Adversarial Attack Strategies on Graph-Based NIDS and Their Latency Impacts Across Datasets

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 4 peer-reviewed papers addressing the following research question: How do different adversarial attack strategies on graph structure affect the inference latency of GNN-based NIDS models when evaluated using the UNSW-NB15 dataset compared to models trained on the. Deep neural networks, while generalize well, are known to be sensitive to small adversarial perturbations. This phenomenon poses severe security threat and calls for in-depth investigation of the robustness of deep learning models. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 6.0/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Graph Universal Adversarial Attacks: A Few Bad Actors Ruin Graph Learning Models. Research question: How do different adversarial attack strategies on graph structure affect the inference latency of GNN-based NIDS models when evaluated using the UNSW-NB15 dataset compared to models trained on the CIC-IDS 2017 dataset?.

2 Methodology

Systematic literature search across multiple databases yielded 4 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 6.0/10.

3 Results

4 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 6.0/10.

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/2104.09369v1
- http://arxiv.org/abs/2002.04784v2
- http://arxiv.org/abs/2305.00866v2