2025 International Conference on Next Generation Computing Systems (ICNGCS) | 979-8-3315-9116-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICNGCS64900.2025.11182771

Deep Reinforcement Learning for Anomaly Detection- A Q-Network Perspective

M. Karthigha
Dept. of Computer Science and Engineering
PSG Institute of Technology and Applied Research
Coimbatore, India
karthigha@psgitech.ac.in

Dhanyasri K
Dept. of Computer Science and Engineering
PSG Institute of Technology and Applied Research
Coimbatore, India
dhanyasri.kkr@gmail.com

***Abstract*—Anomaly Detection System are essential in capturing complex and evolving anomalies thereby securing computer networks against attacks. Traditional systems have limitations in detecting and mitigating modern-day sophisticated attacks. In recent years, Convolutional Neural Networks (CNNs) and Deep Reinforcement Learning (DRL) are the promising approach by providing better decision-making capabilities. This paper presents a novel approach that leverages CNNs and DRL techniques to improve the accuracy and adaptability of anomaly detection. The proposed system employs a CNN-based architecture to extract meaningful features from network traffic. CNNs can capture spatial and temporal patterns, which are crucial for anomaly detection in various applications. To enhance adaptability and adapt to evolving anomalies, Deep Q-Network (DQN) component is added into the system. DQN agents are trained to make decisions based on the CNN-extracted features. It is inferred by the findings that CNN-DQN based anomaly detection system have the potential to significantly improve the detection and mitigation of network attacks with accuracy of 98.01**

***Keywords*—Convolutional Neural Network, Anomaly Detection System, Deep Reinforcement Learning, Rectified Linear Unit.**

1 Introduction

Intrusion Detection Systems (IDSs) play a critical role in ensuring the security of computer networks by identifying and responding to malicious activities. Traditional IDSs rely on predefined rules or signatures to detect attacks, making them less effective against new and unknown threats. To overcome these limitations, researchers have proposed the use of deep reinforcement learning techniques in IDSs [1], [2]. It has been shown that reinforcement learning (RL) can be used for the quick detection of network anomalies to initiate a timely response. Network anomalies are short-lived deviations from the daily operation of the network and can be caused by intruders with malicious intent, such as a denial-of-service (DoS) attack in IP networks, or accidental events, such as an overpass falling in a busy network..,a subfield of machine learning, holds promise in developing IDSs that can learn and adapt from their environment [3], [4]. Through RL, an agent can learn by interacting with its environment, receiving rewards for positive actions and penalties for negative ones. IDS models can be developed using RL to optimize their response to new and emerging threats, learning from experience.

Continuous learning from the environment is possible for RL-based IDSs, allowing them to detect and respond to previously unseen attacks [5], [6]. The reliance on predefined rules and signatures can be reduced, leading to increased detection accuracy. Moreover, RL-based IDSs can adapt their response based on feedback from the environment, which can result in a decrease in false positives and false negatives [9]–[11].In conclusion, the potential for improving network security by developing more adaptable and efficient systems using RL in IDSs cannot be overstated. As the volume and complexity of cyber threats continue to increase, RL-based IDSs are increasingly becoming an important tool for maintaining network security.

1.1 Our Contributions

The main contributions of this paper are as follows:

- A novel CNN-based feature extraction architecture for anomaly detection.
- Integration of Deep Reinforcement Learning to adapt to changing anomaly patterns.
- Experimental results demonstrating the effectiveness of the proposed system on various datasets.
- Comparative analysis with traditional anomaly detection methods, highlighting the system's superior performance and adaptability.

2 Literature Survey

Yao Yu, Yang Wei, Gao Fu-xiang, and Yu Ge [7] proposed a novel anomaly intrusion detection approach using a neural network that combines both Multilayer Perceptron (MLP) and Convolutional Neural Network (CNN) architectures, called a hybrid MLP/CNN neural network. This hybrid model enhances identification of time-delayed attacks by incorporating chaotic neurons, achieving detection rates comparable to real-time attacks, while also reducing false alarms for new attack types.

Mr Mohit Tiwari, Raj Kumar, Akash Bharti, and Jai Kishan [6] described a system for intrusion detection aimed at monitoring network or system activities to identify malicious behavior. Given the rapid growth of internet usage, this system addresses concerns over secure communication and protection of digital information.

training data and are more prone to overfitting if not properly regularized.

Finally, the **Activation function**, typically ReLU (Rectified Linear Unit), introduces non-linearity to the network. This is essential for enabling the model to learn complex mappings from observations to value estimates. ReLU is preferred for its simplicity and ability to mitigate the vanishing gradient problem.

Together, these hyperparameters form the backbone of DQN training and must be carefully tuned based on the task environment, reward structure, and computational resources.

6 Conclusion

Our experimental results on the benchmark IoT-23 dataset demonstrate that the proposed CNN-DQN anomaly detection system significantly outperforms traditional methods, achieving higher detection rates. Moreover, the system exhibits strong adaptability to novel and evolving anomalies, underscoring its suitability for real-world environments where anomaly patterns are dynamic and continuously changing.

In summary, this paper presents an innovative approach to anomaly detection by integrating the capabilities of Convolutional Neural Networks (CNN) with Deep Reinforcement Learning (DRL). The combined architecture leverages the feature extraction power of CNNs and the decision-making strength of DRL, resulting in enhanced detection accuracy and adaptability. These attributes make the proposed system a promising and scalable solution for anomaly detection in complex, real-time IoT-based environments.

References

[1] Y. Sani, A. Mohamedou, K. Ali, A. Farjamfar, M. Azman, and S. Shamsuddin, "An overview of neural networks use in anomaly intrusion detection systems," in *Proc. IEEE Student Conf. Research and Development*, 2009.

[2] M. Karthigha, L. Latha, and R. Madhumathi, "Feature selection and classification models of intrusion detection systems: A review on industrial critical infrastructure perspective," *Cyber Physical Systems - Advances and Applications*, pp. 169–188, 2024.

[3] M. S. Hoque, M. A. Mukit, and M. A. N. Bikas, "An implementation of intrusion detection system," *Int. J. Network Security & Its Applications (IJNSA)*, vol. 4, no. 2, pp. 109–120, 2012.

[4] M. Karthigha et al., "Honeypot-based IDS for cyber attack detection," *AIP Conf. Proc.*, vol. 3204, p. 040018, 2025.

[5] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in *Proc. 15th IEEE Int. Conf. Machine Learning and Applications*, 2016.

[6] M. Tiwari, R. Kumar, A. Bharti, and J. Kishan, "Intrusion detection system," *Int. J. Technical Research and Applications*, 2017.

[7] Y. Yao, Y. Wei, F.-X. Gao, and G. Yu, "An anomaly intrusion detection approach using hybrid MLP/CNN neural network," in *Proc. 6th Int. Conf. Intelligent Systems Design and Applications (ISDA'06)*, 2006.

[8] S. T. F. Al-Janabi and H. A. Saeed, "A neural network based anomaly intrusion detection system," in *Developments in E-Systems Engineering*, 2011.

[9] M. Elsayed, H. Jahromi, M. Nazir, and A. Jurcut, "The role of CNN for intrusion detection systems: An improved CNN learning approach for SDNs," *Int. J. Technical Research and Applications*, 2021.

[10] C.-F. Tsai and Y.-F. Hsu, "Intrusion detection by machine learning: A review," *Expert Systems with Applications*, vol. 36, no. 10, pp. 11994–12000, 2009.

[11] C.-Y. Lin and W.-Y. Lin, "An anomaly intrusion detection system based on intelligent user recognition," *Expert Systems with Applications*, vol. 36, no. 10, pp. 11994–12000, 2009.

[12] S. Mansour and A. Sha'bani, "Fast neural intrusion detection system based on hidden weight optimization algorithm and feature selection," *Neural Computing and Applications*, 2009.

[13] A. Iqbal, M.-L. Tham, and Y. C. Chang, "Convolutional neural network-based deep Q-network (CNN-DQN) resource management in cloud radio access network," *J. Electronics (China)*, vol. 39, no. 1, 2022.

[14] Y.-F. Hsu and M. Matsuoka, "A deep reinforcement learning approach for anomaly network intrusion detection system," in *Proc. IEEE Int. Conf.*, 2020.

[15] M. Karthigha and L. Latha, "Clustered ensemble feature selection with M-GRU classification for efficient intrusion detection system of industrial systems," *J. Intelligent & Fuzzy Systems*, vol. 44, no. 6, pp. 9109–9127, 2023.

[16] A. Seleznyov, "An anomaly intrusion detection system based on intelligent user recognition," M.S. thesis, Univ. of Jyväskylä, 2012.