Semi-Supervised vs. Unsupervised GNN Anomaly Detectors in Temporal Graph Benchmarks

Assignee Research

June 2, 2026

Abstract

This report synthesises findings from 12 peer-reviewed papers addressing the following research question: How does the inference throughput of semi-supervised GNN anomaly detectors like Mul-GAD compare to unsupervised methods (e.g., DOMINANT) when evaluated on temporal graph benchmarks with node sizes. Graph neural networks (GNNs) have recently garnered significant attention for use in network intrusion detection systems (NIDS), owing to their ability to model network traffic as graphs and capture complex dependencies between flows. However, existing GNN-based methods face. 17 claims were extracted from source literature; 14 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.2/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: MGCRL: Multi-Scale Graph Contrastive Representation Learning For Network Intrusion Detection. Research question: How does the inference throughput of semi-supervised GNN anomaly detectors like Mul-GAD compare to unsupervised methods (e.g., DOMINANT) when evaluated on temporal graph benchmarks with node sizes ranging from 10K to 100K, measured in nodes per second (NPS)?.

2 Methodology

Systematic literature search across multiple databases yielded 12 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.2/10.

3 Results

12 papers retrieved. 17 claims extracted; 14 independently verified. Quality review score: 7.2/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

5 Extracted Claims

Claim	Verified	Confidence
Graph neural networks (GNNs) are used in network intrusion detection systems (NIDS) to model network traffic as graphs a	✓	0.31
Existing GNN-based methods for network intrusion detection rely on labeled data.	✓	0.18
Labeled data for network intrusion detection is often scarce or noisy in practice.	✓	0.20
Existing GNN-based methods are unable to address multi-scale threats including localized node anomalies, coordinated sub	✓	0.27
Port scanning is an example of a localized node anomaly.	×	0.10
Botnets are an example of coordinated subnetwork attacks.	×	0.08
DDoS attacks are an example of global network-wide campaigns.	✓	0.16
MGCRL is a semi-supervised framework that hierarchically integrates three perspectives to model network intrusions.	✓	0.25
At the node level, MGCRL constructs semantic subnetworks around individual traffic flows to capture fine-grained behavio	✓	0.33
For subnetwork-level threats, MGCRL employs substructure-aware pooling to identify coordinated anomalies.	✓	0.25
Coordinated anomalies include clusters of devices exhibiting synchronized malicious activity.	✓	0.19
At the global level, MGCRL derives representations that reflect the holistic state of the network.	✓	0.26
MGCRL enables the detection of large-scale threats such as distributed malware propagation at the global level.	✓	0.23
MGCRL couples a shared GNN encoder with a multi-level contrastive loss.	✓	0.26
The multi-level contrastive loss in MGCRL aligns multi-scale representations.	✓	0.21
MGCRL largely eliminates label dependence.	×	0.09
MGCRL learns discriminative features from unlabeled traffic.	✓	0.18

References

- http://arxiv.org/abs/2212.05478v1
- http://arxiv.org/abs/2311.12255v2
- https://www.semanticscholar.org/paper/9cf4f7b347c275b87641acbdd0996d0d2f461026