RADemics

AI-Enhanced Attack Graphs Using Markov Decision Processes for Proactive Threat Hunting and Risk Forecasting

Jagdish Makhijani, Yashwant Pathak, Soumya Bajpai

RUSTAMJI INSTITUTE OF TECHNOLOGY, AMITY UNIVERSITY, IPS COLLEGE OF TECHNOLOGY AND MANAGEMENT.

AI-Enhanced Attack Graphs Using Markov Decision Processes for Proactive Threat Hunting and Risk Forecasting

[1]Jagdish Makhijani, Assistant Professor, Computer Science and Engineering, Rustamji Institute of Technology, BSF Academy, Tekanpur. j_makhijani@yahoo.com

[2]Yashwant Pathak, Researcher, Management, Amity University Madhya Pradesh Gwalior. yashpathak21@gmail.com

[3]Soumya Bajpai, Assistant Professor, CSE, IPS College of technology and management, Shivpuri link Road, Gwalior. soumyabajpai2013@gmail.com

Abstract

The increasing sophistication of cyber threats and the expanding attack surface of modern networks necessitate advanced methodologies for proactive risk assessment and threat mitigation. Traditional attack graphs provide a structured representation of potential attack paths but often struggle with scalability, adaptability, and real-time threat intelligence integration. To address these limitations, this chapter explores the integration of AI-enhanced attack graphs with Markov Decision Processes (MDPs) for proactive threat hunting and cyber risk forecasting. AI-driven techniques, including graph neural networks (GNNs), reinforcement learning, and Bayesian inference, are leveraged to enhance attack graph performance, automate risk assessment, and optimize cybersecurity decision-making. The incorporation of MDPs provides a probabilistic framework for modeling adversarial behavior, enabling predictive analytics for threat evolution and automated mitigation strategies, hybrid AI models improve attack graph scalability by integrating deep learning for pattern recognition, evolutionary algorithms for optimization, and federated learning for distributed security intelligence. The proposed framework shifts cybersecurity from reactive defense mechanisms to a proactive, adaptive, and intelligence-driven approach. Case studies and experimental evaluations demonstrate the efficacy of AI-enhanced attack graphs with MDPs in large-scale, dynamic environments, reinforcing their potential for real-time cyber defense applications. This chapter contributes to advancing risk-aware cybersecurity strategies, fostering automation in cyber risk profiling, and enhancing resilience against emerging threats.

Keywords: AI-enhanced attack graphs, Markov Decision Processes, proactive threat hunting, cyber risk forecasting, graph neural networks, reinforcement learning.

Introduction

The rapid growth and integration of cyber-physical systems (CPS) and large-scale networks have made cybersecurity a critical concern for organizations worldwide. With industries relying heavily on interconnected digital infrastructures, the sophistication and scale of cyber threats have evolved at an unprecedented rate. Traditional security mechanisms, such as signature-based intrusion detection systems and rule-based defense mechanisms, are no longer sufficient to address the diverse and dynamic nature of contemporary cyber threats. As attackers continuously refine their tactics, there is a pressing need for advanced solutions that can proactively predict, identify, and mitigate security risks before they escalate. One promising approach to addressing these challenges involves the use of attack graphs, which model potential attack paths and vulnerabilities within a system. These models allow for a better understanding of how an attacker might move through a network, highlighting weak points and potential entry vectors. However, as networks become more complex, the traditional use of attack graphs alone is no longer adequate to provide timely and comprehensive threat analysis.

Attack graphs have long been an essential tool for cybersecurity practitioners, helping to visualize the potential vulnerabilities and attack surfaces within a system. Traditionally, these graphs have been static, created manually based on known vulnerabilities and risk assessments. However, with the rise of AI technologies, attack graphs have evolved into dynamic models capable of adapting to changing threat landscapes. The integration of machine learning and deep learning algorithms into attack graph analysis enables continuous updates, ensuring that the graph reflects the latest threat intelligence and attack patterns. These AI-enhanced attack graphs offer a more automated and real-time approach to identifying vulnerabilities, allowing for quicker threat detection and response. AI algorithms can automatically generate attack graphs by analyzing network traffic, identifying patterns in historical attack data, and predicting future attack strategies. This adaptability enhances the ability to detect zero-day attacks, insider threats, and other novel security breaches that might be missed by traditional detection methods. Despite their clear advantages, the scalability and real-time processing of these enhanced models remain significant challenges.