RADemics

Graph Neural Networks for Cybersecurity Applications in Network Intrusion and Vulnerability Analysis

Virender Khurana, Neeraj Kumar
VAISH COLLEGE, ROHTAK, DOON INSTITUTE OF ENGINEERING AND TECHNOLOGY.

8. Graph Neural Networks for Cybersecurity Applications in Network Intrusion and Vulnerability Analysis

1Virender Khurana, Professor, Department of Computer Science, Vaish College, Rohtak, Haryana, India.drvkkhurana@gmail.com

2Neeraj Kumar, Doon Institute of Engineering and Technology, Shyampur, Rishikesh, Uttarakhand -249204,India.neerajkumar.mmmec@gmail.com

Abstract

Graph Neural Networks (GNNs) have emerged as a powerful tool for enhancing network intrusion detection systems (IDS) by leveraging the structural relationships inherent in network data. This chapter explores the integration of GNNs into cybersecurity, focusing on their application to network intrusion detection and vulnerability analysis. GNN-based models enable efficient identification of complex attack patterns, including botnets, DDoS, and insider threats, by capturing dynamic interactions between nodes in a network. The chapter delves into key aspects such as graph construction from real-world network data, the role of community detection for identifying malicious clusters, and the comparative analysis of various GNN architectures. Additionally, it addresses the deployment challenges of real-time intrusion detection, emphasizing scalability, latency, and adaptability. By providing an in-depth understanding of GNN applications and challenges, this chapter contributes valuable insights to advancing intrusion detection technologies in the evolving landscape of network security.

Keywords:

Graph Neural Networks, Intrusion Detection, Cybersecurity, Network Vulnerability, Community Detection, Real-Time Systems.

Introduction

In the modern digital landscape, the complexity and sophistication of cyberattacks continue to evolve, presenting a significant challenge for traditional network security solutions [1]. Traditional intrusion detection systems (IDS) primarily rely on signature-based detection methods, which often fail to identify novel or zero-day attacks [2-4]. The rapid growth of interconnected devices, coupled with the increasing use of dynamic and decentralized network topologies, has created a fertile ground for advanced persistent threats (APTs), botnets, and other malicious activities [5-7]. These challenges demand innovative approaches to enhance the accuracy and efficiency of network security systems [8]. One such promising approach was the application of Graph Neural Networks (GNNs), which have the ability to model complex relationships between entities within a network and detect unusual patterns thatotherwise go unnoticed [9]. GNNs offer the potential to

revolutionize the way network intrusion detection systems operate by providing a more robust and adaptive mechanism for identifying cyber threats in real-time [10].

The core strength of GNNs lies in their ability to process and analyze graph-structured data [11]. Networks, by nature, are represented as graphs where nodes represent devices or entities, and edges represent the interactions or communication links between them [12]. In the context of cybersecurity, such graph representations can capture intricate details about network traffic and behavior that traditional IDS techniquesoverlook [13]. For instance, a GNN can track the flow of data between nodes, detect abnormal patterns in node interactions, and flag potential vulnerabilities [14-16]. This graph-based representation allows GNNs to model not just the direct connections between nodes but also the higher-order relationships, enabling the identification of hidden attack paths, complex multi-stage attacks, and anomalies thatotherwise be difficult to detect using conventional methods [17-19]. As cyber threats become more advanced and unpredictable, GNNs provide a powerful tool for understanding and securing network infrastructures [20].

The integration of GNNs into intrusion detection systems presents a paradigm shift in how network security was approached [21]. By leveraging the power of graph-based learning, GNNs can enhance IDS by detecting complex, often subtle, attack patterns [22]. These patterns can range from Distributed Denial of Service (DDoS) attacks to sophisticated insider threats and lateral movement within a network [23]. GNN-based IDS can process real-time network data to dynamically update the graph and provide immediate alerts when anomalies are detected. Additionally, GNNs can facilitate the identification of attack vectors that span multiple nodes, making them more effective at detecting coordinated, multi-stage attacks that bypass traditional detection methods [24]. The adaptability and learning capabilities of GNNs allow them to improve over time, refining their detection models as more data becomes available [25]. As a result, GNN-based systems offer a more proactive and adaptive approach to intrusion detection, with the ability to identify previously unseen attack scenarios and vulnerabilities.