VOL. 21, NO. 7, APRIL 2026 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

MULTI-TASK LEARNING WITH SENSOR FUSION FOR JOINT DETECTION OF MULTIPLE MISBEHAVIORS IN VEHICULAR AD HOC NETWORKS

Zaid Mahmood Abdul Razzaq Hanoosh
Department of Basic Science, College of Dentistry, University of Kufa, Iraq
E-Mail: zaidm.alrazaqhnoosh@uokufa.edu.iq

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) are widely vulnerable to several kinds which threaten the reliability and safety of the network. Traditional diagnosis strategies sometimes concentrate on unique kinds of misbehavior and fail to consider the complicated, complex, simultaneous attacks aspect. Here, we offer a new multi-task learning architecture integrated with sensor fusion methods for diagnosing and concurrently grouping several misbehaviors in VANET areas. Through combining heterogeneous data sources-such as network parameters, behavioral features, and positional info—our model efficiently obtains interrelated features of different kinds of attacks, like denial of service, message forgery, and false location reporting. The multi-task learning framework enables knowledge sharing across tasks, developing whole diagnosis accuracy and strength. Broad simulations performed under different traffic densities show that the presented strategy performs better than conventional unique-task models in the two binary and multi-class classification scenarios. The outcomes highlight the ability of an architecture to develop security in VANETs through presenting a general and effective misbehavior diagnosis system.

Keywords: message forgery, false location reporting, vehicular ad hoc networks (VANET), sensor fusion, machine learning, multi-task learning, misbehavior detection, network security.

Manuscript Received 26 February 2026; Revised 5 April 2026; Published 10 June 2026

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have emerged as the pivotal technology, enabling communication between vehicles and roadside infrastructure to develop infotainment services, road safety, and traffic efficiency. However, because of their decentralized and active aspect, VANETs are greatly susceptible to different threats to security, especially misbehavior by bad nodes, which could degrade network performance and endanger passenger safety [1].

Exchange messages are rarely encrypted in vehicular communication networks, such as fundamental messages, like traffic safety, event-oriented messages, and navigation messages. So, VANETs' open area might cause different attacks like false reports, forgery, and denial-of-service (DoS), which lead to traffic chaos/accidents. In addition, malevolent entities might follow messages and IDs of users with substantial hazard to drivers. So, for VANETs, from a security-preserving nature, bad vehicles must be traced and penalized in any misbehavior event [2].

Misbehavior attacks established by rogue insiders sometimes become complex for diagnosis and including, as bad nodes might alter their activity intelligently over time. However, cryptographic methods can limit outsiders by proposing non-repudiation, integrity, and authentication, and as a first defense layer, they might fall short in diagnosing rogue/dishonest behavior and recognizing V2X insiders with bad intentions. Therefore, exchanged info trustworthiness could not be ensured [3].
VANETs' misbehavior includes various attack types like DOS, message forgery, Sybil attacks, false location reporting, and so on [4]. Such basic tasks include vehicular communications' confidentiality, integrity, accessibility, causing potential accidents, misinformation, and traffic disruptions [5]. Diagnosing several kinds at the same time is a difficult issue because of the attacks' heterogeneous aspect as well as the active network area. Present diagnosis methods normally concentrate on unique misbehavior kinds and sometimes depend on handcrafted features/isolated classifiers that restrict their efficiency in real-life VANET scenarios where hybrid attack kinds might coexist and interact [6]. In addition, such techniques generally utilize data from restricted sources, decreasing their capability to identify the complicated and correlated patterns inherent in multi-attack scenarios. So, a crucial requirement exists for a strong, scalable strategy that could leverage various data sources and concurrently diagnose hybrid misbehaviors with high accuracy.

To consider such issues, the present study offers a new architecture based on multi-task learning (MTL) with sensor fusion methods for multiple misbehaviors simultaneous diagnosis and classification in VANET. Through combining heterogeneous data from network parameters, behavioral metrics, and positional info, the presented model leverages shared representations over relevant tasks for diagnosing accuracy and strength. This paper's basic contributions include:

a) We introduce a multi-task learning architecture tailored for multiple kinds of simultaneous diagnosis in VANET, developing diagnosis performance through exploiting task relevance.

b) We enhance the sensor fusion strategy, which combines various data sources such as positional, network, and behavioral features for enriching the input feature space and developing model strength.
c) We model and perform the general simulation area for creating realistic VANET data with different misbehaviors' kinds under various traffic densities.
d) We present a broad experimental assessment showing that the presented technique performs better than traditional single-task and single-source strategies in the two binary and multi-class misbehavior classification.

This article's remainder is outlined as follows: Part 2 reviews relevant work about misbehavior diagnosis and multi-task learning strategies. Part 3 details the presented multi-task learning architecture and sensor fusion approach. Part 4 defines the simulation setup and dataset creation. Part 5 provides experimental outcomes and complete analysis. At last, part 6 concludes the study and discusses potential directions for further study.

2. RELATED WORKS

VANETs are Intelligent Transportation Systems (ITS), making real-life communication possible among vehicles and infrastructure for developing road safety and traffic effectiveness. Their open and decentralized aspect makes them susceptible to different security threats, such as misbehavior attacks like DOS, Sybil attacks, and message falsification. Accordingly, modelling efficient misbehavior detection systems (MDSs) became the crucial study domain. In the last few years, a broad diagnosis approaches' range was presented, leveraging methods like statistical inference, ML, signal processing, and trust management. This part reviews and analyzes some considerable research that has contributed to the MDSs' improvement in VANETs, highlighting their restrictions, techniques, and strengths.

In [7], the authors present a strategy based on data to diagnose position falsification attacks in VANETs. Instead of depending on traditional cryptographic techniques, it leverages ML models for analyzing features extracted from 2 consecutive Basic Safety Messages (BSMs). The technique shows greater diagnosis accuracy on the VeReMi dataset. Such a strategy offers high diagnosis accuracy benefits as well as the capability to operate in real life, making it especially efficient in contrast to position spoofing. Although the restriction of it depends on the reality that it is specialized to just diagnose position falsification and might not generalize well to other kinds/ areas with quickly shifting traffic dynamics.

In [8], the authors provide a context-aware adaptive misbehavior diagnosis architecture where every vehicle performs plausibility and consistency checks. It actively computes confidence intervals given the local parameters like traffic density, speed, and position. This technique's basic strength is its adaptability to various traffic contexts, which causes a lower false-positive rate and broader attack kinds and coverage, such as Sybil and DoS. On the downside, the efficiency of the system relies on timely and proper access to contextual data, and its complexity might increase in high-density traffic contexts.

In [9], the authors provide a hybrid data-centric misbehavior diagnosis system that integrates grouping and reinforcement learning to control unlabeled data. It adapts to different kinds of attacks via an interactive learning process. The main benefit is the capability to operate in areas where tagged data is not accessible, which could generalize to hybrid kinds. Meanwhile, the dependence on reinforcement learning defines computational burden; the system might perform sub-optimally when attackers behave in an unpredictable way/ actively shift their approaches.

In [10], the authors incorporate vehicular social models, like mobility similarity, into a trust assessment architecture. This integrates spatio-temporal trust and reputation metrics for recognizing bad nodes more reliably. The basic benefit is the robust trust algorithm, which uses mobility history, making it hard for attackers to manipulate. Although such a technique assumes access to long-term mobility data that may not be possible in highly active/ privacy-sensitive areas, it decreases the efficiency in these terms.

In [11], the authors provide the Hypothesis Variance Ratio (HVR) for misbehavior diagnosis in multi-relay VANETs and present analytical expressions to optimize diagnosis thresholds. Such a model takes advantage of mathematical rigor and illustrates robust performance in relay-driven scenarios with decreased computational delay. The restriction, however, is particularly tailored for cooperative multi-relay systems and might not be used in comprehensive VANET scenarios where straight communication dominates.

In [12], the authors provide an iRMDS that combines Kalman filtering and artificial neural networks to develop strength when there is noise. This applies signal strength and direction as main attributes for diagnosis. Such a strategy obtains high accuracy and is especially resilient to noisy/inconsistent data that is usual in VANETs. In spite of its strength, it needs access to physical layer signal metrics and might incur processing overhead, posing issues for real-life operation on resource-restricted devices.

In [13], the authors explore deep unsupervised learning by applying DEMC that groups data in the embedding space, applying a KL-divergence-driven technique. It does not depend on tagged data and adapts to novel kinds. The main benefit is independence from tagged datasets that are sometimes difficult to achieve in real-life VANETs. Meanwhile, its performance is heavily reliant on the learned embeddings, and the deep learning framework might incur high computational costs, restricting its development possibilities on embedded vehicular units.

In [14], the authors provide a light diagnosis system given observable metrics like signal strength,

speed, and packet transmission. This assesses binary and multi-class classification applying popular ML classifiers. Such a technique shows its simplicity and practical, easy-to-collect features, making it possible for simulation and emulation areas. In other words, its efficiency might be ruined under environmental noise/incomplete behavioral data that could cause misclassification in real-life situations.

In [15], the authors present HCA-MDS, a hybrid, modular architecture that contains two data-centric and behavior-centric elements. It supports context updating and reference model creation for continuous adaptation. The main strength depends on its general and flexible framework that enables efficient diagnosis in evolving VANET areas. Although keeping and updating the context model in real life adds a complexity layer, the system's scalability in large-scale developments might be an issue.

The reviewed research reflects the various and evolving misbehavior diagnoses in VANETs. When several strategies focus on data-based methods for high accuracy, others concentrate on light implementation, adaptability, and trust assessment [16] for real-life possibility. Unobserved and hybrid techniques are drawing attention for their potential for controlling untagged data and evolving attack models. However, issues like high computational costs, reliance on contextual/mobility data, and generalizability over attack kinds remain persistent. Such restrictions underscore the requirement for a more scalable, strong, and context-aware diagnosis architecture that could guarantee reliable performance in real-life VANET developments. Creating perspectives from such studies works; our study aims to consider several gaps by offering a more adaptive and effective diagnosis algorithm.

3. PROPOSED METHOD

This part shows the presented multi-task learning architecture details combined with sensor fusion for simultaneous diagnosis of multiple misbehaviors in VANET. The architecture is modelled for efficiently leveraging heterogeneous data sources and identifying interdependencies between different kinds via shared representations. The proposed technique targets at diagnosing and group hybrid events happening in VANET nodes by exploiting data gathered from different sensors and network parameters. Instead of training separate classifiers for every misbehavior, we develop a multi-task learning (MTL) strategy where relevant diagnosis tasks are learned jointly to develop the entire performance.

3.1 Sensor Fusion for Feature Extraction

To accurately characterize every manner of a node, we combine several info sources such as:

- **Behavioral Features:** like speed deviations, packet transmission rate, and number of dropped packets.
- **Positional Features:** obtained from GPS data, such as location consistency, instantaneous speed, and acceleration.
- **Network Features:** like packet delivery rate, Received Signal Strength Indicator (RSSI), and network delay.

Such heterogeneous data flows are preprocessed and concatenated to shape a general feature vector showing every node at each observation interval. Sensor fusion aids in enriching the input feature space and capturing complicated correlations between features that single-source data may miss.

3.2 Multi-Task Learning Architecture

The core of the provided framework is a neural network model designed to solve several misbehavior diagnosis tasks at the same time. Such a framework enables the model to leverage relatedness between tasks, developing learning efficiency and strength in contrast to noisy/incomplete data. The framework includes basic elements as:

a) **Multi-source Sensor Inputs:** Features extracted from parameters of node behavior, GPS, and RSSI are gathered and concatenated to shape the input feature vector at every time stage.
b) **Sensor Fusion Layer:** The heterogeneous features are fused into a unique representation for every node.
c) **1D Convolutional Layers:** Such layers extract local spatial features and correlations from the fused feature vectors across temporal order.
d) **LSTM Layers:** For getting capture temporal reliance and sequential manner models, the outcome from CNN layers is fed into one/more LSTM layers.
e) **Shared Fully Connected Layers:** The LSTM's last hidden state passes through completely connected layers shared over the whole misbehavior diagnosis tasks to learn generalized feature representations.
f) **Task-specific Output Heads:** Divide completely connected layers for every misbehavior diagnosis task to present classification outcomes. Every head predicts the feasibility share across levels, particularly for a specific kind.

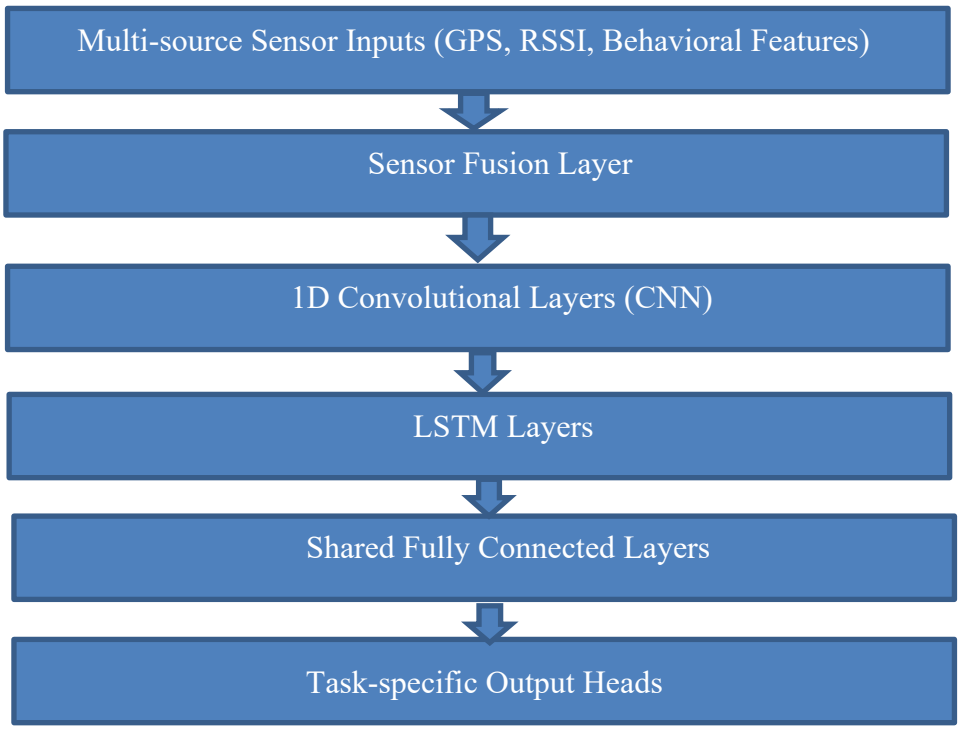

Figure-1. Block diagram of the proposed architecture.

3.3 Training and Optimization

The model is trained end-to-end, applying an integrated loss function that gathers losses from all tasks. We use cross-entropy loss for classification tasks, weighted appropriately to develop every task effectively in training. Optimization is implemented by applying stochastic gradient descent with adaptive learning rate techniques like Adam.

3.4 Mathematical Formulation

Allow input order for a provided node to be X $\{x_1,x_2,\ldots,x_T\}$, where every $x_t \in R^d$ is the fused feature vector at time t.

- The CNN layers perform convolution tasks to extract spatial features [17]:

$$h_t^{(l)}=\sigma(W^{(l)} * h_t^{(l-1)}+b^{(l)}) \quad (1)$$

That * shows 1D convolution, $W^{(l)}$ and $b^{(l)}$ are weights and biases, σ is the activation function (e.g., ReLU).

- CNN layers output shapes are fed into the LSTM [18]:

$$i_t=\sigma(W_i h^t+U_i h_{t-1}+b_i) \quad (2)$$

$$f_t=\sigma(W_f h_t+U_f h_{t-1}+b_f) \quad (3)$$

$$o_t=\sigma(W_o h_t+U_o h_{t-1}+b_o) \quad (4)$$

$$\tilde{c}_t=\tanh(W_c h_t+U_c h_{t-1+}b_c) \quad (5)$$

$$c_t=i_t+c_{t-1} \odot f_t \odot \tilde{c}_t \quad (6)$$

$$h_t=o_t \odot \tanh(c_t) \quad (7)$$

- The last LSTM hidden state h_T is transferred to shared completely connected layers [18]:

$$z=\mathrm{ReLU}(W_s h_T+b_s) \quad (8)$$

- For every misbehavior diagnosis task $k \in \{1,\ldots,K\}$, a task-specific outcome layer predicts class feasibilities:

$$\hat{y}^{(k)}=\mathrm{softmax}(W_k z+b_k) \quad (9)$$

3.5 Loss Function and Training

The whole loss function is the weighted individual cross-entropy losses for every task [19]:

$$L=\sum_{k=1}^{K} L_k \alpha_k \quad (10)$$

That α_k is the weighting coefficient for task k, and

$$L_k=-\frac{1}{N}\sum_{i=1}^{N}\sum_{c=1}^{C_k} y_{i.c}^{(k)} log \hat{y}_{i.c}^{(k)} \quad (11)$$

That N is the batch size, C_k is the levels' number for task k, $y_{i.c}^{(k)}$ is the true label, and $\hat{y}_{i.c}^{(k)}$ is the predicted feasibility.

Training is done by applying the Adam optimizer with learning rate planning and early stopping.

Algorithm 1: Multi-Task Learning for VANET Misbehavior Detection

1. Input: Training data $D=\{(X_i,Y_i)\}$ where X_i is fused input sequence and $Y_i=\{yi(k)\}$ are task labels
2. Initialize network parameters Θ
3. For each epoch:

a. For each mini-batch:

i. Forward pass to compute outputs $\hat{y}_i^{(k)}$

ii. Compute loss L

iii. Backpropagate and update Θ using Adam

4. Repeat until convergence

4. EXPERIMENTAL SETUP

To assess the presented multi-task learning framework's performance for multi-kind misbehavior diagnosis in VANETs, we made a custom Python-driven simulation area that synthetically creates vehicular mobility and communication data. The simulation emulates a 2D grid providing an urban road network where 100 vehicles are randomly initialized with various models of communication, trajectories, and speeds across a simulation duration of 500 seconds. Among them, 70 nodes behave legitimately when the remaining 30 are randomly determined to exhibit one of the following bad manners: Packet Dropping, False Positioning, Sybil Attack, Speed Tampering.

Every vehicle periodically spreads synthetic safety messages, and for each transmission interval, a general feature is logged. They contain kinematic features (deviation, speed, acceleration from expected trajectory), communication metrics (neighbor count, RSSI, packet delivery ratio, delay), and contextual indicators (lane occupancy, vehicle ID consistency, relative density). The feature set is created by applying Python libraries, and the dataset is augmented to reflect differing traffic densities and attacker shares.

To diagnose and group misbehaviors, we performed a multi-task neural framework applying PyTorch. The model includes a shared feature extractor made with the integration of 1D Convolutional layers and Bidirectional LSTMs to capture spatio-temporal dependencies in the data of traffic. The shared backbone is tracked by 4 parallel classification heads, each dedicated to diagnosing a particular kind. The fusion layer based on attention gathers multi-source features before being fed into the shared network.

The model was trained applying Adam optimizer with a learning rate of 0.001 and a batch size of 64 for 100 epochs. The weighted sum of task-specific cross-entropy losses was applied as the sum loss function. The set of data was split into sets of training (80%) and test (20%). Performance was assessed by applying F1-score, recall, accuracy, and precision over the whole task. To show multi-task learning benefit, we compared the outcomes with unique single-task classifiers separately trained for every manner of kind.

Here, we assess our ensemble learning strategy's efficiency for V2X misbehavior diagnosis by performing assessments using the VeReMi dataset.

A. Dataset Description and Preprocessing

VeReMi dataset [20] includes 19 attack variants to simulate various kinds of misbehavior, as defined in part II. 2 vehicular traffic densities are prescribed for every attack scenario: high-density (37.03 vehicles/km2) and low-density (16.36 vehicles/km2). In every scenario, a JSON log file is made for recording raw data exchanged (like smart and attack messages) among neighboring vehicles. BSMs contain 3D vectors for acceleration, position, speed, and heading angle features. While preprocessing, whole JSON files with the raw data were converted to CSV format and concatenated together. It was performed for every attack scenario to compile the CSV file with ordered BSM records, applying the timestamps. Given the feature analysis, we chose 6 domains, such as acceleration, timestamp, heading angle, speed, pseudo-ID, and position, as the most related feature set associated with attack diagnosis. The Euclidean norm of the heading angle, speed, position, and acceleration vectors is later used.

5. RESULTS AND ANALYSIS

Here, we provide and analyze the experimental outcomes achieved from the presented multi-task learning model to diagnose hybrid misbehavior kinds in VANETs. The dataset was assessed by applying 10-fold cross-validation to guarantee model generalization and robustness. Every fold kept a balanced, legitimate, and misbehaving node share over the 4 attack groups.

To assess classification performance, we applied a set of standard assessment metrics described as:

- **True Positive (TP):** The number of bad vehicles appropriately recognized as bad.
- **False Positive (FP):** The number of legal vehicles inappropriately grouped as bad.
- **True Negative (TN):** The number of legal vehicles appropriately recognized as legal.
- **False Negative (FN):** The number of bad vehicles inappropriately grouped as legal.

Given such values, the obtained metrics were calculated as:

Accuracy

$$\text{Accuracy}=(TP+TN)/(TP+FP+TN+FN) \quad (12)$$

True Positive Rate (TPR) (a.k.a. Recall)

$$TPR=TP(/TP+FN) \quad (13)$$

Precision

$$\text{Precision}=TP/(TP+FP) \quad (14)$$

F1-Score

$$F1=2\cdot(Precision\cdot Recall)/(Precision+Recall) \quad (15)$$

To preserve class distribution, 80% of the dataset was used for training and 20% for testing in this study, with stratified sampling. The goal of this experiment was to detect Sybil attacks, a prevalent and serious sort of security vulnerability in vehicle networks. A subset of 11.88 million samples from the original dataset was chosen for examination, which included both normal and Sybil-labeled data. Table-1 summarizes the classification performance of the suggested model.

Table-1. Classification performance of the proposed model.

Metrics	Accuracy	Recall	Precision	F1
Proposed method	98.73%	98.91%	98.54%	98.72%

The classification results show that the model is particularly good at recognizing Sybil attacks in the dataset. With an overall accuracy of 98.73%, the model properly diagnoses the great majority of cases. The precision of 98.54% indicates that the majority of occurrences categorized as Sybil attacks are correct, whilst the recall of 98.91% indicates that almost all actual Sybil attacks were successfully recognized. The F1-score, which measures precision and recall, is 98.72%, demonstrating the model's robustness and efficacy. According to the classification report, class 0 (normal data) had a precision of 0.99 and a recall of 0.98, but class 1 (Sybil attack) had a precision of 0.98 and a recall of 0.99. These results show that the model performs slightly better at recognizing Sybil attacks than it does at identifying normal traffic, which is very desirable in security applications where failure to detect assaults is more critical than incorrectly flagging normal behavior. Overall, the model's outstanding performance across all criteria shows its suitability for real-world use in identifying Sybil assaults in vehicular ad-hoc networks (VANETs), providing dependable and consistent results on a large-scale dataset.

5.1 Multi-task vs. Single-task Comparison

Table-2 shows a comparison of the presented multi-task framework to LSTM, single-task CNN, and classical ML classifier (SVM). The multi-task model achieved significantly higher F1-scores (average ~99%) compared to full tasks, particularly for attack types with overlapping features (e.g., Sybil vs. False Positioning). Attention-driven sensor fusion later led to the development of a model capable of distinguishing tiny differences in communication and motion patterns.

Table-2. Comparison of Multi-task vs. Single-task.

Metrics	Accuracy	Recall	Precision	F1
LSTM	96.25%	96.40%	95.80%	96.10%
Single-task CNN	95.10%	94.80%	95.30%	95.05%
SVM	94.85%	94.60%	94.90%	94.75%
Proposed method	98.73%	98.91%	98.54%	98.72%

5.2 Confusion Matrix Analysis

Figure-2 shows the confusion matrix findings, which confirm the proposed method's good effectiveness in detecting Sybil attacks. Of the total occurrences, the model accurately identified 6,980,050 normal samples and 4,709,803 Sybil attack samples. Meanwhile, only 143,672 normal occurrences were misidentified as Sybil attacks (false positives), while 52,485 Sybil instances were wrongly categorized as normal (false negatives). These low misclassification rates show that the model is quite successful at detecting malicious activities and reducing false alarms. The results demonstrate the model's remarkable capacity to generalize over a large and imbalanced dataset, with good precision and recall for both classes. Such performance indicates that the suggested method is a dependable tool for real-world Sybil attack detection scenarios in automotive networks.

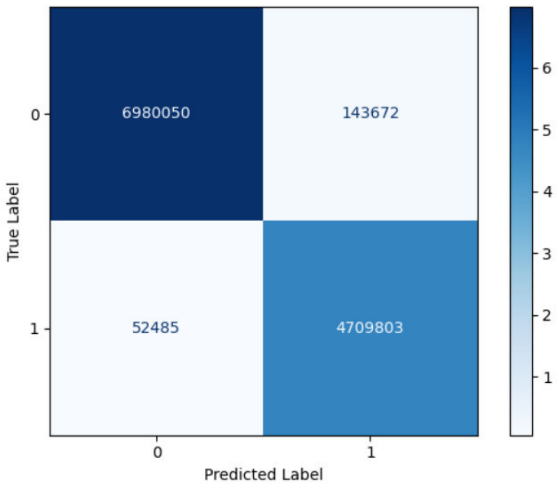

Figure-2. Confusion matrix of the proposed method.

5.3 Comparative Analysis of Detection Performance

A comparison of the suggested method to previous approaches by Sultana *et al*. [8] and Sedar *et al*. [3] shows that the new model outperforms all assessment measures. The proposed method yields an outstanding accuracy of 98.73%, greatly exceeding Sultana *et al.*'s [8] 92.24% and Sedar *et al*.'s [3] 56.90% results. This demonstrates the proposed model's excellent accuracy in discriminating between genuine and malicious signals in VANET systems.

Sedar et al. [3] report 98.73% recall, which assesses the model's ability to properly detect attack events. However, this is accompanied by a very low precision of 56.06%, indicating a significant false positive rate in which many benign messages are wrongly classified as attacks. On the other hand, the proposed method achieves a comparable recall of 98.91% while also maintaining a High precision of 98.54%, demonstrating a balanced and accurate detection procedure with few false alarms.

As a result, the proposed method achieves an F1-score of 98.72%, which is much higher than Sultana *et al*.'s [8] 80.84% and Sedar *et al*.'s [3] 71.50%. This demonstrates the suggested model's robustness and reliability in real-world deployment settings. Overall, the suggested method outperforms earlier techniques by providing both high sensitivity in identifying attacks and great precision in minimizing misclassifications, resulting in a very effective solution for misbehavior detection in vehicular networks.

Table-3. Comparison of the proposed method vs. other methods.

Metrics	Accuracy	Recall	Precision	F1
Sultana et al. [8]	92.24%	69.06%	97.41%	80.84%
Sedar et al. [3]	56.90%	98.73%	56.06%	71.50%
Proposed method	98.73%	98.91%	98.54%	98.72%

6. CONCLUSIONS

Here, we presented a new multi-task learning architecture to diagnose hybrid misbehavior kinds in Vehicular Ad Hoc Networks (VANETs), applying sensor fusion and DL methods. The presented framework jointly learns shared representations over hybrid tasks, enabling simultaneous diagnosis of various misbehaviors, such as packet dropping, speed tampering, Sybil attacks, and false position reports. By combining heterogeneous data sources-like communication logs, signal strength, GPS information, speed, and acceleration-via a feature-level attention-driven fusion algorithm, the model showed developed diagnosis ability even in complicated and noisy areas. Broad tests applying a custom-made dataset and Python-driven simulation illustrated that the presented technique performs better than traditional single-task models and conventional ML strategies in terms of F1-score, accuracy, recall, and precision. In addition, the model's ability to differentiate overlapping manner models over various kinds of attacks validates the multi-task model's efficiency. In the future, this work could be developed by incorporating real-life vehicular data, developing federated/edge-driven training to guarantee scalability and privacy, and combining the architecture into real-life VANET security systems.

REFERENCES

[1] Zolfagharipour L, Kadhim M. H. 2025. A Technique for Efficiently Controlling Centralized Data Congestion in Vehicular Ad Hoc Networks. International Journal of Computer Networks and Applications (IJCNA). 12(2): 267-277.

[2] Xu X., Wang Y., Wang P. 2022. Comprehensive review on misbehavior detection for vehicular ad hoc networks. Journal of Advanced Transportation. 2022(1): 4725805.

[3] Sedar R., Kalalas C., Dini P., Vázquez-Gallego F., Alonso-Zarate J., Alonso L. 2024. Knowledge Transfer for Collaborative Misbehavior Detection in Untrusted Vehicular Environments. IEEE Transactions on Vehicular Technology.

[4] Sangwan A., Sangwan A., Singh R. P. 2023. A classification of misbehavior detection schemes for VANETs: a survey. Wireless Personal Communications. 129(1): 285-322.

[5] El-Rewini Z., Sadatsharan K., Selvaraj D. F., Plathottam S. J., Ranganathan P. 2020. Cybersecurity challenges in vehicular communications. Vehicular Communications. 23: 100214.

[6] Mazhar S., Rakib A., Pan L., Jiang F., Anwar A., Doss R., Bryans J. 2024. State-of-the-art authentication and verification schemes in VANETs: A survey. Vehicular Communications. 31: 100804.

[7] Sharma A., Jaekel A. 2021. Machine learning-based misbehaviour detection in VANET using consecutive BSM approach. IEEE Open Journal of Vehicular Technology. 3: 1-4.

[8] Sultana R., Grover J., Tripathi M., Sharma P. 2024. LA-DETECTS: Local and Adaptive Data-Centric Misbehavior Detection Framework for Vehicular Technology Security. IEEE Open Journal of Vehicular Technology.

[9] Sedar R., Kalalas C., Dini P., Alonso-Zarate J., Vázquez-Gallego F. 2022. Misbehavior detection in vehicular networks: An ensemble learning approach. In GLOBECOM 2022-2022 IEEE Global Communications Conference, (pp. 1850-1855). IEEE.

[10] Lv C., Cheong C., Cao Y., Wang Y., Kaiwartya O., Wu C. 2024. Leveraging geographic information and social indicators for misbehavior detection in VANETs. IEEE Transactions on Consumer Electronics. 70(1): 4411-24.

[11] Ding X., Wang Y. 2022. Misbehavior Detection and Identification in DF Multi-Relay VANETs. IEEE Wireless Communications Letters. 12(2): 222-6.

[12] Alzahrani M., Idris M. Y., Ghaleb F. A., Budiarto R. 2022. An improved robust misbehavior detection scheme for vehicular ad hoc network. IEEE Access. 10: 111241-53.

[13] Rajendran A., Balakrishnan N. 2022. Deep embedded median clustering for routing misbehaviour and attacks detection in ad-hoc networks. Ad Hoc Networks. 126: 102757.

[14] Grover J., Prajapati N. K., Laxmi V., Gaur M. S. 2011. Machine learning approach for multiple misbehavior detection in VANET. In Advances in Computing and Communications: First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part III 1 (pp. 644-653). Springer Berlin Heidelberg.

[15] Ghaleb F. A., Maarof M. A., Zainal A., Al-Rimy B. A., Saeed F., Al-Hadhrami T. 2019. Hybrid and multifaceted context-aware misbehavior detection model for vehicular ad hoc network. IEEE Access. 7: 159119-40.

[16] Zolfagharipour L., Kadhim M. H., Mandeel T. H. Enhance the security of access to IoT-based equipment in fog. In 2023 Al-Sadiq International Conference on Communication and Information Technology (AICCIT).

[17] Jogin M., Madhulika M. S., Divya G. D., Meghana R. K., Apoorva S. 2018. Feature extraction using convolutional neural networks (CNN) and deep learning. In2018 3rd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT), (pp. 2319-2323). IEEE.

[18] Tasdelen A., Sen B. 2021. A hybrid CNN-LSTM model for pre-miRNA classification. Scientific Reports. 11(1): 14125.

[19] Mao A., Mohri M., Zhong Y. 2023. Cross-entropy loss functions: Theoretical analysis and applications. In International Conference on Machine Learning, (pp. 23803-23828). PMLR.

[20] Kamel J., Wolf M., Van Der Hei R. W., Kaiser A., Urien P., Kargl F. 2020. Veremi extension: A dataset for comparable evaluation of misbehavior detection in VANETs. In ICC 2020-2020 IEEE International Conference on Communications (ICC), (pp. 1-6). IEEE.