Robustness of Mul-GAD Against Adversarial Attacks in Graph Anomaly Detection

Assignee Research

June 2, 2026

Abstract

This report synthesises findings from 12 peer-reviewed papers addressing the following research question: What is the robustness of Mul-GAD against adversarial attacks on graph structure or node features compared to other GNN-based anomaly detection methods, as measured by the drop in F1 score under. 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. 16 claims were extracted from source literature; 1 was independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.8/10. 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: What is the robustness of Mul-GAD against adversarial attacks on graph structure or node features compared to other GNN-based anomaly detection methods, as measured by the drop in F1 score under different attack budgets?.

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 3.8/10.

3 Results

12 papers retrieved. 16 claims extracted; 1 independently verified. Quality review score: 3.8/10.

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
The Mul-GAD approach outperforms the state-of-the-art not only on detection performance, but also in terms of generaliza	×	0.14
Experiments show that computing the feature similarity matrix plays an important role in boosting the detection performa	×	0.05
The final model, which equipped with label-oriented objective function and fusion strategies, has a significant improvem	×	0.14
Adequate experimental validation is the foundation for selecting the objective function.	×	0.06
The Mul-GAD approach shows a better generalization due to utilizing the plentiful information from different views.	×	0.13
The Mul-GAD approach uses learnable parameters to control the contribution of each view.	×	0.07
The Mul-GAD approach utilizes the feature similarity matrix to make full use of complementary information while avoiding	×	0.10
The Mul-GAD approach provides two effective fusion strategies at the view and feature level, both of which boost detecti	✓	0.20
The Mul-GAD approach is the first to analyze the anomaly detection problem from the perspective of objective functions a	×	0.08
The Mul-GAD approach can be explained theoretically via the Venn diagram, which is often applied to show mathematical or	×	0.05
Shallow learning methods for anomaly detection include spatial density methods, statistical distribution methods, and va	×	0.08
Spatial density methods for anomaly detection develop based on the hypothesis that there are fewer nodes or lower node d	×	0.07
Local Outlier Factor (LOF) acquires the rank of anomaly scores via computing the spatial density of each node, with lowe	×	0.04
K-nearest neighbor (KNN) seeks out the k closest neighbors and uses the majority class to determine the class of the cur	×	0.01
Spatial density methods are constrained by the inductive bias and are hard to spot abnormal nodes masquerading as normal	×	0.02
Anomaly detection can be categorized into label-oriented, reconstruction-oriented, and SSL-oriented objective functions.	×	0.05

References

- http://arxiv.org/abs/2212.05478v1
- http://arxiv.org/abs/2006.16545v1
- http://arxiv.org/abs/2104.09369v1