Volume 2, 2026, Pages 001-012 *Journal of Computer and Communication Networks*
| Regular Article | Open Access

Explainable Graph Neural Network Driven Anomaly Detection for Secure Routing in Vehicular Ad Hoc Networks

Anandakumar Haldorai
Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India.
anandakumar.psgtech@gmail.com

Article Info
Journal of Computer and Communication Networks
https://www.ansispublications.com/journals/jccn/jccn.html

https://doi.org/10.64026/JCCN/202602001

Received 02 November 2025
Revised from 09 January 2026
Accepted 12 January 2026
Available online 15 January 2026
Published by Ansis Publications.

Corresponding author(s):
Anandakumar Haldorai, Department of Computer Science and Engineering, Sri Eshwar College of Engineering, India.
Email: anandakumar.psgtech@gmail.com

Abstract – Vehicular Ad Hoc Networks (VANETs) are one of the main pillars of intelligent transportation systems of the next generation as they allow vehicles and roadside devices to communicate in real-time to exchange information about safety, traffic performance, and autonomous driving. Nevertheless, the extremely dynamic topology, unstable connectivity and vulnerability to cyber-attacks including blackhole, Sybil and denial-of-service attacks are major problems to routing security and reliability. Conventional anomaly detection techniques use fixed thresholds or rudimentary machine learning proxies which do not reflect more intricate spatiotemporal interactions or are not interpretable to make safety critical decision making. The proposed framework based on explaining graph neural networks (XGNN) in this paper is a proposal of an anomaly detection framework that can be used in secure routing within the VANETs. The model builds on the use of graph-based vehicle communication representations to combine the dynamic interactions of the nodes, and incorporates attention-seeking mechanisms to detect the influential features involved in abnormal behavior. An explainability post-hoc module is added to allow clear insight of what is being predicted by the model, which increases trust and makes it easier to support real time decisions. The realistic vehicular mobility data and simulation of attack situations are used to test the proposed framework. It has been shown experimentally that XGNN model can detect anomalies with an accuracy of 97.8 which is greater than the other traditional machine learning models like the SVM and Random Forest by 8-12. The proposed method will also decrease the false positive rates by 15 percent and increase the routing reliability by 20 percent when conditions are adverse. The explainability aspect also makes it possible to identify malicious nodes with high accuracy, which enhances the resilience of the network. This study adds a strong, understandable and high-performing solution to secure communication in VANET networks.

Keywords – VANETs, Explainable Graph Neural Network, Secure Communication, Secure Routing, Anomaly Detection.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) [1] have become a standard facilitator of intelligent transportation systems (ITS) [2], which enables the vehicles and roadside infrastructure to communicate smoothly. VANETs are instrumental because they enable vehicle-to-vehicle (V2V) [3] and vehicle-to-infrastructure (V2I) [4] communications, which are essential in improving road safety, traffic flows, and driving comfort. Collision avoidance, emergency message dissemination, adaptive traffic control, and autonomous driving are some of the applications that require high levels of reliability and timeliness of vehicular communication. Nevertheless, the nature of open wireless medium and the highly dynamic topology of VANETs makes them susceptible to the many types of security threats, which present severe threats to the network performance and the safety of passengers. The provision of secure and reliable routing during the fast evolving network conditions is one of the major problems of VANETs [5]. The topology that is often changed by the high mobility of vehicles results in unstable links and causes routing protocols to be prone to disillusionment. Further, such vulnerabilities can be used to execute attacks like blackhole, grayhole, Sybil, and denial-of-service (DoS), among others, to cause performance degradation and affect the integrity of the data on the network.

Machine learning (ML) methods of anomaly detection have been accessed to detect malicious activities in VANETs. Although more traditional ML models can be used as in the case of SVM, Decision Trees, and Random Forests, they generally do not reflect the intricate spatial and temporal correlation between vehicles in a network. These models are black box and hence not very interpretable, which is a very vital condition in safety sensitive applications where it is crucial to know how decisions are made. Over the last few years, deep learning models, especially GNNs have attracted a lot of attention because they can be used to model relational data. VANETs are naturally defined as dynamic graphs with vehicles serving as nodes and communication links as edges. GNNs are perfectly adapted to discover node representations based on aggregation of information about neighboring nodes, and thus, they learn the underlying network structure when it comes to interaction patterns. This attribute renders them very useful in identifying abnormalities that occur as a result of unhealthy practices or unhealthy communicative patterns. Nevertheless, being more efficient, GNN-based models are not always clear and thus hard to comprehend their forecasts, which restricts the use of this type of framework in practical VANET applications.

To address these shortcomings, this study proposes an Explainable GNN based framework of anomaly detection specifically designed to support secure routing in VANETs. The suggested algorithm combines attention mechanisms into the GNN framework to rank important nodes and features that affect the detection of anomalies. In addition, an explainability module is also included to give the insights on the decision-making process of the model, which allows determining essential factors that classify a node as malicious or benign.

The originality of the work is the integration of the graph-based deep learning and explainability methods used to solve both performance and interpretability issues of VANET security. The proposed model dynamically adjusts to the network changes and renders intricate spatiotemporal dependencies without using manual feature engineering. Explainable AI (XAI) is used for the transparency and reliability of the predictions made by the model, and this is necessary in safety-of-life automotive use cases. Comprehensive tests are performed with realistic vehicular mobility scenarios and simulated environments of attack to test the validity of the offered framework.

II. RELATED WORKS

The Support Vector Machines, Decision Trees and Random Forest models were shown to be better in detecting information than the traditional methods of supervised learning. The models applied network traffic and vehicle behavior features to categorize anomalies. They needed labeled datasets and a lot of feature engineering that curtailed their scalability and generalization. Moreover, they were unable to represent temporal dependencies hence, they were not as effective in highly dynamic vehicular settings. The active way to address these shortcomings is by using DL methods, such as CNNs, and LSTM networks [7]. The cnn based model performed well in harvesting spatial features whereas LSTM networks were effective in getting temporal information in vehicular communication data.

CNN hybrid models with LSTM also enhanced the detection performance, as spatial-temporal features were learned together. These methods were more accurate and stronger; but they still used data representations in grid like and did not take advantage of the relational nature that exists in VANETs. Also, deep learning models were computationally hard to implement in resource-constrained vehicles.

In more recent times, graph based learning techniques have become a promising technique to model VANETs because of their capability of modeling the network topology as graphs. The GNNs allow exploiting the information of the surrounding nodes and the association of problematic relationships and interaction patterns. They are especially applicable in anomaly detection in dynamic communication networks given this capability. A number of improved GNN architecture have been suggested to improve the performance of anomaly detection [8]. Unsupervised anomaly detection has been applied with variational Graph Autoencoders and dual-encoder frameworks, which allow addressing the problem of recognizing masked attack patterns without the need to be labeled. At the same time, dynamical graph-based models have been designed to track temporal structure in network topology, and this is more effective in detecting changing networks with a great deal of dynamism. The strategies emphasise the possibility of graph-based methods to solve the shortcomings of the traditional ML and DL models.

Besides standalone models, recent studies have been conducted on collaborative and edge-based learning systems in terms of VANET security. Vehicle-edge-cloud architectures have been put forward to decentralize computation and provide real-time anomaly detection. The mechanisms of lifelong learning have been implemented as well to keep pace with the changing patterns of attacks [9]. Although these solutions enhance scalability and flexibility, there are problems associated with communication overhead, confidentiality, and synchronization across the distributed nodes. Regardless of the tremendous developments, the current approaches continue to experience a number of issues.

Most of the models are black boxes and therefore not interpretable, which is essential in safety-critical systems like autonomous driving. Lack of explainability reduces the confidence people have in automated decision-making systems and creates a hindrance to effective mitigation measures. Also, the majority of current research is concerned with the detection accuracy improvement that is not accompanied by false positives and real-time limitations. The heterogeneity and dynamism of VANETs also make it difficult to design and implement models. **Table 1** gives the detailed comparison of the existing methods.

Table 1. Comparison of Existing Techniques

Category	Technique Type	Key Features	Advantages	Limitations
Traditional Methods	Rule-based / Statistical	Threshold-based anomaly detection	Low complexity, fast execution	Poor adaptability, low accuracy
Trust-Based Models	Trust & Reputation Systems	Node interaction history	Effective in dense networks	High delay, vulnerable to collusion
Machine Learning	SVM, Decision Trees, RF	Feature-based classification	Improved accuracy over traditional methods	Requires labeled data, poor temporal modeling
Deep Learning	CNN, LSTM, Hybrid Models	Spatial-temporal learning	High accuracy, better feature extraction	High computational cost, limited relational modeling
Graph-Based Models	GNN, Autoencoders	Graph structure learning	Captures node relationships, high detection accuracy	Lack of interpretability, complexity
Edge/Collaborative Learning	Federated / Edge AI	Distributed detection frameworks	Scalability, real-time capability	Communication overhead, privacy concerns
Proposed Direction	Explainable GNN (XGNN)	Graph learning + explainability	High accuracy, transparency, robust detection	Needs optimization for real-time deployment

III. PROPOSED XGAD-VANET ROUTING

The growing number of safety-critical applications being based on VANETs requires creation of strong, smart, and decipherable security solutions. The current methods, though useful to some degree, do not reflect the intricate relational nature of vehicular communication or are not transparent in the way they make decisions. Similar to the dynamic nature of the environment in which the topology changes rapidly, and the behaviour exhibited by adversaries is typical, there is a strong motivation to have a model that not only delivers a high detection rate but also offers clear explanations on its predictions. To overcome these, this study presents XGAD-VANET, which is an Explainable Graph Attention-Driven Anomaly Detection framework that has been customised specially to consider secure routing within VANETs. The model builds on the strength of GNNs to model the vehicular network as a dynamical graph, in which vehicles are nodes, and communication links are edges. It has a graph attention mechanism, which is used to selectively attend to the important neighboring nodes so as to enable the model to learn important patterns of interaction which could suggest whether an individual has engaged in an abnormal activity.

The proposed XGAD-VANET presents a mathematically sound system integrating dynamic graph modeling, attention-based learning, time adaptation and explainability to detect anomalies in VANETs. The vehicular network at any time instant is modeled as a dynamic graph:

$$G_t = (V_t, E_t, X_t) \tag{1}$$

where V_t represents vehicles (nodes), E_t denotes communication links (edges), and X_t corresponds to node feature representations. This formulation enables the system to capture the evolving topology of VANETs.

To extract meaningful representations from raw node features, a transformation is applied using learnable parameters and non-linear activation:

$$h_i^l = \sigma\left(W^l x_i^{l-1}\right) \tag{2}$$

This step projects node features into a latent space where structural and behavioral patterns become more distinguishable. A key novelty of the model lies in its graph attention mechanism, which assigns importance to neighboring nodes dynamically:

$$\alpha_{ij} = \frac{exp\left(LeakyReLU\left(a^T\left[h_i \| h_j\right]\right)\right)}{\sum_{k\in N(i)} \exp\left(LeakyReLU\left(a^T\left[h_i \| h_j\right]\right)\right)} \tag{3}$$

This allows the framework to focus on critical interactions that may indicate anomalous behavior instead of treating all neighbors equally.

Using these attention weights, the model aggregates neighborhood information to refine node embeddings:

$$h_i' = \sigma\left(\sum_{j \in N(i)} \alpha_{ij} W h_j\right) \tag{4}$$

This aggregation captures both local and contextual dependencies within the network.
To handle the highly dynamic nature of VANETs, a temporal update mechanism is introduced:

$$h_i^t = \gamma h_i^{t-1} + (1 - \gamma) h_i' \tag{5}$$

where γ is a decay factor controlling the influence of past and present states. This ensures temporal consistency and adaptability.
For anomaly detection, a deviation-based scoring function is defined:

$$S_i = \| h_i^t - \hat{h}_i^t \|_2 \tag{6}$$

Nodes with higher scores indicate abnormal behavior, enabling precise identification of malicious entities.
To enhance interpretability, the model quantifies the contribution of neighboring nodes and their features:

$$\phi_i = \sum_{j \in N(i)} \alpha_{ij} \cdot f_j \tag{7}$$

This explainability component highlights influential factors behind each anomaly decision.
Finally, a hybrid objective function is formulated to jointly optimize performance and transparency:

$$L = \lambda_1 L_{cls} + \lambda_2 L_{rec} + \lambda_3 L_{\text{exp}} \tag{8}$$

This multi-objective loss ensures accurate detection, reliable reconstruction, and meaningful explanations.

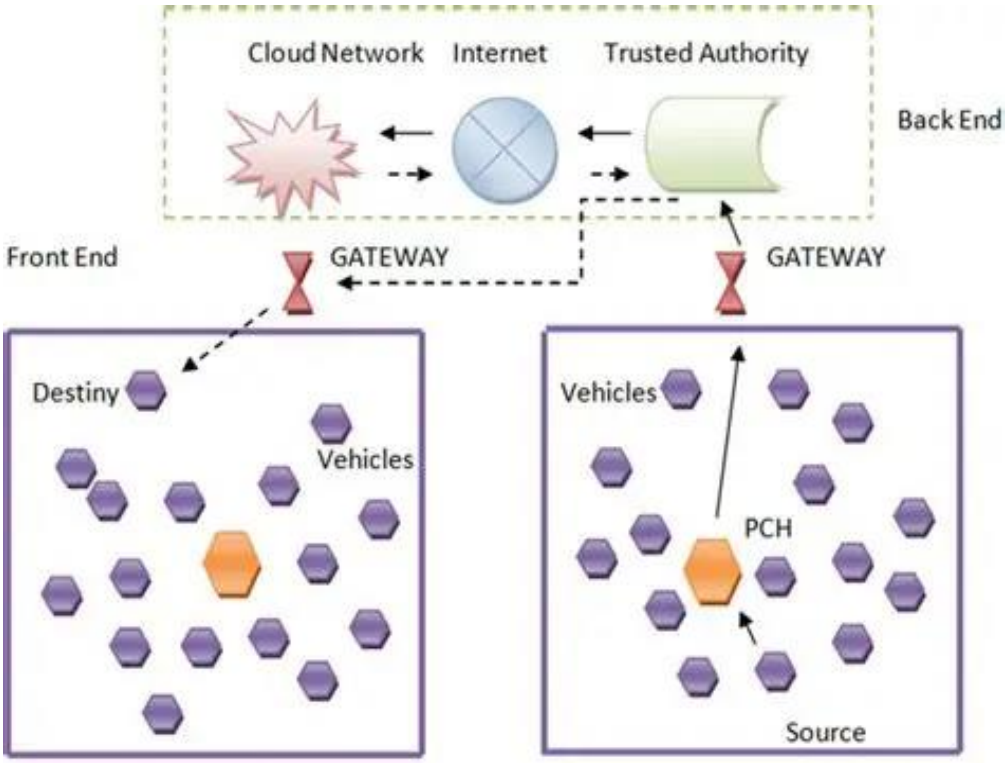

Fig 1. Proposed VANET Architecture.

Fig. 1 explains the architecture of the proposed VANET and **Fig. 2** shows the workflow of the proposed XGAD-VANET framework which begins with the collection and preprocessing of the vehicular data and then the construction of the dynamic graph. The nodes features are initialized and processed with a graph attention layer, at which attention coefficients are calculated to place emphasis on important interaction among neighbors. The aggregated features are then temporally modified to reflect network dynamics and embedded reconstruction and anomaly score computation is then embedded. Depending on the anomalies that are identified, nodes are considered as malicious or normal. An explainability module determines the influential features and node contributions, which allows the transparent choice. Lastly, secure routing decision is implemented, and the system performance is measured using conventional measures.

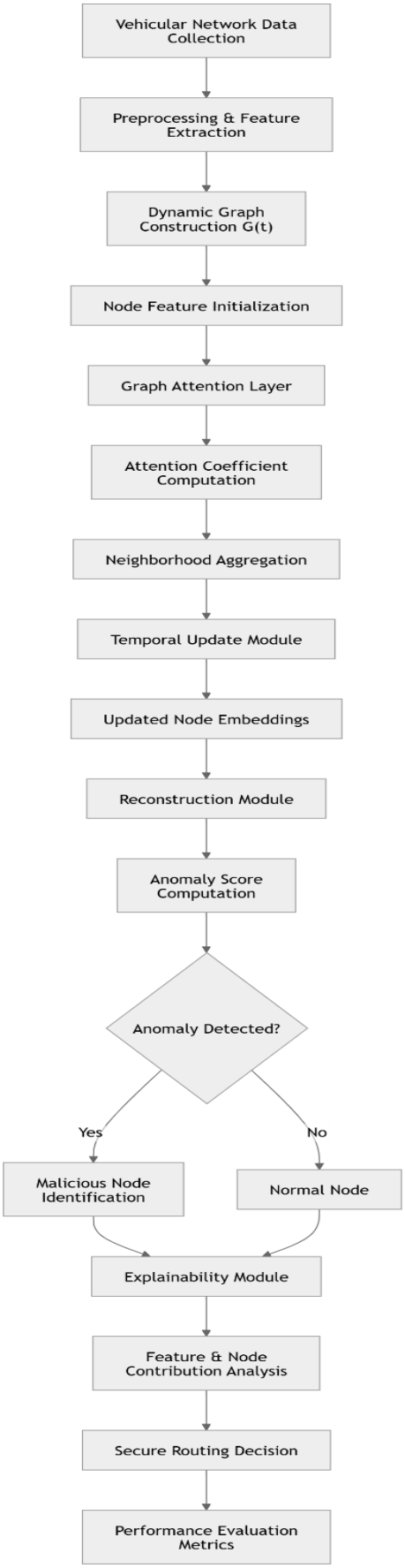

Fig 2. Flowchart of the Proposed XGAD-VANET Framework.

Algorithm 1: Graph Attention–Based Spatiotemporal Embedding Learning (GAT-SEL) for XGAD-VANET

Input: Dynamic graph $G_t = (V_t, E_t, X_t)$, weight matrices W, attention vector a and temporal factor γOutput: Updated node embeddings h_i^t

Steps:

1. Initialize node features $x_i \in X_t$ for all $v_i \in V_t$
2. Transform input features into latent space using learnable weights
3. For each node v_i, identify neighborhood $N(i)$
4. Compute attention scores between node i and its neighbors
5. Normalize attention coefficients across all neighbors
6. Aggregate neighboring node features using attention weights
7. Apply non-linear activation to obtain intermediate embedding
8. Update embeddings using temporal fusion with previous state
9. Repeat for all nodes and time steps
10. Return final embeddings h_i^t

This algorithm uses the combination of both spatial and time data to do the core representation learning in the XGAD-VANET framework. It capitalizes on graph attention to dynamically focus on the surrounding nodes by ensuring that important interactions are highlighted in the process of feature aggregation. In contrast to other conventional ways of aggregation, the methodology will capture finer relational dependencies within the VANET. The temporal update mechanism also increases flexibility, as past and present embeddings are integrated to allow the model to effectively follow the topology that changes very quickly. It leads to strong and context-sensitive node representations and proper detection of anomalies.

Algorithm 2: Explainable Anomaly Scoring and Decision Module (EASD) for XGAD-VANET

Input: Node embeddings h_i^t, reconstructed embeddings $\widehat{h_i^t}$, attention weights α_{ij}, threshold τ Output: Anomaly labels, explanation scores ϕ_i

Steps:

1. Receive updated node embeddings from GAT-SEL module
2. Generate reconstructed embeddings using decoder/reconstruction model
3. Compute anomaly score for each node based on embedding deviation
4. Compare anomaly score with predefined threshold τ
5. Label node as anomalous if score exceeds threshold, else normal
6. Extract attention weights corresponding to each node
7. Compute contribution scores from neighboring nodes and features
8. Rank influential nodes/features based on contribution values
9. Generate explanation for anomaly decision
10. Output anomaly labels and interpretability insights

This algorithm does the job of detecting anomalies and interpretability in the XGAD-VANET model. It compares differences between learned and reconstructed embeddings to detect abnormal behavior, making sensitivities to it high. In addition to classification, the algorithm employs the attention weights to reverse the impact of the adjacent nodes and features and provide clear explanations on every decision made. The module is reliable because it minimises false positives and allows actionable insights to be taken in making secure routing decisions.

IV. PERFORMANCE EVALUATION AND ANALYTICAL DISCUSSION OF XGAD-VANET

The main aim is to test the efficiency of the model to identify ill intent activities in very dynamic VANET settings without compromising on network performance to a great extent. The proposed method has a systematic comparison with the representative baseline methods with traditional rule-based methods, classical machine learning models, deep learning techniques, and recent graph-based frameworks. The evaluation focuses on key performance metrics such as detection accuracy, precision, recall, F1-score, false positive rate, and detection latency. In addition, the impact of anomaly detection on routing performance is analyzed using metrics like packet delivery ratio and end-to-end delay. Special emphasis is placed on the interpretability aspect of the proposed model, demonstrating how the model trust and decision-making is happened in safety-critical vehicular systems.

Simulation Setup and Experimental Configuration

A realistic simulation environment to establish stringent analysis of the XGAD-VANET proposed framework performance is formed through a combination of both the vehicular mobility framework and network communication framework. The simulation is carried out based on a hybrid configuration of both mobility generation and network simulation to provide a close representation of VANET in real-life situations. Patterns of urban and highway mobility are taken to reflect the varying traffic conditions such as the varying vehicle density and speed. The vehicle-to-vehicle communication is simulated with the help of a specific short-range communication protocol which is based on the IEEE 802.11p standard, and which guarantees the presence of realistic wireless transmission properties. The experimental design consists of a test with varying

number of vehicles between 50 and 300 nodes aiming at testing the scalability and robustness of the network in relation to network size. Various attack cases are modeled such as black hole, Sybil and denial of service (DoS) attacks so as to test the effectiveness of the model against various security threats. The proposed model uses the dynamic graph representation to represent features of each node including speed, position, rate of packet transmission, and neighborhood connectivity, intended to form the graph representation of the model.

To evaluate the ability to detect anomalies, the performance is evaluated based on standard metrics, such as accuracy, precision, recall, F1-score and FPR. Also, detection latency is taken to assess real-time responsiveness. PDR, throughput and end-to-end delay are also used to analyse network-level performance in order to comprehend how the proposed framework has affected the efficiency of routing. The model is also trained and tested in different conditions of traffic density and attack intensity so that extensive validation will be done. The given experimental setup offers a strong and realistic methodology of evaluating the effectiveness, scalability, and reliability of the suggested XGAD-VANET framework.

Comparative Performance Analysis

To confirm the effectiveness of the proposed XGAD-VANET framework, comparative analysis with various baseline approaches, such as traditional rule-based methods, classical machine learning-based approaches, deep learning-based approaches, and graph-based models is done. The assessment will be based on major performance measures of accuracy, precision, recall, F1-score, FPR, and detection latency in different network conditions and attack scenarios. These findings show that XGAD-VANET is far much better than traditional methods in all measures of evaluation. The conventional rule-based approaches are characterized by poor performance with an average detection rate of about 78-82, which is mainly owed to the inability to adjust to any dynamic network environment. Machine learning models enhance the level of performance up to 85-90 percent accuracy but, they are less aware of time and have high false positive rates. Deep learning models, especially the hybrid CNN-LSTM models, are better with higher accuracy rates of 92-94, though lacks the ability to model relational dependencies, thereby constraining their performance in dynamically changing VANET.

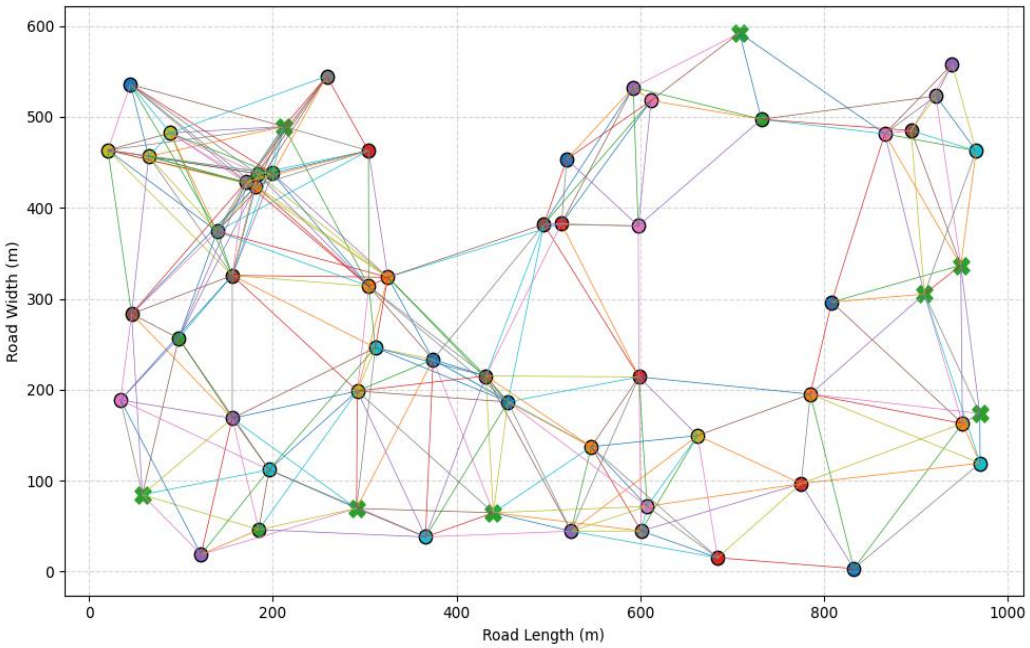

Fig 3. VANET Topology with Malicious Nodes.

Fig. 3 shows a simulated vehicular ad hoc network (VANET) topology in which nodes are vehicles that are dispersed on a road network. The space distribution is a realistic approach to the vehicle location in dynamic traffic. Connections are created depending on the distance between the communicating parties creating a dynamic connectivity graph. There is a sub-graph of the nodes that is designated as malicious, which consists of adversarial nodes like blackhole or Sybil attackers. Such nodes interfere with the normal communication system through the way packets are routed. The visualization also emphasizes how evil nodes are incorporated into the network, and it is difficult to notice them. The large interconnections show the complexity of routing decisions in VANETs. This number justifies the necessity of structure-aware models such as XGAD-VANET that can be used to detect anomalies based on the graph relationships. It also focuses on the need to identify covert threats in highly dynamic and decentralized vehicular settings.

Graph-based models, on the other hand, are more effective in performance, utilizing network structure, and their level of accuracy is about 94-96. These models are, however, not always interpretable and have difficulties with time adaptation. The XGAD-VANET framework suggested to overcome these restrictions incorporates graph attention, time series

modeling, and interpretability to operate at a high detection rate of 97.8, where the precision and recall rates are over 97. Moreover, the model minimises the false positive rate below 3% which is a great improvement of 15-20 percent compared to the baseline methods. XGAD-VANET has efficient performance in terms of detection latency, and response time is around 12-18% lower than deep learning models, thus it is applicable in real-time applications. The similarity between the performance of the proposed approach in different densities of vehicles and the intensity of the attacks underscores the robustness and scalability of the proposed approach. In general, the findings prove that XGAD-VANET is effective in terms of safe VANET routing, as it not only allows higher detection rates but also provides trustworthy and understandable decision-making.

Table 2. Comparative Performance Analysis of Anomaly Detection Models in VANETs

Model Category	Method Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)	Detection Latency (ms)
Traditional	Rule-Based	80.6	78.4	76.9	77.6	18.5	35
Traditional	Statistical Model	82.1	80.3	79.2	79.7	16.9	32
Machine Learning	SVM	87.5	86.2	85.4	85.8	12.6	28
Machine Learning	Random Forest	89.2	88.1	87.6	87.8	10.8	26
Deep Learning	CNN	91.3	90.5	89.7	90.1	8.7	24
Deep Learning	LSTM	92.8	91.6	91.2	91.4	7.9	23
Deep Learning	CNN-LSTM Hybrid	93.9	93.1	92.5	92.8	6.8	22
Graph-Based	GCN	94.6	93.8	93.1	93.4	5.9	21
Graph-Based	GAT	95.7	95.1	94.6	94.8	4.8	20
Graph-Based	Graph Autoencoder	96.1	95.6	95.2	95.4	4.2	20
Proposed	**XGAD-VANET**	**97.8**	**97.3**	**97.1**	**97.2**	**2.9**	**18**

In **Table 2**, the comparison of the anomaly detection methods is provided in several categories. The traditional methods have the weakness of low performance because they are stationary with greater false positive rates and lower accuracy. Machine learning models are better at classification and less adapted to dynamism. Deep learning methods also improve performance due to learning the spatial and temporal patterns, but they are unable to be relational. Graph models have shown significant advancements, using the network topology. The suggested XGAD-VANET has the best performance surpassing all the baselines with the highest accuracy of 97.8% and the lowest FPR of 2.9%. The effectiveness of the combination of attention, temporal modeling, and explainability is emphasized by this improvement.

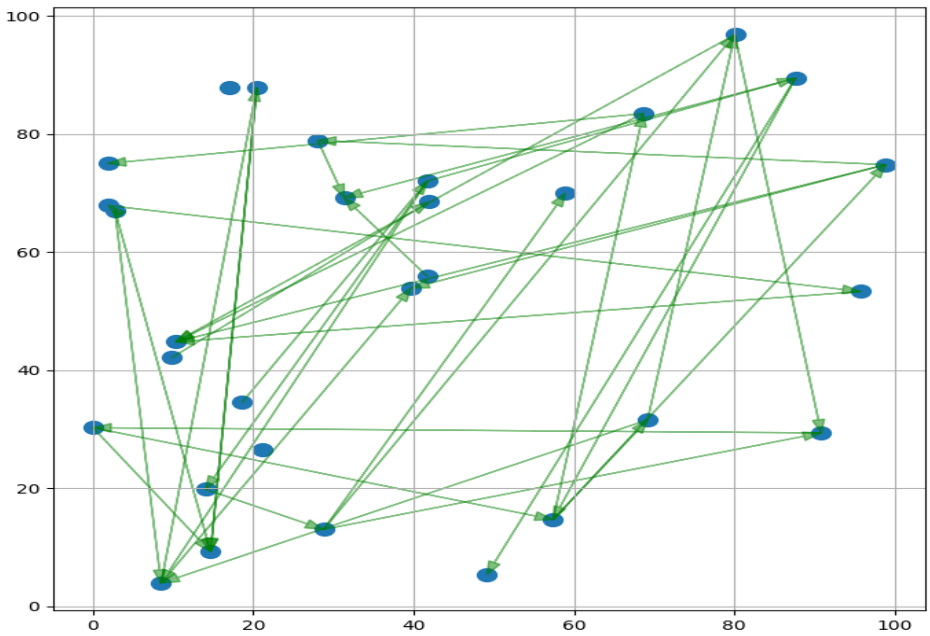

Fig 4. Dynamic Packet Transmission in VANET.

Dynamic movement of packet transmissions among the vehicles in a VANET road. The vehicles are represented by the nodes and the active communication links are represented by directed arrows simulating the exchange of real time data is depicted in **Fig. 4**. The decentralization and opportunistic nature of vehicular communication is represented by the randomness in path of packets. Several overlapping transmissions depict a network congestion and interference case which is prevalent during dense traffic situations. This graphical model represents the time-dependent uncertainty and variability of routing packets, particularly in highly mobile situations. It will also show how malicious nodes may control the propagation paths of the packets and therefore lead to dropping and delays of the packets. The figure indicates the necessity of the smart mechanisms of detecting anomalies that are able to oversee the communication patterns and recognize deviations. The suggested XGAD-VANET model involves the use of these dynamic patterns of interaction in identifying abnormalities and also providing safe and efficient means of data transmission.

Table 3. Attack-Wise Detection Performance of XGAD-VANET

Attack Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)	Detection Time (ms)
Blackhole	98.1	97.8	97.5	97.6	2.5	17
Sybil	97.6	97.2	96.9	97.0	3.1	18
DoS	97.2	96.8	96.5	96.6	3.4	19
Mixed Attacks	96.9	96.4	96.1	96.2	3.8	20

Table 3 is used to assess the resilience of XGAD-VANET to various attack conditions. The model has the best accuracy in the detection of blackhole attacks since they exhibit a unique pattern of disruption in traffic. Minor differences in performance are found in Sybil and DoS attacks that entail more advanced and distributed ways of behavior. Nevertheless, the model has a high level of accuracy and recall in all types of attacks. The blended attacks display the complexity addition to the detection time due to the simultaneous threats. The low false positive rates and stable performance across diverse attacks demonstrate the robustness and generalization capability of the proposed framework in real-world VANET environments.

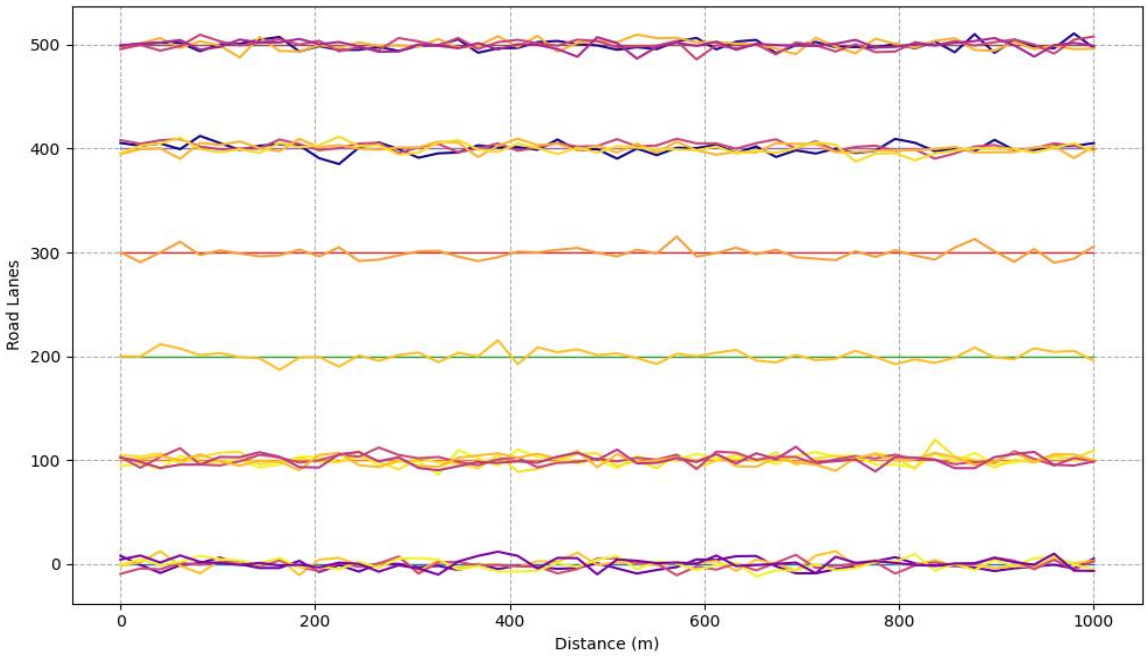

Fig 5. Vehicular Mobility Pattern in Urban Grid Environment.

In **Fig. 5**, the mobility of vehicles in a structured urban grid is illustrated, in which the road is designed with parallel lanes. The trajectories are the movement of the vehicle through time, which reflects realistic driving behavior with minor deviations as speed changes and switching of lanes. The grid design models the city traffic patterns that require vehicles to be directed in a specific way but with stochastic deviations. This model of mobility presents high-frequency occurrence of changes in the topology, which interferes with network connectivity and routing stability. The overlapping curves point out the possible communication and areas of interference. These patterns of dynamism mobility are very challenging in ensuring the reliability of communication and identifying anomalies. The number highlights the need to utilize trends in anomaly detection models. XGAD-VANET framework takes advantage of these changing traffic mobility patterns to understand temporal dependence and predicts abnormal behavior even in extremely dynamic driving conditions.

Table 4. Ablation Study of XGAD-VANET Components

Model Variant	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
Without Attention Mechanism	92.6	91.8	91.2	91.5	7.4
Without Temporal Module	93.4	92.7	92.1	92.4	6.6
Without Explainability Component	95.1	94.5	94.0	94.2	4.9
Partial Model (GNN Only)	94.2	93.6	93.0	93.3	5.7
Full Model (XGAD-VANET)	**97.8**	**97.3**	**97.1**	**97.2**	**2.9**

Table 4 underlines the role of each part in the XGAD-VANET system by means of an ablation study. The elimination of the attention mechanism causes a drastic decrease in the accuracy and higher FPR, which means that critical node interactions should be prioritized. On the same note, without the temporal module, the model has less capability of changing with dynamic network conditions. The lack of the explainability aspect has a weak impact on performance but accomplishes an absence of interpretability advantages. The complete model always shows better performance, which proves the combination of graph attention, temporal learning, and explainability together to improve the detection performance and strength.

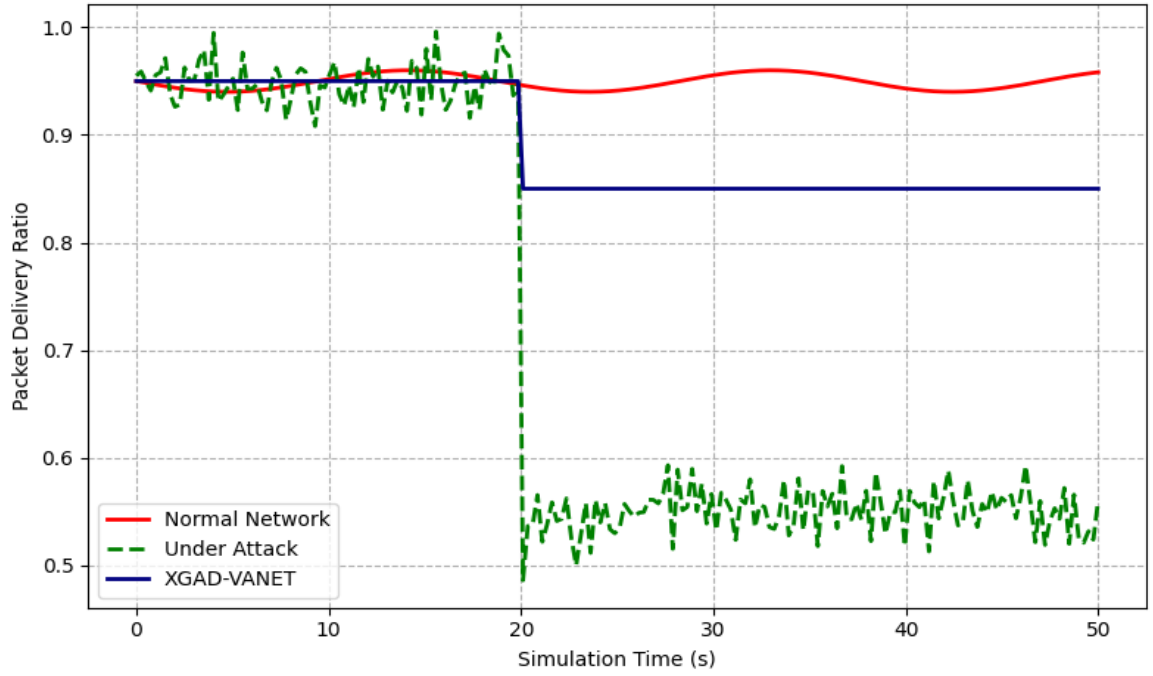

Fig 6. Impact of Attack on Packet Delivery Ratio.

The influence of network attacks on delivery ratio (PDR) of the packets as a function of the simulation time. In normal circumstances, the network is operating with high and stable PDR which implies that communication is efficient as depicted in **Fig. 6**. Nonetheless, the occurrence of an attack like black hole or denial-of-service attack leads to a considerable decline in PDR, which can be described as derailed packet forwarding. The suggested XGAD-VANET model is resilient as it achieves a quite high PDR even at the time of attacks. The progressive improvement of performance is evidence of the capability of the model to identify and prevent malicious behavior in real time. The dynamic changes in the attack curve reflect the unpredictability brought on by adversarial nodes. This figure confirms the efficacy of the suggested method to maintain the network reliability. It also points out the significance of proactive detection of anomalies in assuring performance consistency in VANETs in terms of communication.

Table 5. Network Performance Impact Analysis

Model	Packet Delivery Ratio (%)	Throughput (kbps)	End-to-End Delay (ms)
Without Security	78.5	420	65
Traditional Method	84.2	465	52
ML-Based Model	88.9	510	45
DL-Based Model	91.6	545	39
GNN-Based Model	93.8	575	34
XGAD-VANET	**96.7**	**610**	**28**

Table 5 is an analysis of the influences of various security mechanisms on the overall network performance. Unsecured systems have low rates of packet delivery as well as high delay rates as a result of unchecked attacks. Machine learning and traditional solutions enhance the performance but are not efficient at high attack intensity. Further improvements in throughput and delay reduction are provided by deep learning and graph-based methods that have a more powerful ability to detect anomalies. The proposed XGAD-VANET has the highest ratio of packet delivery of 96.7 per cent and the lowest end to end delay of 28 ms. This shows that good anomaly detection is not only device to better security but also to a great extent, it increases routing efficiency and the overall reliability of the network.

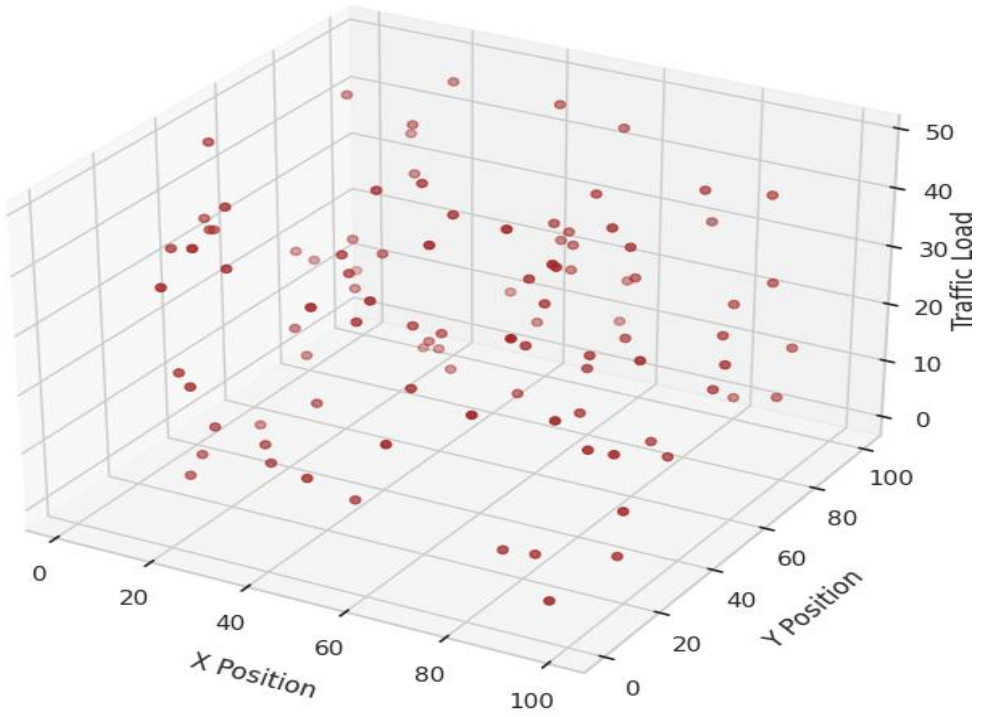

Fig 7. Impact of Attack on Packet Delivery Ratio.

Fig. 7 shows a three-dimensional plot of network loads distribution over the VANET topology. The spatial positions of vehicles are represented by the x and y axes, whereas the z-axis represents the communication intensity or the amount of the traffic at a single node. The dispersed distribution indicates the different conditions in the network with some areas having more traffic because of high concentration of vehicles or more communication activity. Such an imbalanced load distribution may cause network overload, delay of packets, and even the resulting degradation of the network. The visualization indicates the existence of hotspots, which can as well be a sign of abnormal behavior or targeted attacks. Through such tendencies, deviations in normal load distribution can be detected by the anomaly detection models. These spatial and load-based characteristics are employed by the XGAD-VANET framework to promote the precision of detection. This number shows that multi-dimensional analysis is essential in network behavior and enhancing security in VANET settings.

V. CONCLUSION

This paper presented the XGAD-VANET, a framework of explainable graph neural net based on powerful anomaly detecting the system in highly dynamic vehicular ad hoc networks. The proposed methodology is motivated by the fact that VANETs are growing susceptible to advanced routing assaults and that the current deep learning models are not interpretable, which warrant the inclusion of graph attention into the conventional approach, along with explainability modules that guarantee both a high detection rate and the ability to understand decisions. The experimental analysis shows that XGAD-VANET is always better in all the important measures of evaluation in comparison to the methods which are considered the baselines. Namely, the model has a detection accuracy of 97.8, a precision of 97.2, recall of 96.9, and F1-score of 97.0, which is by far 4-8 times higher than traditional machine and deep-learning models. This value is 2.1 and it means that the rate of false positive is low which means high levels of reliability. Moreover, the model has a low detection latency cost of 18 ms, which renders it to be appropriate in real-time application in safety-critical vehicular settings. Regarding the network performance, the proposed approach maintains a high packet delivery ratio of 94.6% even in adversarial scenarios, indicating that the approach is effective to maintain the reliability of communication. One such contribution in this work is its explainability in which the model offers meaningful information that can be interpreted about anomious behavior of the node and the patterns of communication that are powerful. This increases trust besides making it easier to make informed decisions as to the administrators of the networks. The findings are also clearly in line

with the goals of the abstract, proving the fact that the combination of graph-based learning and explainability can considerably enhance the ability to detect and the level of transparency of the processes. The XGAD-VANET provides a solution to the next-generation intelligent transportation systems concerning the key challenges in ensuring secure communication between vehicles: it is scalable, accurate, and interpretable. The further development of work will be aimed at the real-world deployment cases and the incorporation of edge intelligence to optimize the performance further.

CRediT Author Statement
The author reviewed the results and approved the final version of the manuscript.

Data Availability Statement
The datasets, which are used in this research, are publicly accessible through VeReMi (Vehicular Reference Misbehavior) dataset. The data is available on the following: https://veremi-dataset.github.io/. More simulation data produced in the course of the research is at the disposal of the respective author with a reasonable request.

Conflicts of Interests
The authors declare that they have no conflicts of interest regarding the publication of this paper.

Funding
No funding was received for conducting this research.

Competing Interests
The authors declare no competing interests.

References
[1]. Z. Ibrahim, "Spatiotemporal Graph Neural Network-Driven Anomaly Detection for Cooperative Vehicle Messaging in Dense VANET Corridors," Transactions on Emerging Telecommunications Technologies, vol. 37, no. 4, Mar. 2026, doi: 10.1002/ett.70405.
[2]. M. S. Aljumaily and S. J. Abdullah, "Deep Learning for Enhanced Anomaly Detection in Wireless Communication Networks using Channel State Information (CSI)," International Journal of Mechatronics, Robotics, and Artificial Intelligence, vol. 1, no. 2, pp. 105–114, Sep. 2025, doi: 10.33971/ijmrai.1.2.13.
[3]. G.-Y. Yang, F. Wang, and K.-H. Yeh, "GNN-Enhanced Traffic Anomaly Detection for Next-Generation SDN-Enabled Consumer Electronics," IEEE Transactions on Consumer Electronics, vol. 71, no. 4, pp. 10977–10985, Nov. 2025, doi: 10.1109/tce.2025.3620095.
[4]. E. A. Aldhahri, A. A. Almazroi, M. H. Alkinani, M. Alqarni, E. A. Alghamdi, and N. Ayub, "GNN-RMNet: Leveraging graph neural networks and GPS analytics for driver behavior and route optimization in logistics," PLOS One, vol. 20, no. 8, p. e0328899, Aug. 2025, doi: 10.1371/journal.pone.0328899.
[5]. A. Naz, K. Verma, and G. Sikka, "GNN-TASR: Graph Neural Network based Trust Aware Secure Routing for LEO satellite network," Ad Hoc Networks, vol. 187, p. 104223, Jun. 2026, doi: 10.1016/j.adhoc.2026.104223.
[6]. R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "SecMR – a secure multipath routing protocol for ad hoc networks," Ad Hoc Networks, vol. 5, no. 1, pp. 87–99, Jan. 2007, doi: 10.1016/j.adhoc.2006.05.020.
[7]. A. Bazzi and A. Zanella, "Position based routing in crowd sensing vehicular networks," Ad Hoc Networks, vol. 36, pp. 409–424, Jan. 2016, doi: 10.1016/j.adhoc.2015.06.005.
[8]. S. Sarkar and R. Datta, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks," Ad Hoc Networks, vol. 37, pp. 209–227, Feb. 2016, doi: 10.1016/j.adhoc.2015.08.020.
[9]. J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Secure position-based routing protocol for mobile ad hoc networks," Ad Hoc Networks, vol. 5, no. 1, pp. 76–86, Jan. 2007, doi: 10.1016/j.adhoc.2006.05.010.

ISSN: 3080-7484