Supervised GNNs vs Traditional Methods in Adversarial Robustness for Graph Anomaly Detection

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 12 peer-reviewed papers addressing the following research question: How do supervised GNN models compare to traditional methods in terms of robustness to adversarial attacks on graph-structured data in standardized GAD benchmarks. Anomaly detection is defined as discovering patterns that do not conform to the expected behavior. Previously, anomaly detection was mostly conducted using traditional shallow learning techniques, but with little improvement. 17 claims were extracted from source literature; 2 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 4.2/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Mul-GAD: a semi-supervised graph anomaly detection framework via aggregating multi-view information. Research question: How do supervised GNN models compare to traditional methods in terms of robustness to adversarial attacks on graph-structured data in standardized GAD benchmarks?.

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 4.2/10.

3 Results

12 papers retrieved. 17 claims extracted; 2 independently verified. Quality review score: 4.2/10.

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
Mul-GAD optimizes at both view and feature levels.	×	0.09
Mul-GAD uses learnable parameters to control the contribution of each view.	×	0.06
Mul-GAD utilizes a feature similarity matrix to use complementary information while avoiding redundant information.	×	0.12
Computing the feature similarity matrix plays an important role in boosting detection performance.	×	0.04
The final Mul-GAD model, equipped with a label-oriented objective function and fusion strategies, shows significant impr	×	0.15
The authors claim to be the first to analyze the anomaly detection problem from the perspective of objective functions.	×	0.06
Label-oriented objective functions have more generalized performance compared to other types.	×	0.04
Mul-GAD provides two effective fusion strategies at the view and feature level.	✓	0.17
Both fusion strategies provided by Mul-GAD boost detection performance.	✓	0.16
Mul-GAD outperforms state-of-the-art methods in detection performance across the majority of datasets.	×	0.13
Mul-GAD outperforms state-of-the-art methods in terms of generalization across the majority of datasets.	×	0.10
Anomaly detection algorithms can be divided into shallow learning and graph neural network methods.	×	0.13
Anomaly detection objective functions can be categorized as label-oriented, reconstruction-oriented, and ssl-oriented.	×	0.06
Shallow learning handles anomaly problems using spatial density, statistical distribution, and variants of classical mac	×	0.11
Local Outlier Factor (LOF) acquires anomaly score ranks by computing the spatial density of each node, where lower densi	×	0.03
K-nearest neighbor (KNN) determines the class of a node by seeking the k closest neighbors and using the majority class.	×	0.02
Shallow learning methods are constrained by inductive bias, making it hard to spot abnormal nodes masquerading as normal	×	0.02

References

- http://arxiv.org/abs/2212.05478v1
- http://arxiv.org/abs/1404.4679v2
- http://arxiv.org/abs/1909.08072v2