DOI: doi.org/10.47363/JAICC/ICMLAIDS2026/2026(5)13

International Conference on Machine Learning, Artificial Intelligence and Data Science (ICMLAIDS 2026)

Conference Proceedings March 20 - 21, 2026 - Virtual

Adaptive Real-Time Intrusion Prevention Framework Using Double DQN and Prioritized Experience Replay on Live Network Traffic Streams

Vinay Mallikarjunaradhya

Product Management and AI Labs At Megello, Toronto, Canada

Abstract

The study proposes an Intrusion Prevention System (IPS) in real-time that exploits a Reinforcement Learning framework grounded in Double Deep Q-Networks (Double DQN) coupled with Prioritized Experience Replay to address the weaknesses of conventional static and signature-based security implementation. The proposed model is dynamically learned to attain the best preventive measures through continuous interaction with live traffic streams over the network and therefore, it makes adaptive and intelligent decisions. The system has shown a remarkable performance at the UNSW-NB15 dataset with good detection performances of 97% and a big lowering of the false-positive rates. It is designed such that it can quickly infer with low latency, and operate in real-time in high-speed and high-scale network conditions. The strength, stability and efficiency of the presented IPS are tested through extensive experimentation, such as classification measures, ROC-AUC analysis, convergence performance, latency performance and throughput performance. This paper proves the concept of Double DQN with Prioritized Replay and makes it a strong, scalable, and state-of-the-art solution to proactive countering of cyberattacks in contemporary network systems.

Keywords: Reinforcement Learning, Double DQN, Prioritized Experience Replay, Intrusion Prevention System, Real-Time Network Security, Cyberattack Detection, UNSW-NB15 Dataset, Deep Learning, Network Traffic Analysis, Adaptive Cyber Defense