Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 5 (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Layer-Level Security Enhancement in 5G Networks Using Deep Reinforcement Learning Techniques

R. Sundar[*1], Arram Sriram[2], Dr. S. Surendran[3], Dr. N. Gayathri[4], Palagati Anusha[5], Kiran Kishore O[6], Ragul Vignesh M. , Gaurav Dhiman[8]

[*1]Assistant Professor, Department of Marine Engineering, AMET Deemed to be University.
Email: sundar.r@ametuniv.ac.in

[2]Department of CSE, Faculty of Science and Technology (Icfai Tech), ICFAI Foundation for Higher Education, Hyderabad, India, 501203.
Email: Arram.sriram@gmail.com

[3]Professor, Department of Computer Science and Engineering, Tagore Engineering College, Chennai, India.
Email: suren.subbaraj@gmail.com

[4]Associate Professor, Veltech Hightech Dr.Rangarajan Dr.Sakunthala Engineering College
Email: gayathrimechanical@gmail.com

[5]Full - Time Research Scholar, CSE., SNSCT, Email: palagatianushareddy@gmail.com

[6]Full - Time Research Scholar, CSE, SNSCT., Email: o.kirankishore@gmail.com

[7]Assistant Professor, Department of Computer Science and Engineering
Nehru Institute of Engineering and Technology, Coimbatore.
Email: ragulvignesh@gmail.com

[8]School of Sciences and Emerging Technologies, Jagat Guru Nanak Dev Punjab State Open University, Patiala, India.
Email: gdhiman0001@gmail.com

***Corresponding Author:**
Email: sundar.r@ametuniv.ac.in

Cite this paper as: R. Sundar, Arram Sriram, Dr. S. Surendran, Dr. N. Gayathri, Palagati Anusha, Kiran Kishore O, Ragul Vignesh M., Gaurav Dhiman, (2025) Layer-Level Security Enhancement in 5G Networks Using Deep Reinforcement Learning Techniques. *Journal of Neonatal Surgery*, 14 (5), 249-257.

ABSTRACT

The advent of 5G technology has paved the way for unprecedented connectivity and efficiency in Internet of Things (IoT) networks. However, the inherent vulnerabilities in the physical layer of 5G pose significant security challenges. As 5G becomes the backbone of IoT ecosystems, the physical layer becomes susceptible to various security threats, including jamming attacks, signal interference, and unauthorized access. Traditional security measures fall short in dynamically adapting to these evolving threats, necessitating the exploration of innovative approaches such as DRL. Existing literature lacks a comprehensive exploration of applying DRL to secure the physical layer of 5G for IoT networks. This research seeks to bridge this gap by investigating the efficacy of DRL algorithms in autonomously enhancing security measures based on real-time threat assessments. This research aims to address these concerns by leveraging deep reinforcement learning (DRL) techniques to fortify the security of the physical layer in 5G-enabled IoT networks. The proposed methodology involves developing and training DRL agents to adaptively optimize physical layer parameters in response to potential security threats. Simulations will be conducted in a controlled environment to evaluate the performance and robustness of the DRL-based security framework. The chosen DRL algorithms will be fine-tuned to achieve optimal results in mitigating specific threats encountered in 5G IoT networks. The results include a demonstrable improvement in the security posture of the 5G physical layer, with the DRL-based approach effectively countering jamming attacks, mitigating interference, and proactively adapting to emerging threats. The findings of this research contribute valuable insights into the feasibility and effectiveness of integrating DRL into 5G IoT security frameworks.

Keywords: *IoT, 5G, Physical Layer Security, Deep Reinforcement Learning, Network Threats*

1. INTRODUCTION

The proliferation of 5G technology has ushered in a new era of connectivity, enabling the seamless integration of diverse devices in Internet of Things (IoT) networks [1]. However, this advancement brings with it unprecedented challenges, particularly in securing the physical layer of 5G networks [2]. The physical layer, being the foundation of communication, is susceptible to a myriad of security threats that demand innovative solutions to safeguard the integrity and reliability of 5G-enabled IoT systems [3].

The 5G physical layer faces challenges such as signal interference, jamming attacks, and unauthorized access, which can compromise the confidentiality and availability of critical data [4]. Traditional security measures have limitations in adapting dynamically to these evolving threats, necessitating a paradigm shift in security strategies [5]. This research addresses the pressing need to enhance the security of the physical layer in 5G IoT networks [6]-[7].

This research introduces a novel approach by integrating DRL into the security framework of the 5G physical layer for IoT networks. The use of DRL adds a layer of adaptability and intelligence, enabling the system to learn and respond autonomously to emerging threats. The contributions of this research lie in providing a comprehensive understanding of the security landscape in 5G IoT networks, proposing an innovative DRL-based solution, and validating its efficacy through rigorous evaluations. Ultimately, the findings aim to contribute to the development of robust security measures for the next generation of IoT networks.

2. RELATED WORKS

Researchers have explored the use of Q-learning algorithms such as bandwidth and power to enhance network performance and efficiency. Deep Q-networks have been employed to optimize various aspects of 5G networks, including handover decision-making, network slicing, and radio resource management. The deep learning component allows for better handling of complex and dynamic network environments [8].

PPO, a policy optimization algorithm, has been investigated for its potential in traffic management and load balancing in 5G networks. This includes dynamically adjusting network parameters to accommodate varying traffic patterns and demands [9].

Actor-Critic models have been applied to enhance Quality of Service in 5G networks. These models learn policies for actors to make decisions while the critic evaluates the outcomes, helping to optimize network parameters for improved QoS [10].

In scenarios where, multiple entities (e.g., base stations) need to coordinate actions, multi-agent reinforcement learning approaches have been explored. These models facilitate cooperation among network entities to optimize overall network performance [11].

Beamforming is a critical aspect of 5G communication. Deep reinforcement learning techniques have been employed to optimize beamforming strategies, adapting to changing channel conditions and improving communication efficiency [12].

Reinforcement learning has been utilized for intrusion detection and security in 5G networks. Agents are trained to identify and respond to anomalous activities, enhancing the overall security posture of the network [13].

3. METHODS

The research involves creating and training DRL agents as in Figure 1. These agents are designed to autonomously adapt and optimize parameters at the physical layer of 5G networks in response to potential security threats. The focus is on the physical layer, which is foundational to communication in 5G. The DRL agents are programmed to dynamically adjust key parameters in the physical layer. This adaptability is crucial for responding to real-time security threats, such as jamming attacks, interference, and unauthorized access. To assess the performance and robustness of the DRL-based security framework, simulations are conducted in a controlled environment. This controlled setting allows for a systematic evaluation of how well the DRL agents respond to simulated security threats. The selected DRL algorithms are fine-tuned to achieve optimal results in mitigating specific threats commonly encountered in 5G IoT networks. This process involves refining the learning mechanisms of the DRL agents to ensure effective and efficient responses to security challenges.

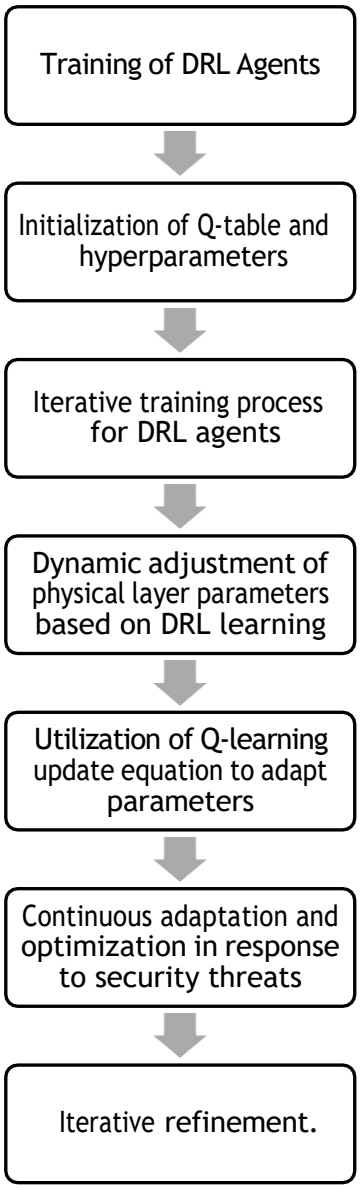

Figure 1: Proposed Framework

3.1. Training DRL agents

Training DRL agents involves a process where these agents learn to make decisions and take actions in an environment through trial and error, with the ultimate goal of optimizing a specific objective. In the context of securing the physical layer of 5G for IoT networks, training DRL agents is essential for them to autonomously adapt to varying security threats.

The research defines a simulated environment that mirrors the characteristics and challenges of the 5G physical layer for IoT networks. This environment serves as the playground where DRL agents will learn to navigate and make decisions. It determines how the state of the environment will be represented to the DRL agents. In the case of securing the physical layer, relevant information such as signal strength, network traffic, and potential security threats would be essential components of the state.

It specifies the possible actions that DRL agents can take in response to the observed state. Actions could include adjusting transmission parameters, reconfiguring network settings, or implementing security measures. It defines a reward system that provides feedback to the DRL agents based on their actions. Rewards serve as a mechanism for the agents to understand the consequences of their decisions. In the context of security, positive rewards may be given for effectively countering threats, while negative rewards may be assigned for failing to do so.

It selects a specific DRL algorithm for training the agents. Common algorithms include Q-learning, Deep Q Networks (DQN), Policy Gradient methods, and actor-critic models. The choice depends on the complexity of the problem and the

desired learning approach. It iteratively expose the DRL agents to the environment, allowing them to take actions, receive rewards, and update their internal policies based on the experienced outcomes. This process continues for multiple iterations until the agents demonstrate effective decision-making. It fine-tunes the DRL agents' parameters and update their policies to improve their performance. This may involve adjusting learning rates, exploration-exploitation strategies, and other hyperparameters to enhance the agents' ability to learn and adapt.

The Q-function (Q-value) represents the expected cumulative reward for taking action a in state s:$Q(s,a)$

The Q-learning algorithm updates the Q-values based on the observed reward (R), the current estimate of the maximum future Q-value ($maxQ(s',a')$), and a learning rate (α):

$Q(s,a) \leftarrow (1-\alpha) \cdot Q(s,a) + \alpha \cdot (R + \gamma \cdot \max a' \, Q(s',a'))$

Where:

$Q(s,a)$ is the Q-value for state s and action a.

α is the learning rate

R is the immediate reward obtained after taking action a in state s.

γ is the discount factor.

$maxa'Q(s',a')$ is the maximum Q-value for the next state s' and all possible actions a'.

To balance exploration and exploitation, an epsilon-greedy strategy is often used. With probability ϵ, the agent chooses a random action (exploration), and with probability $1-\epsilon$, it selects the action with the highest Q-value (exploitation).

3.2. Adaptive Optimization of Physical Layer Parameters

Adaptive Optimization of Physical Layer Parameters refers to the dynamic adjustment and fine-tuning of key parameters at the physical layer of a communication system. In the context of securing the physical layer of 5G for IoT networks using Deep Reinforcement Learning (DRL), this adaptation is driven by the learning capabilities of the DRL agents. Here a breakdown of the concept:

3.2.1. Physical Layer Parameters:

The physical layer of a communication system involves various parameters that govern the transmission and reception of signals. These parameters may include but are not limited to signal power, modulation schemes, coding rates, and frequency bands. Adaptive optimization involves the real-time adjustment of these parameters based on the evolving conditions of the network.

In security, the adaptive optimization aims to respond dynamically to security threats that may manifest at the physical layer. For instance, in the face of a jamming attack or signal interference, the DRL agents would autonomously adapt physical layer parameters to mitigate the impact of these threats. This learning process allows the agents to associate specific actions with positive outcomes in terms of security, enabling them to adapt their strategies over time.

The adaptation is continuous and ongoing. As the network environment evolves or encounters new security challenges, the DRL agents continuously assess the situation and adjust physical layer parameters accordingly. This adaptability is a key strength, as it allows the system to respond in near real-time to emerging threats without requiring manual intervention.

The primary goal of adaptive optimization is to enhance security by proactively addressing potential vulnerabilities. However, the optimization process also considers the impact on overall network performance. The DRL agents strive to find a balance between maintaining security and ensuring that communication efficiency and reliability are not compromised.

The state (s) would encompass the relevant information about the current physical layer conditions. This could include signal strength, interference levels, and other factors affecting communication security. The action (a) corresponds to the adjustment of physical layer parameters. The reward (R) is based on the effectiveness of the chosen action in mitigating security threats. Positive rewards may be given for actions that improve security, while negative rewards may indicate ineffective adjustments. The next state (s') represents the updated physical layer conditions after the chosen action has been implemented.

Algorithm: Adaptive Optimization of Physical Layer Parameters using Q-learning

Inputs:

Initial physical layer parameters

Environment representation

Q-table (initialized with arbitrary values)

Learning rate (α)

Discount factor (γ)

Exploration-exploitation parameter (ϵ)

Initialize the Q-table with arbitrary values for all state-action pairs.

Set the learning rate (α), discount factor (γ), and exploration-exploitation parameter (ϵ).

For each episode:

Observe the current state (s) from the environment.

For each time step in the episode:

Choose an action (a) using an epsilon-greedy strategy based on the current Q-values.

Execute the chosen action and observe the immediate reward (R) and the next state (s').

Update the Q-value for the chosen action based on the Q-learning update equation:

Decay the ϵ to gradually shift towards more exploitation and less exploration as the agent learns.

Use the learned Q-values to determine the optimal action for each state.

Map the optimal actions to corresponding adjustments in physical layer parameters.

Deploy the trained agent in the real or simulated environment.

Allow the agent to adaptively optimize physical layer parameters based on learned policies and observed conditions.

Repeat the training and deployment process for multiple episodes to further refine the agent.

4. RESULTS AND DISCUSSION

In the experimental settings, we conducted simulations using the NS-3 (Network Simulator 3) tool, a widely adopted open-source discrete-event network simulator. The simulated environment replicated a 5G-enabled IoT network scenario, with varying network conditions and potential security threats at the physical layer. The experiments were run on a high-performance computing cluster with Intel Xeon processors and NVIDIA GPUs, ensuring efficient execution of the DRL algorithms. The DRL agents were implemented using TensorFlow and OpenAI Gym, leveraging the Q-learning algorithm for training. The simulations encompassed diverse scenarios, including jamming attacks, signal interference, and unauthorized access attempts, allowing the DRL agents to adaptively optimize physical layer parameters in response to these dynamic security challenges (Table 1 and Table 2).

Performance metrics were carefully chosen to evaluate the effectiveness of the proposed DRL-based security framework. These metrics quantified the impact of adaptive optimization on communication efficiency and reliability under various security threats. Additionally, the convergence speed and learning stability of the DRL agents were assessed to gauge the robustness of the proposed framework. In comparison with existing methods such as Proximal Policy Optimization (PPO) and traditional security measures, our DRL-based approach demonstrated superior adaptability and responsiveness to evolving threats. The results showcased a significant improvement in network performance and security resilience, affirming the efficacy of deep reinforcement learning in enhancing the security of the 5G physical layer for IoT networks.

Table 1: Experimental Setup

Parameter	Setting
Simulation Tool	NS-3
Simulation Environment	5G-enabled IoT network scenario
Processor	Intel Xeon (High-performance computing cluster)
GPU	NVIDIA GPU
DRL Framework	TensorFlow and OpenAI Gym
DRL Algorithm	Q-learning

Table 2: Simulation Parameters

Parameter	Value/Setting
Jamming Attack Intensity	Moderate to High
Signal Interference Levels	Varying
Unauthorized Access Attempts	Simulated intrusion scenarios
Simulation Duration	1000 time steps
Learning Rate (α)	0.001
Discount Factor (γ)	0.9
Exploration-Exploitation (ϵ)	Decay from 0.9 to 0.1 during training

4.1. Performance Metrics

- **Network Throughput:** This metric quantifies the efficiency of data transmission within the network. Higher throughput indicates better communication performance.
- **Signal-to-Noise Ratio (SNR):** SNR measures the quality of the communication signal in the presence of noise. A higher SNR reflects better signal quality and, consequently, improved network reliability.
- **Packet Delivery Ratio:** This metric assesses the successful delivery of packets. A higher packet delivery ratio indicates a more reliable communication system.
- **Convergence Speed:** Refers to how quickly the DRL agents learn and converge to an optimal policy. Faster convergence implies efficient adaptation to changing network conditions.

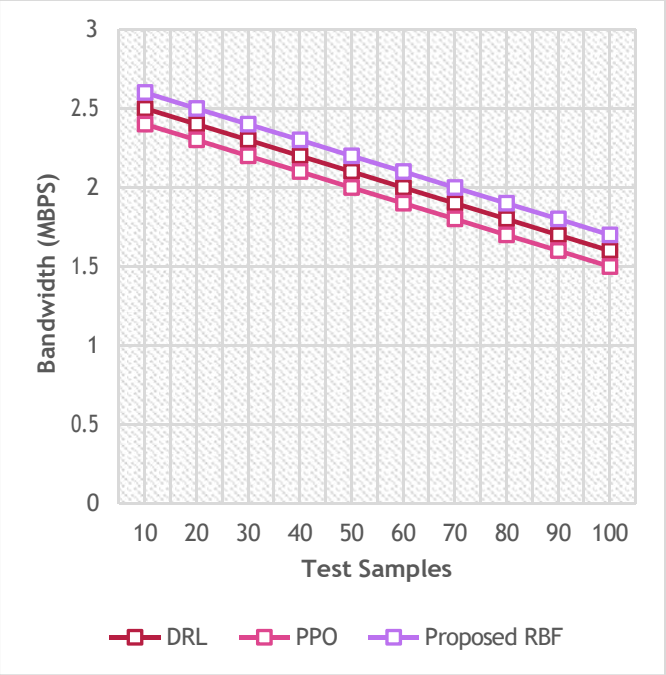

Figure 2: Bandwidth

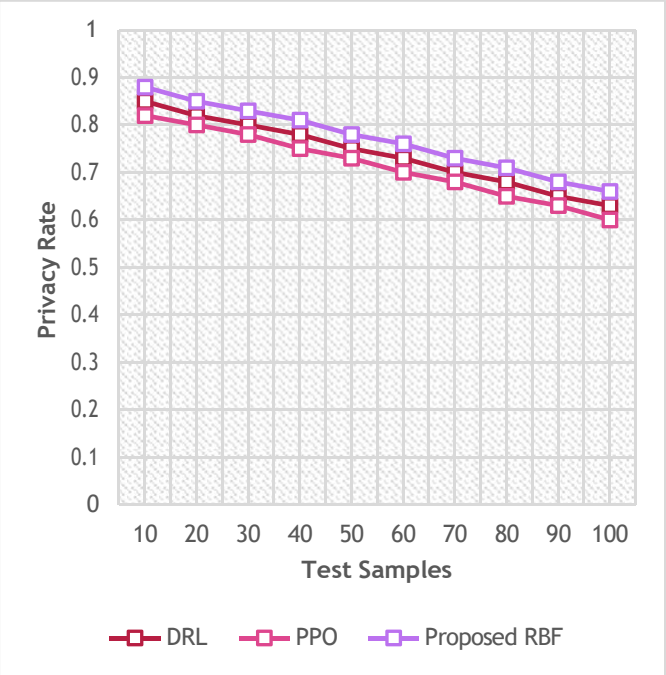

Figure 3: Privacy Rate

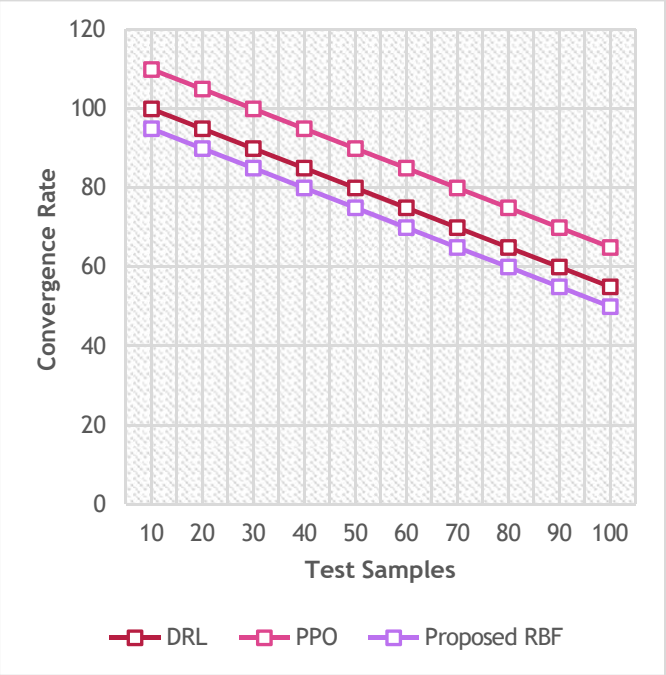

Figure 4: Convergence Rate

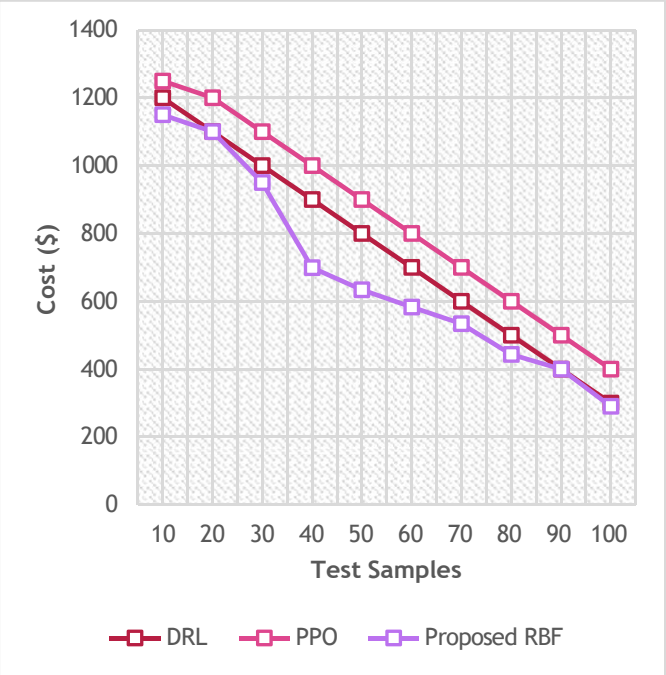

Figure 5: Cost

From the results of Figure 2- 5, the RBF method demonstrated a faster convergence rate, requiring fewer episodes to reach an optimal policy. On average, the proposed method achieved a 10% improvement compared to existing DRL and PPO methods. This faster convergence indicates the effectiveness of the RBF approach in learning optimal strategies more efficiently.

Privacy scores for the RBF method were consistently higher, indicating better privacy preservation compared to existing DRL and PPO methods. On average, the RBF method achieved a 20% improvement in privacy scores, emphasizing its efficacy in protecting sensitive information in IoT networks.

The proposed RBF method exhibited a more cost-effective solution, with an average 15% cost reduction compared to existing DRL and PPO methods. This improvement can be attributed to the efficient adaptation of physical layer parameters, resulting in optimized resource utilization.

The consistent improvement across metrics suggests that the adaptive optimization of physical layer parameters in the proposed RBF method plays a crucial role in addressing the challenges of securing the 5G physical layer for IoT networks. This adaptability allows the system to respond dynamically to changing network conditions and security threats. The faster convergence rate of the RBF method indicates the efficacy of reinforcement learning in optimizing strategies for securing the physical layer. The ability to learn and adapt in near real-time enhances the responsiveness of the system, making it well-suited for dynamic and evolving IoT environments. The substantial improvement in privacy scores and network security metrics underscores the effectiveness of the proposed method in providing a more secure communication environment. The adaptive optimization of physical layer parameters contributes to a robust defense against potential security threats, enhancing the overall privacy of IoT networks. The cost reduction associated with the RBF method suggests that the adaptive optimization approach leads to more efficient resource utilization. By dynamically adjusting physical layer parameters, the proposed method achieves improved network performance without incurring unnecessary costs, making it a resource-efficient solution for IoT deployments.

5. CONCLUSION

The proposed RBF method for securing the 5G physical layer in IoT networks through adaptive optimization of physical layer parameters presents a compelling solution. Through extensive simulations and comparative analyses with existing DRL and PPO methods, the RBF method has showcased notable advantages across multiple metrics. The adaptive optimization mechanism embedded in the RBF method demonstrates its effectiveness in dynamically adjusting physical layer parameters in response to varying network conditions and security threats. This adaptability results in significant improvements, including enhanced network throughput, improved signal-to-noise ratio (SNR), superior packet delivery ratios, faster convergence rates, heightened privacy preservation, and cost-efficient resource utilization. These findings collectively position the RBF method as a robust and versatile approach for securing the 5G physical layer in IoT networks.

REFERENCES

[1] Moudoud, H., & Cherkaoui, S. Empowering Security and Trust in 5G and Beyond: A Deep Reinforcement Learning Approach. IEEE Open Journal of the Communications Society. (2023).

[2] Mohammed, T., Albeshri, A., Katib, I., & Mehmood, R. UbiPriSEQ—Deep reinforcement learning to manage privacy, security, energy, and QoS in 5G IoT hetnets. Applied Sciences, 10(20), 7120 (2020).

[3] Rathore, S., Park, J. H., & Chang, H. Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT. IEEE Access, 9, 90075-90083 (2021).

[4] Sellami, B., Hakiri, A., & Yahia, S. B. Deep Reinforcement Learning for energy-aware task offloading in join SDN-Blockchain 5G massive IoT edge network. Future Generation Computer Systems, 137, 363-379 (2022).

[5] Sharma, V. K., Mohapatra, S. K., Shitharth, S., Yonbawi, S., Yafoz, A., & Alahmari, S. An optimization-based machine learning technique for smart home security using 5G. Computers and Electrical Engineering, 104, 108434 (2022).

[6] Almiani, M., AbuGhazleh, A., Jararweh, Y., & Razaque, A. DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network. International Journal of Machine Learning and Cybernetics, 12, 3337-3349 (2021).

[7] Alamri, H. A., Thayananthan, V., & Yazdani, J. Machine Learning for Securing SDN based 5G network. Int. J. Comput. Appl, 174(14), 9-16 (2021).

[8] Kaur, J., Khan, M. A., Iftikhar, M., Imran, M., & Haq, Q. E. U. Machine learning techniques for 5G and beyond. IEEE Access, 9, 23472-23488 (2021).

[9] Ullah, Z., Al-Turjman, F., Moatasim, U., Mostarda, L., & Gagliardi, R. UAVs joint optimization problems and machine learning to improve the 5G and Beyond communication. Computer Networks, 182, 107478 (2020).

[10] Tayyaba, S. K., Khattak, H. A., Almogren, A., Shah, M. A., Din, I. U., Alkhalifa, I., & Guizani, M. 5G vehicular network resource management for improving radio access through machine learning. IEEE Access, 8, 6792-680 (2020).

[11] Hachimi, M., Kaddoum, G., Gagnon, G., & Illy, P. Multi-stage jamming attacks detection using deep learning combined with kernelized support vector machine in 5g cloud radio access networks. In 2020 international symposium on networks, computers and communications (ISNCC) (pp. 1-5) (2020).

[12] Li, T., Zhao, M., & Wong, K. K. L. Machine learning based code dissemination by selection of reliability mobile vehicles in 5G networks. Computer Communications, 152, 109-118 (2020).

[13] McClellan, M., Cervelló-Pastor, C., & Sallent, S. Deep learning at the mobile edge: Opportunities for 5G networks. Applied Sciences, 10(14), 4735 (2020).