Graph-Based Anomaly Detection Robustness Under Adversarial Structural Perturbations

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 14 peer-reviewed papers addressing the following research question: How does the robustness of graph-based anomaly detection models like Mul-GAD compare to GCN-AE under adversarial structural perturbations on the Reddit dataset. Real-time traffic prediction models play a pivotal role in smart mobility systems and have been widely used in route guidance, emerging mobility services, and advanced traffic management systems. With the availability of massive traffic data, neural network-based deep learning. 15 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.1/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Adversarial Diffusion Attacks on Graph-based Traffic Prediction Models. Research question: How does the robustness of graph-based anomaly detection models like Mul-GAD compare to GCN-AE under adversarial structural perturbations on the Reddit dataset?.

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 3.1/10.

3 Results

14 papers retrieved. 15 claims extracted; 0 independently verified. Quality review score: 3.1/10.

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
Szegedy et al. (2013) discovered that adversarial samples are low-probability but densely distributed in deep neural net	×	0.07
Goodfellow et al. showed that generating adversarial samples is sufficient when DNNs demonstrate linear behaviors in hig	×	0.04
An experiment involving 99 smartphones moving slowly on a handcart caused Google Maps to identify an empty street as a c	×	0.02
Mobile phone-based mapping services such as Google Maps and AutoNavi make traffic state estimation and prediction based	×	0.05
Traffic prediction tasks include traffic state prediction, demand prediction, and trajectory prediction.	×	0.12
Traffic state prediction includes the prediction of traffic flow, speed, and travel time.	×	0.08
Traffic demand prediction aims to predict the number of users and traffic demand, such as taxi requests, subway inflow/o	×	0.04
Trajectory prediction tasks are used for dynamic positioning and resource allocation.	×	0.04
Traffic data is represented in non-Euclidean space due to its association with the topological structure of road network	×	0.04
On the LA dataset, the ST-GCN model achieved a value of 5.46.	×	0.06
On the LA dataset, the A3T-GCN model achieved a value of 12.74.	×	0.05
On the HK dataset, the A3T-GCN model achieved a value of 32.86.	×	0.05
Under attack conditions on the LA dataset, the ST-GCN model showed a performance degradation or error rate of 8.32%.	×	0.08
Under attack conditions on the LA dataset, the A3T-GCN model showed a performance degradation or error rate of 22.77%.	×	0.07
Under attack conditions on the HK dataset, the A3T-GCN model showed a performance degradation or error rate of 70.21%.	×	0.07

References

- http://arxiv.org/abs/2104.09369v1
- http://arxiv.org/abs/1404.4679v2
- http://arxiv.org/abs/2103.15670v3