RADemics

Reinforcement Learning for Automated Intrusion Detection and Adaptive Defense in Zero-Day Attack Scenarios

Krishna Kumar, Aishwaryaa L K, Pradeep K K
ACS COLLEGE OF ENGINEERING, VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY

Reinforcement Learning for Automated Intrusion Detection and Adaptive Defense in Zero-Day Attack Scenarios

[1]Krishna Kumar, AI Expert & Data Scientist, Artificial Intelligence, nitcseac@gmail.com

[2]Aishwaryaa LK, Assistant professor, ECE, ACS college of Engineering, Kambipura, Bangalore-560074, aishukups90@gmail.com

[3]Pradeep K K, Assistant professor, ECE, Velalar College of Engineering and Technology, Thindal, Erode-12, Mail id: pradeep6414@gmail.com

Abstract

The increasing sophistication of cyber threats, particularly zero-day attacks, necessitates the development of intelligent and adaptive security mechanisms capable of real-time threat detection and mitigation. Traditional intrusion detection and prevention systems (IDPS) rely on static rule sets and signature-based techniques, which are insufficient against novel and evolving attack vectors. Reinforcement Learning (RL) offers a promising approach by enabling autonomous agents to learn optimal defense strategies through continuous interaction with network environments. This chapter explores the application of RL for automated intrusion detection and adaptive defense, focusing on its ability to enhance cyber resilience against zero-day attacks. It provides a comprehensive overview of RL-based threat detection frameworks, highlighting key methodologies such as Deep Q-Networks (DQN), actor-critic models, and deep reinforcement learning (DRL) architectures. the chapter examines the challenges associated with RL deployment in cybersecurity, including adversarial manipulation, computational complexity, and data scarcity, it discusses the integration of RL with security information and event management (SIEM) systems, real-time anomaly detection, and self-learning security policies. The proposed RL-driven approach enhances proactive threat hunting capabilities, minimizes false positives, and enables adaptive response mechanisms to emerging cyber threats. By leveraging RL techniques, cybersecurity frameworks can transition from reactive models to autonomous, self-evolving defense systems, ensuring enhanced protection in dynamic and adversarial environments.

Keywords: Reinforcement Learning, Intrusion Detection, Zero-Day Attacks, Cybersecurity, Adaptive Defense, Deep Reinforcement Learning.

Introduction

The continuous evolution of cyber threats, particularly zero-day attacks, has created an urgent need for intelligent and adaptive cybersecurity mechanisms. Traditional security solutions, such as rule-based intrusion detection and prevention systems (IDPS), often struggle to detect previously unknown attack vectors due to their reliance on predefined signatures and heuristics. These static security measures fail to generalize to novel threats, making them ineffective against advanced persistent threats (APTs) and polymorphic malware. As adversaries leverage sophisticated techniques, including adversarial machine learning and evasive attack strategies,

there is a growing demand for cybersecurity solutions that can dynamically learn and adapt in real time. Reinforcement Learning (RL), a branch of machine learning, has emerged as a powerful approach to building autonomous defense systems capable of continuous learning and proactive threat mitigation.

Reinforcement Learning operates on the principle of trial-and-error learning, where an agent interacts with an environment, receives feedback in the form of rewards or penalties, and refines its decision-making strategy accordingly. In the cybersecurity domain, RL-based models can be trained to recognize evolving attack patterns, adjust security policies dynamically, and optimize mitigation strategies without relying on explicit human intervention. Unlike traditional machine learning methods that require large labeled datasets for supervised training, RL enables security systems to learn through direct interaction with network traffic, making it particularly useful for detecting and preventing zero-day attacks. By continuously refining their decision policies, RL-based intrusion detection systems can autonomously respond to new threats with higher precision and lower false positive rates than conventional security models.

The application of RL in cybersecurity involves the use of advanced techniques such as Deep Q-Networks (DQN), actor-critic models, and deep reinforcement learning (DRL) architectures. These models leverage deep neural networks to approximate value functions and optimize decision-making in high-dimensional security environments. By integrating RL into security frameworks, cyber defense mechanisms can transition from passive, rule-based systems to proactive and self-learning security infrastructures. Moreover, RL-based security models can be deployed in real-time environments to continuously monitor network traffic, detect anomalies, and respond to cyber threats autonomously. This capability is particularly valuable in scenarios where traditional signature-based systems fail to detect novel attacks or require frequent manual updates to remain effective.