Adversarial Diffusion Attacks on Multimodal Traffic Prediction Models

Assignee Research

June 15, 2026

Abstract

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 methods, especially the graph convolutional networks (GCN) have demonstrated outstanding performance in mining spatio-temporal information and achieving high prediction accuracy. Recent studies reveal the vulnerability of GCN under adversarial attacks, while there is a lack of studies to understand the vulnerability issu

1 Introduction

This paper examines: Adversarial Diffusion Attacks on Graph-based Traffic Prediction Models. Research question: How do adversarial diffusion attacks impact the reasoning accuracy of multimodal traffic prediction models compared to standard graph convolutional networks?.

2 Methodology

Systematic literature search across multiple databases yielded 12 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

12 papers retrieved. 19 claims extracted; 17 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
Neural networks are vulnerable to deliberately designed samples, known as adversarial samples.	✓	0.23
Adversarial samples can significantly change the performance of deep learning models.	✓	0.17
Adversarial samples are low-probability but densely distributed.	✓	0.18
Neural networks are vulnerable to adversarial samples when they demonstrate linear behaviors in high-dimensional spaces.	✓	0.22
Potential attackers could take advantage of deep learning models and degrade their performance using adversarial samples	✓	0.20
Few studies have investigated the vulnerability and robustness of traffic prediction systems.	✓	0.16
Industry-level traffic information systems can be attacked easily.	✓	0.18
A German artist used 99 smartphones to create virtual vehicles, causing Google Maps to incorrectly identify an empty str	×	0.14
Adversarial attacks on traffic prediction models can affect every aspect of smart mobility systems.	✓	0.19
Smartphone-based mobility applications are vulnerable to adversarial attacks.	✓	0.20
Neural network models demonstrate potentials in traffic prediction with multi-source data on large-scale networks.	✓	0.25
Various neural network models have been used for traffic prediction, including CNN, RNN, attention, and GCN.	✓	0.18
Traffic prediction tasks can be categorized into traffic state prediction, demand prediction, and trajectory prediction.	✓	0.21
Traffic state prediction includes the prediction of traffic flow, speed, and travel time.	×	0.12
Traffic demand prediction aims to predict the number of users and traffic demand, such as taxi request, subway inflow/ou	✓	0.21
Trajectory prediction is used for dynamic positioning and resource allocation.	✓	0.15
Most traffic prediction tasks can be carried out by neural network models.	✓	0.20
Traffic data is closely associated with the topological structure of road networks, making it typical graph-based data.	✓	0.20
Conventional machine learning methods overlook the graph-based inter-relationship in traffic data.	✓	0.18

References

- http://arxiv.org/abs/1909.08072v2
- http://arxiv.org/abs/2303.09051v3
- http://arxiv.org/abs/2104.09369v1