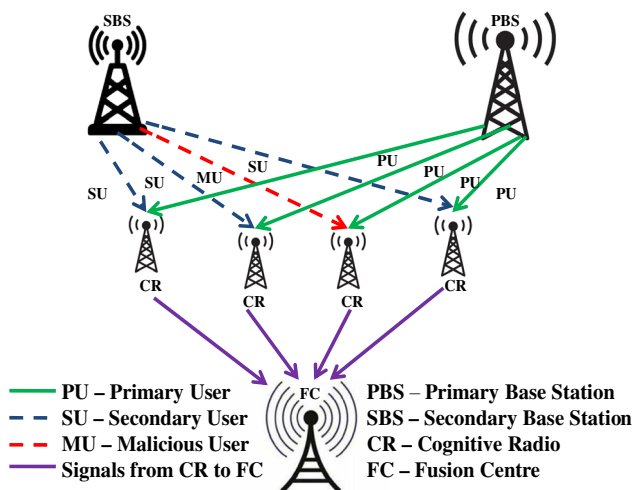


Fig.1 PUEA and its impact on CR networks

network (Jayasree and Suganya 2014). The identification and elimination of PUEA is highly crucial for real time applications that can be deployed through CR networks (Lin et al. 2018).

In this paper the authors (Salam et al. 2016), suggested the usage of localization schemes alone to estimate and authenticate the location of PU. But it is proved to be inefficient since the model can be defeated by attacker by using Antenna arrays with different power levels. “RSSI based PU localization” is one kind of procedure where the decision on validating the PU 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 PU transmission, all RSSI values will be accurate with respect to the distance from each other. But a detailed study states that this method is less reliable if used as the sole technique for nailing down an attack since the so called parameter comparison alone cannot provide an accurate result if the attacker is transmitting from a region nearer to the primary base station.

Wireless link signatures and channel characteristics prediction (Liu and Zhang 2016) can be enabled to detect primary user. This technique is very effective in terms of authenticating primary users which exploits the proximity of Helper node with a PU. 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 PU becomes feeble leading to external disturbances in the signal transmission. There are techniques which aim at differentiating signals using an energy detection scheme which is again a trivial parameter since an attacking node has better possibilities of imitating the energy characteristics of the primary signal rather than

any other parameter in an improved manner (Zheng et al 2017).

The existing techniques fail to provide an exact estimate on the location of a PUE Attacker and tender an inaccurate approximation on the presence of the attacker in the network. Our proposed work therefore is a collaboration of both Localization with much less time 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.

3 Existing localization technique using TDOA in detection of PUEA

Deploying the best defense strategy against PUEA is considered vital in CRNs. Localization using TDOA is an approach which tends to minimize the prospects of PUEA in a cognitive radio network. Based on the parameter estimation and iterative comparisons performed, the transmitter is localized and the PUE attacks are detected successfully in the existing system of the “Time difference of arrival” method.

3.1 Time of arrival estimation and time difference of arrival calculation

The “Time of Arrival” (TOA) of a signal transmitted from a source is most crucial parameter to estimate the area over which the transmitter might lie. The spectrum sensing is incessantly performed using a pair of secondary users namely Authentic Node (AN) and Decision node (DN). 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. The invariable time difference of arrival between the signals from the two authentic nodes defines an area over which the transmitter must lie. The intersections of two or more such estimated results tend to project a clear two dimensional position and area over which the transmitter lies. The TDOA measurement can be obtained as follows,

$$\Delta T_{(i,1)} = \frac{\sqrt{(a_i - a)^2 - (b_i - b)^2} - \sqrt{(a_1 - a)^2 - (b_1 - b)^2}}{C}, \tag{1}$$

$\Delta T_{(i,1)}$ 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) and position of the decision node (a₁, b₁). The reading here is obtained for

two different time of arrival signals and for a pair of dedicated secondary authenticated nodes. Three to four such estimates can be obtained for a much better accuracy in obtaining the Time Difference of Arrival estimation. However the important factor to be kept in mind is the time delay which is apparent since it may lead to the consumption of more energy gradually during both the transmitter localization process and spectrum sensing progression.

The coefficients forming the Distance or length of measurement between the transmitter and the authentic node is expressed as,

$$L_i = \sqrt{(ai - a)^2 - (bi - b)^2}. \tag{2}$$

Similarly, the coefficients forming the Distance or length of measurement between the transmitter and the Decision nodes is expressed as,

$$L_1 = \sqrt{(a1 - a)^2 - (b1 - b)^2}. \tag{3}$$

The TDOA measured 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.

$$L_{(i,1)} = C \{ \Delta T_{(i,1)} \}. \tag{4}$$

The expression for the “Distance between the transmitter and the authentic node” is give by (L_i) and the Distance between the transmitter and the Decision node is given by (L_1).This coordinate is meant to assess the area over which the transmitter lies.

$$L_{(i,1)} = L_i - L_1. \tag{5}$$

The final conclusion over the calculated coordinates gives the exact estimate of the transmitter location and the area over which the transmitter actually lies. However, all the estimates obtained are based upon the fact that the Primary user is an immobile user of the network. If not the area correlation will prove in significant in estimating the transmitter position and in this case we can rely upon RSS estimation as the factor to determine the transmitter position.

3.2 Transmitter localization

The process of locating the primary user emulation attack (PUEA) is illustrated in the flow chart depicted in Fig. 2

The legitimate secondary users or the authentic node tends to perform spectrum sensing. If the spectrum is unoccupied it is evident 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.

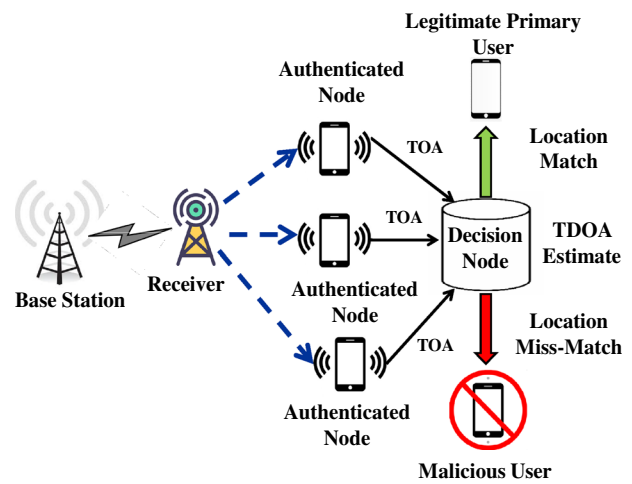


Fig. 2 System model of PUEA detection using area correlation based localization technique (ACLT)

Time of arrival of the transmitted signal by two or more authentic node is recorded. The decision node and the authentic node collaborate to calculate the TDOA. TDOA gives out the estimation of the transmitter location.

The estimated transmitter position is compared with the known Primary user transmitter location. If the parameters match then PUEA illusion is ruled out from the scenario. If mismatch is observed, then the transmitter is concluded to be a PUE attacker. But in this TDOA approach, although the technique is quite accurate, it is required to establish an unyielding synchronization between the transmitter and the received signal which can be quite challenging. The technique is also in-efficient in mobile user’s environment.

4 Proposed localization using time distance and RSS evaluation with extreme learning algorithm

The existing system failed to efficiently exploit the available spectrum bands, owing to the PUEA intervention. The sensing time by the SU’s was also high enough leading to further time delay in calculating the PUEA in the CR network. Also the existing technique is proficient only under the static Primary user and secondary user circumstances. Under mobile conditions of the users, the localization technique keeps failing in nailing down the exact location of the primary user thus resulting in successive errors.

In the proposed technique the traversed distance and time consumption of secondary user are the two major factors that are taken into consideration for predicting the PUE attack in the CR network. In CR domain it is apparent that the Primary user and the corresponding set of secondary users are said to be distributed in a biographic range and

restricted to a certain diameter of operation. Therefore it can also be assumed that the secondary users tend to travel within the bound diameter. In the proposed approach the distance traversed and time of spectrum utilization by each mobile secondary user is recorded for quit some period and an average estimate is obtained for the same. The averaged value is predetermined as the threshold above which any of the received transmission value is considered as a breach and ascertained as the PUE attack.

The technique also provides a major improvement in eliminating the attacks from other secondary users which are out the stipulated circumference of operation. So each time there's a planned attack launched form the secondary users with respect to the neighboring boundary of operation, they tend to fail each time or get detected quickly and the attack is ruled out.

TDSE can be categorized into 3 sub modules of implementation as follows,

- a. Time–distance evaluation of all the secondary users.
- b. RSS estimation of the received signal.
- c. Application of Extreme machine learning to conclude a malicious attack.

4.1 Time–distance evaluation of secondary users

The overall transmission time consumption and Distance traversed by each secondary user bound by a definite circumference of operating area is calculated. Here the sampling circumference of operation is considered to be approximately 10m diameter.

The sampling distance is acquired based on the secondary users traversed across the stipulated diameter per day over a period of 1 week. The acquired values are finally averaged to determine the threshold for the secondary user's maximum traversing distance. Similarly the time consumption of every secondary user present in the operating diameter is acquired from the base station along with the ideal time of Primary User per day. The ideal time is observed over a period of a week and the average value is obtained for determining the threshold above which the time consumption by a user would be considered a violation and the so called transmission would be ascertained as the malicious user and the attack would be ruled out. The recorded tabulation can be observed in Table 1 depicting the sampled outputs and the average values acquired from the base station.

4.2 Receiver signal strength indicator (RSSI)

RSS marks the overall power of the acknowledged radio signal at the receiving antennas. The signal received at the receiver end is deliberated and calculated over a period and then averaged to generate the RSSI value. The Receiver

Table 1 Secondary user transmission distance and time observation with ideal time charting of primary user

S.NO	Secondary users (SU)	SU distance travelled per day at various instances (m)						SU average distance travelled per day (m)	SU channel access duration per day (h)	SU average channel access duration per day (h)	Ideal time of primary user (PU) per day (Hrs)						
		I1	I2	I3	I4	I5	I6				D1	D2	D3	D4	D5	D6	D7
1	S1	6	8	7	8	9	8	7.6	2.2	1.86	8	9	8.5	7.5	8.5	9.5	9
2	S2	9.5	7.5	7.8	8.2	9	8	8.3	1.8								
3	S3	8.5	9	7	8	8	7	7.9	2								
4	S4	8.4	9	8.9	9	7.1	8.6	8.5	1.5								
5	S5	7.8	8.2	6.8	7	8.8	9	7.9	1.8								
											Average ideal time of pu per day (Hrs)		8.5				

signal strength is a decisive parameter to predict the transmitter’s authenticity since it provides a critical influence over differentiating the power ranges of a secondary user from that of the authenticated primary user.

In a wireless communication system, the parameters such as reflections or multipath are not taken into consideration in order to estimate the overall strength of the signal at the receiving antenna. The signal strength of a received signal can be enumerated using the free space propagation model as depicted in Eq. (6):

$$Pr = Ps \times Gs \times Gr \times \left[\frac{\lambda}{4\pi d} \right]^2. \tag{6}$$

Here, Pr is the power obtained at the receiver and Ps would be the power at the surface of the transmitting antenna. Similarly Gs is depicted as the gain at the transmitting antenna and Gr is the gain at the receiver antenna. Here d is the specified distance between the transmitting and receiving antenna.

Assuming the fact that the power ranges of a primary user would always be relatively higher than any secondary user in the network, the obtained RSS can be adjoined with the time distance value for a proportional analysis in acquiring the accurate location of the transmitter.

4.3 Extreme machine learning

Recent advances in wireless communication has highlighted the importance of incorporating learning techniques for rapid decision making & improved utilization of radio electromagnetic spectrum. Learning techniques can be widely classified into two major categories called the supervised learning algorithm and unsupervised learning algorithm. Supervised learning algorithms make use of training and create decision models using labeled data sets. Extreme learning machine (ELM) is one such supervised learning algorithm which utilizes trained data sets to describe the stipulated margins which aids in apparently separating classes of the given input parameters that are taken into consideration.

ELM is an improved learning method, which classifies patterns with distinction and assists in high end function approximations. ELM is a learning algorithm that basically supports single feed forward neural network with a set of single layer of hidden nodes. The randomly assigned weights between inputs and hidden nodes remain constant during the training and predicting phases, whereas the weights connecting hidden nodes to output nodes can be trained with very less time and in a prompt fashion. The performance analysis of ELMs states that this algorithm can generate satisfactory prognostic performance with nominal time duration and their cost of computation is to a great extent lower than the networks trained by the preceding back-propagation algorithm. The study on ELM

has revealed the fact that this so called algorithm is capable of swift learning & brings about a precise distinction between the sensed input models. This algorithm is thus utilized in predicting the presence of PUEA in the cognitive radio environment for a reliable network performance. ELM model has been represented in Fig. 3. The figure depicts the ELM model being trained using jth input samples.

$$y_i = \sum_{i=1}^h \beta_i g(w_i x_j + b_i) \quad j = 1, \dots, N. \tag{7}$$

Here in Eq. (7), h is the number of hidden neurons, g is the neuron activation function, wi is a vector representing input layer weights which is associated with the ith hidden neuron, xj is a vector for the jth input sample, bi is a bias, βi is the output layer weight corresponding to the ith hidden neuron, and N is the number of training samples.

The above equation can be represented in a compact manner using the Eq. (8),

$$H\beta = T. \tag{8}$$

In ELM input layer weights are assigned in a random manner whereas the output layer weights are obtained by performing a generalized inverse of the hidden layer output matrix shown in Eq. (9).

$$H = \begin{bmatrix} g(w_1 x_1 + b_1) & \dots & g(w_i x_1 + b_i) \\ \vdots & \ddots & \vdots \\ g(w_1 x_N + b_1) & \dots & g(w_i x_N + b_i) \end{bmatrix}_{N \times i}, \tag{9}$$

$$\beta = \begin{bmatrix} \beta_1^T \\ \vdots \\ \beta_i^T \end{bmatrix}_{i \times m} \quad \& T = \begin{bmatrix} t_1^T \\ \vdots \\ t_N^T \end{bmatrix}_{N \times m}. \tag{10}$$

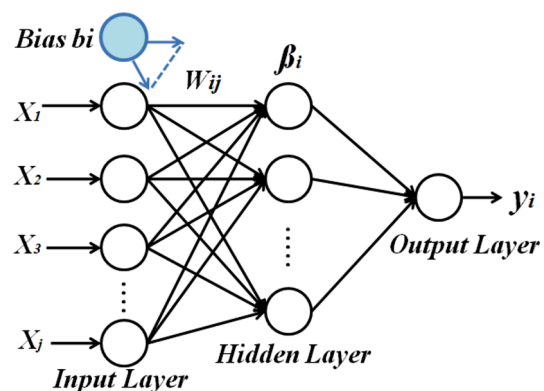


Fig. 3 Extreme machine learning (EML) implementation

The H matrix is a $N \times i$ dimensional hidden layer output matrix, T is the training data target matrix represented by Eq. (10), and m specifies the number of outputs of the system. The resultant weight matrix Y can be calculated by the following Eq. (11),

$$Y = H\beta, \quad (11)$$

Where, β is the so called output weight matrix given by the Eq. (12),

$$\beta = H^\dagger Y. \quad (12)$$

After choosing the sigmoid activation function we need to calculate the Moore–Penrose generalized inverse of H using either iterative method or singular value decomposition (SVD). The Moore–Penrose equation is depicted in Eq. (13),

$$H^\dagger = (H^T \times H)^{-1} \times H^T. \quad (13)$$

The algorithm is initially required to be trained using the necessary input variables so that it could make reliable predictions and determine the PUEA with superior accuracy. During the learning phase the weights between the hidden nodes and the output variables are adjusted with very minimum time duration in order to achieve a faster training and output prediction.

The evaluated mobile secondary users traversed Distance, Time duration of traversal, Receiver signal strength from the oncoming transmitter and the ideal time of the primary user are the four critical input variables that are taken into consideration for training the learning algorithm. Once the algorithm is trained with the given data sets of the input variables it will compare the labeled data sets with the received signal parameters to make an accurate prediction on the presence of PUEA in the network. The weights in the algorithm are tangible characteristics of primary user, which uses the Extreme algorithm and the resultant value adjusted during the training phase for it to attain an appropriate stage at which it could predict and confirm a definite mismatch or otherwise the attack by the emulating node. The input variables would be correlated with that of the match would corroborate the licensed primary user transmission and the mismatch corresponding to any one of the parameter with respect to the distance, time, RSS would be proven to be a malicious attack giving out a rapid and accurate result.

The tabulation in Table 1 shows the observed distance and traversal time values and the channel access duration of the mobile secondary user along with the ideal time status of the primary user. The values have been averaged to obtain the corresponding threshold values for these specified parameters. The infringement of the threshold would result in an immediate exposure of the PUE attacker and thus

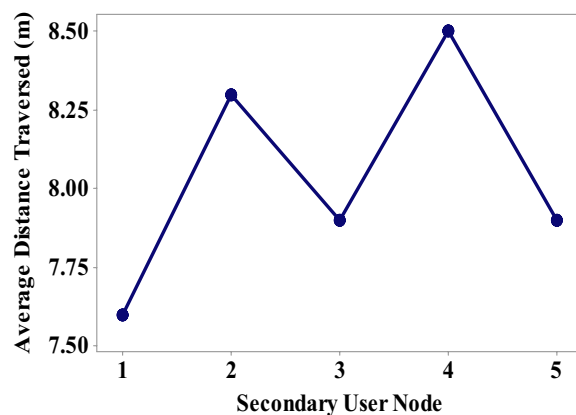


Fig. 4 Mobile secondary nodes distance traversed range

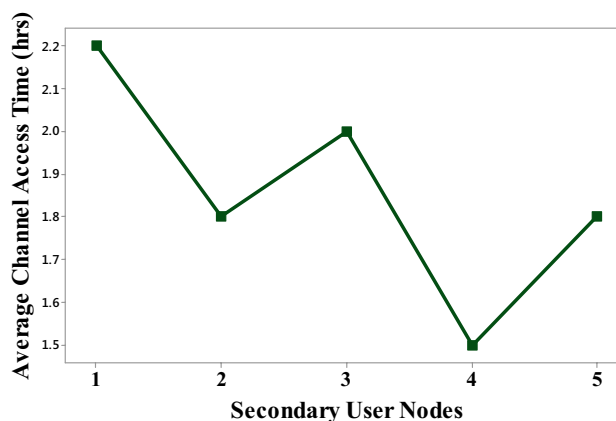


Fig. 5 Mobile secondary nodes average channel access duration

would be ruled out from the network, making it impossible to launch any further attacks in the network.

5 Simulated output analysis

The proposed time distance and strength evaluation technique is validated using network simulator-2. The graphical performance analysis gives a brief insight on the endorsements of the proposed methodology. Figure 4 shows the Distance navigated by the mobile secondary nodes across the defined Circumference of operating area. The overall traversed distance is plotted over definite intervals. This gives an estimate of the possible travel duration and distance taken by these nodes. The assumption is thus made such that the distance and area coverage rate would be more or less same even after a period of time and if any other secondary node gets access to the network, the breach could be perceived immediately using the learning algorithm.

The graph at Fig. 5 shows the channel access duration of the mobile secondary nodes present in the network. The

distribution corroborates the duration of spectrum usage and the variation would only be very minor if the observations were to be estimated over a period of time.

This distribution can be used to fix the overall threshold of the channel access time by every secondary node present in the network.

The performance analysis of the existing and proposed methods with respect to various metrics comparisons can be observed in the upcoming graphs. The proposed TDSE technique is compared with the existing Yardstick based Threshold Allocation (YTA), Angle of Arrival (AOA) and TDOA methods to demonstrate the competence of our proposed methodology. The computation time over the increase in Primary Emulation attack possibility is plotted in Fig. 6.

The existing system of TDOA computes the location each time it encounters a primary like transmission and thus the computation time is quite high. The same problem is encountered in YTA technique since the algorithm has to assign a threshold for the base station and the calculation performed for comparing the threshold verification takes quite some time.

AOA method (Zhao et al. 2014) proves to be time consuming due to the deployment of smart antenna around the secondary users and the algorithm senses the corresponding Omni-directional antennas before concluding and verifying the received signal. The Proposed TDSE technique is shown to have, computed the error with minimum time duration, as the estimated time-distance parameters are all predetermined and the Extreme learning algorithm which is known to have high computation speed, performs a quick

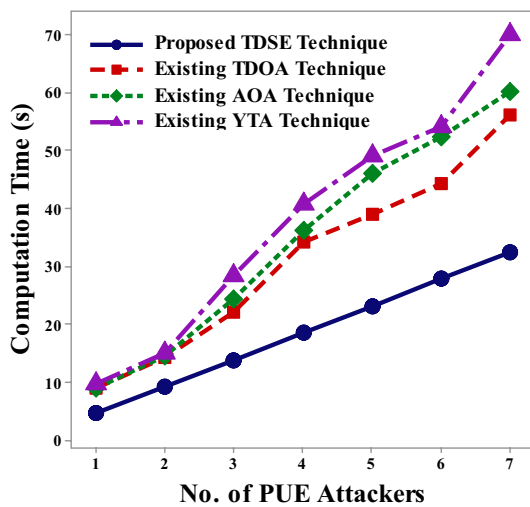


Fig. 6 Computation time between existing and proposed methodology. Existing TDOA technique: Time difference of arrival technique. Existing AOA technique: Existing angle of arrival technique. Existing YTA technique: Yardstick based threshold allocation technique. Proposed TDSE technique: time distance and strength estimation technique

comparative analysis making it feasible for the proposed system to quickly rule out a potential threat in the network.

The existing TDOA technique is known to be range based localization technique and the rough coordinate estimation is taken into consideration for validating a PUEA (Singh et al. 2016). The attack if launched in closer proximity of any secondary user, the Localization error becomes high in the case of the existing system. Similarly in YTA and AOA existing methods, when the angle of an emulating node is closer to the PU, the localization error seems to exceed the tolerable limits.

The graph at Fig. 7 shows how the proposed system has the potential to detect PUEA in mobile secondary user environment, by tabulating the varying parameters and effectively spotting the uncanny breach with the help of the extreme algorithm which is already trained with all the known parameters. By comparing with the recent acquired parameter of the so called attacker, it is easy to validate the difference and locate the attacker identifying a successful detection of PUEA.

With the probability of increase in the number of emulation attack in a network, the emulation inference technique needs to be competent enough to make accurate distinction between the actual attacker and the secondary users. In the existing TDOA, AOA and YTA techniques, capability of dealing with single PUEA is considerable and when it comes to the question of multiple attacks these existing systems are not efficient enough to distinguish the attack within a stipulated time interval.

The Proposed TDSE technique employs advanced sensing technique which is combined with learning algorithm in identifying multiple attacks with the same time duration of spotting a single attack, since any nodes exceeding the channel access time and distance threshold would be identified

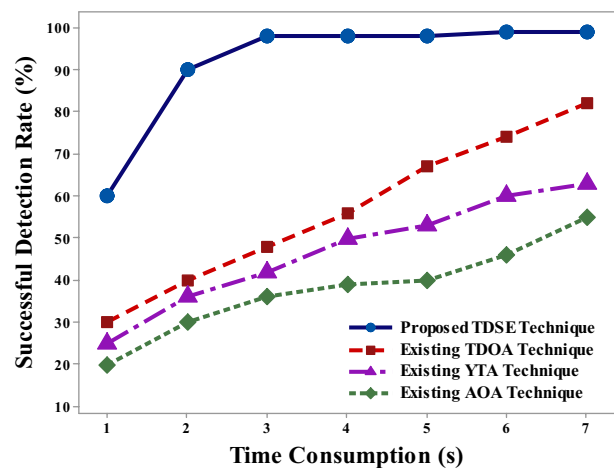


Fig. 7 Successful PUEA detection rate vs time of detection between existing and proposed methodology

immediately as the attacker. Therefore the proposed methodology is proven to have higher success in detecting multiple attacks which is shown in Fig. 8.

Energy efficiency is the most important factor to be taken into account since the complete cognitive radio performance relies on this parameter (Banerjee and Maity 2017). A perceptible TOA observation and TDOA estimation increases sensing time which in turn exponentially increases the energy consumption rate in case of the existing system. AOA and YTA existing methods also tend to consume considerable energy because of the implementation of smart antennas and threshold based attack perception technique respectively. The proposed TDSE technique is a process by which quick conclusion over PUEA breach is determined with minimum sensing and increased rapid approximation utilizing ELM technique. Therefore energy consumption is considerably minimized in case of proposed algorithm. The simulated graph can be observed to have considerable variation in the energy consumption rate with respect to the existing and proposed methods as shown in Fig.9.

Figure 10 depicts the comparative illustration of the localization error encountered by the existing and the proposed methodologies. Localization error is observed to be high in case of the existing TDOA method due to the influence of receiver phase mismatch error and multipath propagation effects in the channel which diminishes the chances of locating the transmitter with exact conviction. In AOA approach the single parameter estimation is not sufficient to substantiate a true attack and varying secondary nodes.

In The YTA technique, the threshold allocation is trivial to distinguish a false alarm and missed detection and therefore truly localizing an emulation probability is less. The proposed technique however is highly effective in accurately localizing the transmitter over an area with greater accuracy,

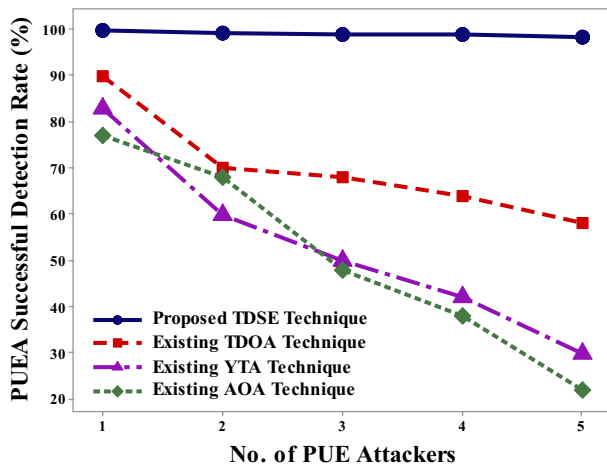


Fig. 8 PUEA detection vs increase in PUEA nodes comparison between existing and proposed methodology

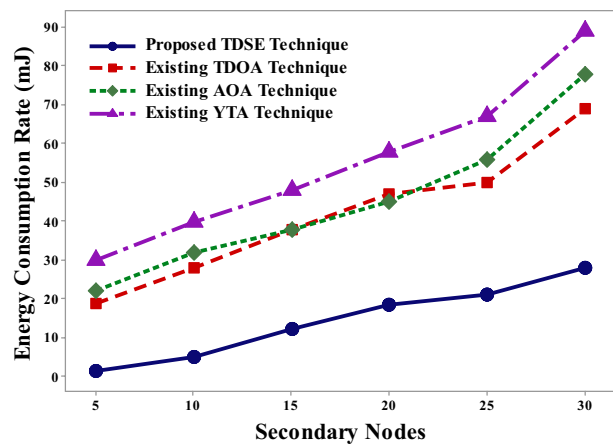


Fig. 9 Energy consumption rate comparison between existing and proposed methodology

owing to the iterative approximation and prediction with RSS comparison techniques deployed.

Detection of the emulation attacker within nominal time duration is highly crucial since this one parameter is vital in determining the performance efficiency of any algorithm implemented for the purpose. The computation time is approximated to be high in case of the existing TDOA method, as the decision that is required to be made for ascertaining the transmitter’s location is estimated based on both the TOA and the TDOA obtained at all the antennas deployed in the network.

In AOA, MUSIC (Multiple Signal Classification) algorithm is used which is efficient only with a set of minimal secondary nodes and so is the case with YTA method which makes use of WSPRT (Wald’s sequential probability Ratio

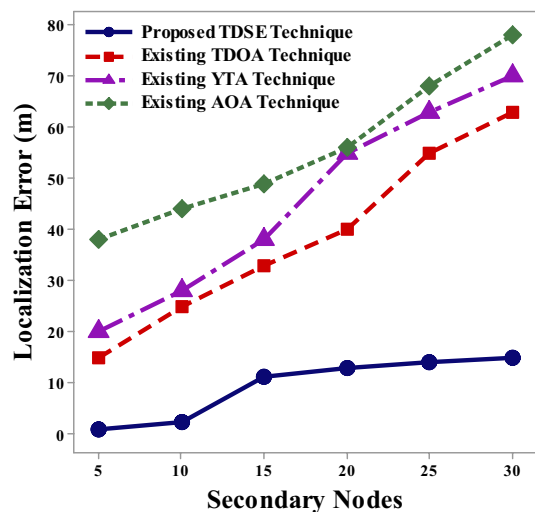


Fig. 10 Localization error estimation between the existing and proposed methodology

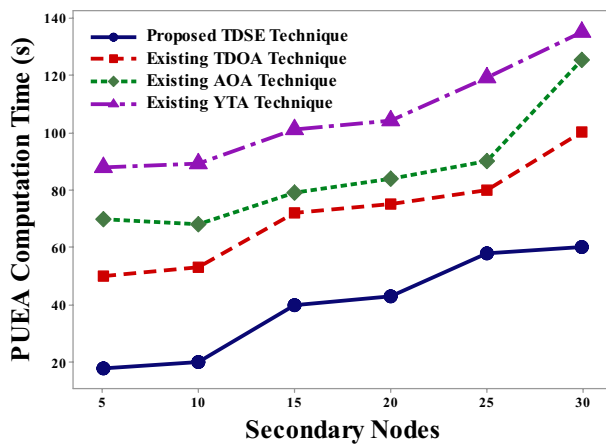


Fig. 11 Computation time between existing and proposed methodology

Test) algorithm, for which the complexity in node differentiation is high when the number of secondary nodes tend to gradually increase in the network. Therefore a final conclusion is possible only based on a 2-dimensional location estimation which is expected to be performed every time a received signal is sensed across the network, which can be a tedious and time consuming task.

TDSE is a rapid violation recognizing algorithm which involves all the secondary users to participate in the evaluation, taking very minimum time in doing so, with the help of ELM algorithm in a systematic attribute comparison. The graph in Fig. 11 is illustrated with the existing and proposed techniques performance with respect to the computation time. The performance metrics comparative analysis between the existing and proposed techniques, have made apparent the fact that the “Time distance strength evaluation Technique” is a competent procedure for both thwarting the multiple attacks and also in accurate timely estimation of PUEA in a cognitive radio network.

6 Conclusion

Investigating all the study performed so far, it is manifested that there are indeed proven techniques for the detection of a PUEA but none so efficient to avoid such attacks repeated occurrences in a CR network. Also multiple attacks have been difficult to tackle so far in a dynamic cognitive radio environment. So 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 deliberated on avoiding the PUEA in the CR network by implementing the Time Distance and Strength Evaluation technique which not only is proven to minimize the transmitter identification time but also is proficient enough to thwart

multiple attacks and recurrence of such emulations by eliminating the attacking node from the network with much less complexity in a mobile secondary user environment.

References

- Banerjee A, Maity SP (2017) On energy minimization in cooperative spectrum sensing using LRT in presence of emulation attack. In: 2016 IEEE international conference on advanced networks and telecommunications systems, ANTS 2016
- Chen R, Park J, Reed JH (2008) Defense against primary user emulation attacks in cognitive radio networks. *IEEE J Sel Areas Commun* 26(1):25–37
- Das D, Das S (2017) Adaptive resource allocation scheme for cognitive radio vehicular ad-hoc network in the presence of primary user emulation attack. *IET Netw* 6(1):5–13
- Dasari R, Venkatram N (2021) Discrete quality factors aware channel scheduling in cognitive radio ad-hoc networks. *J Ambient Intell Humaniz Comput*. <https://doi.org/10.1007/s12652-020-02607-6>
- Fragkiadakis AG, Tragos EZ, Askoxylakis IG (2013) A survey on security threats and detection techniques in cognitive radio networks. *IEEE Commun Surv Tutor* 15(1):428–445
- Jakimoski G, Subbalakshmi KP (2008) Denial-of-service attacks on dynamic spectrum access networks, *IEEE Cog*. In: *Nets Workshop*, IEEE international conference on communications, May 2008
- Jayasree V, Suganya R (2014) A survey on primary user emulation detection mechanisms in cognitive radio networks. *Int J Comput Trends Technol (IJCTT)* 14:75–79. <https://doi.org/10.14445/22312803/IJCTT-V14P117>
- Jin Z, Anand S, Subbalakshmi KP (2012) Detecting primary user emulation attacks in dynamic spectrum access. *Networks* 60(9):2635–2643
- Kshirsagar D, Kumar S (2021) A feature reduction based reflected and exploited DDoS attacks detection system. *J Ambient Intell Humaniz Comput*. <https://doi.org/10.1007/s12652-021-02907-5>
- Li Y, Wang M, Han C, Xie L (2016) A primary user emulation attack detection scheme in cognitive radio network with mobile secondary user. In: *2nd IEEE international conference on computer and communications*
- Lin SC, Wen CY, Sethares WA (2018) Two-tier device-based authentication protocol against PUEA attacks for IoT applications. *IEEE Trans Signal Inf Process Netw* 4(1):33–47
- Liu L, Zhang Z (2016) EM-Based. Algorithm for defeating against primary user emulation attacks in. 1450–1455
- Salam D, Taggu A, Marchang N (2016) An effective emitter-source localization-based PUEA detection mechanism in cognitive radio networks. In: *International conference on advances in computing, communications and informatics (ICACCI)*, Sept. 21–24, 2016
- Singh A, Sharma A (2014) A survey of various defense techniques to detect primary user emulation attacks. *Int J Curr Eng Technol* 4(2):900–908
- Singh AK, Singh AK (2016) Range-based primary user localization in cognitive radio networks. *Proc Comput Sci* 93(September):199–206
- Zhao Y, Huang J, Wang W, Zaman R (2014) Detection of primary user’s signal in cognitive radio networks: angle of arrival based approach. 978-1-4799-3512-3/14-2014 IEEE
- Zheng Y, Chen Y, Xing C, Chen J, Zheng T (2017) A scheme against primary user emulation attack based on improved energy detection. In: *2016 IEEE International Conference on Information and Automation, IEEE ICIA 2016*, (August), pp 2056–2060

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.