GADT3 vs GCN Inference Latency Under Adversarial Graph Perturbations on OGB-LSC

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 8 peer-reviewed papers addressing the following research question: How does the inference latency of GADT3 compare to traditional GCN-based models under varying degrees of adversarial graph structure perturbations, measured using the OGB-LSC traffic prediction. Cyberattacks represent an ever-growing threat that has become a real priority for most organizations. Attackers use sophisticated attack scenarios to deceive defense systems in order to access private data or cause harm. 12 claims were extracted from source literature; 12 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.9/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Graph Neural Networks for Intrusion Detection: A Survey. Research question: How does the inference latency of GADT3 compare to traditional GCN-based models under varying degrees of adversarial graph structure perturbations, measured using the OGB-LSC traffic prediction benchmark?.

2 Methodology

Systematic literature search across multiple databases yielded 8 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.9/10.

3 Results

8 papers retrieved. 12 claims extracted; 12 independently verified. Quality review score: 7.9/10.

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
Cyberattacks represent an ever-growing threat that has become a real priority for most organizations.	✓	0.23
Attackers use sophisticated attack scenarios to deceive defense systems in order to access private data or cause harm.	✓	0.32
Machine Learning (ML) and Deep Learning (DL) have demonstrated impressive results for detecting cyberattacks due to thei	✓	0.34
Flat data fail to capture the structural behavior of attacks, which is essential for effective detection.	✓	0.30
Graph structures provide a more robust and abstract view of a system that is difficult for attackers to evade.	✓	0.26
Graph Neural Networks (GNNs) have become successful in learning useful representations from the semantic provided by gra	✓	0.33
Intrusions have been detected for years using graphs such as network flow graphs or provenance graphs.	✓	0.28
Learning representations from graph structures can help models understand the structural patterns of attacks in addition	✓	0.31
The survey focuses on the applications of graph representation learning to the detection of network-based and host-based	✓	0.32
The survey presents graph data structures that can be leveraged for both network and host levels.	✓	0.21
The survey comprehensively reviews state-of-the-art papers along with the used datasets.	✓	0.15
The analysis reveals that GNNs are particularly efficient in cybersecurity.	✓	0.20

References

- https://doi.org/10.1109/access.2023.3275789
- https://doi.org/10.3390/computers12080151

- https://doi.org/10.48550/arxiv.2407.09618