Multi-View Aggregation in Graph Anomaly Detection: Scalability, F1 Scores, and Latency Trade-offs

Assignee Research

June 1, 2026

Abstract

This report synthesises findings from 10 peer-reviewed papers addressing the following research question: How does multi-view aggregation in graph anomaly detection frameworks affect the F1 score and inference latency when scaling from single-edge devices to distributed edge computing environments. Machine learning techniques are being widely used to develop an intrusion detection system (IDS) for detecting and classifying cyberattacks at the network-level and the host-level in a timely and automatic manner. However, many challenges arise since malicious attacks are. 10 claims were extracted from source literature; 9 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 8.5/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Deep Learning Approach for Intelligent Intrusion Detection System. Research question: How does multi-view aggregation in graph anomaly detection frameworks affect the F1 score and inference latency when scaling from single-edge devices to distributed edge computing environments?.

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 8.5/10.

3 Results

10 papers retrieved. 10 claims extracted; 9 independently verified. Quality review score: 8.5/10.

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
Machine learning techniques are being widely used to develop an intrusion detection system (IDS) for detecting and class	✓	0.42
Many challenges arise since malicious attacks are continually changing and are occurring in very large volumes requiring	✓	0.30
There are different malware datasets available publicly for further research by cyber security community.	✓	0.30
No existing study has shown the detailed analysis of the performance of various machine learning algorithms on various p	✓	0.36
Due to the dynamic nature of malware with continuously changing attacking methods, the malware datasets available public	✓	0.37
A deep neural network (DNN), a type of deep learning model, is explored to develop a flexible and effective IDS to detec	✓	0.39
The continuous change in network behavior and rapid evolution of attacks makes it necessary to evaluate various datasets	✓	0.37
This type of study facilitates to identify the best algorithm which can effectively work in detecting future cyberattack	✓	0.30
A comprehensive evaluation of experiments of DNNs and other classical machine learning classifiers are shown on various	✓	0.39
The optimal network p	×	0.13

References

- https://openalex.org/W1775772884
- https://doi.org/10.1109/access.2019.2895334
- https://doi.org/10.1109/access.2021.3107975