Defence Science Journal, Vol. 74, No. 4, July 2024, pp. 526-534, DOI : 10.14429/dsj.74.19468

An Efficient Spoofing Attack Detection Using Deep Learning-based Physical Layer Security Technique

Swethambri Mohan[#], Atchaya Annadurai[$], and K. Gunaseelan[#,*]

[#]*Department of Electronics and Communication, College of Engineering Guindy, Anna University, Chennai-600025, India*
[$]*Department of Electrical and Computer Engineering, University of California, Irvine-92697, United States*
[*]*E-mail: guna_2012@yahoo.co.in*

ABSTRACT

Spoofing attack detection plays a crucial role in the defence field, involving critical and highly secured data processing. The accurate attack detection mechanism prevents unauthorised access to sensitive information, thereby protecting National security. Physical Layer Security (PLS) is a promising emerging technique that uses the wireless channel's randomness to secure the communication network. The spoofing attack is one of the severe threats to the wireless network, where the attacker imitates the legitimate user to launch an attack against the network. This paper investigates the channel characteristics-based physical layer technique to detect spoofing attacks. For static radio environments, the two-sample independent hypothesis testing is used to identify the spoofing attack, showing an improvement in detection accuracy of 97 %**.** The attack detection problem is considered a Reinforcement Learning (RL) based classification problem for a challenging dynamic radio environment. It is simulated using the actor-critic-based Deep Reinforcement Learning (DRL) technique with the help of the Reformed Deep Deterministic Policy Gradient (Re-DDPG) algorithm. The simulated results show that the proposed method performs better than the existing strategies and achieves a Receiver Operating Characteristics (ROC) value of 0.96. The detection accuracy of the proposed method can reach up to 98 %, with precision and recall of about 98 % and 99 %, respectively.

Keywords: Deep learning; Physical layer authentication; Physical layer security; Reinforcement learning; Wireless communication; Wireless security

NOMENCLATURE

γ	: Mean
δ^2	: Variance
α	: Threshold significance level
D_F	: Degree of freedom
P_f	: Probability of false alarm
P_d	: Probability of detection

1. INTRODUCTION

Wireless communication is the transfer of information between transmitter and receiver through the wireless channel in the form of radio waves. It utilises modulation to encode information and antennas to transmit and receive signals between devices. It is important to secure a communication network to maintain the integrity of information or data. Cryptography is the most widely used technique to secure communication and data. To improve end-to-end security in a dynamic wireless environment, there is a need for secured algorithms to be implemented in the physical layer[3]. PLS uses channel characteristics and randomness of wireless channels to secure communication with the help of generation of artificial noise, dynamic key generation and channel-based authentication to enhance security and prevent unauthorised access.

The fifth-generation (5G) wireless networks significantly impact the life of humankind. For example, smart cities, autonomous driving, the Internet of Things (IoT), etc., are supported by 5G wireless technologies. Therefore, it is essential to consider the security and privacy of 5G wireless networks[1].

Attack detection and prevention is the major challenge in the areas where critical data are involved, like defence and military applications[6]. The security and privacy between the connected devices are significant challenges to the existing technologies[5]. Traditional cryptography-based security mechanisms are undesirable for resource-constrained applications like Wireless Sensor Networks (WSN) and Wireless Body Area Networks (WBAN). Since they introduce additional overhead in terms of computational time, latency in communication, and lack of key management, which may lead to high energy consumption in these applications. Due to this issue, currently, researchers are moving towards the PLS concepts[4].

Communications are vulnerable to many kinds of attacks. One of the common attacks is the attacker impersonates the legitimate entity pretending to be a legitimate user by changing their identity, known as a spoofing attack or identity deception attack, e.g., The impersonation of an attacker involves forging identities, spoofing Internet Protocol (IP) addresses, Medium Access Control (MAC) addresses to make an attacker look like a trusted entity[5]. The physical layer characteristics-

Received : 11 September 2023, Revised : 07 December 2023
Accepted : 16 January 2024, Online published : 24 July 2024

based authentication is a promising technology for wireless communication networks to mitigate this attack.

The spread spectrum technique used in Wireless Sensor Networks (WSN) has some drawbacks, such as key management, susceptibility to jamming, limited scalability, etc., and these disadvantages lead to an underestimation of the system's security[11]. Currently, PLS techniques use hypothesis test methods to compare the Channel Frequency Responses (CFR) of the received messages for authentication with that of the original CFR[6]. The physical layer spoofing detection accuracy depends on the test threshold in the hypothesis test performed at the receiver. It is difficult for the receiver to choose a proper test threshold in the spoofing detector without knowing the exact values of the channel parameters in a dynamic radio environment[9-10].

The attack detection schemes in PLS are classified into hardware-based and channel-based techniques. Hardware-based techniques are energy-based attack detection and spectrum sensing. The channel-based techniques involve Channel State Information (CSI) as a feature and traffic pattern analysis to detect the attack with the help of statistical hypothesis testing[7].

Recent advancements prove that Machine Learning (ML) and Artificial Intelligence (AI) have been widely used in security. With the help of intelligent algorithms, security researchers have improved the attack detection models and enhanced their ability to detect malicious events more accurately[8-9].

To mitigate the existing drawbacks, the proposed work focuses on developing a robust and continuous spoofing attack detection algorithm in a real-time scenario. The channel-based PLS technique, along with the DRL model, a combination of Deep Learning (DL) with RL principles, enables an agent to learn and make decisions in complex and dynamic environments, resulting in the improvement of accuracy and adaptability for the proposed attack detection scheme.

1.1 Objectives of the Paper

- This paper proposes a novel DL based PLS technique to detect spoofing attacks.
- A two-sample hypothesis testing-based spoofing attack detection is performed for a static radio environment and its performance has been analysed.
- A novel approach of Deep Reinforcement Learning (DRL) based Reformed Deep Deterministic Policy Gradient (Re-DDPG) algorithm is proposed to detect spoofing attacks for the dynamic radio environment.
- The performance of proposed algorithm has been analysed by simulation and observed that the accuracy is improved to 98 % with a 3 % false positive rate.

The remaining paper is organised as the Proposed methodology to detect the spoofing attack in static and dynamic radio environments, data visualisation, clustering analysis, Reinforcement learning, Re-DDPG algorithm development for spoofing attack detection, and results and discussions of the proposed method.

2. METHODOLOGY

2.1 Static Radio Environment

The wireless network with N legitimate users (N_L) and M attackers (M_A) is considered. A two-sample independent hypothesis test is used to detect spoofing attacks in a static wireless environment. The principle of hypothesis testing is, it analyses wireless channels characteristics and compares two samples to determine whether the signal comes from a legitimate user or an attacker. The one sample represents null hypothesis(no spoofing) and the other represents alternative hypothesis(presence of spoofing). The wireless channel feature obtained is the Received Signal Strength Information(RSSI). The null hypothesis(H_n) indicates no significant difference between the mean RSSI values of legitimate users and attackers. The alternative hypothesis(H_a) indicates the difference between legitimate users and attackers. The RSSI values are collected, and the mean(γ) and variance(δ^2) of legitimate users and attackers are calculated. The attack detection test statistic is calculated as given in Eqn (1),

$$A_T = \frac{(\gamma_L - \gamma_A)}{\sqrt{\frac{\delta_L^2}{N_L} + \frac{\delta_A^2}{M_A}}} \tag{1}$$

The proposed attack detection statistic test calculates a t-distribution similar to the normal distribution in the presence of a more significant number of samples. The advantage of t-distribution is that it gives accurate results even for small variability of features. The degree of freedom is one of the characteristics of this distribution and is calculated as shown in Eqn. (2),

$$D_F = (N_L + M_A) - 2 \tag{2}$$

The significance level ($\alpha = 0.02$) is set to determine the critical threshold value (c_t). Using Eqns (1) and (2), the c_t is calculated, and the decision to distinguish a legitimate user and an attacker is calculated using Eqns (3) and (4),

$$S_0: P(A_T > c_t \mid H_n) \tag{3}$$

$$S_1: P(A_T < c_t \mid H_a) \tag{4}$$

Eqn (5) gives the Probability of False Alarm rate (P_f), which means the detection of an attack happening when there is no attack.

$$P_f = P(A_T > c_t \mid H_a) \tag{5}$$

The advantages of proposed spoofing attack detection in a static radio environment are adaptability to statistical properties of the wireless channel and early detection of spoofing attack with minimal variations in wireless channel features.

2.2 Dynamic Radio Environment

Compared to RSSI-based localisation in a static environment, the AoA and CSI features provide more accurate positioning of legitimate users and attackers to detect the spoofing attack in a dynamic radio environment.

2.2.1 Attack Model for Dataset Generation

Around 10,000 samples of data are generated for both attack and non-attack cases by simulating the attack scenario model. The dataset is developed in a laptop with Intel Core i5 with 16 GB RAM. The Orthogonal Frequency Division

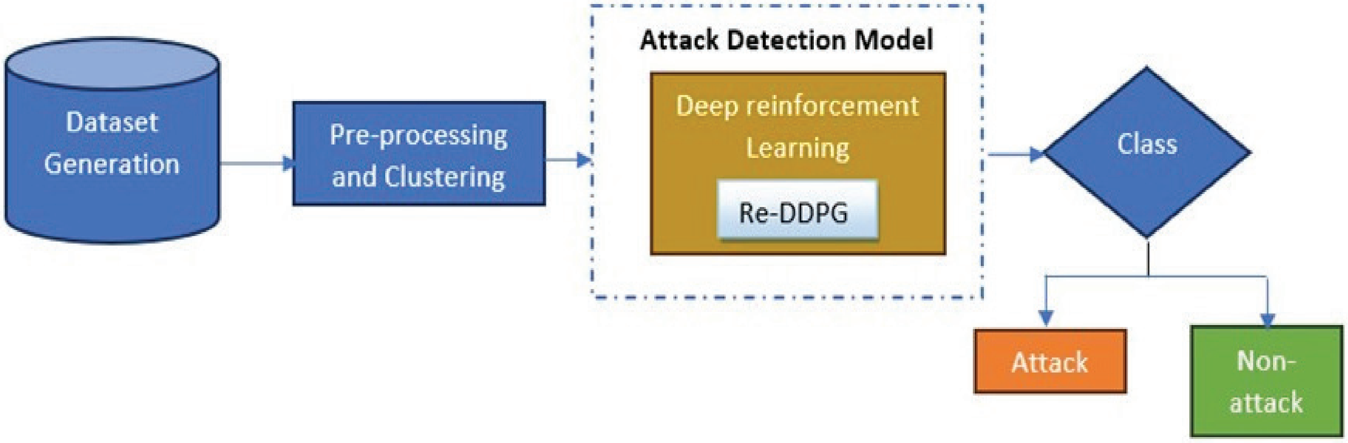


Figure 1. Proposed methodology for attack detection in dynamic radio environment.

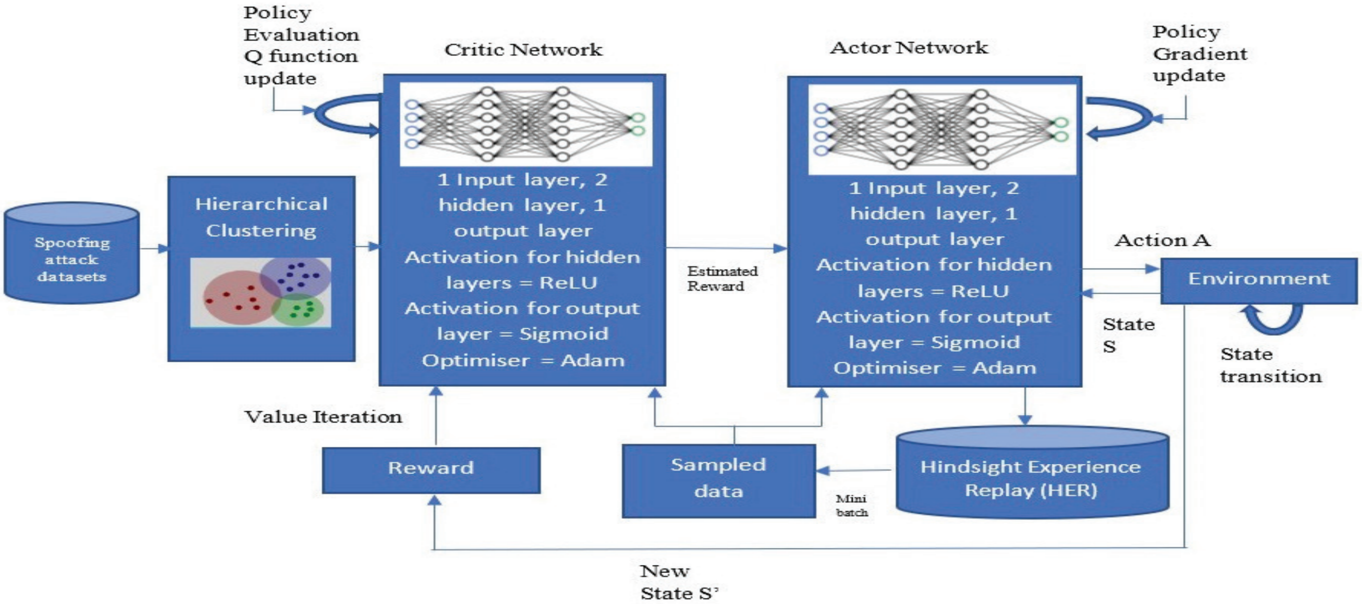

Policy Evaluation Q function update
Critic Network
Actor Network
Policy Gradient update
Spoofing attack datasets
Hierarchical Clustering
1 Input layer, 2 hidden layer, 1 output layer
Activation for hidden layers = ReLU
Activation for output layer = Sigmoid
Optimiser = Adam
Estimated Reward
1 Input layer, 2 hidden layer, 1 output layer
Activation for hidden layers = ReLU
Activation for output layer = Sigmoid
Optimiser = Adam
Action A
Environment
State S
State transition
Value Iteration
Reward
Sampled data
Mini batch
Hindsight Experience Replay (HER)
New State S'

Figure 2. Block diagram of proposed Re-DDPG-based attack detection model.

Multiplexing (OFDM) based wireless environment is modelled to generate spoofing attack scenario, as OFDM's multiple subcarrier nature allows attacker to introduce false signal similar to legitimate user. The non-attack case comprises the signal received at the Access Point (AP) from N legitimate users and the attack case comprises N legitimate users with one or multiple attackers falsifying the legitimate users. Since both legitimate users and attackers are assumed to be in different location the Angle of Arrival (AoA) is estimated to distinguish legitimate users and attackers as given in Eqns (6) and (7).

$$AoA_{non-attack} = \theta + R_s + \eta \qquad (6)$$

$$AoA_{attack} = \theta + R_s + \delta + \eta \qquad (7)$$

where, Θ represents the AoA of a legitimate user, R_S represents the reference signature of a legitimate user, δ represents the AoA for the attacker, and η represents the noise. The attacker manipulates the phase and can mimic the legitimate user. To identify this type of spoofing the CSI values are obtained for both non-attack and attack case from Eqns (8) and (9).

$$CSI_{non-attack} = \alpha e^{j\gamma} \qquad (8)$$

$$CSI_{attack} = \alpha e^{j(\gamma+\theta)} \qquad (9)$$

where, α represents the amplitude, γ represents the phase, and θ represents the continuous phase shift by the attacker. The attack and non-attack are labelled as '1' and '0', respectively.

To address AoA and CSI-based spoofing attack detection, the Access Point(AP) uses the Deep Reinforcement learning-based detection model using Re-DDPG to detect the received signal, as illustrated in the following sections. The proposed methodology for attack detection in dynamic radio environment is illustrated in Fig. 1. Fig. 2. shows the detailed block diagram of the proposed Re-DDPG-based attack detection model. The components of the blocks are explained in sections 3 and 4.

3. CLUSTERING

The datasets are generated, and the pre-processing techniques are performed. The pre-processing steps involve normalisation to rescale the features to a specific range between 0 and 1, and the standardisation is applied to the normalised features, which will have zero mean and unit variance. The dataset has been analysed using the Hierarchical clustering method.

Algorithm 1. Segmentation of spoofing attack dataset

```
Input: Datasets with n data points
1: Assign all data points to an individual cluster
2: Calculate the proximity matrix by finding the  Euclidean distance between n data points
3: Repeat 2 and update the proximity matrix till all the data points are assigned to its appropriate clusters
4: Calculate the Number of clusters using the Dendrogram tree diagram
5: Initialise the horizontal threshold line =2  at the tallest vertical line of the dendrogram plot
6: Number of clusters = Number of vertical lines that the horizontal threshold line intersects.
7: End clustering
Output: Clustered attack and non-attack datasets
```

Algorithm 2. Proposed spoofing attack detection algorithm

```
Initialize  D, $\pi$ , Q , $\pi$' , Q' , $\mu$, $H_R$, hyperparameters
for episode = 1 to K:
    Reset the environment
    Initialize state s , total reward = 0
for time step = 1 to max time steps:
            Choose a = $\pi$(s) + $\mu$
            Execute a and  observe s' and r
            Store (s, a, r, s', Flag ) in D
            Sample a minibatch from D and store in $H_R$
            Compute target Q values:
             for each sample ($s_i$, $a_i$, $r_i$, $s_i$, $Flag_i$) in          minibatch:
                 if $Flag_i$=True:
                     target_Q = $r_i$
                 else:
                     target_a = $\pi$'(s'$_i$)
                     target_Q = $r_i$ + $d_f$ * Q'(s'$_i$, target_a)
end for
            Update critic network Q by minimising loss:
             for each sample ($s_i$, $a_i$, $r_i$, s'$_i$, $Flag_i$) in minibatch:
        Q_l = (Q($s_i$, $a_i$) - target_Q)$^2$
            end for
            Update Q network using critic learning rate and backpropagation
            Update actor network $\pi$ using the sampled policy gradient:
     for each sample ($s_i$, $a_i$, $r_i$, s'$_i$, $Flag_i$) in minibatch:
                 predicted_a = $\pi$($s_i$)
        a_l = Q($s_i$, predicted_a)
           end for
             Update $\pi$ network using actor learning rate and backpropagation
             Update target networks using $H_R$:
              Soft update target actor network: $\pi$' = $\tau$ * $\pi$ + (1 - $\tau$) * $\pi$'
              Soft update target critic network: Q' = $\tau$ * Q + (1 - $\tau$) * Q'
end for
Update s = s'
end for
total reward += r
```

Table 3. Elaboration of symbols in Algorithm 2

Parameters	Description
D	Replay buffer
π	Actor-network
Q	Critic network
π'	Target actor-network
Q'	Target critic network
μ	Exploration noise
H_R	HER Experiences
d_f	Discount factor
K	Maximum episodes
s	Initial state
a	Action
s'	New state
r	Reward
i	Minibatch samples
Q_l	Critic loss
a_l	Actor loss

3.1 Hierarchical Clustering

Hierarchical clustering treats the data as each observation starts in its group, and then the pairs of clusters are merged as one set moves up the hierarchy. Hierarchical clustering bridges the gap from K-means such that it does not require an initial declaration of a number of clusters. The strengths of this algorithm are flexibility and interpretability with different types of datasets. The clustering algorithm for the developed dataset is provided in Algorithm 1.

4. REINFORCEMENT LEARNING

RL operates on the principle of learning from interaction with an environment to obtain better decision by rewarding correct behaviour for the particular scenario. It determines the optimal course of action for any given scenario and aims to maximise cumulative reward over time. It is performed to gain knowledge from its experience with the available datasets and performs well in a real-time scenario[2]. A policy-based reward maximisation Reformed Deep Deterministic Policy Gradient algorithm is proposed for the technique.

4.1 Reformed Deep Deterministic Policy Gradient (Re-DDPG)

DDPG is a reinforcement learning method that combines Deep Neural Network (DNN) with the concept of Q-learning and Policy gradients. Q- Learning learns the optimal action-value function known as the Q function. It uses a neural network to estimate the Q-value. Policy gradients map states to action. It updates the parameters of policy to obtain a deterministic policy function and maximises the cumulative reward. The combination of these two concepts, along with DNN, is the actor-critic technique DDPG. Since DDPG has a sparse reward problem where the agent's action results in a negative reward even after it reaches the end goal, this makes learning a challenging task for the agent to achieve the target. To address this issue, the proposed Re-DDPG uses an Adaptive Learning Rate (ALR) and Hindsight Experience Replay (HER) buffer to improve the training efficiency, thereby increasing the accuracy of the attack detection method. A Q-value network that receives input information from state and action and outputs the Q-value is the critic. The actor-network is trained with policy gradients to improve the reward. HER relabels the failed scenario as an attempt to achieve the goal by the agent so that the agent can get trained effectively.

The ALR improves the stability and convergence speed. Adaptive Moment Estimation (ADAM) optimisation technique is used here, which utilises mean and variance in the data to optimise the model for better performance. The proposed spoofing attack detection algorithm is shown in Algorithm 2. Re-DDPG employs two additional methods from DDPG and DQN[2]:

It uses two target networks, namely the Target Q network for the critic and the Target policy network for the actor. This maximises training stability by allowing target networks to update gradually. It utilises an adaptive learning rate.

Hindsight Experience Replay (HER) is employed. It allows the agent to learn from past experiences. The learning is performed by sampling prior experiences.

These experiences are collected when the agent starts learning from the environment. The sampled batches of data, known as mini batch, are sent to actor and critic networks.

Additionally, it changes the weights in the model at each step, allowing the model to adapt to a dynamic environment immediately. Allocating continuous resources and migrating bandwidth are continual problems, but detecting whether the signal comes from a legitimate user or an attacker is a discrete variable problem. Therefore, the proposed Re-DDPG, which could tackle discrete and continuous problems, is employed and used for spoofing attack detection. Table 3 provides elaboration of symbols mentioned in Algorithm 2.

Figure 3 illustrates the flow of the proposed spoofing attack detection model. The actor neural network gets the states as input, and their corresponding outputs are states with their policy functions. The critic neural network takes the states and actions as input, and the output is the states and actions concerning the Q network. The Q value estimates the decision of the input, whether it is an attack or a legitimate one.

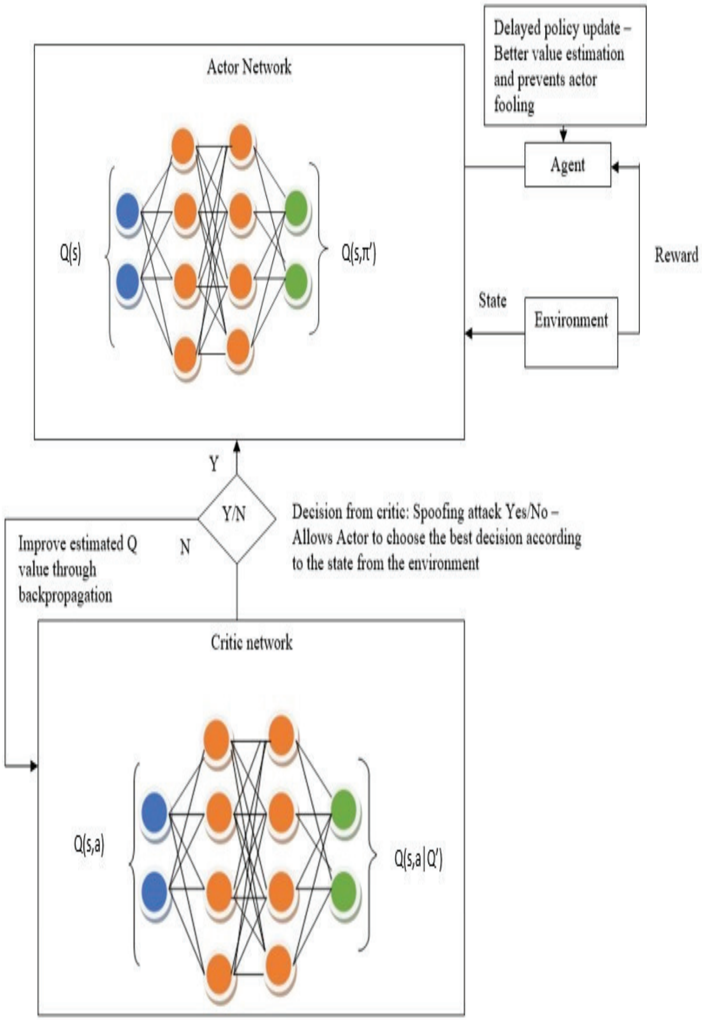

Delayed policy update – Better value estimation and prevents actor fooling
Actor Network
Agent
Q(s)
Q(s,π')
Reward
State
Environment
Y
Y/N
N
Decision from critic: Spoofing attack Yes/No – Allows Actor to choose the best decision according to the state from the environment
Improve estimated Q value through backpropagation
Critic network
Q(s,a)
Q(s,a|Q')

Figure 3. Flow diagram of proposed spoofing attack detection model.

5. RESULTS AND DISCUSSIONS

5.1 Static Radio Environment

The results are implemented using Spyder IDE and developed in Python. Figure 4 compares the Probability of a false alarm (P_f) with the Probability of detection (P_d) for the traditional and proposed scheme in static radio environment. It is evident from the simulation result that the obtained features give better spoofing detection results than the conventional scheme[1].

5.2 Dynamic Radio Environment

Figure 5 and Fig. 6 show the spoofing attack detection simulation results for a Dynamic radio environment for the proposed Re-DDPG method using the developed dataset.

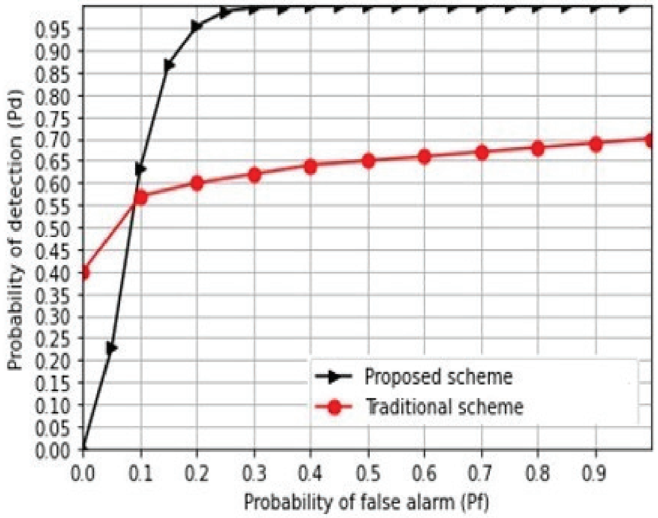


Figure 4. P_f VS P_d for the traditional and proposed scheme in static radio environment.

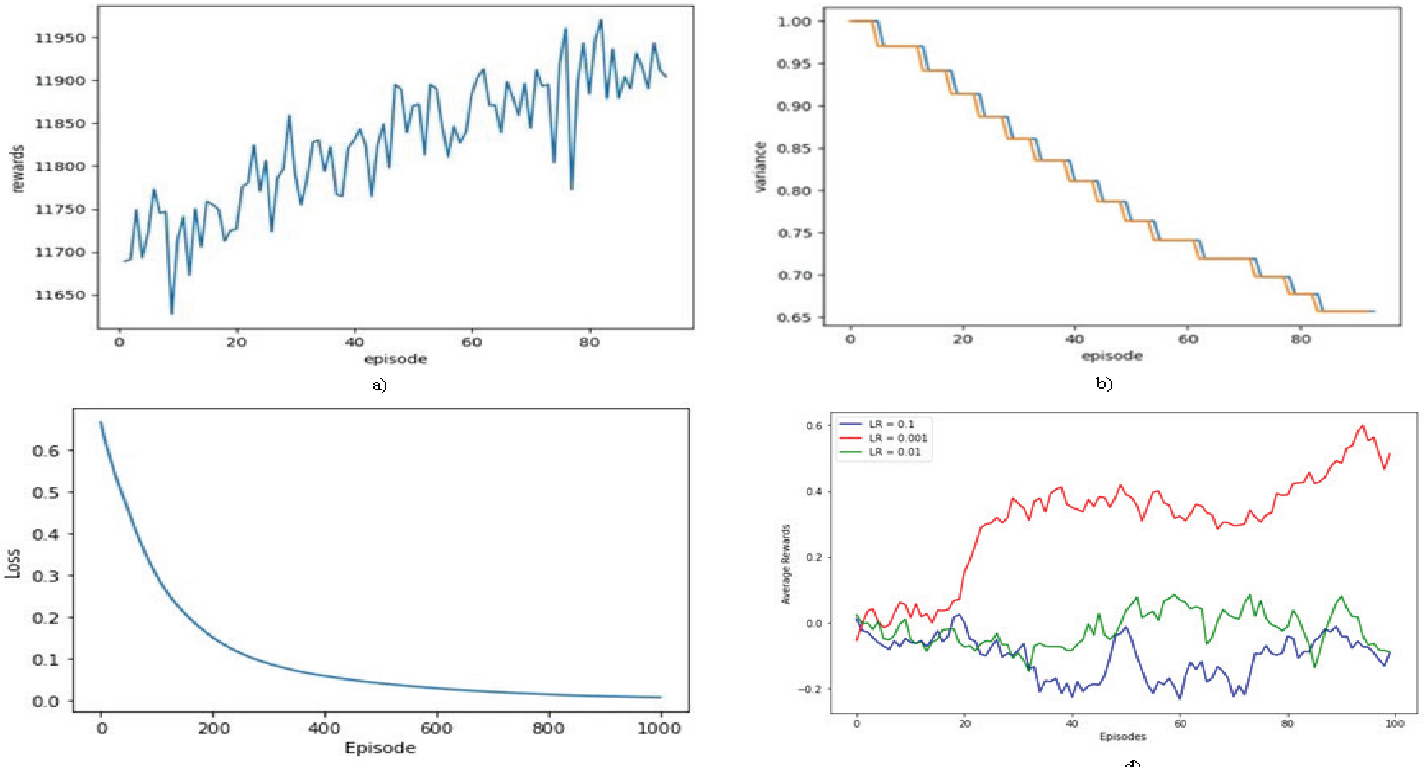
5.2.1 Graphical Results

Figure 5 and Fig. 6 shows the simulation results of the proposed Re-DDPG algorithm to detect spoofing attacks in a dynamic radio environment. Figure 5(a) compares Episodes and Rewards. It shows that increases in rewards till a maximum value of 11950 for 100 episodes conclude that the agent correctly classifies attack and non-attack cases even for a few episodes and requires less computational time for prediction. Figure 5(b) compares Episodes and variance. It illustrates the decrease in variance plots (1-0.65) for each episode (0-100), indicates that the agent's performance is becoming stable and consistent for an increased number of episodes.

Figure 5(c) is the comparison between Episodes and Loss. It gives the decrease in loss curve with an increase in the number of episodes. It indicates that the agent can refine its policy and estimate better values of action for the given state in a real-time environment. The Table 4. gives corresponding loss values for particular episode. From Table 4 it can be seen that the loss value starts decreasing from 100th episode. Figure 5(d) shows the average rewards for various learning

Table 4. Loss values for corresponding episode ranges

Episode number	Loss value
50	0.4531
100	0.2995
200	0.1510
400	0.0875
600	0.0284
800	0.0135
1000	0.0063



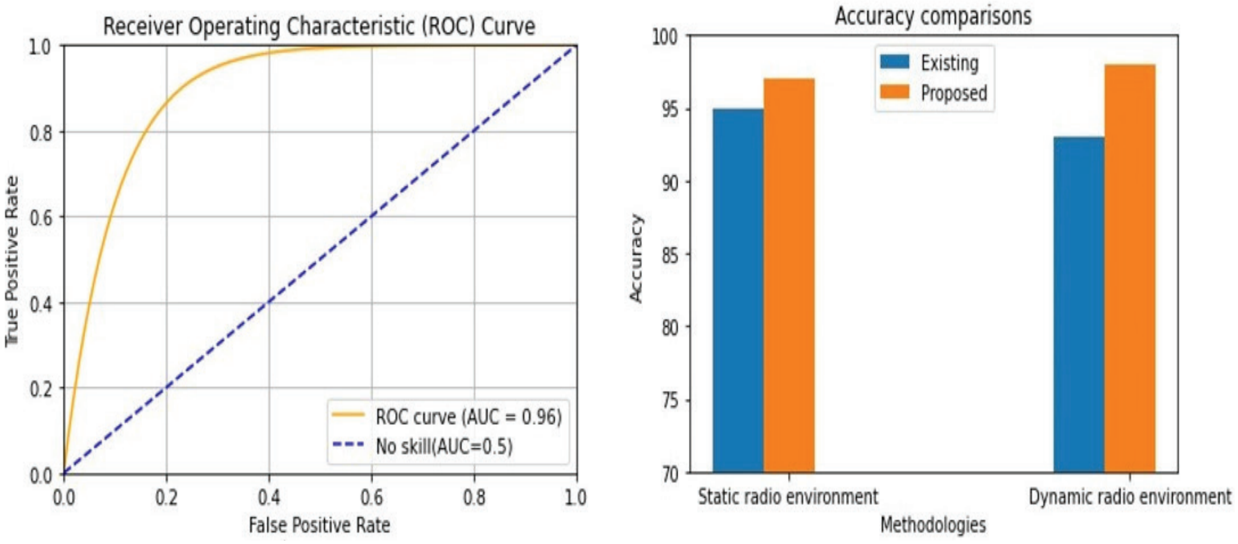
a)

b)

Figure 5. Measured metrics with respect to episodes; (a) Episodes vs. Rewards of DRL; (b) Episode vs. Variance of DRL; (c) Episode vs. Loss of DRL; (d) Average rewards for different learning rates.

Table 5. List of Hyperparameters utilized for the proposed spoofing attack detection model

Hyperparameters	Value	Impact
Learning rate of actor	0.001	To converge at the optimal solution given by a critic
Learning rate of critic	0.001	Step size to estimate reward optimally
Reward discount	0.99	Plays a role in the agent's decision-making process
Mini Batch size	64	Number of transition samples to update actor and critic
Tau	0.001	Stability and convergence of the algorithm
Activation function in Hidden layer	ReLU	To reduce the computational load
Activation function in Output layer	Sigmoid	To make class predictions
Loss function	Binary cross entropy	For attack and non-attack classification



(a) (b)

Figure 6. Performance measures; (a) ROC curve for the proposed model and (b) Accuracy comparison for the existing and proposed model.

rates(0.1,0.001,0.1). The cumulative rewards increase for the value 0.001, and the algorithm adapts the agent to learn at this rate for improved performance.

5.2.2 Evaluation Metrics

Table 5 lists the values of the defined hyperparameters for the proposed Re-DDPG based spoofing attack detection model. The standard evaluation metrics are considered for the spoofing attack detection model[20].

Figure 6 illustrates the performance measures of the proposed method. Figure 6(a) shows the Receiver Operating Characteristics (ROC) for the proposed model. It is a graphical measure that distinguishes the data between attack and non-attack cases with the help of a decision threshold value set to 0.5, indicating the importance of both positive and negative classes.

The area under the ROC(AUC-ROC) curve quantifies the overall performance of the attack detection model. A higher AUC indicates better discrimination. The AUC value of Re-DDPG (0.96) indicates that the proposed model classifies and detects spoofing attacks with a high accuracy rate. Table 6 gives the results of the evaluation metrics for the developed model.

Figure 6(b) illustrates the accuracy comparisons for the proposed and existing model in static[1] and dynamic radio environments. The proposed hypothesis test gives a 97 % accuracy rate for a static environment. For a dynamic radio environment, the proposed Re-DDPG method's accuracy reaches up to 98 % compared to the existing method[2].

Table 6. Evaluation metrics

Metrics	Formula	Value in percentage
Accuracy	(TP+TN)/(TP+TN+FP+FN)	97.9
Precision	TP/(TP+FP)	97.8
Recall	TP/(TP+FN)	98.5
F1 score	(2*Recall*Precision)/ (Recall+Precision)	98.3
Sensitivity	TP/(TP+FN)	98.47
Specificity	TN/(TN+FP)	97.3

6. CONCLUSION

A new approach to detect the spoofing attack using wireless channel characteristics has been proposed, which uses a two-sample independent hypothesis test and reinforcement-based Re-DDPG algorithm. The proposed methods for both static and dynamic radio environments have achieved a spoofing detection accuracy of 97 % and 98 %, respectively.

The proposed DRL technique using the Re-DDPG algorithm and the ADAM optimisation technique for dynamic radio environments can handle sparse data in noisy environments. This achieved high detection accuracy with a lower false detection rate, significantly better than the existing Q-learning technique. The ROC value of 0.96 confirms that the proposed method has high performance in enabling reliable and secured communication in a dynamic wireless environment. The high recall and sensitivity values of 99% minimise the false negatives, which makes the proposed method solve continuous action space problems in a dynamic environment and give the exact actions for each dynamic state in a deterministic way. Overall, this approach shows great promise for effectively identifying and classifying security threats, improving the accuracy of channel characteristics based on spoofing attack detection in both static and dynamic radio environments.

REFERENCES

1. Li, W.; Wang, N.; Jiao, L.; & Zeng, K. Physical layer spoofing attack detection in Mm Wavemassive MIMO 5G networks. *IEEE Access*, 2021, **9**, 60419-60432, doi:10.1109/ACCESS.2021.3073115.
2. Xiao, L.; Li, Y.; Han, G.; Liu, G.; & Zhuang, W. PHY-Layer spoofing detection with reinforcement learning in wireless networks. *IEEE Trans. on Vehicular Techn.*, 2016, **65**(12), 10037-10047. doi:10.1109/TVT.2016.2524258.
3. Nooraiepour, A.; Bajwa, W.U. & Mandayam, N.B. Learning-aided physical layer attacks against multicarrier communications in IoT. *IEEE Trans. on Cognitive Commu. and Netw.*, 2021, **7**(1), 239–254. doi:10.1109/TCCN.2020.2990657.
4. Wang, N.; Li, W.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; & Zeng, K. Physical layer authentication for 5G communications: Opportunities and road ahead. *IEEE Network*, 2020, **34**(6), 198-204. doi:10.1109/MNET.011.2000122.
5. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; & Zeng, K. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet of Things J.*, 2019, **6**(5), 8169–8181. doi:10.1109/JIOT.2019.2927379.
6. Lavanya, D.; Ramaprabha, R.; & Gunaseelan, K. Privacy preserving physical layer authentication scheme for LBS based wireless networks. *Def. Sci. J.*, 2021, **71**(2), 241-247. doi:10.14429/dsj.71.15355.
7. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; &Gurtov, A. Overview of 5G security challenges and solutions. *IEEE Comm. Stand. Magazine*, 2018, **2**(1), 36–43. doi:10.1109/MCOMSTD.2018.1700063.
8. Zhang, T.; & Mao, S. Energy-efficient power control in wireless networks with spatial deep neural networks. *IEEE Trans. on Cog.Commu. and Netw.*, 2020, **6**(1), 111–124. doi:10.1109/TCCN.2019.2945774.
9. Dorner, S.; Cammerer, S.; Hoydis, J.; & Brink, S.T. Deep learning basedcommunication over the air. *IEEE J. Sele. Topics in Sig. Proce.*, 2018, **12**(1), 132–143. doi:10.1109/JSTSP.2017.2784180.
10. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.K.; & Gao, X. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE J. on Sele. Areas in Commu.*, 2018, **36**(4), 679–695, doi:10.1109/JSAC.2018.2825560.
11. O'Shea, T.; & Hoydis, J. An introduction to deep learning for the physical layer. *IEEE Trans. on Cog.Commu. and Netw.*, 2017, **3**(4), 563–575. doi:10.1109/TCCN.2017.2758370.
12. Sureka, N. & Gunaseelan, K. Investigations on detection and prevention of primary user emulation attack in cognitive radio networks using extreme machine learning algorithm. *J. of Ambient Intel. and Human. Compu.,* 2021. doi:10.1007/s12652-021-03080-5.
13. Wang, N.; Jiao, L.; Wang, P.; Li, W.; & Zeng, K. Machine learning-based spoofing attack detection in MmWave 60GHz IEEE 802.11ad networks. *In* Proceedings of the IEEE Conference on Computer Communications, Toronto, ON, Canada, 2020. doi:10.1109/INFOCOM41043.2020.9155382.
14. Wang, N.; Jiao, L.; Wang, P.; Dabaghchian, M.; & Zeng, K. Efficient identity spoofing attack detection for IoT in mm-Wave and massive MIMO 5G communication. *In* Proceedings of the IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018. doi:10.1109/GLOCOM.2018.8647707.
15. Zeng, K. Physical layer key generation in wireless networks: challenges and opportunities. *IEEE Commun. Magazine*, 2015, **53**(6), 33–39. doi:10.1109/MCOM.2015.7120014.
16. Yue, Wu.; Tao, Jing.; Qinghe, Gao.; Yingzhen, Wu.; & Yan, Huo. Game-theoretic physical layer authentication for spoofing detection in internet of things. *Digital Commun. Networks*, 2023. doi:10.1016/j.dcan.2022.12.016.
17. Yılmaz, M.H. & Arslan. H. A survey: Spoofing attacks in physical layer security *In* Proceedings of the IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), Clearwater Beach, FL, USA,2015, doi:10.1109/LCNW.2015.7365932.
18. Yengi, Y.; Kavak, A. & Arslan, H. Physical layer detection of malicious relays in LTE-A network using unsupervised learning. *IEEE Access*, 2020, **8**, 154713–154726,. doi:10.1109/ACCESS.2020.3017045.

ACKNOWLEDGEMENT

This research is supported by State University Research Excellence(SURE) scheme under Science and Engineering Research Board(SERB), New Delhi. (Project file number: SUR/2022/004874)

CONTRIBUTORS

Ms. Swethambri Mohan is pursuing a PhD in Electronics and Communication at the College of Engineering, Guindy, Anna University, Tamil Nadu, India. She received her ME degree in Embedded system technologies from the College of Engineering Guindy, Anna University, Tamil Nadu, India, in 2019. Her main research interests are information security, wireless communication, deep learning and machine learning algorithms.

Her contribution to this paper includes: Conceptualisation, mathematical formulation, implementation of the proposed technique and preparation of manuscripts.

Ms. Atchaya Annadurai obtained her BE in Electronics and Communication from the College of Engineering Guindy, Anna University, Tamil Nadu, India. Her areas of interest are wireless communication, machine learning and security algorithms.

Her contribution to this paper includes: Data preparation, data analysis and implementation of the proposed technique.

Dr K. Gunaseelan is working as a Professor with the Department of Electronics and Communication, College of Engineering Guindy, Anna University, Chennai, India. He obtained his PhD degree from Anna University, Chennai. His research interests include: Digital signal processing, wireless communication systems, information security and machine learning.

His contributions to this paper include: Overall conceptualisation, analysis of results and manuscript preparation.