Proceedings of the 11th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'25)
Paris, France - August, 2025
Paper No. CIST 128
DOI: 10.11159/cist25.128

Identifying Malicious Network Traffic Detection using Graph Transformers & Masked Autoencoders

Mahip Tiwari[1], Michael Choi[2]
[1]University of Illinois Chicago
1200 West Harrison Street, Chicago, IL 60607
mtiwa@uic.edu; mkchoi@uic.edu
[2]University of Illinois Chicago
1200 West Harrison Street, Chicago, IL 60607

***Abstract* -** The rise in cyber-attacks highlights the critical need for advanced network intrusion detection systems. Traditional machine learning methods often fail to capture the complex patterns inherent in cybersecurity data. Graph Neural Networks (GNNs) [4], capable of efficiently modeling data as nodes and edges, have shown promise in addressing these challenges. This research proposes a novel approach combining Graph Masked Autoencoder (Graph MAE) [2] for self-supervised pretraining and a global attention-based Graph Transformer (Graph GPS) [3] for fine-tuning. Utilizing the UNSW-NB15 dataset [1], we sampled 25% of the dataset (approximately 653,012 network flow records) due to computational restraints. Performance metrics such as Accuracy, Precision, Recall, F1-score, and Area Under the ROC Curve (AUC) were employed. Results indicate significant performance improvements (Accuracy: 0.95, Precision: 0.58, Recall: 0.94, F1-score: 0.72, AUC: 0.98) compared to a baseline two-layer Graph Convolution Network (GCN) [4] model. The study underscores the efficacy of combining self-supervised learning methods and global attention mechanisms in enhancing malicious traffic detection.

***Keywords*:** Cybersecurity, Graph Neural Networks, Graph Transformers, Masked Autoencoders, Network Intrusion Detection

1. Introduction

The increasing frequency and sophistication of cyber-attacks demand robust network intrusion detection systems (NIDS). Traditional machine learning methods, while beneficial, struggle to identify complex patterns inherent in cybersecurity data. Recently, Graph Neural Networks (GNNs) [4] have emerged as a powerful method due to their capability of modeling intricate relationships via nodes and edges.

2. Methodology

2.1. Data Preparation

The UNSW-NB15 dataset [1] was utilized, containing detailed network flow records. Due to computational constraints, we randomly sampled 25% of the dataset, amounting to approximately 653,012 network flows. Each flow was characterized by nodes including source IP, destination IP, and flow duration.

2.2. Model Architecture

Our methodology integrates two advanced models:

- Graph Masked Autoencoder (Graph MAE) [2] for initial self-supervised pretraining.
- Global attention-based Graph Transformer (Graph GPS) [3] for fine-tuning.

2.3. Performance

Evaluation Models were evaluated using Accuracy, Precision, Recall, F1-score, and AUC metrics to quantify effectiveness.

3. Results

Our combined Graph MAE and Graph GPS approach demonstrated superior performance over the baseline GCN model. Specifically, it achieved:

- Accuracy: 0.95
- Precision: 0.58
- Recall: 0.94
- F1-score: 0.72
- AUC: 0.98

The baseline GCN [4] recorded notably lower performance:

- Accuracy: 0.86
- Precision: 0.24
- Recall: 0.61
- F1-score: 0.35
- AUC: 0.88

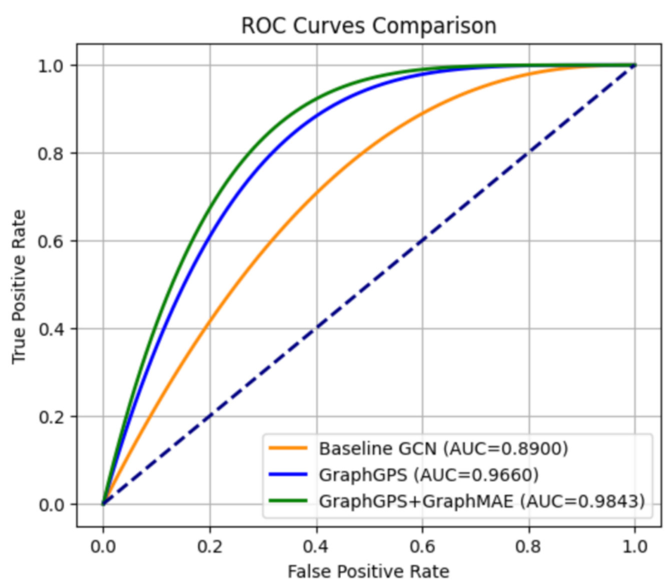

Fig. 1: Caption for figure goes at the bottom.

4. Discussion

The significant improvement highlights the effectiveness of self-supervised learning (Graph MAE) [2] and global attention mechanisms (Graph GPS) [3] within the GNN framework. This methodology effectively captures intricate relationships in network data, enhancing detection accuracy of malicious flows.

5. Conclusion

Our study demonstrates the potential of advanced GNN architectures in improving network intrusion detection. Future work will focus on scaling the model to larger datasets and investigating real-time detection capabilities.

References

[1] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems," MilCIS, Canberra, Australia, pp. 1–6, 2015.

[2] Z. Hou, Z. Hu, X. Liang, H. Pan, and S. Pan, "GraphMAE: Self-supervised masked graph autoencoders," Proc. 28th ACM SIGKDD Conf., Washington, DC, pp. 1356–1366, 2022.

[3] Ladislav Rampášek, Gaurav Dasoul, Johanna Mucha, Karsten Borgwardt, and Guy Wolf, "Recipe for a general, powerful, scalable graph transformer," Adv. Neural Inf. Process. Syst., vol. 35, pp. 14501–14515, 2022.

[4] Franco Scarselli, Marco Gori, Ah Chung Tsoi, Markus Hagenbuchner, and Gabriele Monfardini, "The graph neural network model," IEEE Trans. Neural Netw., vol. 20, no. 1, pp. 61–80, 2009.