Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2022.026098
Article

Tech Science Press

Enhanced Primary User Emulation Attack Inference in Cognitive Radio Networks Using Machine Learning Algorithm

N. Sureka* **and K. Gunaseelan**

Anna University, College of Engineering Guindy, Chennai, India
*Corresponding Author: N. Sureka Email: sureka.ns05@gmail.com
Received: 15 December 2021; Accepted: 09 February 2022

Abstract: Cognitive Radio (CR) is a competent technique devised to smart sense its surroundings and address the spectrum scarcity issues in wireless communication networks. The Primary User Emulation Attack (PUEA) is one of the most serious security threats affecting the performance of CR networks. In this paper, machine learning (ML) principles have been applied to detect PUEA with superior decision-making ability. To distinguish the attacking nodes, Reinforced Learning (RL) and Extreme Machine Learning (EML-RL) algorithms are proposed to be based on Reinforced Learning (EML). Various dynamic parameters like estimation error, attack detection efficiency, attack estimation rate, and learning rate have been examined with the Network Simulator 2 (NS2) tool.

Keywords: Cognitive radio network (CRN); primary user emulation attack (PUEA); reinforced learning (RL); extreme machine learning based reinforced learning (EML-RL) algorithms

1 Introduction

Wireless communication has achieved tremendous growth in recent years and has evolved into a medium that has created an exceptional mark in human life with its ever-evolving applications and services. The diversity and widespread use of wireless communication has led to spectrum scarcity and heavy network traffic which ought to be resolved circumspectly without creating conflicts to the busy users of the network. Dynamic spectrum allocation is an imperative key to formulate mutual active networks and a resourceful management of idle spectrum in a dynamic wireless network. Cognitive radio is a smart device that dynamically assigns unused spectrum holes that are in urgent need of data transmission and thereby profoundly avoids spectrum wastage and resourcefully manages network traffic in a wireless communication network. The Primary User (PU) and the Secondary User (SU) are the active participants that tend to cooperatively utilize spectrum bands in each channel and carries out data transmissions across the networks. Spectrum sensing is an essential action that needs to be performed by the SU's to estimate & efficiently utilize free spectrum holes. Spectrum sensing also plays a key role in detection of PU's (Licensed users) transmission probabilities in a particular spectrum band. The accurate estimation of the primary user transmission probability is mandatory for the SU's (Unlicensed users) to choose an appropriate spectrum band for its own use. With the various compensations that are offered by

the wireless communication medium it is still prone to various security threats, one among which is the Primary User Emulation Attack (PUEA) that decreases the spectrum access probability of unlicensed users. The malicious attack is launched by one of the SU's of the network which turns malicious by emulating the characteristics of the PU to capture the idle or active spectrum intrinsically for its own exploitation, creating unwanted confusions and seizes the potential prospect from the other good SU's to utilize the leveraged spectrum band for its own use. The PUEA model in a wireless environment is illustrated in Fig. 1.Wireless spectrum usage etiquette states that the secondary users must instantly withdraw from the spectrum bands once a primary transmission is detected. To overcome this etiquette, the malicious SU's pretends to be a PU and launches this unethical Denial of Service (DoS) attack that hugely confuses the other good SU's affecting the overall performance in the network. This opens to an

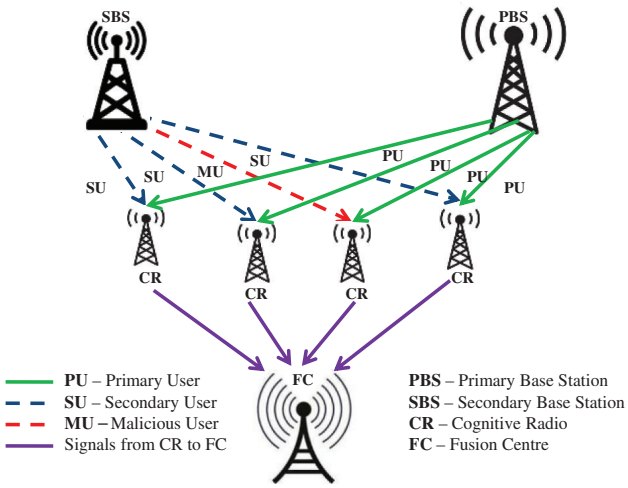

Figure 1: PUEA and its impact on CR networks

extensive debate over improving the network defense and spectrum management strategies in a dynamic cognitive radio network.

Numerous schemes have been proposed so far, based on the principles of localization of PU [1,2], Wireless signature authentication of the received signal [3], Channel encryption methodologies, Angle detection of the received signal [4], Energy detection [5,6], and so on, to detect PUEA threats in wireless communication networks. But all these methodologies may fail when the users are deployed in a mobile environment. The Doppler spread and variance detection [7] approach that has been used to detect PUEA in a mobile environment can capitulate inaccurate results when the malicious node arrives closer to a PU, leading again to a missed detection. The existing theories are observed to articulate widely around node detection principles with localization perspectives in a static environment. It is therefore evident that a more competent scheme needs to be devised to accurately nail down such an intelligent PUEA that can alter its characters dynamically.

In this paper, machine learning (ML) algorithms have been proposed to detect emulation attacks in a dynamic cognitive radio deployed wireless communication environment. ML is the most advanced prediction algorithm and is known for its better decision-making ability and ability to handle multivariate and multi-dimensional data with high competency, yielding a highly precise output. In this paper, two innovative learning principles have been proposed, namely the Reinforced Learning (RL) algorithm and a conjoint influence of both EML and RL (EML-RL) algorithm, that tracks and detects the PUEA pattern proficiently with the least amount of time. This way of locating emulation attackers accurately with a

minimum duration will be a breakthrough in differentiating and identifying the attack model and avoiding PUEA probability in a CR network. The simulation results illustrate that the PUEA has been considerably detected with a minimum error, complexity, and time of detection while the users of the network exceptionally exploit a high degree of spectrum utilisation etiquette.

Contributions

a. Execution of Reinforced Learning algorithm with Q-learning factor for iterative updates to distinguish PUEA.
b. Implementation of a decisive scheme collaborating EML & RL algorithm to competently identify PUEA.
c. A comparative analysis has been carried out to analyze the efficiency factors of each proposed algorithms with that of the existing methodologies.

The rest of the manuscript is organized as follows. Section II would make evident the aspects of ML algorithm, touching upon the relevant applications & compensations that have been applied in the analysis. Section 3 elaborates on the algorithms of existing technique. The proposed Reinforced algorithm and its significance have been furnished in Section 4. The improved EML-RL algorithms with its detection & defense procedures have been briefed in Section 5. Performance analysis illustrations using NS2 is depicted in Section 6. Section 7 is a summary about the conclusion drawn from the analysis performed.

2 Machine Learning Algorithm

Recursive learning is an advanced branch of science that can be used to make the process of prediction much simpler and more accurate through a recursive training process. Machine learning has been considered as the most excellent methodology that can be integrated with a specific function or application and successfully achieve the desirable outcome. Machine learning can be classified into three specific groups: supervised learning, which means the algorithm comprises of a target or dependent variable/factor which must be estimated from a given set of given independent variables/factors. With the help of these given variables, the algorithm must formulate a function that needs to map the inputs to the desired output. The training that is carried out using the variable must be sustained till a certain level of desired accuracy is achieved.

Unsupervised Learning: This algorithm is not expected to predict or estimate any given input values or achieve an outcome, but rather is just used to cluster or segment a given group of input variables for specific intercession. Reinforced Learning: This algorithm is also used to take data-driven decisions over a particular environment in which it is deployed. The algorithm helps a particular machine learn continuously from its surrounding environment with minimum human intervention on a trial-and-error basis, and by assimilating the knowledge procured from the environment, it takes the best possible accurate decision. ML is a significant technique that enables artificial intelligence to solve complex problems without the assistance of explicit programming. ML tools can be further exploited to design novel resource administration and control techniques for optimising the performance of wireless communication networks. ML principles can be integrated with wireless communication systems to fabricate the level of intelligent radio access networks with better security enhancements. The algorithms that have been proposed are extremely automated decision-making machine principles that offer zero human intervention and a scope for frequent up-gradations depending upon the diverse learning factors and tend to improve the precision and rate of final decision-making aspects in any deployed environment. The advances in ML techniques have been utilised in this paper to enhance the security of cognitive radio networks by proficiently detecting and thwarting potential PUEA.

3 Existing Techniques on Detecting PUEA in CR Networks

The approach of various researchers has been analyzed in identifying the PUEA with respect to a mobile & immobile user environment. Various detection and preventive measures for PUEA have been devised so far, which to some extent had proved to be efficient in reducing the probability of PUEA in an immobile user environment. The existing theories articulate widely about the detection probabilities with few decisive factors among the measures adapted to detect a PUEA model in a mobile user environment. The study so concludes that the real time workable model for eradicating the PUEA with mobile users has not yet been discussed successfully.

In [8], the usage of localization scheme & Received Signal Strength (RSS) alone to estimate and authenticate the location of PU has been proposed. But it is proved to be in-efficient since the model can be defeated by attacker by using Antenna arrays with different power levels. Localization Technique to detect the PUEA by applying Time of Arrival (TOA) of a Signal from the SOI (System of Interest) and evaluating the Time Difference of Arrival (TDOA) of the signal could be feasible [9], for the users of the network to be stationary. With mobile users the technique itself would be a failed model. In [10], the authors perform sensing using "Multiple classification algorithms" and estimated the "Angle of Arrival" (AoA) of the signal from the transmitter that employed Smart antenna technology in which each SU receiver is equipped with a smart antenna to detect arrival angles of all incoming signals. Here the detection resolution depended on the number of antenna elements. This practical difficulty paved way to inaccuracy and probability of numerous missed detections, which made the process more time consuming and less cost-effective approach.

In [11], a novel scheme where the attack estimation is possible by differentiating the signals of SU and PUE by Doppler spread and variance of signal power calculation using the NS2 simulator under mobile secondary user conditions was introduced. However, this scheme produced better results when the conditions for Doppler spread calculation were favorable, with well-chosen parameters such as Signal-to-Noise Ratio (SNR), frames, user coordinates, and received signal velocity having a significant impact on the accuracy of the final attack detection.

New trends in multilayer learning of the EML algorithm have been proposed in [12]. The advances in the field of machine learning with respect to the state-of-the-art application of different EML techniques have been compared and implemented. The EML proves to have the highest generalisation and the quickest possible anomaly detection rate compared to the other conventional models like Artificial Neural Networks (ANN), Back Propagation Networks (BPN's), Support Vector Machines (SVM) etc. In [13], the classification accuracy of various machine learning algorithms like ANN, Naive Basis, and EML, including the Logistic Regression (LR) algorithm, has been compared. Even though LR is an efficient algorithm in performing classifications with relevance to a given problem or a group of data sets, EML is observed to have achieved better accuracy. The simplicity demonstrated in implementing a given classification has made EML more popular in real-time applications where a quick result and a compact structure realisation are of prime importance.

The paper [14] demonstrates the reinforcement learning approach in cognitive radio networks with respect to a wide range of CR schemes such as dynamic spectrum selection, channel sensing, etc. The performance and system optimizations of RL are observed to be better compared with other traditional proposals adapted to the CR networks. Even though the benefits of the RL methodology are obvious, it still has a "dimensionality issue" that needs to be addressed. The RL technique also has a complex structure, which makes it impracticable for simplex functions. [15] proposed an Extreme Machine Learning-based Reinforced Learning (EML-RL). The main aims are to overcome the limitations of EML and RL schemes for better security enhancements and quicker patter classifications in the communication field. Special care is taken to gyrate the EML-based RL algorithm to minimise the computational

complexity and enhance the accuracy of character estimations and its speed of convergence. The authors in [16] have demonstrated the mutual participation of both EML and RL in function approximation and improvised speed of deciphering a given character. Based upon the research survey performed, the machine learning algorithms are more efficient in detecting the PUEA with better accuracy and less time.

4 Proposed Reinforced Learning (RL) Algorithm in PUEA Detection

The RL algorithm is applied to the CR network to enable the Secondary Users (SU) to proactively observe & learn from the environment. The system model of RL implementation is illustrated in Fig. 2.

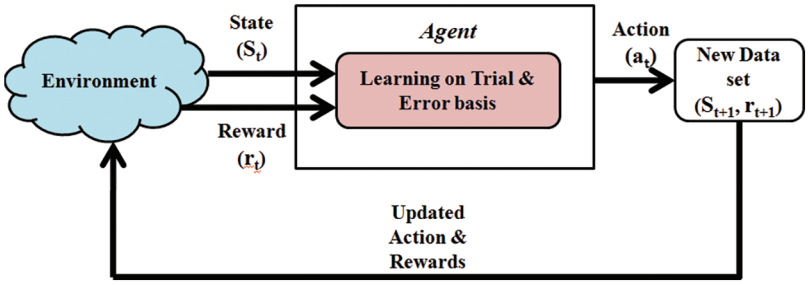

Figure 2: System model of RL algorithm

The RL algorithm is synthesized to sense the basic parameters like frequency of Primary User (PU) channel utilization in a given spectrum band, the idle time of the PU's, the dynamic channel allocation to the SU's and the random movements & traversed loci of each SU's. Based on the observed parameters it makes decision on the vacancy and authenticity of the channel occupancy by either an authenticated PU or a breaching PUEA attack. It applies the Q-Learning factor in which the decision taken by a SU leads to either a false output or the correct output.

The secondary user or the agent monitors the cognitive radio network environment to sense the current state (St) over a decision time period of 't'. The agent opts for the corresponding action (Ut) with respect to the observed current state (St) of the environment. The state of the network changes to the next corresponding state (St+1), with respect to the previous action (Ut) during the next corresponding decision period 't+1'. Depending upon the action applied, the reward is consequently decided, which may get delayed represented by (rt+1(St+1)). The knowledge possessed by an agent i for a sensed state & its corresponding actions at time 't' for 'Q' function is given by the Eq. (1),

$$Q_{t+1}\ (S_t,\ U_t) = (1 - \ \propto)\ Q_t\ (S_t,\ U_t) + \ \propto \ \left[r_{t+1}\ (S_{t+1}) + \gamma \max_{u_{t+1}} Q_t\ (S_{t+1},\ U_{t+1}) \right] \tag{1}$$

where the decision time period is given by,

$$t \in T = \{1,\ 2,\ \ldots\} \tag{2}$$

Here '$\propto$' is the learning factor controlling the learning rate. So it is specified by $0<\propto<1$. The 'γ' denotes the concession factor affecting the obtained reward or a favorable result in the remote future with respect to the obtained reward being obtained in the immediate future.

If 'γ' is 0 the condition denotes that the agent is interested just about the rewards of immediate future and is not interested in long term rewards that would be procured in the remote future.

Whereas if 'γ' is 1 the condition denotes that the agent is interested in both the reward being gained in the immediate future and the rewards that would be procured in the remote future.

So, the agent must consider various network parameters to obtain the reward that would be acquired in the remote future which could gradually affect the next action correspondingly. The Q-Learning searches the best action for a state which is through maximizing the value functions of Q-factor $V\pi\ (S_t)$ as in Eq. (3).

$$V\pi\ (S_t) = \underset{u_{t+1}}{max}\ \left(Q_t\left(S_{t,}\ U_t\right)\right) \tag{3}$$

The best possible policy obtained after successive iterations & Q-table updates a best policy is perceived to appropriately distinguishing the Primary user signal from that of the PUE attacking signal over a particular channel, which is given by the following Eq. (4),

$$\pi\ (S_t)\ = \arg \underset{u_{t+1}}{max}\ \left(Q_t\left(S_{t,}\ U_t\right)\right) \tag{4}$$

Reinforced learning considers just the parameters that are closely related with the overall system performance improvement rather than considering the wide range of parameters in general. Therefore, it is much faster in deducing & differentiating a signal feature of a system on to which it is deployed. The exploitation of Q-function update is about choosing the best action at all time instants thereby improving the performance of the system. Further exploration tends to improve the estimates of all Q-functions aiming at iteratively fine tuning the algorithm to get the superior preeminent policy each time. Also the RL does not require prior knowledge of the network environment & its observed parameters. RL algorithm learns the states gradually & changes its actions correspondingly to get the best possible outcome & as time evolves the algorithm produces result with at most precision thereby helping the secondary users to get the best possible results of PUEA detection and improving the overall system performance.

5 Proposed Extreme Machine Learning Based Reinforced Learning (EML-RL) Algorithm in PUEA Detection

Reinforced Learning (RL) has been proved to have good learning & great intelligence which is convenient for it to be applied in various control & optimization applications. But the RL algorithm has been witnessed to have dimensionality issues & a complex structure. When the PUEA Detection was performed with just the EML algorithm, it was short of accuracy which raised question on its overall efficiency. Irrespective of the recompenses offered by RL & ELM algorithm implemented individually, there were certain negative aspects when employed as a sole technique in mitigating the effects of PUEA thus raising question on its development & application from various perspectives. Extreme Learning Machine (ELM) based Reinforced learning algorithm is a novel scheme in detecting the PUEA as, EML offers great generalization, simple structure & fast learning speed along with RL contributing to better accuracy.

The algorithm supports the principle of sliding time window, which reduces overall sample space thereby improving speed of the learning further. The system model for EML based RL algorithm is illustrated in Fig. 4. The block diagram in Fig. 3 illustrates the functionality of the ELM based RL algorithm in successfully spotting the attack model with improved accuracy and reduced time of distinguishing the attack pattern. In the proposed technique, the input to the RLM model will be the same feature vector representation as the time of secondary user, distance travelled and the RSS values of a given secondary users as samples. At the EML model stage the output samples from the RL machine are fed back to the agent into the EML framework which offers faster learning & approximation with the help of hidden node approximation. Q-Learning factor uses the iterative algorithm in RL to successively obtain better learning updating the consequent actions to be taken by the system thereby appropriately

choosing the best possible outcome in detecting the attack model. Approximation of the Feedforward neural networks is performed using the Extreme Machine Learning (EML) algorithm, which basically depends on the 'n' number of the input samples about to be observed by an agent or the secondary user of the network. With a given training set or sample sets the ELM tends to randomly assign the input weight vectors denoted as '∝i' and the hidden node bias 'ßi. Here the 'i' denotes the 'N' number of arbitrary samples to be obtained by the agent when it interacts with the environment. The input samples are represented in Eq. (5),

$$(\mathrm{S_t},\ \mathrm{U_t}) = [x_{t1},\ x_{t2}, \ldots\ldots\ldots, x_{tn}]^{\mathrm{T}} \tag{5}$$

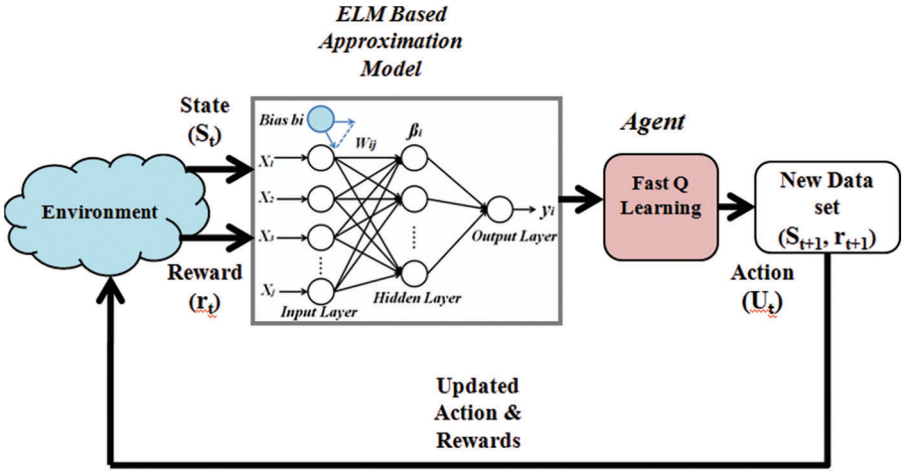

Figure 3: System model of EML-RL algorithm

And the output samples are given by the Eq. (6),

$$Q_t = Y_t = [y_{t1},\ y_{t2}, \ldots\ldots\ldots, y_{tn}]^{\mathrm{T}} \tag{6}$$

The ELM can move towards the given samples functions with zero error, provided the input weight vectors '∝i' and the hidden node bias 'ßi and the output weight matrix 'T' satisfy the following formula in Eq. (7),

$$\sum_{i=1}^{N} T.f(\alpha_i x_{tj} + \beta_i) = Q_{tj} \qquad (j = 1,\ 2 \ldots .\mathrm{N}) \tag{7}$$

The above equations can be simplified as,

$$\mathrm{HT} = \mathrm{Y} \tag{8}$$

where,

$$H(\alpha_{1,\ldots\ldots}, \alpha_N, \beta_{1,\ldots\ldots}, \beta_N, x_{1,\ldots\ldots}, x_N) = \begin{bmatrix} f(\alpha_1 x_1 + \beta_1) & \cdots & f(\alpha_N \mathrm{x}_1 + \beta_N) \\ \vdots & \ddots & \vdots \\ f(\alpha_1 x_N + \beta_1) & \cdots & f(\alpha_N \mathrm{x}_N + \beta_N) \end{bmatrix}_{N\mathrm{x}N} \tag{9}$$

and,

$$T = \begin{bmatrix} t_1^T \\ \vdots \\ t_N^T \end{bmatrix}_{Nxm}, \; Y = \begin{bmatrix} y_1^T \\ \vdots \\ y_N^T \end{bmatrix}_{Nxm} \tag{10}$$

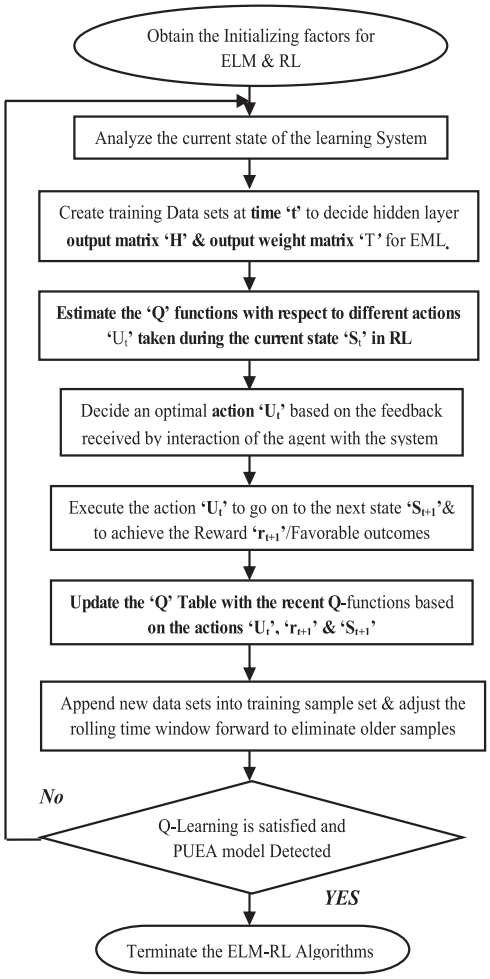

Figure 4: Flow diagram of EML-RL algorithm in detecting PUEA

The initialization parameters for a ELM & RL is obtained using inputs like the channel access duration by each secondary user, Receiver Signal Strength (RSS) of each of the user, including the idle time observed by the Primary Users, Secondary user distance traversed limits and SU maximum channel access requests etc. This is being recursively monitored by one of the designated secondary user for supervising the network environment called the agent. Based on these observations the agent decides on the actions to be taken during next training period. If the decision is not accurate the agent has to undergo the consequence of its derailed performance and throughput in terms of punishments. If the decision was favorable it would achieve better gain in terms of reward. Based on the previous actions, and its corresponding punishment or rewards status the agent learns through its fault and experience in order to fine tune its actions further. The agent then iteratively performs the regression to ultimately come to a proper

conclusion over the learned factors & decides the attack perception by distinguishing the given inputs as depicted in the flow diagram of Fig. 4.

The significance of this model is about updating itself continuously so that any new malicious attack can be quickly detected with the continuous inference made by the network model. All it needs is to observe the environment and update itself with the application features to detect and classify the learned patter with respect to its deployed network. With respect to Eqs. (9) and (10), The output weight matrix 'T' Can be calculated by getting the product of the Moore Penrose generalized inverse of the 'H' matrix & the output samples of Y matrix which is given by the Eq. (11).

$$T = H \dagger Y \tag{11}$$

The algorithm is not restricted to a given set of inputs and correlations. This makes it more robust for applications in a dynamic mobile network environment.

6 Simulated Output Analysis

To investigate the performance of the proposed algorithms, simulations have been performed using NS2 simulator. The graph in Fig. 5 illustrates the learning rate of the proposed algorithms. The machine learning has one of the greatest advantages of "learning" which helps in analyzing various factors by minutely differentiating a given attribute. It is clearly being observed that the learning factor is enhanced in the EML-RL algorithm since it has the combined perquisites of both the EML & the RL algorithm where EML is observed to have pertinent optimization over the RL Q-function due to which the updations in the Q-table is much quicker compared with the procedure of sole RL algorithm.

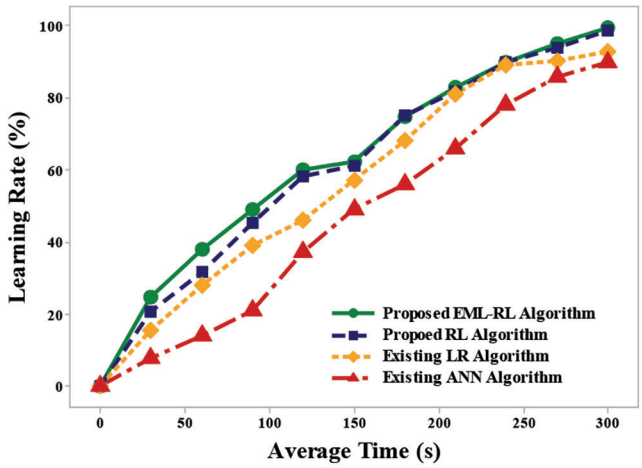

Figure 5: Learning *vs.* average time

In ANN & LR algorithms the observation & updates of the so-called input parameters in a feed forward neural network take quite a while due to which drawing a proper conclusion of the perceived output weight matrix takes longer, therefore slowing the learning pace

The test classification of input sets by RL provides a better accuracy estimating the emulation attacking node therefore the overall time consumed in estimation i.e., the approximation times over the Q-function gets considerably reduced thus offering accurate result in a very less time. Therefore, the overall computation time of the PUEA model in EML-RL algorithm is least compared to the other existing estimation schemes like the RL, LR & ANN methods as depicted in Fig. 6. With the increase in the secondary nodes, EML-RL algorithm

is observed to enclose minimum computation time since the Q-value approximation by the EML training samples does not depend on the number of secondary nodes. Due to this a very minute change in the computation time is entailed as shown in the Fig. 7.

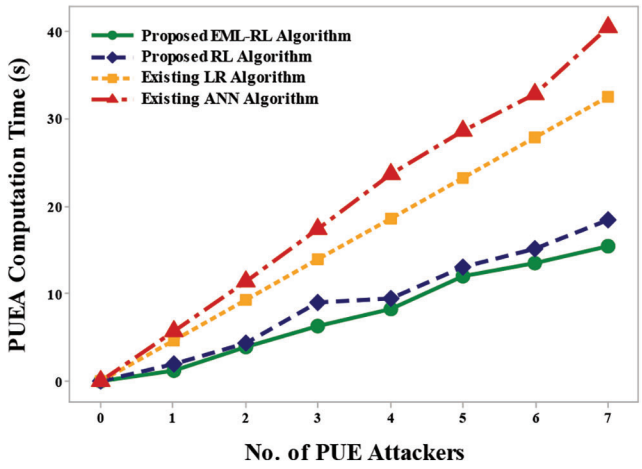

Figure 6: Computation time *vs.* PUEA

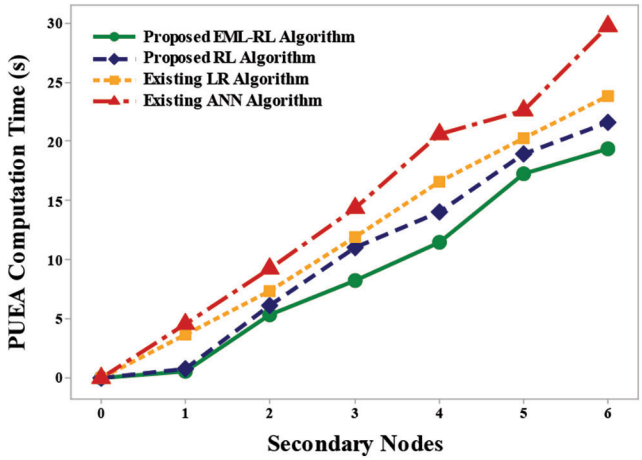

Figure 7: Computation time *vs.* secondary nodes

The proposed EML-RL algorithm having the prior training data values, successfully detects a varying factor with much better accuracy in less time owing to the application of the rolling time window that prunes the older training data sets and allow only the new observed training inputs. This considerably reduces the time of computation & creates a favorable platform for the EML-RL algorithm to focus only on the current data sets unlike ANN & LR which are subjected to testing and training for variable parameters that slows down their performance considerably.

This demonstrates an improved detection rate with minimum time delay for even a surge in secondary nodes in case of EML-RL algorithm compared to the other two existing techniques as illustrated in Figs. 7 and 8.

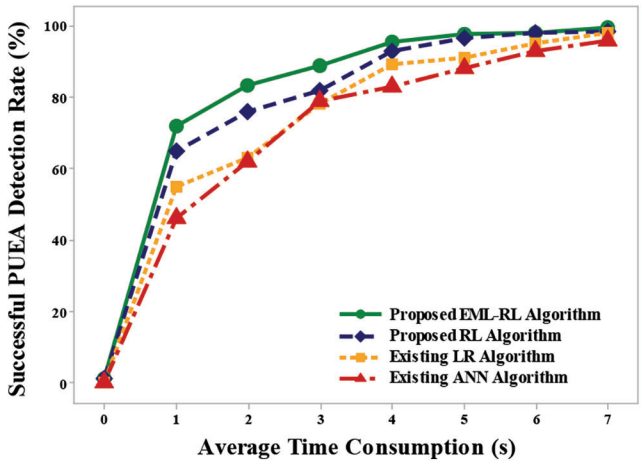

Figure 8: Successful PUEA detection rate *vs.* average time

With the increase in the PUEA nodes the performance of detection rate is still higher in case of the EML-RL algorithm as the learning rate is better with the random sample set formation during every training phase. The feedback acquired with the observed parameters by the agents are updated each time in Q-table making the next consequent state get a much accurate detection policy. This process remains same even under the changing PUE numbers as the next state captures the difference in the node activity correspondingly. In the existing technique however feature detection technique are employed that has to be recreated and analyzed for each sensed signal & its verification thereby causing a substantial impediment in the detection rate. The Fig. 9 exemplifies the successful detection rate for the both the proposed techniques out of which, it is evident that the ELM-RL algorithm has better accomplishment.

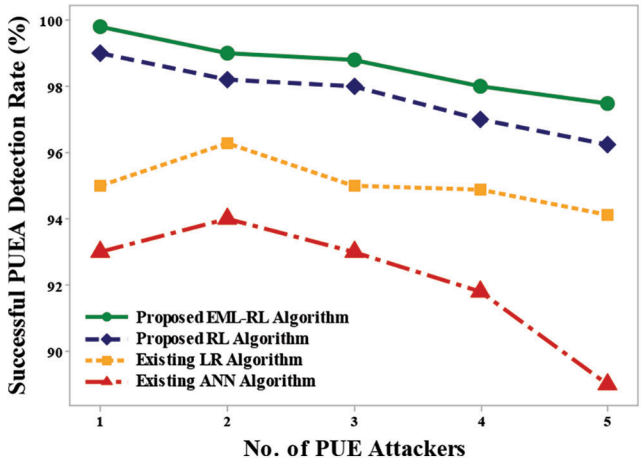

Figure 9: Successful PUEA detection rate *vs.* average time

The iterative updates of Q-table not only renew the functions but also signify the next action to be performed that decides on an optimal solution to the prior perceived network parameters. The decisions to be taken are pre-checked with the feedback signals of RL & the optimization performed by EML over the Q-functions. This is because the difference of any additional secondary node will be successfully learned and the corresponding action for the next state will be optimized based upon the concurrently learned feedback thereby inflicting very minimum change between the perceived output and the predicted

output thereby succeeding towards better consecutive rewards and trying to avert punishments in the name of detection error as illustrated in Fig. 10, even under the effect of more numbers of PUEA. The existing ANN & LR technique are influenced by noise factors that are captured during sensing and computation leading to inaccurate results.

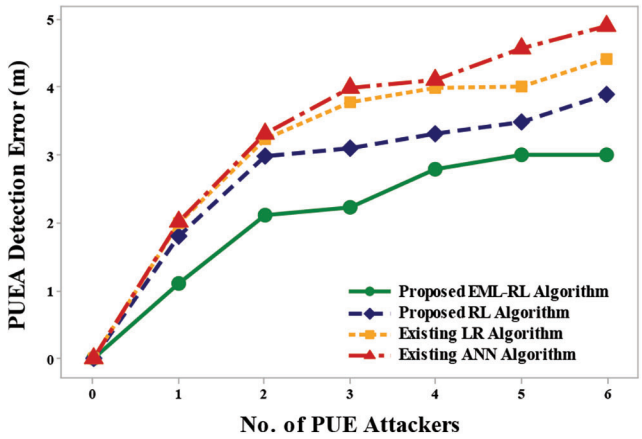

Figure 10: PUEA detection error *vs.* PUEA

With the increase in secondary nodes the EML in the proposed EML-RL algorithm gets better training data sets and analyzes the samples construction by taking some time. But the feedback signal tends to optimize the final output leading to much precise decision over an investigated parameter.

But the time taken is less compared to the time consumed by the LR, RL & other traditional algorithms as shown in the Fig. 11. This conjoint effort of both EML & RL makes the EM-RL algorithm to carefully decrease the errors in final PUEA model perception compared to the other existing techniques even with more number of PUEA nodes or the secondary nodes as shown in the graph of Figs. 10 and 11.

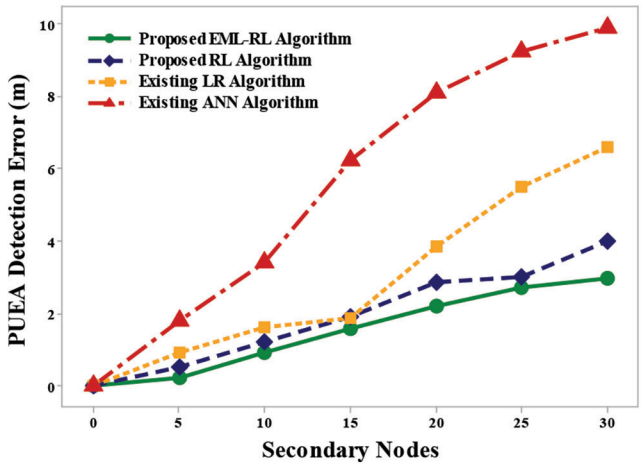

Figure 11: PUEA detection errror *vs.* secondary nodes

In an EML-RL scheme the training samples are quickly analyzed, producing a superior estimating factor. Also the sample size reduction using rolling time window is said to further reduce the observation factor thereby enabling the algorithm to focus on only the required parameters. When RL is implemented from

this stage the learning time is better which ministers the detection & differentiation of an observed parameter much faster thus reducing the overall energy consumption considerably in the network. In the existing ANN & LR the recurrent training and testing with more hidden layer neurons deploy more sensing time with higher degree of energy exploitation. Therefore, the energy consumed is the least compared with the other existing systems as illustrated in the graph of Fig. 12. The performance metrics proves that the proposed RL & EML-RL algorithms have superior competence in detecting an emulation attack model compared to the other existing techniques with respect to the various approximation parameters like rate of attack estimation, overall errors perception, energy consumption rate and the learning efficacy in a dynamic and mobile CR network.

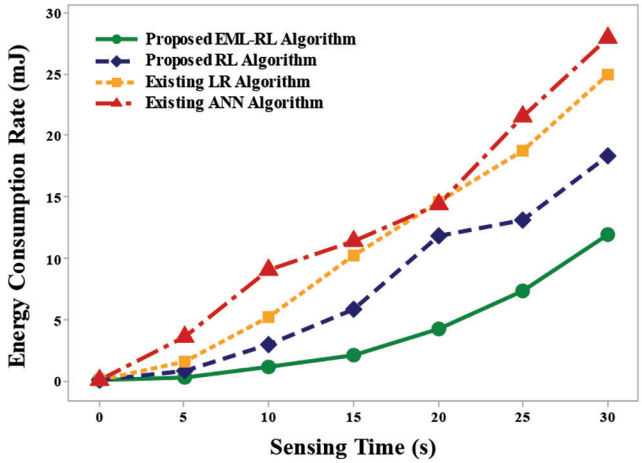

Figure 12: Energy consumption rate *vs.* sensing time

7 Conclusion

In this paper, investigations have been carried out to assess various methods & its efficiency factors in detecting the PUEA in a dynamic cognitive radio network. The two advanced attack estimation schemes that have been proposed to detect and prevent PUEA in a mobile user network environment are meticulously examined using machine learning algorithms and the performance results have been recorded for comparison. The machine learning algorithms have been observed to possess better learning ability and higher accuracy in detecting the PUEA compared to the existing methods. These efficient learning algorithms with low complex improved detection rate have been formulated to be applied in dynamic cognitive radio environment. The proposed methodologies offer minimum error rate with superior energy efficiency owing to optimized sensing time that can be applied in multiple attack scenarios. The future extension of this research work is to analyze the efficacy of deep learning over machine learning for detecting PUEA in a mobile user cognitive radio environment.

Funding Statement: The authors received no specific funding for this study

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Li, C. Han, M. Wang, H. Chen and L. Xie, "A primary user emulation attack detection scheme in cognitive radio network with mobile secondary user," in *2016 2nd IEEE Int. Conf. on Computer and Communications (ICCC)*, Chengdu, pp. 1076–1081, 2016.

[2] Y. Zhao, J. Huang, W. Wang and R. Zaman, "Detection of primary user's signal in cognitive radio networks: Angle of Arrival based approach," in *2014 IEEE Global Communications Conf.*, Austin, TX, USA, pp. 3062–3067, 2014.

[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] G. Jakimoski and K. P. Subbalakshmi, "Denial-of-service attacks on dynamic spectrum access networks," in *ICC Workshops - 2008 IEEE Int. Conf. on Communications Workshops*, Beijing, China, pp. 524–528, 2008.

[5] V. Jayasree and R. Suganya, "A survey on primary user emulation detection mechanisms in cognitive radio networks," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 14, no. 2, pp. 1209–1216, 2014.

[6] D. Salam, A. Taggu and N. Marchang, "An effective emitter-source localization-based PUEA detection mechanism in cognitive radio networks," in *2016 Int. Conf. on Advances in Computing, Communications and Informatics (ICACCI)*, Jaipur, India, pp. 2557–2561, 2016.

[7] A. Karimi, A. Taherpour and D. Cabric, "Smart traffic-aware primary user emulation attack and its impact on secondary user throughput under rayleigh flat fading channel," *in IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 66–80, 2020.

[8] A. Banerjee and S. P. Maity, "On energy minimization in cooperative spectrum sensing using LRT in presence of emulation attack," in *2016 IEEE Int. Conf. on Advanced Networks and Telecommunications Systems (ANTS)*, Bangalore, India, pp. 1–6, 2016.

[9] D. Das and N. Behera, "Adaptive resource allocation for cognitive radio-enabled smart grid network," *Advances in Electrical Control and Signal Systems. Lecture Notes in Electrical Engineering*, vol. 665, pp. 1–8, 2020.

[10] X. Xie and W. Wang, "Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding," *Procedia Computer Science*, vol. 21, no. 2, pp. 430–435, 2013.

[11] 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, 2018.

[12] Y. Zheng, Y. Chen, C. Xing, J. Chen and T. Zheng, "A scheme against primary user emulation attack based on improved energy detection," in *2016 IEEE Int. Conf. on Information and Automation (ICIA)*, Ningbo, China, pp. 2056–2060, 2016.

[13] N. Usha, K. V. Reddy and N. N. Nagendra, "Dynamic spectrum sensing in cognitive radio networks using ml model," in *2020 Third Int. Conf. on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, pp. 975–979, 2020.

[14] Q. Song, S. Guo, X. Liu and Y. Yang, "CSI amplitude fingerprinting based NB-IoT indoor localization," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1494–1504, 2017.

[15] X. Lin, "Positioning for the Internet of Things: A 3GPP perspective," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 179–185, 2017.

[16] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe and A. Ghosh, "NB-IoT system for M2M communication," in *IEEE Wireless Communications and Networking Conf. (WCNC)*, Doha, Qatar, pp. 428–432, 2016.