Adversarial Graph Perturbations on Contrastive GNNs and Autoencoders in Intrusion Detection

Assignee Research

June 2, 2026

Abstract

This report synthesises findings from 10 peer-reviewed papers addressing the following research question: What is the impact of adversarial graph perturbations on the detection accuracy of contrastive graph neural networks versus autoencoder models in intrusion detection tasks, as evaluated on standard. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.0/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: CAGN-GAT Fusion: A Hybrid Contrastive Attentive Graph Neural Network for Network Intrusion Detection. Research question: What is the impact of adversarial graph perturbations on the detection accuracy of contrastive graph neural networks versus autoencoder models in intrusion detection tasks, as evaluated on standard benchmarks like GIN, GAT, and GCN with metrics such as robustness (accuracy drop ratio) and generalization across different attack types?.

2 Methodology

Systematic literature search across multiple databases yielded 10 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.0/10.

3 Results

10 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 7.0/10.

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.

References

- http://arxiv.org/abs/2512.10637v2
- http://arxiv.org/abs/2503.00961v3
- http://arxiv.org/abs/2104.09369v1