Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

An Energy-Efficient Traffic-Aware Dynamic Cluster Head Selection in EMAO-MTRUST for VANETs

Parimala Garnepudi

garnepudi.parimalaphd@gmail.com

Saveetha Engineering College

M Vanitha

Saveetha Engineering College

Article

Keywords: VANET, Mobility Prediction, Bidirectional Long Short-Term Memory, Efficient Routing, Adaptive Trust Reinforcement, TDMA

Posted Date: September 17th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10747610/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.

Abstract

Vehicular Ad Hoc Networks (VANETs) are becoming an important communication model in Intelligent Transportation Systems (ITS), which allows real-time vehicle-to-vehicle and vehicle-to-infrastructure communications. The high mobility of vehicles, dynamic topology and security risks have a devastating effect on the routing reliability, energy efficiency and trust management. To overcome these issues, this study proposes MOTMER-VANET, a multi-objective trust and mobility prediction-based energy-efficient routing framework that guarantees dynamic, secure and efficient communication within the dynamic vehicular conditions. In proposed framework, a mobility prediction module based on Bidirectional Long Short-Term Memory (BiLSTM) estimates future positions and generates a stability score for each node to improve cluster reliability using historical movement data. Simultaneously, Adaptive Trust Reinforcement (ATR) mechanism is used to dynamically assess the behavior of each node on the basis of successful packet forwarding, consistency in interactions and reputation in the past through reinforcement learning principles hence isolating malicious nodes. A Weighted Cluster Head (CH) Selection process then selects the most appropriate CHs after taking into account node stability, residual energy and trust value in a composite weighting function. Furthermore, a Hybrid Stellar-Mayfly Optimization Algorithm (HSMOA) is constructed for optimize routing. In addition, a priority-based dual emergency handling module ensures timely delivery of critical messages using a queue-based adaptive scheduler integrated with TDMA and CSMA hybrid transmission.

The proposed model is implemented in MATLAB, and tested in the case of black hole as well as flooding attacks. The simulation findings indicate that the proposed framework shows 98.9 PDR, 63 ms end-to-end, 374 kbps throughput, and 1.91 J energy consumption, which is significantly high in comparison with traditional protocols. The MOTMER-VANET framework is successful combination of mobility intelligence, trust adaptation, and hybrid optimization to increase the reliability of routing, security, and network life in the next generation of vehicular networks and smart transportation systems.

1. Introduction

Vehicular Ad Hoc Networks (VANETs) are a specialized type of Mobile Ad Hoc Networks (MANETs) that can be used to support a dynamic wireless communication between vehicles (Vehicle-to-Vehicle, V2V) and a vehicle and a roadside infrastructure (Vehicle-to-Infrastructure, V2I) [1] [2] [3]. Cooperative communication aims at the main objective of VANET, which is to improve road safety, efficiency of traffic management, and infotainment services [4] [5]. Yet, VANETs are highly mobile in nature, their topology is frequently modified, and the network density is dynamic, which creates a significant challenge to research into the stable and reliable communication [6]. Conventional routing and clustering strategies can no longer maintain the performance in such fast-changing vehicular conditions resulting in deteriorated throughput, delay and frequent route disconnection [7]. Therefore, the challenge of developing a resilient, adaptable, and even intelligent routing infrastructure that would provide high-quality connectivity and efficient use of the resources is an urgent open problem.

One of the major weaknesses of current VANET routing protocols including Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Geographic Routing protocols is that they assume instant topology or constant parameters which tend to become outdated because of vehicle mobility [8] [9]. The stability can be significantly increased by predicting mobility patterns and incorporating them in routing decisions [10]. In addition, trust management mechanisms have to be incorporated to reduce the risks of malicious nodes, malicious data injection, and selfishness in vehicular systems [11]. In this regard, mobility prediction and trust assessment can be combined and create the basis of guaranteeing reliable and secure routing in VANETs [12].

To deal with such challenges, there are recent studies that study diverse machine learning and optimization-based methods. Deep learning algorithms like neural networks have shown a good response in the modeling of patterns of temporal mobility of vehicles [13]. Nevertheless, the existing models are based on one-parameter mobility measurements, which are not a multi-feature temporal learning required in traffic conditions [14]. On the same note, trust-based routing models usually utilize either static or probabilistic trust computation schemes that are not capable of responding to dynamic vehicle behaviors [15]. The limitations drive the necessity of a multi-level, adaptive, and learning-based routing policy, which dynamically incorporates mobility prediction, trust reinforcement and energy efficiency into an overall optimization system.

Moreover, cluster-based communication is important to reduce the routing overhead and enhance the scalability in VANETs [16]. Gathering vehicles into smaller units (Cluster) where a Cluster Head (CH) is a local coordinator in order to aggregate and send data to the base station or to other clusters [17]. Nevertheless, the stability of clusters is very dependent on the selection criteria of CH [18]. Conventional methods which only use measurements like node degree, residual energy, or distance tend to result in re-election of CH and division of the network frequently [19]. It is thus imperative to ensure that multi factor decision mechanisms that involve mobility prediction, node trustworthiness and the remaining energy are introduced in such a way that stability is achieved alongside reliability in the formation of clusters.

To achieve even better routing decisions, multi-objective optimization algorithms have become inseparable tools to achieve trade-offs between incompatible channels like delay, link stability, trust, and energy consumption. VANET optimization has been popularly done using swarm intelligence and evolutionary algorithms, including Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Genetic Algorithms (GA) [20]. However, these approaches have problems of premature convergence and lack of the balance between exploration and exploitation [21]. It is therefore necessary to have a hybrid optimization algorithm that combines the global search power of stellar-inspired algorithms and the local refinement power of swarm-based approaches in order to get an optimal routing configuration. Based on these observations, this paper proposes an innovative framework of multi-objective trust and mobility prediction-based energy-efficient routing (MOTMER-VANET) framework that combines deep learning-based mobility prediction, adaptive trust reinforcement, and multi-objective optimization in a hybrid approach to select head nodes of the cluster and efficiently route them. The major contributions of this study are summarized as follows:

- This study proposes MOTMER-VANET, a multi-objective trust and mobility prediction-based energy-efficient routing framework to promote stability of routing, security and energy efficiency of dynamic vehicular ad hoc networks. The proposed MOTMER-VANET architecture combines deep learning-assisted mobility prediction, adaptive trust reinforcement, multi-objective hybrid optimization, and dual emergency processing methods into a single architecture.
- The study employs Bi-directional Long Short-Period Memory (BiLSTM) to forecast the future positions and velocities of vehicles, is used. The model can foresee temporal mobility interactions in both the forward and backward directions, and thus, predicts topology changes, allowing to form the clusters proactively and in a stable manner when the traffic speed is high.
- The proposed MOTMER-VANET framework incorporates Adaptive Trust Reinforcement (ATR) model to assess the behavior of nodes through direct interactions, neighbor recommendation as well as the historical data. Trust values are revised using the concept of reinforcement learning to determine and isolate malicious nodes to maintain a secure and trustworthy communication.
- A weighted CH selection process based on three parameters is suggested and includes the predicted node stability, remaining energy, and reliability. This weight-based method is composite, which guarantees the use of trusted and energy-saving cluster heads, which improves the long life of clusters and consistency in communication.
- The study develops A Hybrid Stellar-Mayfly Optimization Algorithm (HSMOA) to solve the multi-objective optimisation of routing.
- The proposed framework incorporates Priority-Based Dual Emergency Handling which is a queue-based adaptive scheduling mechanism with dual channel access control to provide delivery of differentiated QoS delivery. The PDEH module prioritizes dynamically the data packets in accordance with the urgency, the trust, and the remaining energy, guaranteeing that the safety critical messages are allocated a minimum delay and at the same time, fairness is provided to the non-emergency data.

The remainder part of this document is systematized as follows: Section 2 presents an extensive review of existing VANET approaches, Section 3 provides a detailed description of the proposed framework including its modular architecture and working flow, Section 4 details the simulation environment, configurations, and performance metrics used to evaluate the proposed model, comparative analysis with existing protocols is also discussed, Section 6 summarizes the research findings, emphasizing the contributions of proposed framework with future scope of study.

2. Related Work

VANETs have involved noteworthy attention over the past decade, leading to the development of diverse routing protocols that address mobility, and security requirements. This section reviews the existing studies to identify the gaps to develop an innovative framework in this area. Ali *et al.*, [22] presented a strong cryptographic protocol for safe data delivery in VANET that limits the role of the trusted authority and uses the communication ID of the vehicle to conduct communication as opposed to real entities. The security analysis presented shows the strength of the proposed protocol in various types of security attacks. ul Hassan *et al.*, [23] proposed an intelligent cluster-based routing protocol to overcome those problems in VANET routing. The system is operational through two essential stepping stones: firstly, it is based on an Artificial Neural Network (ANN) model to mask harmful nodes, and secondly, a cluster is formed on modified clustering algorithms, having cluster heads (CHs) respectively. The intelligent routing protocol then determines an optimum route for the path to decrease packet transmission delays. More particularly, to adopt a modified ad hoc on-demand distance vector (AODV) protocol, which implements on-request route discovery and loop-free route selection.

Reddy *et al.*, [24] proposed a trust-enabled routing for VANETs approach that combines direct, indirect, situational, and experiential trust to determine node reliability. Mobility influences both direct trust (DT), which involves punishment and reward scenarios, communication amount and consistency, and delay times. Indirect trust (N-DT) is determined by feedback trust, mobility, and link reliability. Situational trust involves the time of day, location, weather conditions, and traffic density. Communication allows us to build experience and trust. Giridhar *et al.*, [25] proposed a protocol for VANET, which combines adaptive neural fuzzy cluster (ANFC) and quantum glowworm swarm

optimization-based routing (QGSOR). In the ANFC-QGSOR that is proposed here, vehicles communicate with each other in the first phase. The ANFC technique is used in the three conditions required when selecting a cluster head (CH) and forming clusters with two inputs: residual energy, distance, and node degree. The QSGOR technique was also employed in route selection, utilizing fitness function that selects the optimal routes to the destination. Dhakad *et al.*, [26] evaluate a new technique of congestion in VANET technology using Dynamic Grouping of Vehicles for Safety (DGVS). DGVS permits vehicles to communicate directly with others in the same DGVS and does not require an entire network broadcast of their message. The long-term objective is to achieve a drastic reduction in traffic, while still allowing important data transfer for VANET traffic control and safety purposes. It also indicates the effectiveness of the proposed dynamic grouping of vehicles for safety (DGVS) method in finding a solution for VANET congestion.

Gopalan *et al.*, [27] presented Data Dissemination Protocol (DDP). The VANET routing protocols can be categorized into topology-based routing protocols and location-based routing protocols. The intention aimed at flooding an emergency message to reach the fixed sources as soon time possible. The standard messages are routed to First in First Out (FIFO) queue. Using Time delay-based Multipath Routing (TMR) approach, routes have been found to transport these messages to a destination node and to find the best secure route. Rashid *et al.*, [28] described new trajectory to increase reliability to maximum or trust and mobility-based evaluation for intelligent collaborative (TMIC)-unmanned aerial vehicle (UAVs) aided VANETs. The reactive multipath greedy routing protocol (RMGR) and this hybrid routing protocol are combination of ad hoc on-demand multipath distance vector (AOMDV) with greedy geographic forwarding (GGF), which is conducted when routing within frequently mutable network topology. Trust evaluation (TE), based on direct trust and indirect trust, also known as effective trust evaluation (ETE), is to be performed the protect against the network's failures.

Xu *et al.*, [29] presented Secure and Reliable Opportunistic Routing (SROR) mechanism, which selects candidate forwarding nodes based on their relative velocity, connectivity probability, and packet forwarding ratio to an optimal forwarding node. SROR uses a Markov Decision Process (MDP) to identify the best relay node whilst learning from the forwarding behavior of previous nodes in the past to avoid malicious node selections. Ali *et al.*, [30] developed new reliable model for Vehicle Ad hoc Networks aimed at supporting reliable route finding in VANETs. The focus was on link reliability, or the likelihood of maintaining an operational link of communication between vehicles for an extended period of time. However, to determine link reliability with accuracy through vehicular location, velocity, and directional information on roadways. Lastly, the proposed route-finding protocol, AODV-R, is based on the ad hoc on-demand distance vector (AODV) routing protocol. Ahmad *et al.*, [31] proposed a received signal strength (RSS)-based localization method relying on roadside units (RSUs) detecting signals in range for the vehicle's positioning is proposed. VANETs are vital to ITS, providing functions for vehicle tracking and positioning and alerting in emergencies. Urban environments pose a difficult vehicle localization problem as GPS-based vehicle localization is often inaccurate. This method takes advantage of high signal-to-noise ratios provided by nearby RSUs and also utilizes the CRLB to estimate the vehicle's position accuracy. [32] proposes a novel emergency handling scenario.

The current routing schemes are primarily topological/geographical based in targeted route development without considering dynamic movement of vehicles, changing network density and network security weaknesses. The protocols tend not to support stable route when the situation is highly mobiles, causing more loss of packets and low delivery proportion. Besides, conventional protocols use security systems that depend on cryptographic validation, which is computationally intensive and adds latency-inappropriate in vehicle communication. Moreover, routing systems based on clustering usually only use the static parameters of CH such as residual energy or node degree. These single parameters methods overlook other contributing factors like mobility prediction, trustworthiness, and stability of the network leading to repeated CH re-election and fragmentation of the network. Although some studies have proposed the use of trust-based models to improve security, most of them employ trust evaluation based on a static or a threshold, which are not very effective in countering adaptive or intelligent adversaries. Moreover, classic optimization methods of routing are prematurely convergent and cannot balance the three goals of stability, energy saving and trust. The other major weakness that was mentioned in the previous works is that it lacks adaptive scheduling and prioritization of the way in which emergency messages are handled. Delays in the transmission of emergency data may have serious consequences in a real-time traffic situation. Nevertheless, the vast majority of existing frameworks handle all data packets equally without taking the context of the importance of safety-related communications into consideration. Therefore, even though there are various improvements, there is still a major gap in research to develop a multi-objective, trust-based, mobility-predictive, and energy-efficient VANET that will provide secure, stable, and real-time communication within dynamic vehicular systems. To solve these issues, this study introduces MOTMER-VANET that combines the BiLSTM-based mobility prediction, ATR approach and a weighted CH (CH) selection mechanism, HSMOA of routing optimization with multi-objectives and priority-based dual emergency handling to allow reliably the delivery of critical messages when there is an attack and congestion situation is also introduced.

3. Proposed Methodology

The MOTMER-VANET framework includes several adaptive and connected modules that can guarantee reliable communication within the vehicular network. The first step is to initialize a network, which each vehicle is assigned its own ID, energy, position, and trust, and neighbor discovery is provided by exchanging beacons. Mobility prediction module is a prediction module which is based on BiLSTM model and it can predict the future positions and velocities of vehicles to estimate the stability of the nodes. At the same time, an ATR mechanism trains nodes with a history of packet forwarding and response by the neighbouring vehicles and dynamically re-evaluates the trust scores to counter malicious actions. The parameters of predicted stability, trustworthiness and residual energy are then weighted together to create secure and long-lasting clusters in a weighted CH selection process. A HSMO algorithm is used to compute the best path interconnecting clusters considering the trade-off of various objectives like the level of trust, status of congestion and energy used. Lastly, an adaptive scheduling and dual emergency handling scheme based on queue model gives priority of message transmission based on level of urgency through an integrated TDMA-CSMA hybrid model of access. This process reduces the waiting time of safety issues messages but does not reduce the fair access to regular message transmissions. On the whole, the MOTMER-VANET architecture can be seen as the list of intelligent and complex routing approach that is dynamically adjusted to different vehicular conditions. Figure 1 illustrates the pipeline of proposed framework. With the help of predictive stability evaluation, trust-based communication, and multi-objective optimization, the framework ensures safe, congestion-free, and energy-efficient data transmission via vehicular networks.

3.1. Network Initialization

The initial stage of proposed MOTMER-VANET model is the network setup process, which creates a simulated scenario in MATLAB to simulate a real-world communication of vehicles in a VANET. K vehicles are deployed randomly on a two-dimensional road topology of $M \times N$ size. Every vehicle node has its starting set of parameters such as a unique identification in terms of Node ID, initial position, velocity, direction and communication range. A mobility model like Gauss-Markov model is used to update vehicle positions and movement trajectories dynamically to allow realistic vehicular motion patterns to be simulated. Here, the functional behavior of On-Board Units (OBUs) and communication standards including IEEE 802.11p are simplified to be represented by equivalent network parameters, such as the range of transmission, data rate, bandwidth, propagation delay and the ratio of packet loss. The GPS feature is virtually modelled by the mobility tracking with coordinates, where the node constantly changes its position vector (P_i, Q_i) with time t. At the stage of initialization, all nodes send a hello message to identify their one-hop neighbors and fill a neighbor table (T_N) with IDs, location, and remaining energy of accessible nodes. These interactions are dealt with by the environment in the form of data structure matrixes that capture inter-node distances and connectivity information. The T_N is the foundation of the other processing like trust evaluation and cluster formation. A distance threshold T_D is set to have efficient topology setup, and only the node that is within this range is regarded as an active neighbor. The model of the standard communication energy is utilized to simulate energy consumption, depending on the cost of transmission, reception, and processing as Eq. (1).

$$E_R(t) = E_I - (E_{Tx} + E_{Rx} + E_\delta + E_P)$$

1

Where $E_R(t)$ signifies residual energy at time, E_I represents initial energy of node, E_{Tx} and E_{Rx} are indicates consumed energy during data transmission and reception respectively, E_δ and E_P are energy consumed in idle state, and processing operations respectively.

The initialisation makes every simulated node have an updated situational awareness of its environment, allowing realistic testing of trust modules, clustering modules and routing modules in later steps.

3.2. Mobility Prediction using BiLSTM

In proposed MOTMER-VANET framework, mobility prediction module is designed to predict the future movement of vehicles to provide the stability in creating clusters and providing stable routing in highly dynamic vehicular environments. Due to time-varying and non-linearity characteristics of vehicular mobility patterns, classical prediction models, including Markov models or Kalman filters, are less accurate when the vehicles move at high velocities, or when they move irregularly. To this end, the framework uses BiLSTM based predictive model that successfully considers long-term dependence and other time-based associations between vehicular mobility parameters (speed, acceleration, direction, and position). Each vehicle V_i periodically records its mobility feature vector that represented as Eq. (2).

$$M_i(t) = \{(p_i(t), q_i(t)),\ a_i(t), v_i(t), \theta_i(t)\}$$

2

Where $M_i(t)$ represents mobility feature vector, $(p_i(t), q_i(t))$ denotes vehicle's geographical coordinates, $a_i(t)$ signifies acceleration, $v_i(t)$ denotes velocity, and $\theta_i(t)$ stands for heading direction at time t. These sequential features collected over a time window $T = \{t_1, t_2 \ldots, t_k\}$ form the input sequence to the BiLSTM predictor, which outputs the predicted mobility vector represented as $\widehat{M}_i(t+1)$.

BiLSTM is made up of two parallel LSTM layers with a forward layer that takes input sequences at $t_1 \rightarrow t_n$ and a backward layer that takes input sequences at $t_n \rightarrow t_1$ as shown in Fig. 2. The results of both layers are added together creating complete hidden representation of motion dynamics. There are computations at every time step t, which can be defined in the following way:

The Forget Gate is essential in the control of the passage of past memories in the BiLSTM memory cell. It dictates what features of previous state of the cell needs to be remembered or forgotten depending on the input at present and previous hidden state. Considered within the context of vehicular mobility prediction, this strategy enables the network to erase outdated or less important motion data and maintain important mobility trends, which can be used in building accurate future trajectory predictions. It is possible to define the forget gate as Eq. (3).

$$f_t^{\rightarrow} = \sigma\left(\omega_f^{\rightarrow}\left[h_{t-1}^{\rightarrow}, z_t\right] + b_f^{\rightarrow}\right)$$

3

Where $\sigma(\bullet)$ denotes sigmoid activation function, $f_t^{\rightarrow}$ represents forget gate vector of forward layer, $\omega_f^{\rightarrow}$ indicates weight matrix for forget gate, z_t represents current input vector, $h_{t-1}^{\rightarrow}$ denotes hidden state from prior time step, and $b_f^{\rightarrow}$ signifies bias term.

The Input Gate determines the acceptance of new motion information into the memory of the LSTM. It determines the significance of the present state of the vehicle and the proportion of it that must be reflected on the changed cell state. The mathematical representation of input gate is represented as Eq. (4).

$$i_t^{\rightarrow} = \sigma\left(\omega_i^{\rightarrow}\left[h_{t-1}^{\rightarrow}, z_t\right] + b_i^{\rightarrow}\right)$$

4

Where $\omega_i^{\rightarrow}$ and $b_i^{\rightarrow}$ weight and bias term of input gate respectively.

At the same time, the Candidate State ($\widetilde{C}_t$) generates a potential new content vector, which is the possible modifications to the cell memory given the current features of motion input. The sigmoid activation function at the input gate determines how much weight this candidate information has and the tanh activation is used to make the numbers normalized between − 1 and 1 to be numerically stable. In VANET situations, the mechanism can be used to make the model learn how recent changes in the motions such as acceleration change or lane change influence the future path so that the model can adapt the learning based on the contemporary driving conditions. It is mathematically presented as Eq. (5).

$$\widetilde{C}_t^{\rightarrow} = tanh\left(\omega_C^{\rightarrow}\left[h_{t-1}^{\rightarrow}, z_t\right] + b_C^{\rightarrow}\right)$$

5

Cell State Update operation combines the forget and input gates output to compose the updated memory state. It is an accumulation of the old long-term data of the last time step with the newly acquired mobility patterns of input. This mathematically is a weighted summation of old cell state and candidate state. This architecture is such that the BiLSTM retains the historical context as well as adapts to new data. This is useful especially in vehicular network where it is used to model long-term driving patterns and soften short-term changes in behavior using Eq. (6).

$$C_t^{\rightarrow} = f_t^{\rightarrow} * C_{t-1}^{\rightarrow} + i_t^{\rightarrow} * \widetilde{C}_t^{\rightarrow}$$

6

Output Gate determines the percentage of updated cell state information that will be added into the hidden output which will be passed across to the next time steps. It initially establishes the applicability of the existing memory content using a sigmoid function and then processes the tanh-transformed cell state to produce the final output Hidden State as Eq. (7) and Eq. (8).

$$O_t^{\rightarrow} = \sigma\left(\omega_O^{\rightarrow}\left[h_{t-1}^{\rightarrow}, z_t\right] + b_O^{\rightarrow}\right)$$

7

$$h_t^{\rightarrow} = O_t^{\rightarrow} * tanh\left(C_t^{\rightarrow}\right)$$

8

This latent state summarizes a balance in time between both long-term and recent mobility information. Within the MOTMER-VANET framework, this allows the BiLSTM to successfully summarize the dynamic behavior of the vehicle over time to generate a predictive feature vector capable of predicting the future positions, and changes in connectivity. The resulting hidden state is a high-level temporal embedding that increases the accuracy and robustness of mobility prediction even in case of highly changing traffic conditions.

In the backward LSTM layer, data are processed with reversed temporal sequences with the same equations using $f_t^{\leftarrow}$, $i_t^{\leftarrow}$, $\widetilde{C}_t^{\leftarrow}$, $C_t^{\leftarrow}$, $O_t^{\leftarrow}$, $h_t^{\leftarrow}$. The last hidden representation at every time period t is the combination of both forward and backward hidden states as Eq. (9).

$$h_t = \left[h_t^{\rightarrow} \bigoplus h_t^{\leftarrow}\right]$$

9

Where $\bigoplus$ denotes concatenation operation.

This joint representation cuts across both historical and anticipatory motion characteristics hence enhancing the accuracy of subsequent state prediction. A dense output layer is then used to obtain predicted mobility state as Eq. (10).

$$\widehat{M}_i(t+1) = \omega_o \bullet h_t + b_o$$

10

Where ω_o and b_o are output weight matrix and bias term, respectively. The BiLSTM is trained with Mean Squared Error (MSE) loss value with the help of following Eq. (11).

$$MSE = \frac{1}{M}\sum_{i=1}^{M}\left\|M_i(t+1) - \widehat{M}_i(t+1)\right\|^2$$

11

Where M signifies total number of samples, $M_i(t+1)$ and $\widehat{M}_i(t+1)$ are actual next mobility and predicted vector respectively.

After the prediction of next position, Predicted Link Stability (PLS) between two vehicles i and j is evaluated using Eq. (12).

$$PLS_{i,j} = exp\left(-\frac{\left|d_{ij}(t+1) - d_{ij}(t)\right|}{\tau_c}\right)$$

12

Where $d_{ij}(t)$ and $d_{ij}(t+1)$ are current and predicted distance between vehicles x and y, and τ_c stands for communication range. A higher PLS value signifies stronger and more reliable connectivity.

3.3. Adaptive Trust Reinforcement

The ATR mechanism is a key component of MOTMER-VANET system that can ensure the security, reliability, and cooperation of vehicular nodes in communication. As VANETs work in dynamic and decentralized settings, malicious nodes can disrupt routing by falsely delivering messages, dropping packets or flooding. Thus, ATR model is needed to constantly review the behavioral integrity of every node using direct and indirect observations, and adapt to the mobility and environmental dynamics. Each V_i maintains a trust table of all its one-hop neighbors which contains the dynamic trust values $T_{xy}(t)$. There are two key elements in the computation of trust, which include direct and indirect trust.

3.3.1. Direct Trust Evaluation

Direct trust is a measure of the reliability of node V_y on a direct communication with node V_x. It is calculated as the ratio between the successful packet forwarding and cooperative communication behavior as Eq. (13).

$$DT_{xy}(t) = \alpha \bullet \frac{P_{S,xy}(t)}{P_{T,xy}(t)} + (1-\alpha) \bullet \left(1 - \frac{P_{D,xy}(t)}{P_{T,xy}(t)}\right)$$

13

Where $DT_{xy}(t)$ represents direct trust of node y as perceived by node x at time t, $P_{T,xy}(t)$ indicates total number of packets communicated from x through y, $P_{S,xy}(t)$ and $P_{D,xy}(t)$ are denotes number of successfully forwarded packets from x to y, and packets dropped by node y respectively. α represents weighting coefficient that balances successful forwarding and packet dropping behavior with range of 0 and 1.

3.3.2. Indirect Trust Evaluation

In case of a situation where direct communication is inaccessible or in the short term, indirect trust is obtained based on the recommendation of neighbouring nodes that have earlier on interacted with V_y. It is calculated as Eq. (14).

$$IDT_{xy}(t) = \frac{1}{|M_x|} \sum_{k \in M_x} \beta_k \bullet DT_{xy}(t)$$

14

Where $IDT_{xy}(t)$ denotes indirect trust value of node y as perceived by node x, M_x represents set of neighbors of node x, β_k indicates recommendation weight allocated to node k based on its reliability.

3.3.3. Adaptive Trust Reinforcement and Update Mechanism

Adaptively, the total trust value of a node is formed by summing up direct and indirect trust, and the time decay of trust reinforcement based on reinforcing-inspired reward mechanism. The adaptive update of trust function is represented using Eq. (15).

$$T_{xy}(t+1) = \delta \bullet DT_{xy}(t) + (1-\delta) \bullet IDT_{xy}(t) + \gamma \bullet R_{xy}(t) + \omega \bullet D_{xy}(t)$$

15

Where $T_{xy}(t+1)$ indicates updated trust of node y as observed by node x at time $t+1$, $\delta \in [0,1]$ denotes weight factor highlighting direct trust over indirect trust, $R_{xy}(t)$ signifies reward term, reinforcing trust if node y effectively forwards or delivers packets as predicted, γ and ω are adaptive learning rates that regulates the degree of trust increase and decrease, respectively, and $D_{xy}(t)$ defines penalty term, reducing trust if node y exhibits malicious behavior.

The reward term $R_{xy}(t)$ is expressed as Eq. (16)

$$R_{xy}(t) = \omega_1 \bullet e^{-\frac{E_{c,y}(t)}{E_{i,y}}} + \omega_2 \bullet PLS_{i,j}(t)$$

16

Where $\omega_1, \omega_2 \in [0,1]$ are represents weighting coefficients satisfying $\omega_1 + \omega_2 = 1$, $E_{c,y}(t)$ denotes energy consumed by node y during time t, $E_{i,y}$ indicates initial energy, and $PLS_{i,j}(t)$.

The penalty term $D_{xy}(t)$ can be expressed as Eq. (17).

$$D_{xy}(t) = \lambda_1 \bullet \frac{P_{D,xy}(t)}{P_{T,xy}(t)} + \lambda_2 \bullet \left(1 - PLS_{i,j}(t)\right)$$

17

Where $\lambda_1, \lambda_2 \in [0,1]$ are indicates coefficients for packet loss behavior and link instability penalties. This penalization dejects untrustworthy forwarding performance.

3.3.4. Trust Normalization

It is necessary that trust be normalized and classified. To make all trust values consistent irrespective of the changes in network conditions, all trust values are normalised within the interval [0,1] as Eq. (18).

$$T_{xy}^{Norm}(t+1) = \frac{T_{xy}(t+1) - T_{min}}{T_{max} - T_{min}}$$

18

Where T_{max} and T_{min} are maximum and minimum trust values observed across all nodes. A decision threshold τ (typically between 0.5–0.7) is applied to classify nodes as trusted if $T_{xy}^{Norm}(t+1) \geq \tau$, and malicious if $T_{xy}^{Norm}(t+1) < \tau$.

Even though no particular reinforcement learning agent is trained in the proposed ATR module, it adheres to the concepts of reinforcement learning, where successful collaborative behavior is rewarded (increased trust), whereas malicious behavior is punished (reduced trust). This dynamically-adjusting update, as a result of adaptive feedback, enables the trust system to dynamically adjust to the vehicular situation, being robust to topology changes, energy changes, and temporary misbehaviour. The ATR module is used to make sure the vehicles that are up and stable, yet energy-efficient and reliable in their behaviors are only subject to routing and cluster-head positions. The MOTMER-VANET framework is able to provide both security and stability by exploiting ongoing direct and indirect trust updates through a reinforcement-based adaptive learning process, which improves the resilience of the communication to blackhole, flooding and collusion attacks.

3.4. Weighted CH Selection

CH selection process is one of the most important processes in the given MOTMER-VANET framework since it directly determines the stability, reliability, and energy efficiency of the vehicular network. The CHs in this research are chosen based on a Weighted Multi-Factor Decision Model which combines data of the predicted node stability, trustworthiness and residual energy of vehicles. The primary aim of the proposed process is to achieve the capability of the chosen CHs to be strongly connected, maintain reliable communication, and have energy-efficient operations in dynamic driving conditions. Assume that each node in the network is represented by V_i, where $i = 1,2,3,\ldots,M$, and M is the total number of vehicles. The three fundamental metrics used to evaluate each node are node stability (S_i), trustworthiness (T_i) and residual energy (E_i). The total Weighted CH Selection Score (ω_i) of a particular node is calculated using Eq. (19).

$$\omega_i = \alpha_1 \bullet S_i + \alpha_2 \bullet T_i + \alpha_3 \bullet E_i$$

19

Where α_1, α_2, and α_3 are weight coefficients allocated to stability, trust, and energy, respectively, such that $\alpha_1 + \alpha_2 + \alpha_3 = 1$ and these coefficients are dynamically adjusted based on network conditions. S_i signifies stability score of vehicles i, resulting from BiLSTM-based mobility prediction. It signifies the predicted link lifetime between node i and its adjacent nodes. T_i denotes trust score attained from ATR module, representing behavioral reliability of node over time. E_i denotes normalized residual energy of node i, specifying its presented energy capacity.

3.4.1. Node Stability Estimation

The stability of node S_i reflects the stability of vehicle to stay connected with its neighbors during long period of time which minimizes the overhead of vehicle having to re-select CH frequently. The link lifetime (LL) between node i and j is estimated on the basis of BiLSTM model determine position $\widehat{\rho}_i(t + \Delta t)$ of a node using Eq. (20).

$$LL_{ij} = \frac{R - \|\widehat{\rho}_i(t+\Delta t) - \widehat{\rho}_j(t+\Delta t)\|}{V_r}$$

20

Where R denotes communication range of node, $\|\widehat{\rho}_i(t+\Delta t) - \widehat{\rho}_j(t+\Delta t)\|$ denotes Euclidean distance between predicted future positions of nodes i and j, and V_r indicates relative velocity between two nodes.

The stability score S_i for node i is then calculated as the average link lifetime with all its neighbors using Eq. (21).

$$S_i = \frac{1}{|M_i|} \sum_{j \in M_i} LL_{ij}$$

21

Where M_i denotes set of neighbouring nodes of vehicle i.

3.4.2. Trustworthiness Evaluation

The ATR mechanism, which combines direct interactions, indirect feedback, and reinforcement learning updates, generated the trust score T_i. This guarantees that the nodes that have good communication behavior and are most reliable are assigned a higher value of trust, whereas malicious and unpredictable nodes are downgraded.

3.4.3. Residual Energy Estimation

Energy-aware selection is added to eliminate the frequent CH failures. The normalized residual energy of a node is provided by Eq. (22).

$$E_i = \frac{E_i^R}{E_i^I}$$

22

Where E_i^I and E_i^R are denotes initial and residual energy of node i.

3.4.4. CH Selection Process

Once ω_i has been computed on all the nodes in a cluster; the node with the largest score is chosen as CH using Eq. (23).

$$CH = \underset{i \in C}{\operatorname{argmax}} (\omega_i)$$

23

Where C signifies the set of candidate nodes in cluster.

The Weighted CH selection approach provides a trade-off between mobility stability, trustworthiness, and energy sustainability which has made the CHs resilient and dependable even in the high mobility vehicle settings. Besides, the weighting factors α_1, α_2, and α_3 are dynamically revised according to network dynamics, with HSMOA tuning strategy, which provides the best CH distribution and minimizes the communication overhead. This trust and mobility-based CH selection mechanism dramatically increases the network lifetime; ratio of packet delivery and reliability of communication as opposed to the traditional single parameter CH selection mechanisms.

3.5. Multi-Objective Routing Optimization using HSMOA

VANETs are dynamic and heterogeneous, and therefore they need an adaptive routing optimization mechanism that can ensure network stability, energy efficiency, and reliability between nodes. To overcome these difficulties, this study proposes a Multi-Objective Routing Optimization model created on HSMA. The HSMOA combines the exploration oscillation of Stellar Oscillation Optimizer (SOO) and social interaction strategy of exploitation of Mayfly Optimization Algorithm (MOA). This hybridization allows the concurrent optimization of various opposing goals- i.e. node stability, residual energy, and trustworthiness thus improving the overall routing efficiency and reliability in dynamic vehicular setting.

3.5.1. Objective Formulation

The optimization problem is stated as a multi-objective optimization problem consisting of an objective task to choose the best possible combination of CHs and routing paths to the minimum link instability, maximum residual energy and maximum node trust. The total fitness F_{total} is defined as Eq. (24).

$$F_{total} = \omega_1(1 - S_i) + \omega_2 \bullet \left(\frac{1}{E_i}\right) + \omega_3(1 - T_i)$$

24

Where ω_1, ω_2, and ω_3 are weight coefficients such that $\omega_1 + \omega_2 + \omega_3 = 1$, indicating the relative significance of each metric.

The HSMOA objective is to reduce F_{total} in the entire network and thus determine an optimum of stable, reliable and energy efficient nodes to act as cluster heads and routing intermediaries. The mathematical model HSMOA is described in subsequent sections:

3.5.2. Initialization

The optimization starts with the initializing of HSMOA. Every $H_i = [h_{i1}, h_{i2}, \ldots, h_{iD}]$ is a candidate routing configuration signature and D represents the size of search space. Position value h_{id} represents the decision by a node d is to be a CH or a relay. The starting positions are randomly selected on the search range using Eq. (25).

$$H_i = lb + R \times (UB - LB)$$

25

Where UB and LB are upper and lower bounds of search domain, respectively.

3.5.3. Stellar Oscillation Exploration Phase

The SOO element assists the global searching in the first stage of exploration; oscillatory movement driven by the stellar pulsation. The oscillatory positions of each solution H_i are defined by Eq. (26).

$$H_i^S = H_{best}(t) - R_1 R_2 \left[\omega(t) S(t) R_1 - S(t)\right] \left(H_i(t) - |R_1 sin(R_2)| R_3 H_{best}(t)\right)$$

26

Where $H_{best}(t)$ indicates global best solution at iteration t, $\omega(t)$ represents oscillation frequency at iteration t, $S(t)$ denotes time-decaying scaling factor.

This type of search using oscillation is better at exploration and avoids premature convergence by adjusting dynamically the search direction and amplitude. The best k solutions of the SOO phase are the elite oscillators which are refined further in the mayfly phase.

3.5.4. Mayfly Exploitation Phase

Localised exploitation is applied in MOA which resembles mating and movement of mayflies. Positions of the male and female mayflies are denoted by position H_i^M, and H_i^F respectively with respective velocities V_i^M and V_i^F. The update equation of the male velocity is expressed in Eq. (27).

$$V_i^M(t+1) = \delta_1 e^{-\alpha E_p^2}(PBest_i - H_i^M) + \delta_2 e^{-\alpha E_g^2}(GBest_i - H_i^M) + \gamma(t)(H_{elite}^S - H_i^M)$$

27

Where δ_1, α_2 are acceleration coefficients for personal and global learning, α denotes visibility coefficient that controlling decay with distance, $\gamma(t)$ signifies adaptive oscillation influence factor, dynamically decreasing as t increases to shift from exploration to exploitation. E_p and E_g are Euclidean distances from present mayfly to its personal and global best positions, respectively

The updated position is then computed as Eq. (28).

$$H_i^M(t+1) = H_i^M(t) + V_i^M(t+1)$$

28

There is an operation depending on its fitness with reference to its mate male for every female mayfly as Eqn. ().

$$V_i^F(t+1) = \begin{cases} V_i^F(t) + \delta_3 e^{-\alpha E_{mf}^2}\left(H_i^M - H_i^F\right); if\ f\left(H_i^F\right) > f\left(H_i^M\right) \\ V_i^F(t) + \tau \bullet Rand(-1,1) \end{cases}$$

29

Where δ_3 denotes female attraction coefficient, τ indicates random flight coefficient for stochastic movement, E_{mf} signifies male–female distance.

3.5.5. Mating and Offspring Generation

Elite male-female pairs are crossovered to produce offspring after they are updated with velocities and positions using Eq. (30) and Eq. (31).

$$MO_1 = \varphi\, H_i^M + (1-\varphi\,)\, H_i^F$$

30

$$MO_2 = \varphi\, H_i^F + (1-\varphi\,)\, H_i^M$$

31

Where φ denotes random crossover coefficient. The child inherits the characteristics of the two parents and fittest individuals take the place of the unfit individuals in the culture.

3.5.6. Fitness Evaluation

The fitness function F_{total} is used to evaluate each candidate solution (node or cluster configuration). The personal best and global solutions are updated using Eq. (32) and Eq. (33) respectively.

$$Pbest_i = \begin{cases} H_i;\ \ if\, f\,(H_i) < f\,(Pbest_i) \\ Pbest_i\,; otherwise \end{cases}$$

32

$$gbest = Min\,(f\,(Pbest_i))$$

33

It is repeated until the termination criterion is satisfied, either by reaching the maximum number of iterations Tis or by finding the improvement in fitness insignificant.

3.5.7. HSMOA integration in Routing

The last solution $Pbest_i$ is derived by HSMOA is optimal CH and routing configuration that maximizes trust, energy efficiency, and stability. This pattern is transmitted to the VANET to refresh the memberships of clusters and routing paths. The algorithm re-examines dynamically the nodes depending on the periodical update of the mobility, energy, and trust values in which routing decisions are always adaptive to network dynamics.

3.6. Priority-Based Dual Emergency Handling

VANETs are frequently subject to dynamic and time sensitive emergency cases. Management of such emergency cases is critical to ensure that there is no delay in communication, collisions of packets, and loss of messages. A priority-based dual emergency handling mechanism is introduced in MOTMER-VANET framework to achieve priorities-based, fast and reliable delivery of emergency messages without interruption of the normal flow of data. The bifurcated character of this mechanism is two complementary layers of emergency management (1) Priority-Aware Queue Scheduling, and (2) Dual Channel Access Control that are jointly used to ensure Quality of Service (QoS) in the conditions of critical network conditions.

3.6.1. Priority Classification

Every message that is produced in the network is categorized to be of one of three levels of priorities depending on the urgency and nature of message using Eq. (34).

$$PL_m = \begin{cases} 1\ for\, Critical\, Emergency\, Messages \\ 2\ \ for\, high\, priority\, messages \\ 3\ for\, nomal\, communication\, messages \end{cases}$$

34

Where PL_m is the level of priority of message m. This priority is attached to each message and it is sent to the Queue-Based Adaptive Scheduler (QAS). Messages with critical emergency type are assigned absence of a delay, and the low-priority messages are temporarily withheld or re-scheduled depending on the load in the network at a specific time.

3.6.2. Queue-Based Adaptive Scheduling

The priority-based dual emergency handling module incorporates queue-based adaptive scheduler approach to control the transmission of messages when traffic is congested and there is an emergency. The scheduler has three individual queues $q_1,\ q_2,\ q_3$, which are critical messages, high-priority, and normal respectively. A queue is assigned a dynamic weight scheduling ω_D based on message priority and existing network level of congestion as Eq. (35).

$$\omega_D = \frac{PL_m}{1+\gamma_c}$$

35

Where ω_D represents dynamic scheduling weight for priority $PL_m,\ \gamma_c$ signifies channel congestion coefficient, defined as the ratio of busy slots to total available slots in communication channel.

Then the Transmission Probability (ρ_T) of each message m is computed as Eq. (36).

$$\rho_T = \frac{\omega_D}{\sum_{n=1}^{3}\omega_n}$$

36

This ensures that as the number of congestions rises, the delay of lower priority messages is proportionate and high priority and critical packets prevail in the channel access. The queue is re-assessed on the basis of Δt time interval to adjust to the network dynamics.

3.6.3. Dual Channel Access Control

Besides the queue scheduling, the priority-based dual emergency handling uses a dual channel access control model that incorporates Time Division Multiple Access (TDMA) and Carrier Sense Multiple Access (CSMA) models. In regular circumstances, the CSMA mechanism is used to deal with conventional communications, which will allow elastic access to the medium. Nevertheless, the TDMA slots are automatically adapted during emergencies to ensure that high priority messages with high priorities receive collision and deterministic access. The condition of switching between CSMA and TDMA is a hybrid and determined by an Emergency Switching Coefficient (ESC) ζ as given in Eq. (37).

$$\zeta = \begin{cases} 1; if\ \psi_e \geq\ \psi_{th} \\ 0; otherwise \end{cases}$$

37

TDMA slots are deterministically allocated to CH and the associated nodes when $\zeta = 1$ so that the CH and the nodes can disseminate emergency messages. The time slot T_{slot} is dynamically calculated on the basis of message load as expression given in Eq. (38).

$$T_{slot} = \frac{M_e}{C}$$

38

Where M_e denotes number of emergency messages awaiting transmission, and C stands for channel capacity.

This scheduling approach ensure that messages related to emergencies are provided with exclusive and non-interrupted access without entirely interrupting any non-critical transmission involved.

3.6.4. Priority-based Forwarding Decision

After the emergency message has been received by a CH it calculates the next-hop forwarding node using a combined Priority Forwarding Metric (PFM). The metric includes the score of the trust and the estimated stability of links between CHs and neighbor vehicles as expression given in Eq. (39).

$$PFM_{ij} = \alpha_1 \bullet\ T_j + \alpha_2 \bullet\ S_{ij}$$

39

Where PFM_{ij} denotes forwarding score from node i to node j; T_j represents trust score of candidates forwarding node j; S_{ij} defines predicted stability score between nodes i and j.

The next-hop node with highest PFM_{ij} is designated for message forwarding as expression stated in Eq. (40).

$$NH = \underset{j}{\operatorname{argmax}} \left(PFM_{ij} \right)$$

40

This ensures that the emergency messages are always passed over the most stable and reliable routes which minimizes the loss of packets even during a state of attack or congestion.

The priority-based dual emergency handling allows merging adaptive scheduling with dual-channel switching and priority-based routing, which has low latency, less congestion, security, dynamic adaptability. Therefore, priority-based dual emergency handling mechanism presents a smart, coherent way of ensuring high reliability, stability, and timeliness in emergency data dissemination to VANET environment.

4. Results and Discussion

The simulation outcomes and detailed analysis of proposed MOTMER-VANET framework are explained in subsequent sections.

4.1. Experimental Setup

To assess the functionality of the proposed MOTMER-VANET framework, the simulations were performed in large-scale simulations with the MATLAB R2023b. The simulation environment was developed such that it simulated a very dynamic urban vehicle network with changing vehicle density, mobility behavior, and communication limitations. The experiments were aimed at the investigation of the routing stability, accuracy of trust, and energy efficiency in various attack conditions, blackhole and flooding attacks. Table 1 shows the parameters settings of experiment.

Table 1
Simulation Parameters

Parameter	Description / Value
Simulation tool	MATLAB R2023b
Simulation area	2000 m × 2000 m
Number of vehicles	50–200
Vehicle speed	10–30 m/s
Mobility model	Random Waypoint Model
Communication range	300 m
MAC layer protocol	IEEE 802.11p
Simulation time	500 s
Packet size	512 bytes
Transmission rate	4 packets/s
Transmission power	0.4 W
Attacks simulated	Blackhole attack, Flooding attack

4.2. Performance Metrics

To determine the effectiveness of proposed MOTMER-VANET framework in a comprehensive manner, a number of quantitative measures were used to measure network stability, routing efficiency, energy consumption, and trust accuracy. Each of the metrics offers information about a particular area of vehicular network performance when traffic is at different densities and attack conditions. The metrics that are chosen are:

4.2.1. Packet Delivery Ratio (PDR)

PDR is used to measure the reliability in the transmission of data in the network and gives the percentage of data packets received successfully to the destination nodes in comparison with the number of data packets sent by the source nodes. The mathematical expression of PDR is stated in Eq. (41). A better PDR is the capability of the routing algorithm to reduce congestion, link-related failure, or malicious node packet drops.

$$\varvecP\varvecD\varvecR = \frac{\sum_{\varveci=1}^{\varvecK_{\varvecp}} \varvecP_{\varvecr}(\varveci)}{\sum_{\varveci=1}^{\varvecK_{\varvecp}} \varvecP_{\varvecs}(\varveci)} \times 100$$

41

Where K_p indicates number of packet transmissions, $P_s(i)$ stands for number of packets sent from source node i, and $P_r(i)$ indicates number of packets successfully received at destination node i.

4.2.2. End-to-End Delay

The average end to end delay is used to measure the delay of traversing a data packet through the network between the source and the destination. It takes into consideration queuing delay, transmission delay, processing delay and propagation delay at the intermediate nodes. With a smaller D_{avg} a lower value means increased speed in data transmission, which is necessary in time-sensitive car uses like collision warning systems and traffic lights timing.

$$\varvecD_{\varvecavg} = \frac{1}{\varvecK_{\varvecr}} \sum_{\varveci=1}^{\varvecK_{\varvecr}} \varvect_{\varvecr}(\varveci) - \varvect_{\varvecs}(\varveci)$$

42

Where K_r denotes total number of received packets, $t_s(i)$ and $t_r(i)$ are represents transmission and reception time of i^{th} packet.

4.2.3. Throughput

Throughput is a measure of data passing a communication channel successfully within a specific time period. It assesses the bandwidth usage and effectiveness of the network in the transfer of useful information. Increase in throughput indicates the ability to control congestion and maximize the use of resources on the vehicular network.

$$Throughput = \frac{\sum_{i=1}^{K_r} P_r(i) \times M_p}{T}$$

43

Where K_r denotes total number of packets successfully received, M_p indicates size of each data packet (in bits), and T denotes total simulation time.

4.2.4. Energy Consumption

Energy consumption is an important parameter in VANETs particularly in ensuring connectivity on a long-term basis among the vehicles and roadside units. It is the sum of energy consumed by all nodes in transmission, reception and processing control packets. Reduced average energy consumption implies more energy-efficient routing algorithm and increased network life.

$$E = \frac{1}{K_n} \sum_{i=1}^{K_n} E_{in}(i) - E_{res}(i)$$

44

Where K_n denotes total number of nodes, $E_{in}(i)$ and $E_{res}(i)$ are initial and residual energy of node i.

4.2.5. Cluster lifetime (CL)

CL is defined as the time interval during which a cluster remains effective without CH re-election. It replicates the stability of cluster construction influenced by mobility prediction and CH selection.

4.3. Performance Analysis Under Attack Scenarios

Black hole and flooding attacks are two of the most common malicious activities of VANETs that can have severe effects of compromising routing system performance, augmenting data loss, and destabilizing networks. In order to test the resilience of proposed model in an adversarial environment, simulation tests were performed based on Blackhole and Flooding attack cases.

A blackhole attack is made when a rogue node claims to have the shortest and most reliable path to his destination, which attracts neighbouring traffic, and he instead of sending the packets, he discards them or modifies them. It leads to a high packet loss, reduced throughput and retransmission. The black hole attackers were set to 10–20 percent of the nodes in the MATLAB simulation, meaning that they maliciously dropped packets received. The results of proposed performance when compared to the base protocols are depicted in Table 2.

Table 2
Performance Analysis of Blackhole Attack Scenario

Protocol	PDR (%)	Throughput (kbps)	Trust Detection Accuracy (%)
AODV	63.5	174	72.6
DSR	68.4	198	76.3
GPSR	72.1	219	80.4
SAODV	83.7	265	91.2
Proposed	**94.8**	**312**	**97.6**

The proposed framework retains a Packet Delivery Ratio of 94.8, even in the case of blackhole attacks by 11.1 percent as compared to SAODV and more than 31 percent as compared to AODV. This is mainly because of ATR mechanism, which keeps checking forwarding behavior, fines abnormal packet drop and isolates malicious nodes. The HSMOA-based route selection also provides the fact that the transmission of a packet is carried only by the nodes with the trusted and stable scores. Also, BiLSTM based mobility prediction lessens the reliance on susceptible dynamic associations hence restraining the propagation impact of the attack.

Flooding attack is a kind of attack that is carried out by malicious nodes, where the malicious nodes send massive numbers of bogus route requests or data packets in a bid to use up bandwidth as well as raise congestion and disrupt legitimate communications. This will increase delays, throughput and power consumption. In the given experiment, around 10 percent of node was coded to spew out the network with recurrent route demands. The outcome of the flooding attack is as shown in Table 3.

Table 3
Performance Analysis of Flooding Attack Scenario

Protocol	PDR (%)	End-to-End Delay (ms)	Energy Consumption (J)
AODV	69.8	148	3.21
DSR	72.4	136	2.94
GPSR	76.3	127	2.71
SAODV	85.6	101	2.38
Proposed	**93.1**	**78**	**1.97**

In flooding attack environment, proposed attains a 93.1% PDR that is 8.8 and 23 percent higher than SAODV and AODV. The adaptive scheduler incorporated into the Priority-Based Dual Emergency Handling (PDEH) mechanism is a queue-based packet prioritization mechanism which is effective to differentiate legitimate packets and redundant packets and helps to avoid the possibility of queue overflow and reduce the number of packets that are dropped. The trust reinforcement layer also reduces flooding by detecting those nodes that send out too many control packets and as a result lowering their transmission priority or isolating them. As a result, the proposed model achieves a lower average end-to-end delay, and energy consumption by 22.7% and 17.2% than SAODV, respectively, and all ensures its stability and the ability to compete with other models in high-load and adversarial conditions.

4.4. Analysis of Scalability

The scalability and adaptability of the proposed framework was tested through a simulation experiment by controlling the number of vehicles (50 to 200). This analysis is aimed at investigating the impacts of network density on the performance of the communication, routing stability, and the energy efficiency of the system. With the growth in the number of vehicles, the network topology dynamically changes, leading to changes in the connectivity, lifetime of links and interference. Table 4 displays the results that were obtained with the proposed model under varying densities of vehicles.

Table 4
Performance of Proposed Framework under Varying Number of Vehicles

Number of Vehicles	PDR %	End-to-End Delay (ms)	Throughput (kbps)	Energy Consumption (J)	Cluster Lifetime (s)
50	96.8	72	341	2.14	79.6
75	98.1	67	357	2.02	83.5
100	98.9	63	374	1.91	87.3
150	98.6	66	368	1.96	85.8
200	98.2	71	359	2.08	82.4

The PDR improves from 96.8% (50 vehicles) to 98.9% (100 vehicles) due to accurate BiLSTM-based mobility prediction and trust-based routing, then slightly decreases at higher densities because of channel contention. The End-to-End Delay decreases to 63 ms at 100 vehicles owing to optimal path selection via HSMOA, but rises marginally beyond 150 vehicles due to congestion. Throughput follows a similar trend, peaking at 374 kbps for 100 vehicles, confirming efficient bandwidth utilization. Energy Consumption drops to its minimum of 1.91 J at medium density, highlighting the benefit of adaptive clustering and energy-aware routing, and increases slightly under heavy loads. The Cluster Lifetime extends to 87.3 s at 100 vehicles, reflecting stable CH formation and prolonged network connectivity. Overall, the proposed framework achieves optimal performance at medium vehicular density while retaining strong scalability and resilience under both sparse and dense network conditions. This confirms the proposed model's suitability for large-scale, and Intelligent Transportation System (ITS) applications.

4.5. Performance Comparison of Proposed and Baseline Methods

The proposed MOTMER-VANET framework is compared with four benchmark routing protocols an Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Greedy Perimeter Stateless Routing (GPSR) and Secure AODV (SAODV) frameworks to compare the performance of the proposed system. All the protocols were compared in terms of reliability of packet delivery, delay, throughput and energy efficiency, lifetime of the cluster and accuracy of detection of trust as summarized in Table 5.

Table 5
Performance Analysis of Proposed and Baseline Methods

Performance Metric	AODV	DSR	GPSR	SAODV	Proposed
Packet Delivery Ratio (PDR) (%)	87.9	89.3	91.2	93.5	**98.9**
End-to-End Delay (ms)	108	97	88	79	**63**
Throughput (kbps)	276	295	318	334	**374**
Energy Consumption (J)	2.86	2.71	2.43	2.28	**1.91**
Cluster Lifetime (s)	51.7	58.3	66.4	72.9	**87.3**

The PDR is the proportion of received packets that are received successfully at the destination and the packets that are sent by the source. An increased PDR is a sign of increased dependability and stability of the routing protocol. The proposed MOTMER-VANET has the highest PDR of 98.9 which is better than SAODV (93.5%), GPSR (91.2%), DSR (89.3%), and AODV (87.9%). This significant improvement can be explained by the fact that it involves the BiLSTM-based mobility prediction and adaptive trust reinforcement that are effective in predicting movements of the nodes and removing untrustworthy nodes. The HSMOA based routing optimization also helps in the effective path discovery as it chooses the nodes that have better stability, left over energy and trust scores. These modules combine to reduce the breakages of routes, retransmissions and loss of packets. The MOTMER-VANET design therefore guarantees an average data delivery even in high mobility conditions with up to 12.6 percent better results compared to AODV and 5.4 percent compared to SAODV, thus proving that it is effective in dynamically evolving situations. The delay is the mean value of data packet time spent on the route between the source and destination. Reduced delay means improved and quick communication particularly critical in delay-sensitive vehicular

usage. The average delay of the proposed MOTMER-VANET (63 ms) is much lower than AODV (108 ms), DSR (97 ms), GPSR (88 ms), and SAODV (79 ms). Improvement of about 41.6 percent over AODV is attributed to the queue based adaptive scheduler and priority-based dual emergency handling module, which gives priority to important messages to the safety of the network and dynamically adjusts network congestion. Further, the hybrid TDMA-CSMA transmission model provides efficient use of the channel with minimum retransmission overheads and collisions. The BiLSTM mobility predictor ensures the connections between clusters are kept constant, which further decreases the amount of time route rediscovery takes. On the whole, this delay minimization through MOTMER-VANET justifies its applicability in real-time traffic safety applications with regard to latency. Throughput is a metric that measures the rate at which data is transferred successfully (in kbps) over the network. An increased throughput means that there is better utilization of available bandwidth and the congestion is managed. The proposed MOTMER-VANET has throughput of 374 kbps which is higher than the SAODV (334 kbps), GPSR (318 kbps), DSR (295 kbps) and AODV (276 kbps). This is largely attributed to the multi-objective optimization of routing through HSMA where the trust, stability, and energy parameters are balanced in order to preserve the optimum paths. Also, adaptive scheduling mechanism minimizes the transmission delays and the packet drop due to congestion in the network guaranteeing high data delivery rates. The collaborative functionality of the BiLSTM mobility predictor and the trust assessment module avoids route failure and malicious node interference and maintains constant throughput during dynamic vehicular conditions. Consequently, MOTMER-VANET has a 12 and 26 per cent greater throughput than SAODV and AODV, respectively, which attests to its capacity to work in high-density traffic settings.

Energy usage is an important aspect in VANETs because energy-saving communication guarantees the long-term network operation and stable functioning of on-board units. The average power used by the suggested MOTMER-VANET during a communication round is 1.91 J, and this value is significantly less than that of SAODV (2.28 J), GPSR (2.43 J), DSR (2.71 J) and AODV (2.86 J). The weighted CH selection mechanism ensures this 15–33 percent of energy saving through servicing nodes with greater residual energy and stability to manage the cluster. The HSMOA routing optimizer also chooses energy efficient routes so that no single node has to be overloaded and redundant transmissions are minimized. The MOTMER-VANET architecture ensures sustainable energy use during the entire network life cycle by avoiding energy wastage on the particular nodes and ensuring that energy is evenly distributed among clusters. The findings of this paper support the idea that the given framework can be used to not only improve the security and performance but also make a significant contribution to green and energy-aware vehicular communication. Cluster lifetime is the time period of cluster stability before a reconfiguration is to be done because of mobility or energy losses among nodes. The longer cluster lifetime implies a better stability and low control overhead. The proposed MOTMER-VANET has a cluster lifetime of 87.3 s, which is better than other methods. The improvement of the latter is explained by the fact that BiLSTM mobility prediction is incorporated with trust and energy-based CH selection which guarantees that extremely stable and reliable nodes become cluster leaders. The adaptive trust reinforcement mechanism ensures that unstable or malicious nodes are not converted to CHs and therefore the frequency of cluster reformation is minimized. As a result, MOTMER-VANET shows 19.7% increased cluster longevity than SAODV, which confirms its design as a stable and low-maintenance clustering framework that can be used in large-scale vehicular deployments.

5. Conclusion

The study proposed MOTMER-VANET framework that resolves mobility management, trust-based routing and multi objective optimization of vehicular networks that are critical. Through the inclusion of BiLSTM-based mobility prediction, the framework is able to successfully predict vehicle paths and thus stabilizes the formation of links and minimizes route breakages. Adaptive Trust Reinforcement strategy will provide the dynamic update of trust based on the reinforcement-based learning, which will prevent the blackhole attacks and flooding attacks. The mechanism of Weighted Cluster Head Selection balances the residual energy, the trustworthiness and stability of the mobility, resulting to the cluster longevity and effective use of energy. Global exploration and local exploitation of Multi-objective Routing HSMOA is an effective method to improve routing performance via the integration of global exploration and local exploitation. This strategy assures the choice of the best routes that have the shortest delay time, highest reliability, and energy economy. Also, the priority based dual emergency handling system ranks the messages that are important during congestion to facilitate the real time communication of vehicular safety messages. The simulation experiments confirmed the efficiency of proposed approach compared to the conventional routing protocols including. The framework realized tremendous gains in PDR98.9%), End-to-End Delay (63 ms), and Cluster Lifetime (87.3 s), and minimized energy consumption and maximized throughput. Moreover, the system was very resilient to blackhole and flooding attacks and was scaled with different vehicle densities. The proposed framework offers a powerful, intelligent, and secure routing framework of the contemporary vehicular networks. Future expansion will be done in terms of incorporating 6G-enabling vehicular edge intelligence, cross-layer optimization, and real-world trace-based simulations to enhance its real-time flexibility and implementation in large-scale intelligent transportation systems.

Declarations

FUNDING

On Behalf of all authors the corresponding author states that they did not receive any funds

for this project.

CONFLICTS OF INTEREST

The authors declare that we have no conflict of interest.

COMPETING INTERESTS

The authors declare that we have no competing interest.

DATA AVAILABILITY STATEMENT

The data supporting the findings of this study were generated through MATLAB-based simulations of the proposed MOTMER-VANET framework. The simulation data, including mobility information, network performance results, and experimental configurations used to evaluate the proposed framework under black hole and flooding attack scenarios, are available from the corresponding author upon reasonable request.

ETHICS APPROVAL

No ethics approval is required.

CONSENT TO PARTICIPATEEnergy-Efficient Traffic-Aware

Not Applicable

CONSENT FOR PUBLICATION

Not Applicable

Author Contribution

Mrs Parimala Garnepudi, the corresponding author, contributed to the conceptualization of the study, methodology design, implementation, data analysis and presentation of the original manuscript draft.

Dr M Vanitha, contributed to supervision validation of the research methodology and critical review and editing of the manuscript.

All authors have read and approved the final version of the manuscript.

Data Availability

The data supporting the findings of this study were generated through MATLAB-based simulations of the proposed MOTMER-VANET framework. The simulation data, including mobility information, network performance results, and experimental configurations used to evaluate the proposed framework under black hole and flooding attack scenarios, are available from the corresponding author upon reasonable request.

References

1. Hussein, N. H., Yaw, C. T., Koh, S. P., Tiong, S. K. & Chong, K. H. A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions. *Ieee Access.* **10**, 86127–86180 (2022).
2. Albattah, W. et al. An overview of the current challenges, trends, and protocols in the field of vehicular communication. *Electronics*, *11*(21), p.3581. (2022).
3. Cunha, B. et al. Smart traffic control in vehicle ad-hoc networks: a systematic literature review. *Int. J. Wireless Inf. Networks*. **28** (3), 362–384 (2021).

4. Kaul, A. & Altaf, I. Vanet-TSMA: A traffic safety management approach for smart road transportation in vehicular ad hoc networks. *Int. J. Commun Syst*. **35** (9), e5132 (2022).
5. Bintoro, K. B. Y. A study of V2V communication on VANET: characteristic, challenges and research trends. *JISA (Jurnal Informatika dan. Sains)*. **4** (1), 46–58 (2021).
6. Cunha, B. et al. Smart traffic control in vehicle ad-hoc networks: a systematic literature review. *Int. J. Wireless Inf. Networks*. **28** (3), 362–384 (2021).
7. Chatterjee, T., Karmakar, R., Kaddoum, G., Chattopadhyay, S. & Chakraborty, S. A survey of VANET/V2X routing from the perspective of non-learning-and learning-based approaches. *IEEE Access.* **10**, 23022–23050 (2022).
8. Sehrawat, P. & Chawla, M. Interpretation and investigations of topology based routing protocols applied in dynamic system of VANET. *Wireless Pers. Commun.* **128** (3), 2259–2285 (2023).
9. Azzoug, Y. & Boukra, A. Bio-inspired VANET routing optimization: an overview: a taxonomy of notable VANET routing problems, overview, advancement state, and future perspective under the bio-inspired optimization approaches. *Artif. Intell. Rev.* **54** (2), 1005–1062 (2021).
10. Marwah, G. P. K. & Jain, A. A hybrid optimization with ensemble learning to ensure VANET network stability based on performance analysis. *Scientific Reports*, *12*(1), p.10287. (2022).
11. AlMarshoud, M., Sabir Kiraz, M., Al-Bayatti, H. & A Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions. *ACM Comput. Surveys*. **56** (10), 1–39 (2024).
12. Alharthi, A., Ni, Q., Jiang, R. & Khan, M. A. A computational model for reputation and ensemble-based learning model for prediction of trustworthiness in vehicular ad hoc network. *IEEE Internet Things J.* **10** (20), 18248–18258 (2023).
13. Mathivanan, S. K., Rajadurai, H., Cho, J. & Easwaramoorthy, S. V. A multi-modal geospatial–temporal LSTM based deep learning framework for predictive modeling of urban mobility patterns. *Scientific Reports*, *14*(1), p.31579. (2024).
14. Modi, Y., Teli, R., Mehta, A., Shah, K. & Shah, M. A comprehensive review on intelligent traffic management using machine learning algorithms. *Innovative infrastructure solutions*, *7*(1), p.128. (2022).
15. Alharthi, A., Ni, Q., Jiang, R. & Khan, M. A. A computational model for reputation and ensemble-based learning model for prediction of trustworthiness in vehicular ad hoc network. *IEEE Internet Things J.* **10** (20), 18248–18258 (2023).
16. Mujahid, M. A., Bakar, K. A., Darwish, T. S. & Zuhra, F. T. Cluster-based location service schemes in VANETs: current state, challenges and future directions. *Telecommunication Syst.* **76** (3), 471–489 (2021).
17. Naeem, A. et al. Enhanced clustering based routing protocol in vehicular ad-hoc networks. *IET Electr. Syst. Transport.* **13** (1), e12069 (2023).
18. Saleem, M. A. et al. Deep learning-based dynamic stable cluster head selection in VANET. *Journal of Advanced Transportation*, *2021*(1), p.9936299. (2021).
19. Alghamdi, S. A. Stable zone-based 5G clustered MANET using interest-region-based routing and gateway selection. *Peer-to-Peer Netw. Appl.* **14** (6), 3559–3577 (2021).
20. Kaushal, P., Khurana, M. & Ramkumar, K. R. A systematic review of swarm intelligence algorithms to perform routing for VANETs communication. *ECS Transactions*, *107*(1), p.5027. (2022).
21. Azzoug, Y. & Boukra, A. Bio-inspired VANET routing optimization: an overview: a taxonomy of notable VANET routing problems, overview, advancement state, and future perspective under the bio-inspired optimization approaches. *Artif. Intell. Rev.* **54** (2), 1005–1062 (2021).
22. Ali, W., Ninoria, S. Z., Khan, G. & Gola, K. K. Robust cryptographic scheme for reliable data communication in VANET (RCSRC) using clustering approach. *EURASIP Journal on Wireless Communications and Networking*, *2024*(1), p.82. (2024).
23. ul Hassan, M. et al. Y.A., Ann-based intelligent secure routing protocol in vehicular ad hoc networks (vanets) using enhanced aodv. *Sensors*, **24**(3). (2024).
24. Reddy, M. V. K., Kumar, G. K., Terlapu, P. V., Jayaram, D. & Samreen, S. Trust Enabled Secure Routing in Vehicular Adhoc Networks. *Int. ARAB. J. Inform. Technol.* **22** (3), 592–613 (2025).
25. Giridhar, K., Anbuananth, C. & Krishnaraj, N. Energy efficient clustering with Heuristic optimization based Ro/uting protocol for VANETs. *Measurement: Sensors*, *27*, p.100745. (2023).
26. Dhakad, B. et al. Dynamic clustering based risk aware congestion control technique for vehicular network. *Scientific Reports*, *14*(1), p.24774. (2024).

27. Gopalan, S. H., Ashok, J., Manikandan, A. & Ramalingam, S. Data dissemination protocol for VANETs to optimize the routing path using hybrid particle swarm optimization with sequential variable neighbourhood search. *Telecommunication Syst.* **84** (2), 153–165 (2023).
28. Rashid, S. A., Mustafa, A. S., Abbas, A. D., Abdullah, H. Q. & Mohammed, M. J. On the design of trust and mobility based evaluation for intelligent collaborative UAVs assisted VANETs. *Bull. Electr. Eng. Inf.* **12** (5), 2993–2999 (2023).
29. Xu, H. & Wang, Y. SROR: A Secure and Reliable Opportunistic Routing for VANETs. *Vehicles* **6** (4), 1730–1751 (2024).
30. Ali, W., Ninoria, S. Z., Khan, G. & Gola, K. K. Efficient Route Reliability Algorithm for Vehicular Ad Hoc Networks. *Int. J. Comput. Inform. Syst. Industrial Manage. Appl.* **17**, 19–19 (2025).
31. Ahmad, W., Husnain, G., Ahmed, S., Aadil, F. & Lim, S. Received Signal Strength-Based Localization for Vehicle Distance Estimation in Vehicular Ad Hoc Networks (VANETs). *Journal of Sensors*, *2023*(1), p.7826992. (2023).
32. Parimala Garnepudi, M. V. EMAO-MTRUST: A Robust Trust-Based Routing Protocol with Emergency Handling for Secure and Efficient VANETs in Technical Gazette. (2026).

Figures

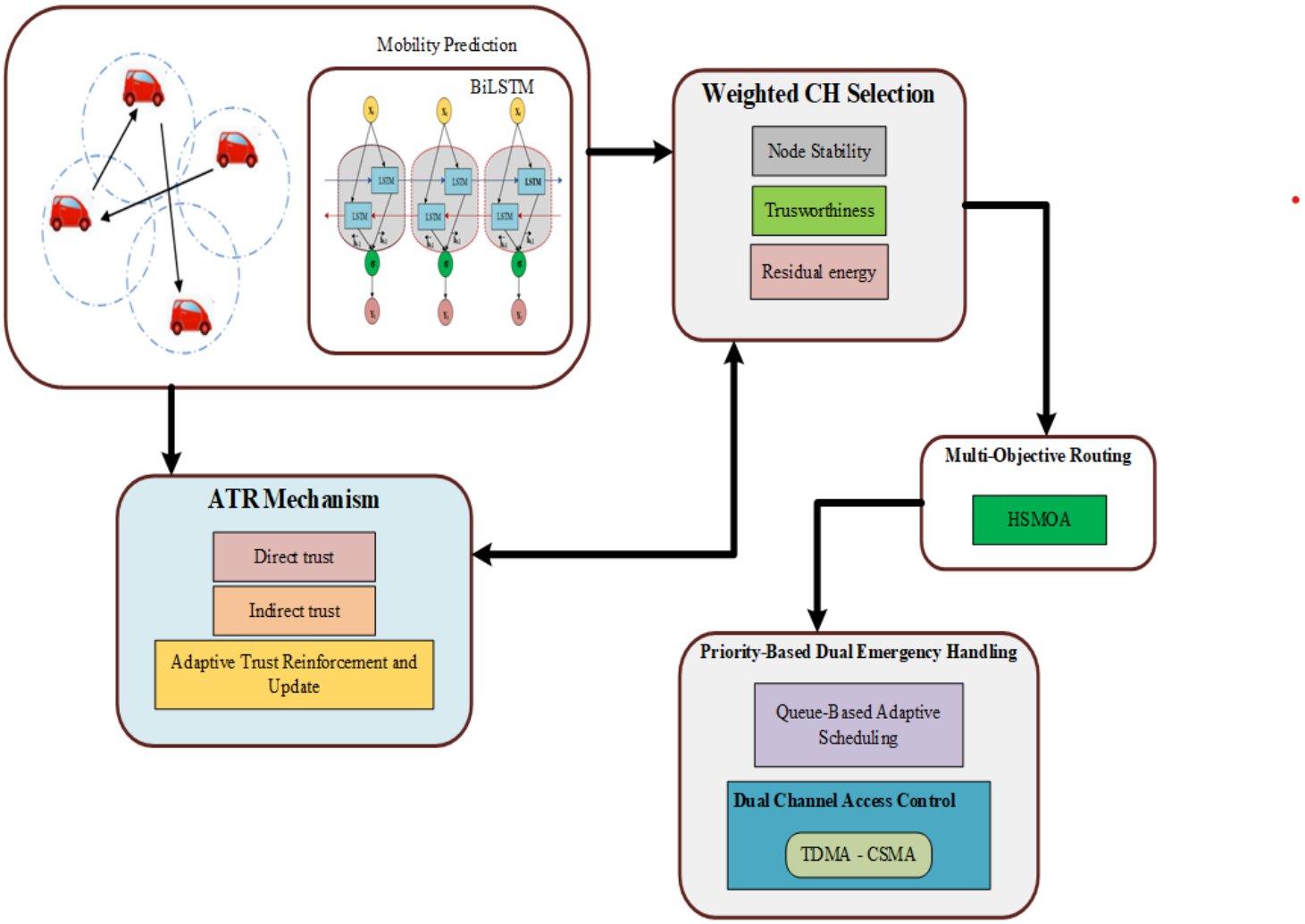


Figure 1

Overview of Proposed Framework

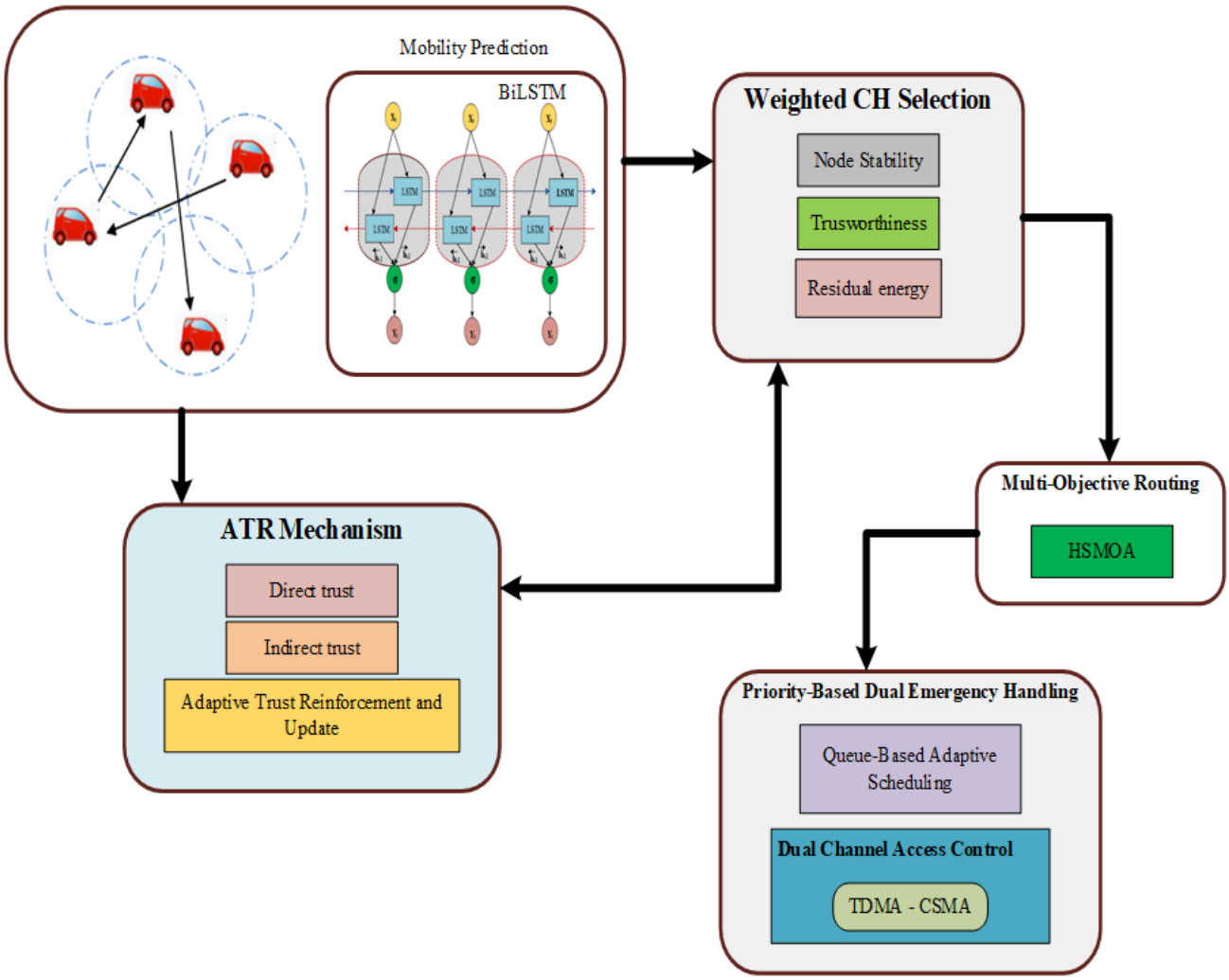


Figure 1

Overview of Proposed Framework

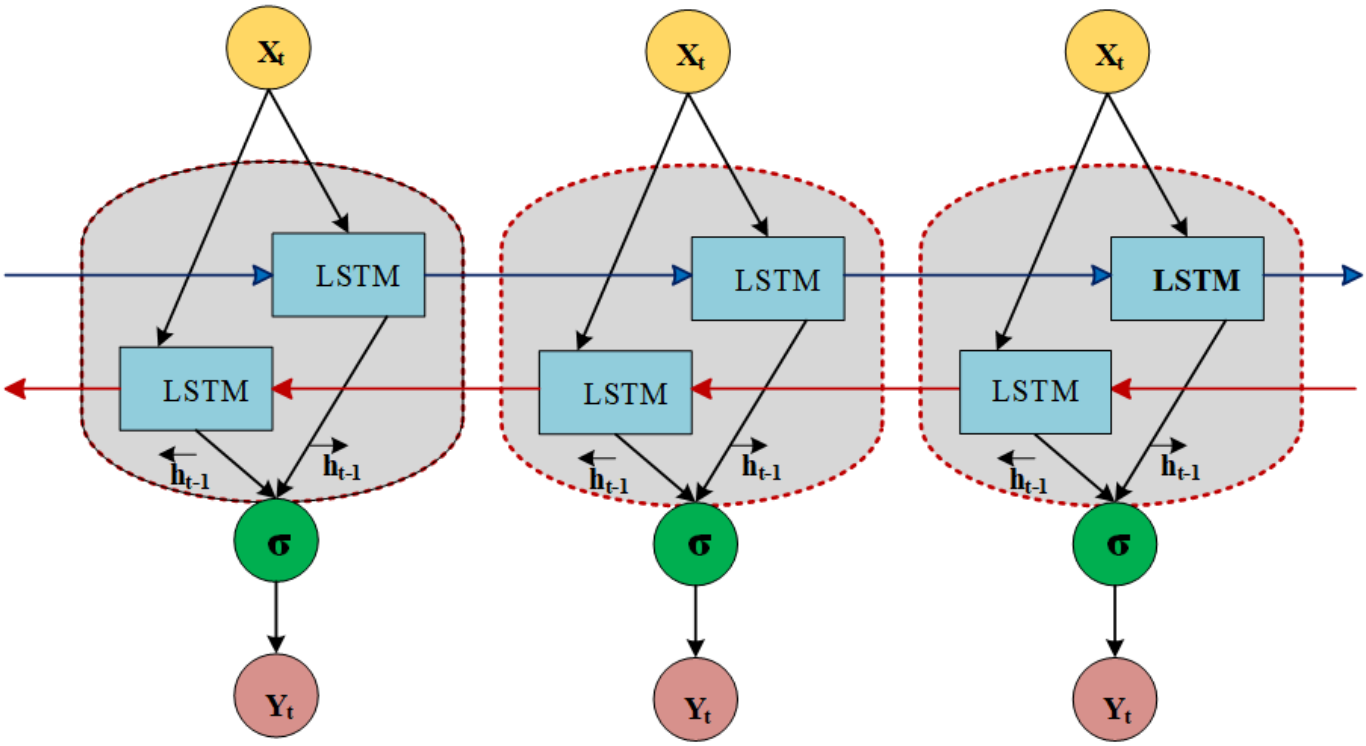


Figure 2

Architecture of BiLSTM

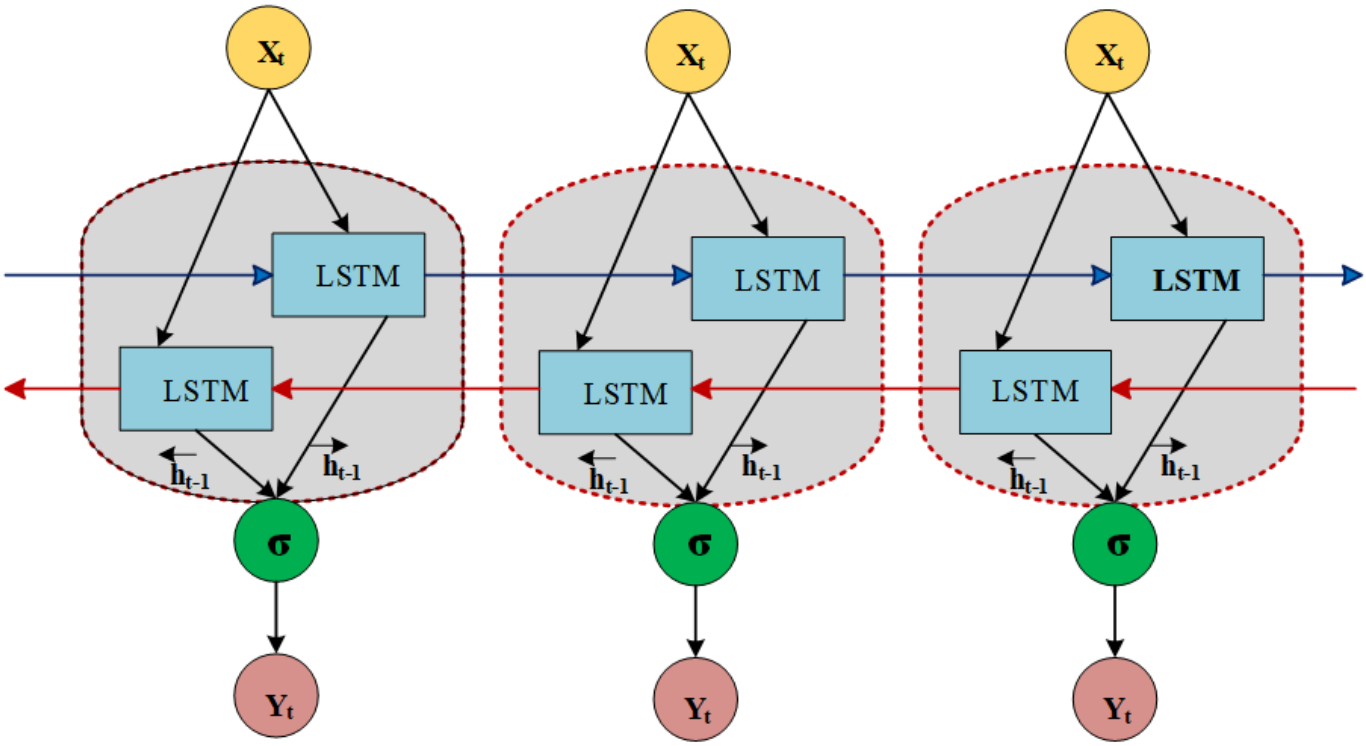


Figure 2

Architecture of BiLSTM

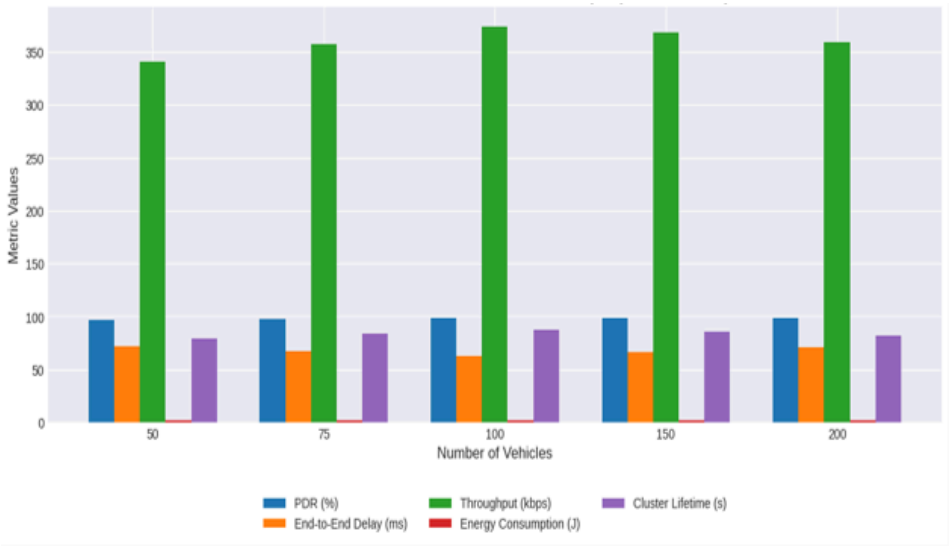


Figure 3

Analysis of Proposed Framework under Varying Number of Vehicles

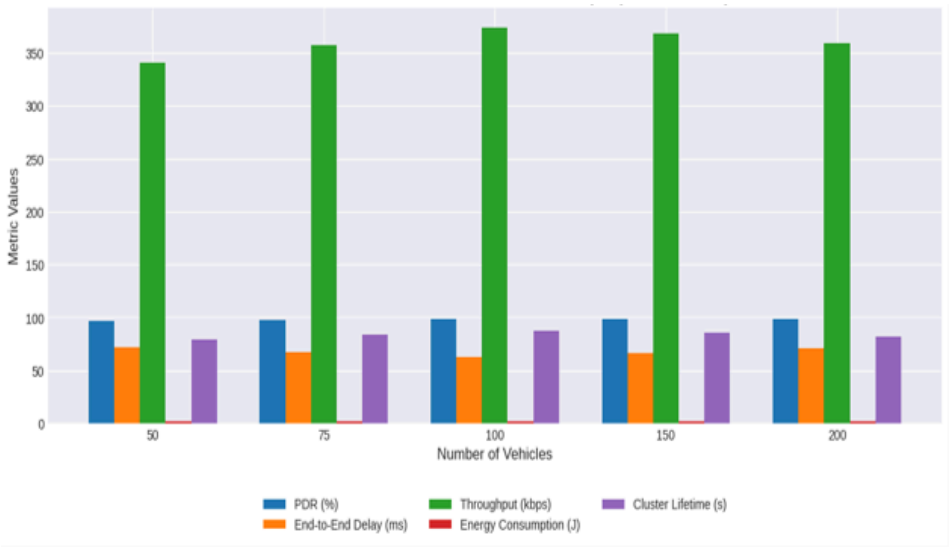


Figure 3

Analysis of Proposed Framework under Varying Number of Vehicles

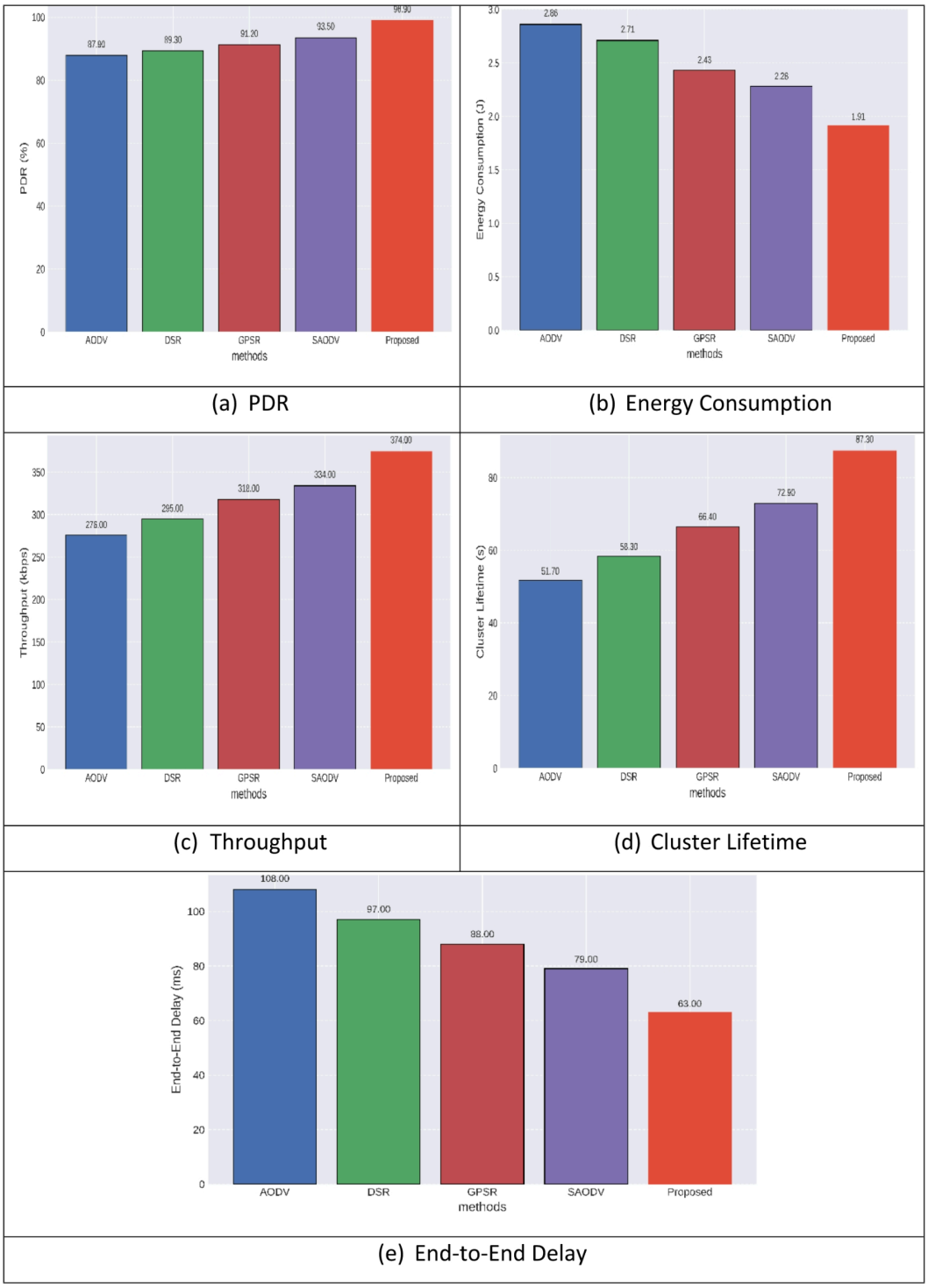


Figure 4

Analysis of Proposed and Existing Methods

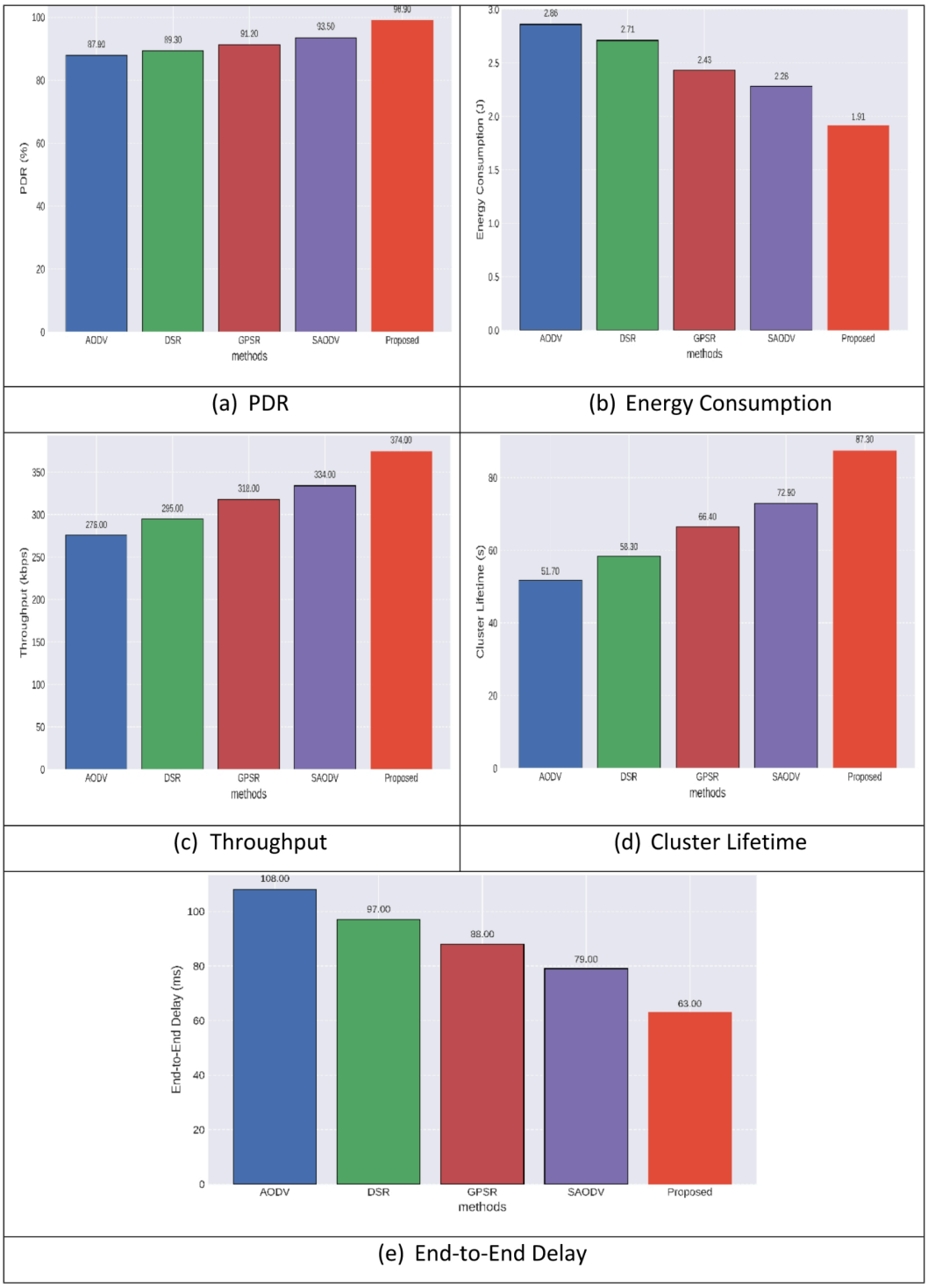


Figure 4

Analysis of Proposed and Existing Methods