CAGN-GAT Fusion Robustness Against Adversarial Graph Perturbations in Intrusion Detection

Assignee Research

June 3, 2026

Abstract

This report synthesises findings from 5 peer-reviewed papers addressing the following research question: How does the robustness of CAGN-GAT Fusion compare to autoencoder-based models in intrusion detection when evaluated under adversarial graph perturbations using the accuracy drop ratio metric on GIN,. 12 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: Network intrusion detection using a hybrid graph-based convolutional network and transformer architecture. Research question: How does the robustness of CAGN-GAT Fusion compare to autoencoder-based models in intrusion detection when evaluated under adversarial graph perturbations using the accuracy drop ratio metric on GIN, GAT, and GCN benchmarks?.

2 Methodology

Systematic literature search across multiple databases yielded 5 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

5 papers retrieved. 12 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
Cloud computing growth increases exposure to sophisticated intrusion attacks that can evade traditional security mechani	✓	0.27
Many AI-based intrusion detection models are limited by their dependence on extensive, high-quality attack datasets.	✓	0.26
Many AI-based intrusion detection models have insufficient capacity to capture complex, dynamic patterns in distributed	✓	0.30
The study presents a hybrid intrusion detection model named 'GConvTrans' that combines a graph convolutional layer and a	✓	0.29
The GConvTrans model was evaluated using the CIC-IDS 2018 dataset.	✓	0.16
In the GConvTrans model, tabular network traffic data was transformed into computational graphs.	✓	0.20
The GConvTrans model leverages local structural information through graph convolutional layers.	✓	0.17
The GConvTrans model leverages global context through multi-head self-attention mechanisms.	✓	0.17
The GConvTrans model obtained 84.7% accuracy on the training set.	×	0.12
The GConvTrans model obtained 96.75% accuracy on the validation set.	×	0.11
The GConvTrans model obtained 96.94% accuracy on the testing set.	×	0.15
Combining graph learning techniques with standard deep learning methods is robust for detecting complex network intrusio	✓	0.33

References

- https://doi.org/10.56553/popets-2024-0121
- https://doi.org/10.3390/fi15120377
- https://doi.org/10.1371/journal.pone.0340997