

Quantile cosh loss-based Dense Residual Dual-Shuffle Attention Network for Malicious Node Detection in VANET

Raghunath Kumar Babu. D

Department of Cybersecurity

Rajeev Gandhi Memorial College of Engineering and Technology College

Nandyal District, Andhra Pradesh 518501

raghunath.d29@gmail.com

Abstract: In Vehicular Ad-hoc Networks (VANETs), detecting malicious nodes is essential to ensure secure data transmission and maintain trust among communicating vehicles. To address emerging threats, modern VANET architectures increasingly rely on intelligent detection models capable of learning complex attack patterns from large-scale mobility data. Such detection is crucial because compromised nodes can disrupt network functionality, spread false information, and endanger overall traffic safety. However, existing detection techniques often face challenges, like high computational overhead and difficulty in identifying sophisticated attacks in dynamic network environments. Therefore, there is a pressing need to develop a more efficient and adaptive model that can accurately detect malicious nodes while minimizing system complexity and performance degradation. Here, a model named Quantile cosh loss-based Dense Residual Dual-Shuffle Attention Network (Qcosh-loss_DRDA-Net) is devised for malicious node detection in VANET. This model leverages quantile-aware optimization to handle outliers effectively while using multi-level attention to capture nuanced behavioral deviations of malicious nodes. At first, VANET is simulated, and at the Base Station (BS), data pre-preparation is performed by handling missing values and feature normalization. Moreover, feature screening is accomplished by Hybrid similarity measures. At last, malicious nodes are detected by Qcosh-loss_DRDA-Net. The integration of dense residual connections and dual-shuffle attention modules enables the model to learn deeper representations while avoiding gradient vanishing issues. The efficacy of Qcosh-loss_DRDA-Net is analyzed by considering the metrics, namely accuracy, hit rate, miss rate, precision, recall, and rejection rate, which obtained superior values of 96.70%, 0.959, 0.204, 94.74%, 95.99% and 0.032.

Keywords: Vehicular Ad-Hoc Networks, Malicious Nodes, Dense Residual Dual-Shuffle Attention Network, Feature Normalization, Feature Screening.

Nomenclature

Abbreviation	Description
VANET	Vehicular Ad-hoc Network
MANET	Mobile Ad-hoc Network
ITS	Intelligent Transportation System
V2V	Vehicle-to-Vehicle Communication
V2I	Vehicle-to-Infrastructure Communication
OBU	Onboard Unit
RSU	Roadside Unit
BS	Base Station
DRDA-Net	Dense Residual Dual-Shuffle Attention Network
DRB	Dense Residual Block
CA	Channel Attention
RDAB	Residual Dual Attention Block
ML	Machine Learning
AI	Artificial Intelligence
DPGHA	Dynamic Preventing Gray-Hole Attack mechanism
DAMASCO	Detection of Anomalous Behavior in Smart Conveyance Operations

1. Introduction

VANETs represent an advanced subclass of MANETs specifically designed to support communication between vehicles and roadside infrastructure. As the density of connected vehicles continues to rise, VANETs are becoming indispensable components of smart mobility ecosystems. They form a crucial backbone for the development of ITS, enabling applications such as accident avoidance, traffic management, and autonomous driving coordination. VANETs operate through dynamic wireless

connections that allow vehicles to exchange information about their position, speed, and environment in real time, thereby promoting safer and more efficient transportation [1] [2]. The highly mobile nature of vehicles further adds to the complexity, requiring communication protocols that can rapidly adapt to changing topologies. By facilitating the exchange of safety messages, traffic updates, and infotainment data, VANETs enhance road safety, improve traffic flow, and support autonomous driving technologies. However, this constant flow of information also increases the attack surface, giving adversaries multiple opportunities to compromise network integrity.

However, the decentralized and open-access nature of VANETs also makes them highly vulnerable to various security threats. Among these threats, the presence of malicious nodes poses one of the most severe challenges. Malicious nodes can intentionally inject false data, alter routing paths, impersonate other vehicles, or disrupt communication channels, resulting in misinformation and potential road hazards. Such manipulations not only misguide individual drivers but can also mislead entire traffic management systems. The fast-moving and self-organizing characteristics of vehicular networks make the identification and isolation of these malicious entities particularly difficult. Without effective countermeasures, VANET communication can be easily compromised, leading to effects on road safety, user privacy, and network reliability [3]. Therefore, continuous research is required to strengthen VANET security models against both known and emerging attack vectors. Consequently, detecting and mitigating the influence of malicious nodes has become an essential priority in securing VANET environments and ensuring that information dissemination within these systems remains accurate, trustworthy, and efficient [4].

The detection of malicious nodes within VANETs has attracted considerable research attention due to its significance in maintaining reliable and secure vehicular communication. As VANET infrastructures evolve, detection strategies must also adapt to handle increasing data complexity and diverse mobility patterns. Various detection mechanisms have been developed, each aiming to identify abnormal behaviors and prevent compromised nodes from spreading false information [4]. Among the most common strategies are trust-based and reputation-based techniques, which evaluate the consistency of a node's actions over time to determine its reliability. Nodes exhibiting suspicious or contradictory behavior are flagged as potentially malicious and isolated from the network. Cryptographic approaches enhance this process by securing message exchange through digital signatures, encryption, and authentication protocols, ensuring that transmitted data originates from legitimate sources. However, cryptographic solutions alone cannot detect insider attacks, where compromised nodes possess valid credentials. More recently, Machine Learning (ML) and Artificial Intelligence (AI) models have emerged as powerful tools for malicious node detection, capable of learning behavioral patterns from historical vehicular data to predict future threats. Deep learning models, in particular, offer adaptive and high-accuracy detection capabilities under dynamic driving conditions [5]. Furthermore, hybrid detection frameworks, which integrate trust management, cryptography, and intelligent algorithms, aim to balance computational efficiency and detection accuracy. However, these techniques still face limitations, such as high processing costs, communication overhead, and scalability issues in densely populated traffic environments. Therefore, ongoing research continues to focus on designing lightweight, real-time, and adaptive detection systems that can ensure secure communication in VANETs without compromising performance or user privacy. Such systems must not only detect malicious activity but also minimize false alarms to avoid unnecessary network disruptions. Robust malicious node detection mechanisms are vital for sustaining the reliability, safety, and overall integrity of next-generation vehicular networks [3] [6].

The research aims to implement a Qcosh-loss_DRDA-Net for the detection of malicious nodes in VANET. Initially, the VANET system model is simulated, where vehicles communicate dynamically with each other. At BS, data pre-preparation is done by handling missing values and feature normalization. Such preprocessing ensures that the input data is consistent and free from distortions that might impair model performance. Moreover, feature screening is accomplished utilizing Hybrid Similarity Measures. Finally, malicious nodes are detected using the Qcosh-loss_DRDA-Net model. The loss function of DRDA-Net is modified using the Qcosh-loss, which is developed by combining the Quantile loss and the log cosh loss.

The contribution of the research is summarized as follows:

Devised Qcosh-loss_DRDA-Net for malicious node detection in VANET: An advanced framework named Qcosh-loss_DRDA-Net is developed to identify malicious nodes in VANET. The loss function of DRDA-Net is modified by Qcosh-loss, which is the combination of Quantile loss and log cosh loss. This modification enables the model to achieve higher convergence stability and improves classification accuracy even under noisy conditions.

The remaining sections are structured as follows: Section 2 reviews the strengths and issues of preceding schemes, Section 3 presents the system model, Section 4 describes the methodology of Quantile loss_DRDA-Net, Section 5 discusses the results, and Section 6 concludes the research.

2. Motivation

Detecting malicious nodes in VANETs is important because false or tampered information from such nodes can cause traffic accidents and disrupt communication between vehicles. Even minor falsified updates, such as incorrect speed or position data, can trigger serious chain reactions that affect multiple vehicles simultaneously. The fast-changing network structure and lack of centralized control make it difficult to identify and manage these malicious behaviors. Therefore, there is a strong need for an intelligent and efficient method to detect and prevent malicious activities, ensuring safe and reliable communication in VANETs.

2.1 Literature Review

S. Masood, *et al.*, [7] developed Fake node and counterfeit message algorithms for preventing false node messages. This method achieved better network stability by ensuring that only genuine messages were exchanged between vehicles. However, its heavy dependence on frequent verification processes resulted in increased latency during peak traffic conditions. However, it failed to reduce the communication overhead caused by continuous message verification. T. Anjali, *et al.*, [8] presented X-GEVON to detect multiple attacks in VANET. This method achieved improved detection of multiple attacks by integrating explainable intelligence, which enhanced transparency and trust in VANET security decisions. The use of explainable models also made it easier to interpret system behavior during attack scenarios. However, it failed to minimize the computational complexity, making it less suitable for real-time applications in dense vehicular environments. A. Malik, *et al.*, [9] designed for preventing DPGHA Gray-Hole attacks. Though this method effectively detected and prevented gray-hole attacks, ensuring smoother data transmission and improved network reliability in VANETs, it failed to maintain performance in large-scale networks with high vehicle density. The model's performance degradation under heavy traffic suggests its limited adaptability to city-level VANET deployments. E. P. Valentini, *et al.*, [10] introduced Detection of Anomalous Behavior in Smart Conveyance Operations (DAMASCO) for misbehavior detection in vehicular networks. Though this method efficiently identified misbehaving nodes in vehicular networks, enhancing overall network trust and safety, it did not handle sudden spikes in network traffic, which affected real-time detection performance. Moreover, its sensitivity to abrupt behavioral fluctuations could result in an increased number of false alarms during high-mobility scenarios.

2.2 Challenges

The problems of current methods are summarized as follows:

- ❖ The X-GEVON framework presented in [8] enhanced the detection of coordinated and stealthy attacks in VANETs by providing interpretable attack patterns, which helped network administrators to understand potential threats. Despite its strengths, the model relies heavily on computationally intensive operations, limiting its deployment on low-resource vehicular units. Despite this, it struggled with scalability issues, making it less effective in large networks with numerous vehicles and high data traffic.
- ❖ The DAMASCO mechanism introduced in [10] improved early identification of anomalous behaviors, allowing preventive actions before attacks could propagate across the network. Its multi-layered anomaly evaluation enhances detection accuracy but contributes significantly to processing load. However, it suffered from high energy consumption and processing overhead, which could limit its deployment in resource-constrained vehicular devices.
- ❖ Detecting malicious nodes in VANETs in real-time remains challenging due to high vehicle mobility, frequent topology changes, and unpredictable traffic conditions. Furthermore, the increasing sophistication of attackers demands models capable of recognizing subtle and evolving threat signatures. There is a need for adaptive and lightweight frameworks that can efficiently detect and mitigate malicious behavior without compromising communication efficiency or network performance.

3. System Model

In the system model of VANET [11], vehicles communicate directly with one another through a decentralized ad hoc network, forming a system known as IVC. This decentralized architecture eliminates reliance on a central controller, allowing the network to self-organize even under highly dynamic mobility conditions. The network primarily operates through two communication modes, V2V, which enables data exchange among moving vehicles, and V2I, which connects vehicles to roadside infrastructure. Each vehicle is equipped with an OBU that manages communication, data processing, and network services within the

VANET framework. The OBU also assists in running security protocols, participating in routing decisions, and performing initial threat assessment when suspicious activity is detected. The infrastructure consists of multiple RSUs placed along roadways, facilitating seamless data transmission, network coordination, and connectivity with external networks. Fig. 1 portrays the system model of VANET.

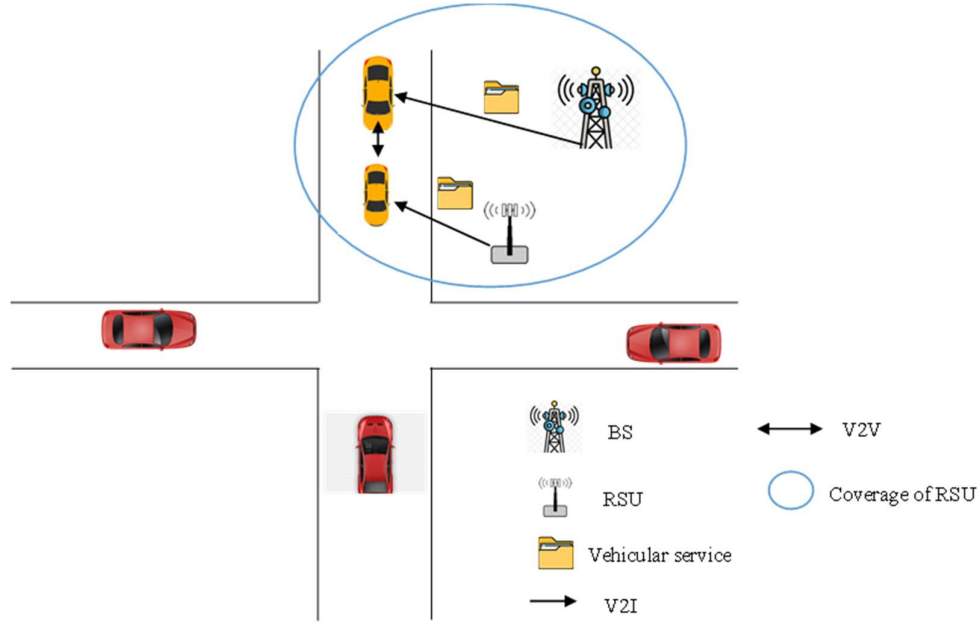


Fig. 1. System model of VANET

4. Proposed Quantile-log cosh loss-aware Dense Residual Dual-Shuffle Attention Network to Detect Malicious Nodes in VANET

Detecting malicious nodes is critical for ensuring secure data transmission and maintaining trust among vehicles. Even a single compromised node can influence nearby vehicles and trigger a chain of misinformation, leading to widespread network disruption. Malicious nodes can disrupt network operations, propagate false information, and compromise overall traffic safety. However, existing detection methods often face challenges, like as high computational overhead and difficulty in identifying sophisticated attacks in highly dynamic network environments. Here, Qcosh-loss_DRDA-Net is proposed for malicious node detection in VANETs. Initially, the VANET is simulated [11]. In BS, data is taken from the dataset [12] and is subjected to data preprocessing that is performed utilizing handling missing values and feature normalization [13]. Such preprocessing ensures that the input data retains consistency, preventing noise and irregularities from degrading model performance. Then, feature selection is carried out using hybrid similarity measures [14]. Finally, malicious nodes are identified using the Qcosh-loss_DRDA-Net model [15] [16]. Fig. 2 displays the block diagram of Qcosh-loss_DRDA-Net to detect a malicious node in VANET.

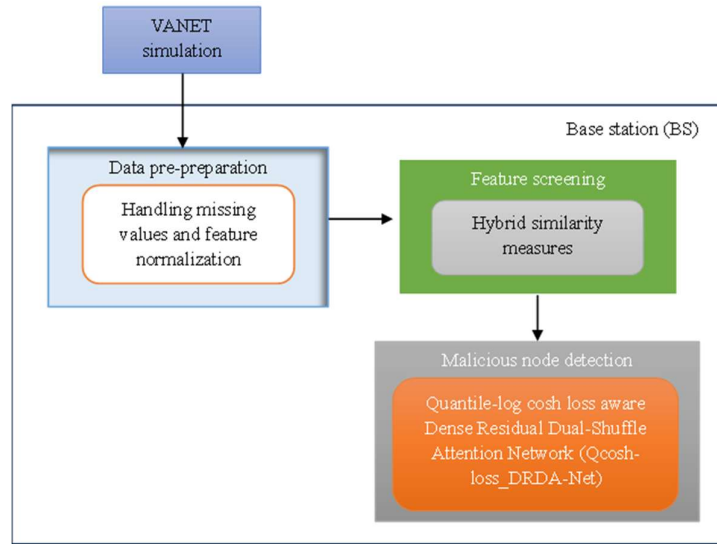


Fig. 2. Block diagram of *Qcosh-loss_DRDA-Net* for detecting malicious nodes in VANET

4.1 Data Collection for Malicious Node Detection

The VANET-MaliciousNode dataset [12] contains communication data from vehicles in a simulated vehicular ad-hoc network, including both normal and malicious nodes. The dataset provides a realistic representation of VANET communication behavior, enabling effective training of the proposed model. It provides features, namely node ID, location, speed, and message details, along with labels indicating whether a node's behavior is legitimate or malicious. The input data taken is expressed as,

$$M = \{M_1, M_2, \dots, M_i, \dots, M_n\} \quad (1)$$

where M_i denotes i^{th} data taken from the database M , and the entire data in the database is implied as M_n .

4.2 Data Pre-Preparation using Handling Missing Values and Feature Normalization

Data pre-preparation involves refining raw input data to ensure consistency and reliability before model training and analysis. This stage is crucial because any inaccuracies in the raw dataset directly affect the performance of the learning model. The input data M_i with dimensions of $[l \times c]$ is subjected to the data pre-preparation phase. The collected VANET data with a specific dimension is processed by handling missing values and performing feature normalization [13]. Missing values are addressed using appropriate imputation techniques to prevent data distortion, while normalization scales all features to a uniform range, ensuring fair contribution of each attribute. Normalization also accelerates training by improving gradient stability. This process enhances model stability and accuracy by reducing bias caused by uneven data distribution. The rows containing missing values are expressed as,

$$Y = Y \setminus \{y_k \mid y_k = \infty \text{ or } y_k = -\infty\} \quad (2)$$

$$Y = Y \setminus \{y_k \mid y_k = Nan\} \quad (3)$$

As the dataset includes numerical attributes with different ranges, Z-score normalization is used to standardize them and convert all feature values to a uniform scale. This transformation ensures that features with naturally larger magnitudes do not overshadow those with smaller ranges. Here, feature normalization is expressed as,

$$N_i = \frac{\vartheta - \sigma}{\eta} \quad (4)$$

where, N_i with dimension of $[l \times c]$ signifies the output, ϑ is the value of the original feature, η is the standard deviation, and σ represents the mean value.

4.3 Feature Screening Utilizing a Hybrid Similarity Measure

Feature screening is carried out to identify and retain the most informative features that contribute effectively to model performance. This step is essential because high-dimensional data often contains redundant information that increases computational burden. The pre-prepared data N_i with a dimension

of $[l \times c]$ undergoes feature screening, where irrelevant or redundant attributes are filtered out. A Hybrid Similarity Measure [14] is utilized to compare relationships between features and select those with stronger significance for analysis. By combining multiple similarity criteria, the method provides a more balanced and reliable feature evaluation. This method combines different similarity criteria to achieve a balanced evaluation of feature importance. By reducing unnecessary features, the hybrid similarity-based screening helps to improve model accuracy and decrease computational effort. The output obtained from this phase is indicated as W_i with a dimension of $[l \times o]$, such that $c > o$.

4.4 Malicious Node Detection using Qcosh-loss_DRDA-Net

Malicious node detection involves identifying nodes in a network that perform harmful activities, namely, data manipulation or false message transmission. Early detection of such behaviors prevents the spread of misinformation across the vehicular network. It ensures secure and trustworthy communication by isolating or neutralizing nodes that threaten network integrity. Here, malicious nodes are detected by using Qcosh-loss_DRDA-Net.

4.4.1 Structure of DRDA-Net

In DRDA-Net [15], screened data W_i with a dimension of $[l \times o]$ first passes through a sequence of dense residual and dual-shuffle attention layers designed to extract meaningful representations from raw features. These layers ensure that both global and local feature relationships are effectively captured. Initially, the model applies stacked transformations that refine low-level attributes and generate more abstract feature patterns for further analysis. These operations integrate normalization and activation functions to stabilize learning and enhance the representation capability of the network. The dense residual structure ensures efficient gradient flow and feature reuse, helping the model capture both shallow and deep dependencies within the data. This significantly reduces the risk of vanishing gradients, particularly in deep architectures. The dual-shuffle attention mechanism further strengthens this process by dynamically emphasizing the most relevant features while suppressing redundant information, allowing the model to focus on critical patterns associated with malicious node behavior. By combining dense connectivity, residual learning, and adaptive attention, DRDA-Net achieves robust feature extraction, reduced information loss, and improved detection accuracy for complex data patterns in VANET environments.

a) Building element

The network is organized into three main modules, including DRB, CA block, and RDAB. Each module plays a distinct role in improving representational depth and discriminative capability. The DRB and CA blocks operate independently, each focusing on different aspects of feature extraction and refinement. The RDAB module integrates both DRB and CA functionalities to combine their strengths by enabling effective feature learning and representation.

b) Dual-shuffle residual block

The DRB serves as a core component of the DRDA-Net architecture. Its enhanced design allows the extraction of multi-scale features crucial for identifying subtle anomalies. It is designed as an enhanced version of the traditional bottleneck structure that allows deeper feature learning while maintaining computational efficiency with fewer parameters. Within this block, information flows through two parallel residual paths by enabling diverse feature extraction and improved gradient propagation. This parallelism helps capture a wider range of spatial and behavioral cues from VANET data. The use of different kernel operations across these paths helps the network capture a wider range of feature relationships from the input data.

c) Channel attention block

The CA block is designed to enhance feature representation by focusing on the most relevant attributes. By recalibrating channel-wise feature responses, the CA block ensures that important features receive higher priority during training. It assigns higher importance to features that contribute significantly to capture complex patterns, while reducing the influence of less relevant features. This selective weighting improves the network's ability to learn meaningful relationships and enhances overall detection performance.

d) Residual dual-shuffle attention block

The RDAB serves as a key modular component of DRDA-Net, along with multiple RDABs stacked to form the complete network. Stacking multiple RDABs allows deeper and more expressive hierarchical feature learning. Each RDAB consists of a CA block and a configurable number of DRBs by allowing flexibility based on the complexity of the task. Within the RDAB, DRBs are arranged sequentially, with the output of one DRB serving as the input to the next, combined with batch normalization and activation functions to stabilize learning. This arrangement ensures proper gradient flow across the network and enhances

convergence. The CA block operates in parallel through a residual connection, emphasizing important features while preserving the original feature dimensions. The output attained from RDAB is expressed as,

$$P = \ell_2(J_{ca} + \ell_1(J_m)) \quad (5)$$

where, ℓ_1 and ℓ_2 are the sigmoid and ReLU operations, and J_m denotes the feature map.

e) Loss function

A novel loss function is formulated by integrating Quantile loss with Log-Cosh loss to balance robustness and sensitivity during model training. This hybrid loss is particularly effective in handling asymmetric error distributions common in VANET data. This combined approach enhances the model's ability to handle outliers while maintaining smooth gradient behavior for improved convergence and prediction accuracy. The combined log function [16] utilized is represented as,

$$L_{Quantile}(r, \hat{r}) = u \max(r - \hat{r}, 0) + (1 - u) \max(\hat{r} - r, 0) \quad (6)$$

where $\hat{r}$ implies the predicted values and true values are indicated as r . The final joint loss function becomes,

$$L_{Joint} = \gamma L_{Quantile} + \chi L_{\log-cosh} \quad (7)$$

where, γ and χ are the re-scaling coefficient constants. The detected output attained is indicated as S_i . This final output determines whether a given vehicular node is classified as malicious or legitimate.

4.4.2 Training of DRDA-Net utilizing Adam optimization

The DRDA-Net is trained using the Adam optimization algorithm to ensure efficient and adaptive weight updates during learning. Adam's adaptive learning capability accelerates convergence, especially when dealing with high-dimensional VANET data. This approach enhances convergence speed and stability, that allows the model to effectively capture complex patterns in the data.

5. Results and Discussion

The results obtained by Qcosh-loss_DRDA-Net in detecting malicious nodes are given below.

5.1 Experimental Setup

The Qcosh-loss_DRDA-Net in detecting malicious nodes is implemented utilizing Python.

5.2 Description of Dataset

The VANET-MaliciousNode dataset [12] captures realistic vehicle movements, communication activities, trust evaluations, and attack scenarios, offering a practical resource for research on security in intelligent transportation systems.

5.3 Evaluation Metrics

The metrics utilized to evaluate Qcosh-loss_DRDA-Net are deliberated below.

5.3.1 Accuracy

Accuracy [17] refers to the ratio of correctly identified malicious and non-malicious nodes to the total number of evaluated nodes and is expressed as,

$$\hat{o}_1 = \frac{C + D}{C + D + E + F} \quad (8)$$

where, C and D specifies true positive and negative, whereas E and F implies false positive and negative.

5.3.2 Hit Rate

Hit rate [17] refers to the ratio of correctly detected malicious nodes to the total number of actual malicious nodes.

5.3.3 Miss Rate

Miss rate [17] indicates the ratio of malicious nodes that were not detected to the total number of actual malicious nodes.

5.3.4 Precision

Precision [17] refers to the proportion of nodes identified as malicious that are actually malicious.

$$\partial_2 = \frac{C}{C + E} \quad (9)$$

5.3.5 Recall

Recall [17] refers to the proportion of actual malicious nodes that were correctly identified by the system and is expressed as,

$$\partial_3 = \frac{C}{C + F} \quad (10)$$

5.3.6 Rejection Rate

Rejection rate [17] indicates the proportion of nodes for which the system could not make a decision regarding their malicious behavior.

5.4 Comparative Analysis

Comparative analysis is done by varying training data for estimating the performance of Qcosh-loss_DRDA-Net, which is compared with preceding approaches. This comparison helps determine whether the proposed model maintains consistent performance advantages across different evaluation perspectives.

5.4.1 Comparative Analysis with Training Data

The comparative analysis for training data=90% is illustrated in Fig. 3. This proportion ensures that the model is sufficiently trained while still providing a meaningful test set to measure generalization. Fig. 3 a) depicts the analysis depending on accuracy. The Qcosh-loss_DRDA-Net attained accuracy of 96.70%, while the preceding methods, namely Fake node detection + prevention algorithm, X-GEVON, DPGHA and DAMASCO attained 90.35%, 92.30%, 94.38%, and 94.58%. The performance of Qcosh-loss_DRDA-Net is improved by 6.565%, 4.557%, 2.406%, and 2.186%. This substantial gain in accuracy demonstrates the ability of the proposed network to better capture complex malicious node behavior patterns compared to traditional and optimization-based models. Fig. 3 b) presents the hit rate analysis, where Qcosh-loss_DRDA-Net yielded 0.959 and devised model gained 0.772, 0.790, 0.827 and 0.909. A higher hit rate indicates more effective recognition of true malicious nodes, which is vital for preventing attacks in real-time vehicular communication. Fig. 3 c) illustrates the analysis in terms of miss rate evaluation. The proposed method achieved a miss rate of 0.204, whereas prior methods gained 0.230, 0.221, 0.212 and 0.209. Although the improvement margin in miss rate is narrower, it still reflects a more reliable detection mechanism with reduced oversight of harmful nodes. Fig. 3 d) shows the precision assessment. Qcosh-loss_DRDA-Net attained 94.74%, while previous models obtained 91.56%, 92.69%, 91.75% and 92.70%. Higher precision suggests that the proposed model significantly minimizes false alarms, thereby improving trust in the detection system and reducing unnecessary interventions. Fig. 3 e) presents the analysis based on recall, where Qcosh-loss_DRDA-Net yielded 95.99%, outperforming preceding models that attained 88.56%, 90.54%, 92.66% and 94.06%. The consistently high recall score confirms that the model successfully captures nearly all instances of malicious activity, even under varying network dynamics. Fig. 3 f) shows the rejection rate evaluation. The Qcosh-loss_DRDA-Net attained rejection rate of 0.032 and devised model attained 0.095, 0.075, 0.055 and 0.040.

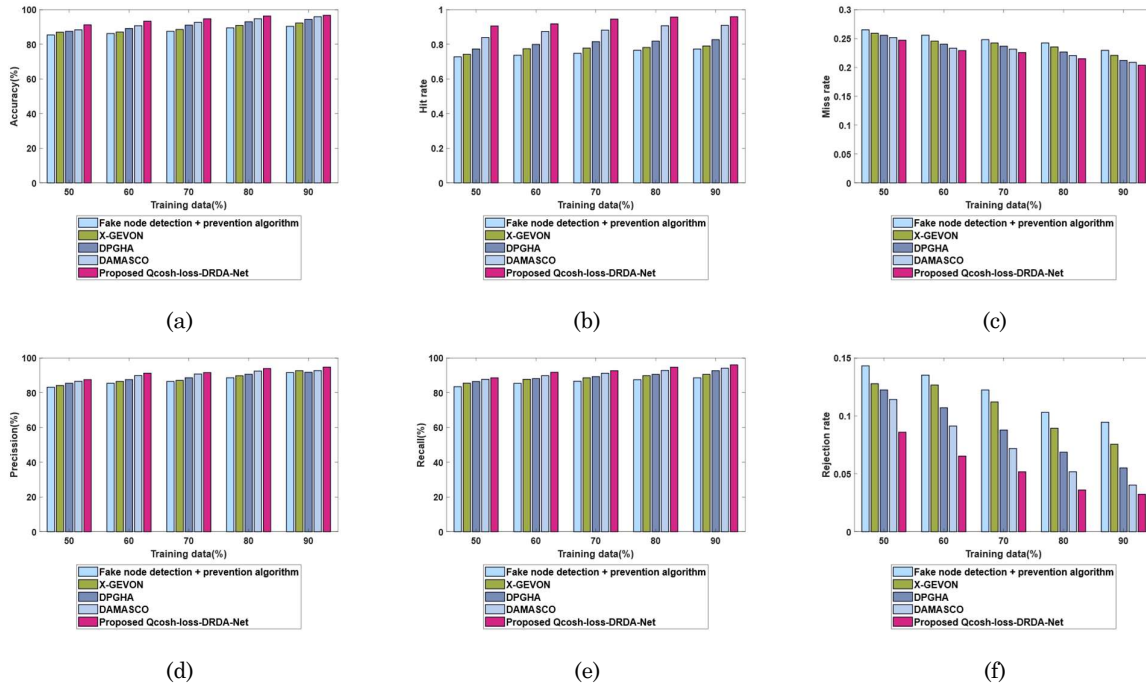


Fig. 3. Comparative analysis based on training data, a) Accuracy, b) Hit rate, c) Miss rate, d) Precision, e) Recall, f) Rejection rate

5.5 Comparative Discussion

The comparative evaluation of Qcosh-loss_DRDA-Net with existing models is summarized in Table 1. This comparison provides a consolidated view of how the proposed approach performs in relation to established VANET detection techniques under identical experimental conditions. Considering the training data of 90%, Qcosh-loss_DRDA-Net gained accuracy of 96.70%, while the existing methods, namely Fake node detection + prevention algorithm, X-GEVON, DPGHA and DAMASCO yielded accuracy of 90.35%, 92.30%, 94.38% and 95.89%. The Qcosh-loss_DRDA-Net obtained hit rate of 0.959, outperforming the prior models with hit rates of 0.772, 0.790, 0.827 and 0.909. In terms of hit rate at 50% training data, Qcosh-loss_DRDA-Net attained 0.906, surpassing prior methods with values of 0.728, 0.742, 0.773 and 0.839. The ability of the model to maintain strong performance even with significantly reduced training data reflects its superior generalization capability and resilience to data scarcity. The Qcosh-loss_DRDA-Net gained precision of 94.74%, surpassing the prior models that yielded 91.56%, 92.69%, 91.75% and 92.70%. Overall, Qcosh-loss_DRDA-Net obtained accuracy, hit rate, miss rate, precision, recall and rejection rate of 96.70%, 0.959, 0.204, 94.74%, 95.99% and 0.032, while considering training data = 90%.

Table 1. Comparative discussion of Qcosh-loss_DRDA-Net

Analysis based upon	Metrics/Methods	Fake node detection + prevention algorithm	X-GEVON	DPGHA	DAMASCO	Proposed Qcosh-loss_DRDA-Net
Training data=50%	Accuracy (%)	85.39	86.96	87.51	88.35	91.24
	Hit rate	0.728	0.742	0.773	0.839	0.906
	Miss rate	0.265	0.259	0.256	0.252	0.247
	Precision (%)	83.17	84.13	85.41	86.55	87.54
	Recall (%)	83.44	85.45	86.44	87.70	88.56
	Rejection rate	0.143	0.128	0.122	0.114	0.086
Training data=90%	Accuracy (%)	90.35	92.30	94.38	95.89	96.70
	Hit rate	0.772	0.790	0.827	0.909	0.959
	Miss rate	0.230	0.221	0.212	0.209	0.204
	Precision (%)	91.56	92.69	91.75	92.70	94.74
	Recall (%)	88.56	90.54	92.66	94.06	95.99
	Rejection rate	0.095	0.075	0.055	0.040	0.032

6. Conclusion

Detecting malicious nodes in VANETs plays a critical role in safeguarding communication reliability and preventing potential threats that could compromise the entire network's integrity and safety. This becomes increasingly important as modern vehicular systems rely heavily on timely and trustworthy data exchanges to support autonomous driving and intelligent transportation functions. Existing methods often fail to keep up with the rapidly changing network conditions and increasingly sophisticated attack strategies, limiting their effectiveness in real-world VANET scenarios. Here, Qcosh-loss_DRDA-Net is proposed for malicious node detection in VANETs. Initially, VANET is simulated. At BS, the data is taken from the dataset and undergoes data preprocessing, which is performed by handling missing values and normalizing features. Feature selection is then conducted using hybrid similarity measures. Finally, malicious nodes are identified using the Qcosh-loss_DRDA-Net model. The integration of dense residual architecture with dual-shuffle attention further strengthens the model's ability to extract deep and discriminative features crucial for accurate malicious behavior identification. The performance of Qcosh-loss_DRDA-Net is evaluated using metrics, like accuracy, hit rate, miss rate, precision, recall, and rejection rate, achieving superior values of 96.70%, 0.959, 0.204, 94.74%, 95.99% and 0.032. In future, the model can be extended to incorporate real-time adaptive learning to better respond to emerging attack patterns. Additionally, integrating blockchain technology could enhance data integrity and trustworthiness across the VANET.

Compliance With Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

- [1] K. Rashid, Y. Saeed, A. Ali, F. Jamil and R. Alkanhel, "An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs)," *Sensors*, vol. 23, no. 5, p. 2594, 2023.
- [2] V. Chandrasekar, V. Shanmugavalli, T. R. Mahesh, R. Shashikumar and N. Borah, "Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm," *Scientific Reports*, vol. 14, no. 1, p. 7818, 2024.
- [3] B. Igried, A. Alsarhan, I. Al-Khawaldeh and A. AL-Qerem, "A novel fuzzy logic-based scheme for malicious node eviction in a vehicular ad hoc network," *Electronics*, vol. 11, no. 7, p. 2741, 2022.
- [4] M. Alkhalidy, A. F. Al-Serhan, A. Alsarhan and B. Igried, "A new scheme for detecting malicious nodes in vehicular ad hoc networks based on monitoring node behavior," *Future Internet*, vol. 14, no. 8, p. 223, 2022.
- [5] H. Baharlouei, A. Makanju and N. Zincir-Heywood, "Comprehensive Host-Based Malicious Behaviour Detection in VANETS," *Authorea Preprints*, 2025.
- [6] H. Baharlouei, A. Makanju and N. Zincir-Heywood, "Exploring real-time malicious behaviour detection in vanets," *ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, pp. 1-8, 2023.
- [7] S. Masood, Y. Saeed, A. Ali, H. Jamil, N. A. Samee and H. Alamro, "Detecting and preventing false nodes and messages in vehicular ad-hoc networking (VANET)," *IEEE Access*, vol. 11, pp. 93920-93934, 2023.
- [8] T. Anjali, R. Goyal and G. N. Balaji, "X-GEVON-a novel explainable intelligent network to detect the multiple attacks in vanet systems," *Discover Computing*, vol. 28, no. 1, p. 185, 2025.
- [9] A. Malik, M. Z. Khan, S. M. Qaisar, M. Faisal and G. Mehmood, "An efficient approach for the detection and prevention of gray-hole attacks in VANETs," *IEEE Access*, vol. 11, pp. 46691-46706, 2023.
- [10] E. P. Valentini, G. P. R. Filho and R. E. d. Grande, "A novel mechanism for misbehavior detection in vehicular networks," *IEEE Access*, vol. 11, pp. 68113-68126, 2023.
- [11] S. A. E. Mohamed and K. A. AlShalfan, "Intelligent traffic management system based on the internet of vehicles (IoV)," *Journal of advanced transportation*, vol. 2021, no. 1, p. 4037533, 2021.
- [12] "VANET-MaliciousNode Dataset," [Online]. Available: <https://www.kaggle.com/datasets/ziya07/vanet-maliciousnode-dataset>.
- [13] A. Hossain, "Deep Q-Learning Intrusion Detection System (DQ-IDS): A Novel Reinforcement Learning Approach for Adaptive and Self-Learning Cybersecurity," *ICT Express*, 2025.

- [14] J. K. Singh and D. Kakkar, "Hybrid similarity based feature selection and cascade deep maxout fuzzy network for Autism Spectrum Disorder detection using EEG signal," *Computational Biology and Chemistry*, vol. 113, p. 108177, 2024.
- [15] S. Chattopadhyay, A. Dey, P. K. Singh and R. Sarkar, "DRDA-Net: Dense residual dual-shuffle attention network for breast cancer classification using histopathological images," *Computers in biology and medicine*, vol. 145, p. 105437, 2022.
- [16] J. Terven, D.-M. Cordova-Esparza, J.-A. Romero-González and A. Ramírez-Pedraza, "A comprehensive survey of loss functions and metrics in deep learning," *Artificial Intelligence Review*, vol. 58, no. 7, p. 195, 2025.
- [17] D. Durairaj, T. K. Venkatasamy, A. and S. Umar, "Intrusion detection and mitigation of attacks in microgrid using enhanced deep belief network," *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, vol. 46, no. 1, pp. 1519-1541, 2024.