RADemics

GraphBased Risk Analysis Using Graph Neural Networks for Mapping Cyber Threat Propagation in LargeScale Networks

S. Shanthi, Sathea Sree. S, M. Sindhu
AUXILIUM COLLEGE FOR WOMEN (AUTONOMOUS), VELS INSTITUTE OF SCIENCE, TECHNOLOGY & ADVANCED STUDIES, KNOWLEDGE INSTITUTE OF TECHNOLOGY

GraphBased Risk Analysis Using Graph Neural Networks for Mapping Cyber Threat Propagation in LargeScale Networks

[1]S. Shanthi, Assistant Professor, Computer Science & Applications, Auxilium College for Women (Autonomous), Vellore. shanthi.s2011@gmail.com

[2]Sathea Sree.S, Assistant professor, Computer Science Engineering, Vels Institute of Science, Technology & Advanced Studies, Pallavaram,Chennai. Mail ID: satheasree.se@vistas.ac.in

[3]M. Sindhu, Assistant Professor, Mathematics, Knowledge Institute of Technology, Kakapalayam, Salem, Mail id: msindhu0387@gmail.com

Abstract

The increasing complexity and scale of cyber-physical systems have amplified the challenges associated with real-time cyber threat detection and mitigation. Traditional anomaly detection methods often struggle to capture the intricate dependencies and temporal dynamics of evolving cyber threats in large-scale networks. Graph Neural Networks (GNNs) have emerged as a powerful tool for modeling cyber threats; however, their scalability, computational efficiency, and real-time adaptability remain critical research challenges. This book chapter presents a comprehensive study on Graph-Based Risk Analysis using Graph Neural Networks (GNNs) and Temporal Graph Neural Networks (TGNNs) to map cyber threat propagation in large-scale networks. It explores key aspects such as dynamic graph representation, sequential modeling of attack patterns, and trade-offs between accuracy and computational efficiency in real-world cybersecurity applications, the scalability challenges of graph-based anomaly detection systems are analyzed, including computational complexity, memory constraints, and parallel processing limitations. Several optimization techniques, including graph sampling, model compression, and distributed graph learning, are discussed to enhance real-time threat detection performance. The chapter also highlights future research directions, such as federated graph learning for decentralized cybersecurity, adversarial robustness in GNNs, and energy-efficient architectures for large-scale threat monitoring. By addressing these challenges, this study provides a foundation for developing scalable, efficient, and resilient graph-based cyber risk assessment frameworks that can effectively combat emerging cyber threats in interconnected digital ecosystems.

Keywords: Graph Neural Networks, Temporal Graph Neural Networks, Cyber Threat Propagation, Anomaly Detection, Large-Scale Network Security, Scalable Threat Intelligence

Introduction

The rapid evolution of cyber threats, driven by sophisticated attack techniques and the increasing complexity of interconnected digital ecosystems, has created significant challenges in cyber risk assessment and mitigation. Traditional security frameworks often rely on rule-based detection mechanisms and signature-based intrusion detection systems, which struggle to adapt to emerging threats characterized by zero-day vulnerabilities, advanced persistent threats (APTs), and coordinated cyber-attacks. These limitations highlight the need for more advanced analytical models capable of understanding complex attack patterns and predicting their evolution. Graph-based risk analysis, combined with Graph Neural Networks (GNNs), provides a powerful approach to modeling the intricate relationships between various cyber entities, enabling a more adaptive and scalable methodology for cyber threat detection.

Graph representations allow security analysts to capture structural dependencies within networks, modeling the interactions between users, devices, applications, and network connections. This capability is particularly useful in cybersecurity, where threats often manifest as anomalous interactions within an otherwise legitimate network structure. Unlike traditional machine learning models that treat data as independent and identically distributed, graph-based models leverage relational information to infer hidden attack patterns. Temporal Graph Neural Networks (TGNNs) further extend this capability by incorporating time-dependent attack sequences, enabling predictive modeling of threat propagation paths, lateral movements, and stealthy network infiltrations. These models offer a crucial advantage in cyber defense by identifying attack trends before they escalate into large-scale security breaches.

Applying GNNs and TGNNs to large-scale cybersecurity applications presents several challenges. The computational cost associated with processing high-dimensional network data, the difficulty of maintaining up-to-date graph representations in rapidly evolving environments, and the need for real-time inference create significant hurdles. Cybersecurity graphs, unlike social or biological networks, are highly dynamic, adversarial in nature, and often incomplete due to missing or encrypted data. Efficiently handling these factors while maintaining detection accuracy requires advanced graph learning techniques, scalable architectures, and robust optimization methods. Addressing these challenges is crucial for ensuring the practicality and effectiveness of graph-based cyber risk analysis in real-world scenarios.