Edge-Level Ego-Network Encodings Enhance GNN Robustness Against Adversarial Attacks

Assignee Research

June 3, 2026

Abstract

This report synthesises findings from 14 peer-reviewed papers addressing the following research question: What is the impact of edge-level ego-network encodings on the robustness of GNNs against adversarial perturbations in node classification tasks. 9 claims were extracted from source literature; 9 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.4/10. 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: What is the impact of edge-level ego-network encodings on the robustness of GNNs against adversarial perturbations in node classification tasks?.

2 Methodology

Systematic literature search across multiple databases yielded 14 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.4/10.

3 Results

14 papers retrieved. 9 claims extracted; 9 independently verified. Quality review score: 7.4/10.

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	✓	0.32
Flat data fail to capture the structural behavior of attacks, which is essential for effective detection.	✓	0.31
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	✓	0.30
Intrusions have been detected for years using graphs such as network flow graphs or provenance graphs.	✓	0.27
Learning representations from graph structures can help models understand the structural patterns of attacks, in additio	✓	0.31
GNNs are particularly efficient in cybersecurity, since they can learn effective representations from graph-structured d	✓	0.22

References

- https://doi.org/10.1609/aaai.v36i4.20335

- https://doi.org/10.1109/access.2023.3275789
- https://doi.org/10.1145/3474085