Enhancing GNN-Based IDS by using Memory-Based Continual Learning

Dinh-Hau Tran, Minho Park

Soongsil Univ.

hautransns@soongsil.ac.kr, mhp@ssu.ac.kr

Memory-Based Continual Learning 을 사용하여 GNN 기반 IDS 강화에 관한 연구

Dinh-Hau Tran, 박민호

숭실대학교

Abstract

Intrusion detection systems (IDS) play a crucial role in cybersecurity, aiming to identify and warn early about potential threats. However, traditional IDS approaches often face limitations in detecting unknown attacks. This paper proposes a novel framework that leverages the power of graph neural network (GNN) and memory-based continual learning techniques to enhance the performance and adaptability of IDS. By representing network traffic as graphs and employing GNNs, the proposed method can capture complex relationships and patterns within the data. Furthermore, the integration of continual learning allows the system to continuously learn and adapt to new attack scenarios without forgetting previously acquired knowledge. The proposed approach addresses the current limitations of IDS and offers potential improvements in terms of detection accuracy and adaptability to dynamic network environments.

Ⅰ. Introduction

In today's digital era, with the widespread use of the internet, network systems have become increasingly vast and complex. Despite their benefits, these network systems also pose numerous risks that can cause significant harm to businesses and organizations. Indeed, cyberattacks are escalating in both quantity and sophistication, presenting a substantial challenge for protective systems such as intrusion detection systems (IDS) and intrusion prevention systems (IPS). Among these, network-based intrusion detection systems (NIDS) consistently hold a pivotal and essential role in safeguarding business and organizational network systems. However, in the face of these challenges, NIDS systems are experiencing significant limitations in effectively detecting unknown attacks or zero-day attacks. The primary detection mechanisms employed by NIDS, such as signature-based or anomaly-based methods, are increasingly susceptible to evasion by modern attacks or generate high rates of false alarms.

The signature-based method utilizes pre-defined attack signatures through rule sets to effectively identify known threats and malicious patterns. While this method enables accurate and prompt responses to known attacks, it is largely ineffective at detecting new attacks or other variations of known attacks. On the other hand, the anomaly-based method establishes baselines of normal network behavior, allowing it to detect anomalous activities that deviate from regular patterns and flag them as suspicious behaviors, alerting administrators. However, this method does not guarantee reliability, as it still has limitations such as high rates of false positives and false alarms.

Many deep learning techniques have been widely applied to IDS to address the challenges of detecting unknown and sophisticated attacks. Among these techniques, GNN-based detection systems are considered the most suitable and effective for the data that IDS monitors. The ability of GNN to learn from neighboring nodes allows them to effectively exploit complex relationships between flows generated within the system. However, these models are based on the assumption that networks are static. In reality, network traffic exhibits real-time characteristics, varying in nature over time due to changes in network structure, service types, and the emergence of new traffic patterns. To obtain updated representations, the GNN model needs to learn both the existing patterns from the previous model and new patterns. The challenge arises from the fact that such retraining can lead to increased computational complexity. On the contrary, if the model focuses solely on training with new data, it may experience catastrophic forgetting and a severe performance decrease on previously learned tasks. Therefore, the GNN model needs to learn new tasks while simultaneously retaining previously acquired knowledge. Continual learning techniques can provide a solution to this problem. Continual learning, also known as lifelong learning, is a paradigm that enables machine learning models to continuously acquire and retain knowledge

over time, mitigating the issue of catastrophic forgetting. By integrating continual learning strategies, the GNN model can adapt to new data while preserving and consolidating its existing knowledge, ensuring long-term effectiveness and resilience in the dynamic network environment. In this study, we proposed a novel research direction that aims to enhance GNN-based IDS by incorporating memory-based continual learning techniques. By leveraging the powerful representation learning capabilities of GNNs and the adaptability of continual learning, the proposed framework can provide a robust and resilient solution for intrusion detection in dynamic network environments.

In the remainder of this paper, we provided essential background on continual learning techniques and proposed a new approach for the current GNN model. Finally, we concluded this paper with directions for future research.

Ⅱ. Method

A. Continual learning

Continual Learning, also known as Incremental Learning or Lifelong Learning, is a concept where a model is trained on a large number of tasks sequentially without forgetting the knowledge obtained from preceding tasks, even though the data from previous tasks is no longer available during the training of new ones [1]. In practice, many deep learning and machine learning models often need to be retrained frequently to maintain efficiency. This necessity arises because the real-world data these models encounter frequently changes in both nature and quantity, causing the knowledge the model was trained on to become outdated. As a result, the model's performance significantly degrade in real-world applications. The phenomenon where a model is retrained with new data and forgets previously learned information is known as catastrophic forgetting [2]. The goal of continual learning is to help the model avoid this phenomenon when learning from new data.

Continual learning techniques can be categorized as regularization-based, memory-based, and architecture-based methods [3]. Regularization-based methods keep the model architecture fixed during incremental training. To enable the model to learn new data without forgetting the past, they use techniques like knowledge distillation, loss function modification, selection of parameters that should (or should not) be updated, or simple regularization. Memory-based continual learning methods involve saving part of the input samples into a memory buffer during training. The idea is to use these examples later for model training along with currently seen data to prevent catastrophic forgetting. The architecture-based approach is the method of modifying the deep learning model architecture to accommodate new data. The model can be rebuilt at any time necessary.

B. Proposed Method

Continual graph learning (CGL) is an emerging field that applies continual learning techniques to GNN models. Similar to other continual learning models, the goal of CGL is to address the issue of catastrophic forgetting when the model is trained with new data, enabling lifelong learning capabilities. The complexity of graph-structure data poses two major challenges for CGL models: node-level dependencies and graph-level dependencies.

Among the various continual learning techniques, the memory-based method is the most suitable for application in GNN-based detection systems. Firstly, due to the ever-changing nature of network data and the potential emergence of new attack patterns, using a memory buffer can help store diverse data samples. This memory buffer in the model acts similarly to the rule set established in the signature-based detection mechanism of an IDS. Additionally, memory-based method are typically easier to deploy compared to other techniques. This is particularly useful when working with the complex graph structures of GNN networks. Moreover, this method utilizes a memory buffer to continuously store data samples across tasks. This enables the model to simultaneously learn from both old and new data, effectively reducing the occurrence of catastrophic forgetting.

In this paper, we propose the integration of memory-based techniques into an existing GNN-based detection model. In this model, graph data is formed from flow data. Specifically, nodes in the graph represent important features extracted from the flow data, and edges are created based on the relationships between those flows. Network data is continuously monitored to capture and send to the model for classification. After the model training, some of nodes are selected to be stored in a memory buffer. The stored node samples serve for the next training task when the model receives new flow data. At this point, the new graph data and data from the memory buffer are aggregated to learn the graph representation for classification. At the same time, representative nodes of this graph continue to be selected and sent to the memory buffer as in the previous task. This process is repeated for each task the model performs.

The challenge in this model lies in selecting representative nodes to store in the memory buffer. Selecting too many nodes can lead to memory overload, reducing computational efficiency and increasing operational costs. Conversely, if the selected nodes are not representative of previous data, the memory buffer becomes ineffective for model training. Some node selection methods we consider include Mean of Feature and Coverage Maximization [4]. These methods have been introduced and widely applied and are most suitable for our graph data. The integration of new and stored data helps keep the proposed model up-to-date, while the memory buffer ensures the retention of previously trained knowledge.

Ⅲ. Conclusion

In this paper, we have proposed an idea to apply memory-based continual learning techniques to a GNN-based IDS model. This combination enhances the current model's training process to adapt to new data while retaining past knowledge. This approach promises to be a new direction to improve the performance of IDS systems in increasingly complex network environments. However, to build an effective model, designing useful methods for selecting representative nodes is crucial. These will be significant challenges in future research.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2023R1A2C1005461).

REFERENCES

[1] G. I. Parisi, R. Kemker, J. L. Part, C. Kanan, and S. Wermter, “Continual lifelong learning with neural networks: A review,” Neural Networks, vol. 113, pp. 54-71, 2019.

[2] G. M. van de Ven, N. Soures, and D. Kudithipudi, “Continual learning and catastrophic forgetting,” 2024.

[3] G. M. van de Ven and A. S. Tolias, “Three scenarios for continual learning,” 2019

[4] Q. Yuan, S.-U. Guan, P. Ni, T. Luo, K. L. Man, P. Wong, and V. Chang, “Continual graph learning: A survey,” 2023.