International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/60 Volume 12, Issue 6, November – December (2025)

RESEARCH ARTICLE

V-MARS: Velocity-Aware Multi-Attribute Reinforced Secure Routing for Efficient Data Transmission in Vehicular Networks

V. Sakthi Priyanka
Department of Computer Science, Avinashilingam Institute for Home Science & Higher Education for Women, Coimbatore, Tamil Nadu, India.
vsakthipriyanka@gmail.com

V. Radha
Department of Computer Science, Avinashilingam Institute for Home Science & Higher Education for Women, Coimbatore, Tamil Nadu, India.
radha_cs@avinuty.ac.in

Received: 15 August 2025 / Revised: 14 November 2025 / Accepted: 01 December 2025 / Published: 30 December 2025

Abstract – The needs of Vehicular Ad hoc Networks (VANETs) include high data rate, reliability and security; the routing in the given dynamic scenario is one of the primary concerns. The current routing plans cannot handle the speed of the vehicles, the high frequency of link breakages, fluctuating route and the occurrence of numerous features in the decision making that increases the delay, loss of packets and loss of security. Besides that, the vast majority of the existing models do not possess the context-sensitive trust, cannot be adjusted to the current state of the network, and cannot learn with the help of reinforcement to make sure that the route will always be the best possible. To fill in these gaps, this paper shall propose V-MARS (Velocity-aware Multi-Attribute Reinforced Secure Routing), a new routing policy involving a combination of velocity-awareness, multi-attribute path selection, and reinforced trust-based decision making. V-MARS relies on the path disregarding the velocity of the vehicle, remaining energy, and stability of the links, the quality-of-service measures and the reliability as the assumption and is founded on the reconsidered strategy of learning to keep on updating the path choice under diverse conditions of the mobility. The simulations have shown enormous evidence of the truth that V-MARS is better than planned protocols in terms of the end-to-end delay ratio of the packet delivery throughput and restraint against security especially in the case scenario where high mobility is the order of the day. These findings support the fact that V-MARS is a more adaptable, predictable and robust routing solution to the next generation intelligent vehicular networks.

Index Terms – Mobility Prediction, Multi-Attribute Optimization, Secure Routing, Reinforcement Learning, Trust Management, Vehicular Ad Hoc Networks.

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANET) is one of the core technologies that are behind intelligent transportation systems that are used to facilitate the implementation of applications like traffic management, safety notifications and infotainment. Nevertheless, because vehicles are highly mobile, their network topology forms a highly dynamic network topology and extreme challenges of reliable and secure routing. This causes packet losses, high latencies and insecurity due to the frequency of link breakages, route instability, and malicious nodes.

In addition to addressing substantial challenges created by dynamic environments, routing protocols must consider the limited computational processing and energy resources available to vehicles and thus provide routing algorithms that are lightweight, adaptive, and fast in dynamic environments.

A number of routing mechanisms have been investigated as potential solutions to these issues. Various artificial intelligence methods such as Ant Colony Optimization have been reviewed for path selection purposes in static and mobile sensor networks, which show good routing performance but have too much overhead requirement and limited adaptability to rapidly changing VANET environments [1]. Mobility-aware cluster-based routing with hybrid optimization algorithm provides gains in network stability, but lacks scalability and has great overhead when maintaining clusters [2]. Zone-assisted multipath routing protocols improve energy efficiency in mobile ad hoc networks but require fixed zones that limit flexibility in dynamic network conditions [3]. QoS-aware data congestion control routing could yield improvements in throughput and latency; however, there are poor security and observational measures in place [4]. Intelligent federated learning-based vehicle route optimization models improve sustainability initiative, but require extensive

RESEARCH ARTICLE

computational resources unsuitable for real-time VANET implementations [5].

Recent works concentrate on energy-efficient clustering and the current and mobility-aware forwarding models to improve the reliability and efficiency of routing [6], [7]. A reinforcement learning algorithm was utilized for risk aware relay selection, allowing it to make better decision towards routing [8]. Geographic multicast routings and location-aided protocols using directional antennas with sleep scheduling allow for improved message spreading and energy savings, but like the other protocol research, the unreliability of links and the dynamic topologies cause issues [9], [10]. However, few of the existing methods cover full mobility prediction, trust assessment, multi-criteria optimization and security aspects. These limitations will hinder routing in highly dynamic and adversarial environments prevalent to VANET, as the literature suggests.

To address these gaps, this paper proposes Velocity-aware Multi-Attribute Reinforced Secure Routing (V-MARS), an adaptive routing protocol adapted for high-mobility VANETs. V-MARS uses a Kalman filter to predict vehicle velocity and estimate link lifetimes, facilitating proactive and stable route selection. It proposes a Multi-Attribute Route Vector (MARV) that balances such critical considerations as link stability, reliability, trustworthiness, hop count, as well as energy consumption.

Reinforcement learning is a dynamic optimization of routing decisions, which also makes it fast to failover and reduces control overhead. A Threshold Group Key Agreement scheme to generate collaboratively session keys is used to enhance security and a lightweight hash-chained ledger to build data integrity and auditability. Such a combination solution is effective to address common link failures, malicious attacks and resource constraints, to offer reliable, efficient and secure data transmission to dynamic vehicular networks.

1.1. Problem Statement

Even though VANET routing protocols have made great progress, there are still some key limitations to the current protocols:

- There is high mobility of vehicles hence the topology changes very rapidly which creates frequent link failures, unstable routes and poor performance of packet delivery.
- The existing routing techniques do not have inbuilt mobility forecasting, stability forecasting and multi-criteria decision making that is required in highly dynamic environments.
- There are still unresolved security vulnerabilities because malicious nodes have the ability to do black hole, gray hole, false information dissemination and integrity attacks.
- The currently available solutions are characterized by high computational or communication cost, which is not suitable in real-time VANET nature which need lightweight, responsive, and speedy routing protocols.

1.2. Research Objectives

The suggested study is supposed to satisfy the following:

- To include mobility-sensitive routing protocol this makes predictions about the speed of the vehicle and lifetime of links to choose the route ahead of time.
- To design a multi- attribute routing scheme that uses stability, trustworthiness, reliability, hoop count and energy.
- To apply reinforcement learning in order to maximize dynamic route and high mobility fail over fast.
- To introduce a secured key agreement and data integrity framework to avert the use of malicious attacks on routing.

1.3. Research Contributions

V-MARS deliverables include the following key ones:

- Kalman filter of velocity prediction model to predict the lifetime of links and improve the stability of the routes among the dynamic vehicle's mobility.
- Multi-Attribute Route Vector (MARV) is a new method of route selection which is a mixture of stability of links, trust, reliability, hop count and energy consumption.
- A routing decision engine based on reinforcement learning and adapting to the existing network conditions and consuming less control overhead.
- An integrated security control system that has Threshold Group Key Agreement and lightweight hash-chained ledger to provide confidentiality, integrity and audit.

This paper is organized in the following way: section 2 describes the related works. Section 3 outlines the proposed V-MARS. In section 4, the discussion and findings are elaborated. Its conclusion is explained in section 5. Finally, the references are provided in the section.

2. RELATED WORKS

Vehicular Ad Hoc Networks (VANETs) have received much consideration due to the significance in the intelligent transportation systems. This is not an easy task however because of their dynamic topology, high mobility and its susceptibility to attacks.

In various perspectives, different studies have sought to improve the stability, reliability as well as security of routes.

RESEARCH ARTICLE

A secure routing plan of the data delivery in MANETs is proposed by Sankaran and Hong (2024) [11], which is based on the trust of information by the availability of the most appropriate selection of Cluster Head (CH). The method uses a model of trust evaluation as well as an optimization and mechanism of CH selection to enhance the level of stability and reduce maliciousness during the routing process. They study is founded on the improvement of the packet delivery by filtering the nodes which cannot be trusted and strengthening the secure forward paths. It also has a drawback, large computational cost, inability to work in high mobility environments, and does not support multifactor routing measures, such as mobility prediction, link lifetime estimation, or reinforcement learning.

The research by Cao et al. (2024) [12], suggests SMART as an economic service migration path selection model, which is deployed in the intelligent transportation systems, where deep reinforcement learning (DRL) is used. The model optimizes the optimal migration path based on service cost, latency and network state transitions since it takes into account efficient service continuity. They report superior decision making to the dynamic condition of the vehicle since they forecast the optimum migration patterns. However, it has a mathematically complex approach; it involves large training sets and cannot be applied to lightweight and real-time VANET routing since it is not specifically concerned with the stability of links, trusting, and safety of data transmission.

Brito et al. (2023) [13] present a personalized route choice model merging the user experience, mobility conditions, and environmental factors to smart mobility applications. Their system is based on multi-criteria decision-making model which takes into account the travel time, comfort, user preferences and traffic conditions as one of the ways to provide the best routes. The paper has shown the necessity of user-oriented routing to enhance the effectiveness of mobility. However, the model fails with dynamic VANET routing but smart city navigation; it does not forecast link quality in the real-time, does not offer security system, and trust management, and it is not applicable in adversarial vehicular environment.

The article by Sri Lakshmi et al. (2022) [14] suggests a secure optimization-driven routing algorithm in MANETs, which includes a trust computation algorithm with an optimization mechanism to select the energy-efficient and trustful routes. The strategy works out the behavior of the nodes along with the energy left and the quality of the links to improve the transmission of the data in a safe manner. Their work contributes value in the provision of packets and reduction of attacks by isolated low trust nodes. However, the technique is not mobile aware and has lower functionality in high-speed networks like VANET and the processing overhead is also high and is therefore not suitable when working with dynamic vehicle scenarios that experience a dynamically changing topology.

According to Velmurugadass et al. (2023) [15], a QoS-sensitive model of secure data transmission on IoT-enabled wireless sensor network is proposed which integrates security services with quality-of-service service. The model also takes into account the parameters of latency, reliability and energy efficiency in addition to ensuring security in the packet forwarding. Through this approach, the security of the data and network in the resource-limited IoT is enhanced. The methodology can only be applied to non-moving or low-moving WSN, no mobility prediction, and not to fast moving vehicles, hence not a perfect fit in the routing method of VANET.

The multipath routing protocol of the Internet of Mobile Things (IoMT), QFS-RPL, introduced by Alilou et al. (2024) [16], is directed to mobility-awareness and energy efficiency, as well as load balancing. Queues scheduling, fuzzy logic and mobility measures are used in the protocol to design stable and energy efficient paths. They improve the transmission of packets and reduce the breakdowns of routing in mobile IoMT networks in their study. However, the protocol is still characterized in terms of high control overhead, lack of real time link lifetime prediction and failure in terms of supporting security and trust assessment which constrains its usage in highly dynamic adversarial VANET environments.

An intertwine connection-based routing path selection model developed by Vijay et al. (2022) [17] enhances data transmission over mobile cellular and wireless sensor networks. The plan is grounded on the guarantee of consistent connection by evaluating quality of links as well as number of nodes which can be connected and the network status to select optimal routes of connection. Their study improves the packet transmission and reduces the route discontinuities under moderate mobility. However, it does not apply to high-mobility dynamics like VANETs, and lacks trust and security analysis, and is limited to responding to high-rate changes in topologies.

Musa et al. (2022) [18] propose a mobility-aware proactive edge caching scheme to the information-centric Internet of Vehicles (IoV) networks. The model predicts vehicle mobility to memory content in optimal edge nodes conjecturing latency and network congestion. Their research demonstrates the significant modifications in the QoS and the availability of the data. The scheme does not however offer much content caching as compared to secure multi-criteria routing and does not offer any trust management, link stability prediction and routing decision optimization mechanisms that are required in a dynamic VANET environment.

The proposed mobility-based cyber-physical system by Razaque et al. (2022) [19] will provide secure and efficient smart healthcare applications. They integrate mobility prediction, network optimization, and lightweight security in order to improve reliability of the data and monitoring patients in the human-centric IoT. The system enhances the performance since the system is dynamically adjusted to control the communication paths based on the mobility patterns. However, the work is optimized to healthcare IoT, which is contrary to high-speed VANET, lacks real-time routing optimization, predicting a link lifetime, and multi-attribute decision-making, which is essential in vehicular routing.

Sarker et al. (2023) [20] propose a solution to VANETs by providing a reinforcement learning-based neighbour selection approach that optimises the utilisation of adaptive trust management to eliminate malicious behaviours. The best neighbour nodes are identified through the system which is based on the trust measures, packet behaviour and environmental dynamic to increase reliability and security of routing. Their works increase the trust-based communication during dynamic automotive scenarios. It does not however choose the neighbours, but only the neighbours; does not predict mobility; and combines multi-criteria optimization (such as link stability, energy or hop count) does not combine this restricting the overall performance of routing.

Hussain et al. (2025) [21] provide a route optimization model based on reinforcement learning, which can be used to make more energy efficient Internet of Vehicles (IoV). The framework trains ideal route plans depending on the energy consumption patterns, the quality of communication and car movements. Their design is suitable so as to reduce the consumption of energy and their routing performance is not bad. However, the model is heavily energy-focused, lacks security and trust evaluation, lacks integration of the multi-attribute decision-making, and therefore has poor performance as a high-mobility VANET situation in which link prediction and quick failover are critical.

Sree and Sharma (2024) [22] examined the autonomous vehicle networks this is proposed to be supported by a machine learning-assisted secure routing protocol with UAV support. The protocol makes routes more reliable since it uses UAVs as air relay nodes and applies ML models to identify bad actions and optimize the forwarding decisions. They have an improved network coverage and security coverage in low vehicle density regions as they are used. However, it is subject to the existence of the UAVs, and is not predictive of the mobility, optimizable routes which consider several factors and cannot be applied in dense urban VANETs where it is essential to make routing decisions within a few seconds and grounded vehicles can do so.

Graph Neural Networks (GNNs) and Deep Reinforcement Learning (DRL) are presented in the article by Bi et al. (2025) [23] to demonstrate a dynamic routing algorithm to VANETs because this algorithm simulates complex vehicular topology. The spatial correlation between the nodes is learned using the GNN and the optimal routing decisions are learned using the DRL against the network conditions. Their approach is far more superior because it makes the routes more flexible and closer in a highly dynamic environment. It is however quite computationally intensive, training requirements are huge, explicitly measures trust, remote and is not lightweight in design, which is why it is not as well adapted to real-time VANET implementation.

Almuseelem (2025) [24] proposes a framework to offload computations and maximize energy consumption to ensure security in vehicular edge-cloud computing systems based on deep reinforcement learning. The strategy focuses on the selection of optimal methods of offloading the work, and the workload of the devices, as well as the latency and the security concerns are balanced. The architecture is useful in reducing the computation costs to vehicles. The model, however, does not make routing decisions and thus places much emphasis on offloading decisions but not routing, lacks mobility predictions and multi attributes secure routing, which restricts its application to the fundamental VANET routing problems.

Suh et al. (2025) [25] proposed a resilient routing protocol within MANETs through unsupervised learning to cluster network states as well as deep reinforcement learning (DRL) that reduce the cost of routing update. The protocol is a dynamic scheme which uses the topology adjustment based on the learned pattern, which increases the resilience of changing topologies. They are better due to their routing stability and reduced control overhead. However, the model does not offer mobility prediction, multi-featured decision-company, and secure/trust structures; therefore, it cannot be applied in VANET environments of high dynamics and disputes.

Ma et al. (2025) [26] developed a dynamic routing model (based on a reinforcement learning algorithm) aiming to maximize the network traffic flow and minimized network congestion. According to the existing traffic reality, the RL agent continues to learn forwarding policies, which increases the stability and efficiency of routes to an important extent. The study is more flexible in all sorts of network conditions. However, the strategy does not possess vehicle mobility behavior, evaluation of trust, and security and assumes quite stable training conditions, limiting the use to high-speed VANET routing.

Jiang et al. (2024) [27] offer one of the areas of research that are relatively close this VANET topic because they introduce an environment-aware reinforcement learning routing scheme. According to ACO, Lee et al. (2024) [28] present a traffic-sensitive routing algorithm, that can be applied in multi-junction city networks, and provides a fine starting point in

RESEARCH ARTICLE

terms of comparing the congestion and dynamism management initiatives of metaheuristic schemes. According to Anupama and Nagaraj (2025) [29], quantum-resilient and trust-based secure routing protocol, the key administration can be verified, meaning the protocol will be used in comparison with the security and trust features of this model. Finally, the paper by Kumar et al. (2025) [30] offers a road-aware version of the reinforcement learning, that is also unique to dense urban VANETs and directly overlaps with the research conducting, which is concerned with mobility adaptation, learning routing, and reliability improvement. Overall, these publications assist in accepting the required dimensions mobility awareness, traffic adaptation, security and intelligent learning, on which the performance of the provided method can be reasonably compared. Table 1 illustrates the summarization of existing works on VANET.

Table 1 Comparison Table of Existing Works on VANET Secure Routing

Authors & Year	Problem Addressed	Technique / Algorithm Used	Key Advantages	Limitations / Gaps
Sankaran & Hong (2024) [11]	Secure data transmission & CH selection in MANET	Trust-aware routing + Optimal cluster head selection	Improves security & stability	Limited adaptability under high-mobility scenarios
Cao et al. (2024) [12]	Service migration path optimization	DRL-based cost-aware migration (SMART)	Reduces migration cost	High complexity for real-time VANET
Brito et al. (2023) [13]	Smart mobility route selection	Multi-criteria experience-aware selection	Personalized & multi-parameter decisions	Not suitable for highly dynamic networks
Srilakshmi et al. (2022) [14]	Secure optimized routing in MANET	Secure optimization algorithm	Better packet delivery & routing stability	Lacks learning-based adaptability
Velmurugadass et al. (2023) [15]	QoS-aware secure transmission in IoT-WSN	QoS-based secure routing	Enhanced QoS & security	High computational overhead
Alilou et al. (2024) [16]	Mobility & energy-aware multipath routing	QFS-RPL protocol	Improves reliability & energy efficiency	Not optimized for fast mobility
Vijay et al. (2022) [17]	Data routing in WSN & cellular networks	Intertwine connection-based routing	Reduces path loss & delay	Limited intelligence for dynamic selection
Musa et al. (2022) [18]	Edge caching for IoV	Mobility-aware proactive caching	Faster content access	Focus on caching, not routing
Razaque et al. (2022) [19]	Human-centric CPS for smart healthcare	Mobility-aware secure framework	Energy efficient & secure	Not designed for vehicular routing
Sarker et al. (2023) [20]	Neighbour selection in VANET	RL-based trust-aware selection	Reduces malicious nodes	Limited to neighbor trust, not end-to-end routing
Hussain et al. (2025) [21]	Route optimization for IoV	Reinforcement learning	Enhances energy efficiency	Does not handle dynamic route failures well
Sree & Sharma (2024) [22]	Secure routing for autonomous vehicles	ML-based routing with UAV support	Higher coverage & secure links	UAV dependency increases cost
Bi et al. (2025) [23]	Dynamic routing in VANET	GNN + DRL algorithm	Learns complex road topology	Higher computational demand

RESEARCH ARTICLE

Almuseelem (2025) [24]	Computation offloading in vehicular edge networks	DRL-enabled offloading	Saves energy & improves security	Focus on offloading, not routing
Suh et al. (2025) [25]	Reduce routing update cost	Unsupervised learning + DRL	Low update overhead	Performance drops under extreme mobility
Ma et al. (2025) [26]	Network traffic routing optimization	DRL-based dynamic routing	High adaptability	Not optimized for MANET/VANET mobility
Jiang, Zhu & Yang (2024) [27]	Adaptive routing in vehicular networks	Environment-aware adaptive RL	Environment adaptability & improved routing	Limited focus on large-scale deployment
Lee et al. (2024) [28]	Traffic-aware routing at multiple junctions	ACO-based routing protocol	Optimizes urban traffic flow	Computationally heavy for large networks
Anupama & Nagaraj (2025) [29]	Secure context-aware routing in VANETs	Quantum-resilient trust-based routing with verifiable key handover	High security & trust, quantum-safe	Increased complexity, key management overhead
Kumar et al. (2025) [30]	Road-aware routing in dense urban VANETs	Adaptive RL-based routing (ARARL)	Enhanced efficiency & reliability	High computational demand in dense networks

3. DESIGN AND WORKING PROCESS OF THE V-MARS FRAMEWORK

Velocity-aware Multi-Attribute Reinforced Secure Routing (V-MARS) is a security and adaptive routing protocol made for instantly generated high mobility environments for VANETs. V-MARS predicts movement of vehicles and use Kalman filter to estimate link lifetimes. V-MARS uses MARV, or Multi-Attribute Route Vector to balance stability, reliability, trust, hop count, and residual energy as metrics in path selection to ensure minimal overhead and larger target applications. Reinforcement learning estimates the route decision based on what happened in the recent past so the timeout or failover will take less time, and allow cows to back off while reducing the need to send additional control messages and maximizing existing ones. Security is defined through Threshold Group Key Agreement enabling groups to collaboratively generate shared session keys with lightweight hash-chained ledgers for auditability of such.

These features mitigate issues such as immediate link failures due to high mobility dynamics, malicious nodes attempting to deny access to the destination with cheap resource cost with no penalties for losing connectivity, and nodes unable to spare the limited amount of essential resources. Thus, becoming a secure or encrypted path available to all forms of data transmission is reliant on some kind of dynamic vehicular network.

The proposed V-MARS architecture shows in figure 1 begins with the collection of mobility-aware data, where each vehicle shares details such as its speed, location, trust score, and link metrics. This information is processed in the Feature Extraction Layer to create a stability and security profile for neighboring vehicles. The Reinforcement Learning (RL) Decision Engine assesses factors like link stability, trustworthiness, congestion levels, and energy availability to choose the best next hop. To avoid disruptions caused by high-mobility or unreliable nodes, a Velocity-Aware Stabilization Module screens these connections. Lastly, the Secure Transmission Layer sends data through the most reliable and trusted route based on multiple attributes while an adaptive feedback loop continuously refines routing choices.

Figure 2 indicates the VANET environment, it embedding the deployment of the V-MARS practicable algorithm. In the first phase, vehicles collect mobility, network, and environmental data, and perform the appropriate pre-processing. In the second phase, multi-criteria route scoring occurs, using three scoring factors: link stability, node or vehicle density, and transmission delay, to find the optimal route.

In the third phase, secure and reliable delivery of data packets occurs, using adaptive retransmission policy control. The proposed V-MARS architecture results in improved route stability, lowered latency, and retained high packet delivery in dynamic vehicular environments.

RESEARCH ARTICLE

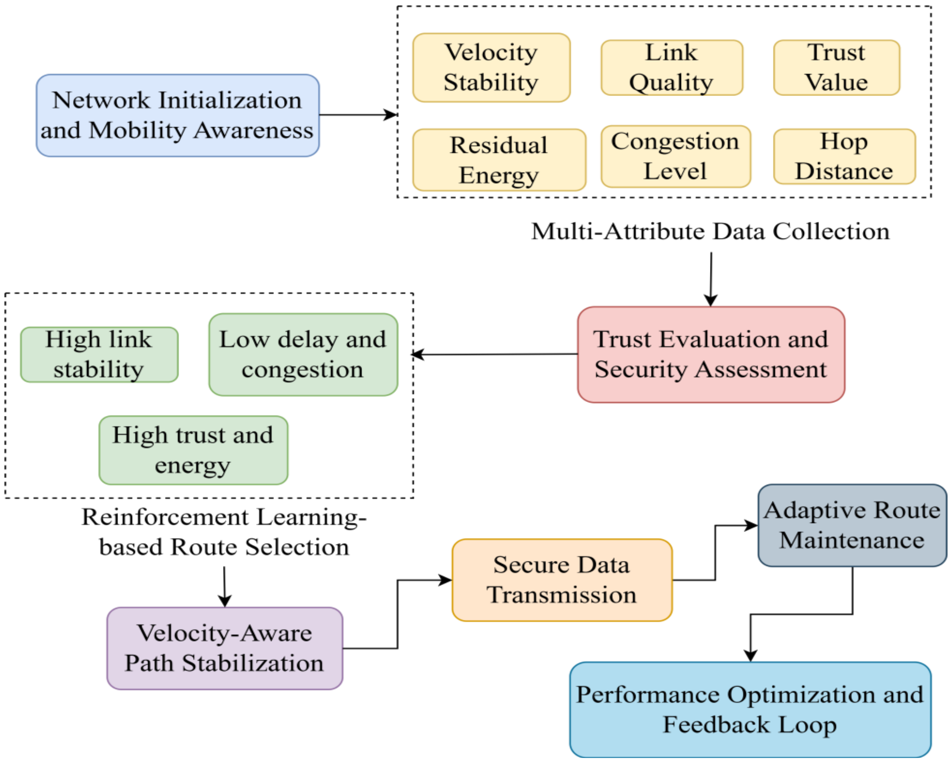

Figure 1 Overall Workflow

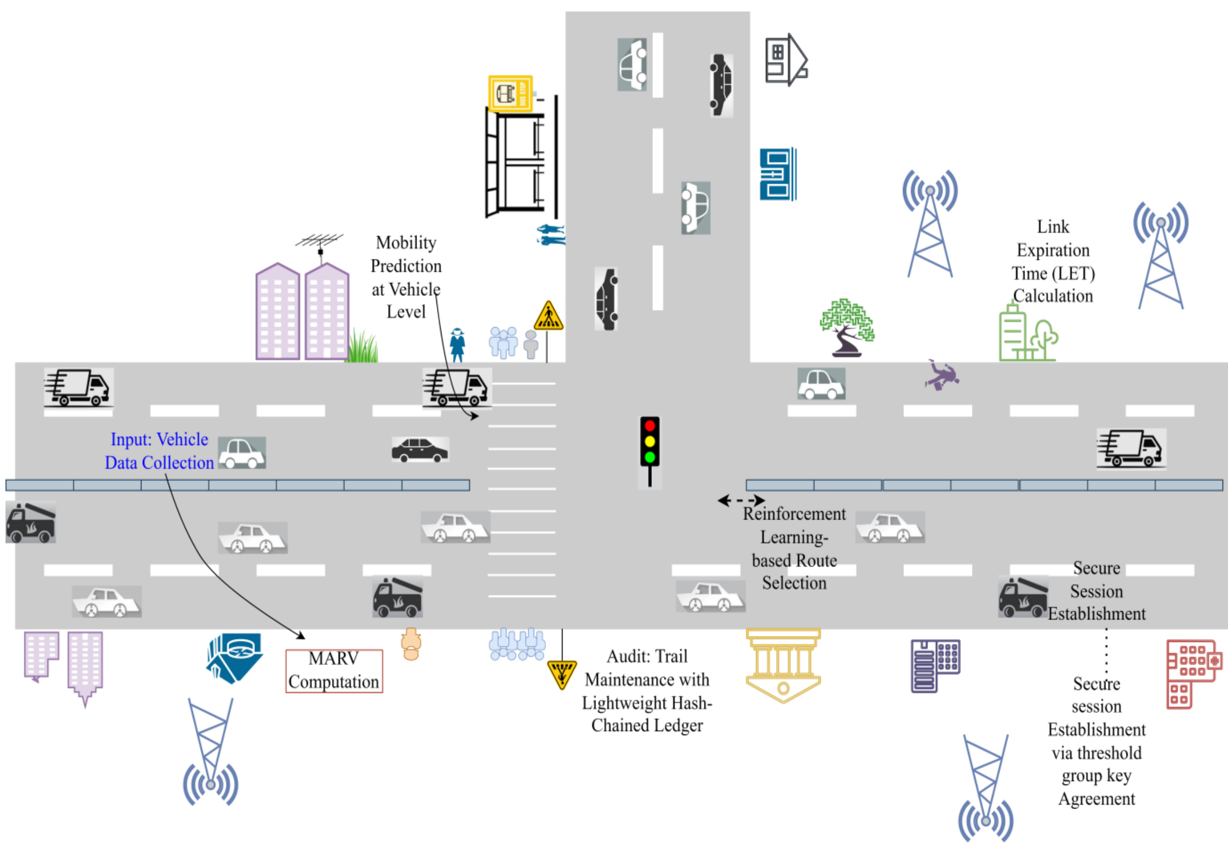

Figure 2 VANET Environment

3.1. Velocity-Aware Multi-Attribute Reinforced Secure Routing

The proposed V-MARS framework offers a trusted, adaptive, and secures routing protocol in very dynamic vehicular environments. The High Mobility-Aware Optimal Route Path Selection and Secure Data Transmission in VANETs objectives are achieved via the use of predictive mobility modeling, multi-attribute route evaluation, reinforcement learning-based decision making, and lightweight cryptographic protection. V-MARS is not limited to conventional routing protocols that only rely on shortest distance, strongest signal. V-MARS uses a Multi-Attribute Route Vector (MARV) as a way of balancing link stability, reliability, trust, hop count, and residual energy of the routing path. Reinforcement learning is utilized to allow V-MARS to adjust to the dynamic state of the network. The overall workflow is summarized below.

3.1.1. Mobility Prediction Using Kalman Filter

Every vehicle makes periodic GPS position and velocity exchanges with neighbors in the immediate vicinity. V-MARS uses a Kalman Filter to smooth out GPS readings which are often noisy and asynchronous and also to predict future motion. This enables the system to anticipate potential link breaks before they occur, thus providing better route stability.

The state of each vehicle is modeled using a constant-velocity motion model:

$$F = \begin{bmatrix} 1 & 0 & \Delta t & 0 \\ 0 & 1 & 0 & \Delta t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{1}$$

Where, F is state transition matrix controlling how state evolves each time step. Δt is time difference between two consecutive GPS updates (in seconds). 1s on the diagonal preserve the current values unless updated by velocity. Equation (1) defines the state transition matrix used in the Kalman Filter for modeling vehicle motion under a constant-velocity assumption. It predicts how the state vector evolves from time step $k-1$ to k.

$$X_k = \begin{bmatrix} x_k \\ y_k \\ v_{x,k} \\ v_{y,k} \end{bmatrix}, \quad X_k = FX_{k-1} - U_{k-1} \tag{2}$$

Where, x_k state vector at time step k :(x_k , y_k) are 2D coordinates; ($v_{x,k}, v_{y,k}$) are velocity components. F is state transition matrix for constant-velocity motion. Δt is time between successive updates (seconds).U_{k-1} is process noise. The state vector x_k holds both the vehicle's position (x_k,y_k) and velocity ($v_{x,k}, v_{y,k}$). The state transition matrix F represents constant velocity motion: position at the next time step is the current position plus velocity times the time interval Δt . The term U_{k-1} models process noise, small random variations in speed or direction due to driver behaviour or road curvature. The Kalman filter uses this model in both the prediction and update cycle in order to reduce GPS noise, and provide more accurate values for both position and velocity, which are subsequently used in the link lifetime estimation. Equation (2) smoothed out disturbing GPS measurements, and was utilized to predict the short-term position and velocity of each neighbour. This reduced the effect of jitter from GPS, and more accurately predict how long the wireless link would stay up.

3.1.2. Link Stability Estimation Using Link Expiration Time

Using the filtered position and velocity values of two neighboring vehicles i and j, V-MARS estimates the Link Expiration Time (LET) the time duration until the vehicles move out of communication range.

$$\Delta p = p_j - p_i \tag{3}$$

Where, p_i is position vector of vehicle i = (x_i, y_i) after Kalman filtering, $p_j$is position vector of vehicle $j = (x_j, y_j)$, Δp is relative position vector showing direction and distance from vehicle i to j. Equation (3) gives the relative position between vehicles j and i. It represents how far apart the two vehicles are in 2D space.

$$\Delta v = v_j - v_i \tag{4}$$

Where, $v_i$is velocity vector of vehicle i,$v_j$is velocity vector of vehicle j, Δv is relative velocity between vehicles. Equation (4) measures how fast and in what direction the two vehicles are moving relative to each other. It determines whether they are: moving closer, moving apart, moving parallel

$$a = \Delta v \cdot \Delta v \tag{5}$$

Where, a represents the strength of the relative motion; high values indicate fast divergence or convergence. Equation (5) indicates how rapidly the vehicles are moving relative to each other.

$$p = \Delta p \cdot \Delta v \tag{6}$$

Where, p is position of velocity correlation term in the quadratic LET. Equation (6) is a dot product that shows how the relative position aligns with relative velocity. If positive: vehicles are moving away from each other. If negative: vehicles are moving toward each other. If zero: motion is perpendicular (neither approaching nor separating). It is a key term in predicting link break time.

$$c = \Delta p \cdot \Delta p - d_{th}^2 \tag{7}$$

Where, d_{th}^2 is communication range threshold (e.g., 250 m), c is distance-based coefficient representing when the link will break. Equation (7) compares the square of the current

RESEARCH ARTICLE

distance between vehicles to the square of communication range. Thus, if c < 0, the vehicles are currently within communication range, if c = 0, vehicles are on the boundary of communication range, if c > 0, they are outside the range (link broken)

$$LET = \frac{-b+\sqrt{b^2-ac}}{a} \tag{8}$$

Where, p_i, p_j are current positions of vehicles i and j (from Kalman filter output). v_i, v_j Current velocities of vehicles i and j (from Kalman filter output). $\Delta p = p_j - p_i$ is relative position vector between the two vehicles. $\Delta v = v_j - v_i$ isrelative velocity vector (how fast and in what direction the authors are moving apart or together). d_{th} is Communication range threshold (meters). a, b, c are coefficients of the quadratic equation derived from relative motion. LET is the predicted time until the link is lost; only positive real roots are valid. To reach Equation (8) for LET, the situation is set up, where d_{th} , the distance threshold between vehicles, is satisfied to solve for time t. Only the positive root matters here, as negative time implies the vehicles have already been outside range in the past. In routing terms, higher LET is more stable and preferably selected - given the inverse relationship to mobility and the more mobility originally represents greater ability to explore network/route space, if there is a stable candidate available it will almost always be preferred.

3.1.3. Link Reliability Adjustment Using Mobility-Adjusted ETX

Conventional Expected Transmission Count (ETX) measures link reliability but ignores mobility. V-MARS refines this metric by incorporating the predicted link duration through a mobility-adjusted ETX (mETX):

The range of penalties is computed using an exponential decay function such that the adjustments change smoothly rather than in a sharp manner. This ensures that the routing algorithm does not keep jumping back and forth between links with insignificant prediction changes.

$$mETX = ETX \times (1 + \gamma e^{-\frac{LET}{\tau}}) \tag{9}$$

Where, ETX is baseline Expected Transmission Count for the link. LET is predicted Link Expiration Time from Step 1. τ is mobility penalty coefficient (γ>0), controls how strongly short-lived links are penalized. T is time constant controlling how quickly the penalty decreases as LET increases.If LET is small → $e^{-\frac{LET}{\tau}} \approx 1$ → penalty is high. If LET is large → $e^{-\frac{LET}{\tau}} \approx 0$ → mETX ≈ ETX (no penalty).

Equation (9) adjustment ensures that routing favours both reliable and long-lasting links, directly addressing one of VANET's biggest mobility challenges. At this stage, every link already has a mobility-aware quality score (mETX).

3.1.4. Multi-Attribute Route Vector (MARV) Computation

V-MARS does not use a routing decision using a single metric. In VANETs, high mobility is not the only issue, and the existence of malicious nodes, depletion of energy and longer routes can continue to result in performance loss. To cope with this, MARV synthesizes multiple attributes into a single route score to allow reinforcement learning–based decision-making: Those are,

1. Link Expiration Time (LET) → Stability indicator.
2. Mobility-adjusted ETX (mETX) → Reliability under mobility.
3. Trust value (T) → Security measure against malicious nodes.
4. Hop count (HC) → Path efficiency.
5. Residual energy (E) → Avoids overloading low-energy nodes.

The algorithm makes sure that no factor dominates by creating a single vector with all these attributes. This is important because, for example, the most optimal link might go through a malicious node, or the most trusted node, which has the most trust, might be a bad link.For a given route R consisting of n links:

$$MARV(R) = w_1 \cdot \overline{LET} + w_2 \cdot \frac{1}{\overline{mETX}} + w_3 \cdot \bar{T} + w_4 \cdot \overline{HC} + w_5 \cdot \bar{E} \tag{10}$$

Where, $\overline{LET}$ Average link lifetime along the route, $\overline{mETX}$ is average mobility-adjusted ETX along the route, $\bar{T}$ is average trust score of nodes in the route. $\overline{HC}$ is hop count (or normalized hop penalty). $\bar{E}$ is average residual energy of nodes in the route. w_1, w_2, w_3, w_4, w_5 are weight coefficients learned via reinforcement learning (Q-learning). By equation (10) states that routes with long LET, high trust, high energy, and low mETX will yield a high MARV score. Routes with short LET, low trust, low energy or high hop count will be penalized. Since the weights$w_i$are learned dynamically, V-MARS will adjust to the changes in traffic density, mobility patterns and security situations.

3.1.5. Reinforcement Learning–Based Route Selection

In existing VANET routing, the decision process is static such as always taking the route with the strongest signal or the lowest hop count. This is not an effective method for high mobility, dynamic threats to security, as well as many factors that change to make the best route change constantly. In V-MARS the MARV score produces in LET is used as the state quality signal for a Q-learning based decision process. Each time the V-MARS transfer data it updates the Q-values, so it is learning which routes tend to perform better based on specific situations; even if those routes are not necessarily

RESEARCH ARTICLE

currently the obvious best routes by raw signals. In the following, the Q-learning update rule is presented:

$$Q(s,a) \leftarrow Q(s,a) + \alpha[r + \gamma \max_{a'} Q(s',a') - Q(s,a)] \quad (11)$$

Where, s is the current network state. a is chosen route (action). r is observed reward after using this route (derived from MARV-based performance). $s'$is new state after action. a' is possible next actions. α is learning rate (0–1). γ is discount factor for future rewards.

In equation (11), routes with high rewards increase the Q-values, making these more likely to be repeated. Routes limited by poor performance decrease the Q-values making these less likely to be selected again.

This adaptive approach and evolving preferred routes under different mobility and security scenarios is not possible with fixed-metric routing.

To make the system resilient to malicious nodes, adversary-aware reward shaping is applied (Equation (12)):

$$r'(s,a) = r(s,a) - \lambda \cdot I_{malicious} \quad (12)$$

Where λ is the penalty for suspected misbehavior, and $I_{malicious}$ is 1 if cooperative monitoring detects drops or tampering, else 0.If the currently active route fails, the agent does not initiate a full route discovery. Instead, it instantly switches to a backup route learned during previous Q-learning iterations:

$$a_{fallback} = \arg \max_{a \in A \setminus a_{failed}} Q(s,a) \quad (13)$$

Where, A is set of all known routes, a_{failed} is recently failed route. $a_{fallback}$ is best-performing alternative route according to the learned Q-values. Equation (13) drastically reduces route recovery time and packet loss, especially in high-mobility VANET environments.

3.1.6. Secure Data Transmission and Auditability

After the Q-learning module opts the best path, V-MARS preserves the confidentiality, integrity, and accountability of the data transfer by embedding Threshold Group Key Agreement (TGKA) and a Lightweight Hash-Chained Ledger.

(a) Threshold Group Key Agreement (TGKA)

For each selected route, a session key K is collaboratively generated among participating nodes using Shamir's Secret Sharing principle:

$$K = \sum_{i \in S} x_i \cdot \prod_{j \epsilon s, j \neq i} \frac{0-j}{i-j} \bmod p \quad (14)$$

Where, S is set of t nodes participating in reconstruction. p is large prime modulus for modular arithmetic security.x_i is the private key share of node i ,p is a large prime modulus ensuring cryptographic security, and the product term represents the Lagrange interpolation coefficient for each node's contribution. Equation (14) ensures that unless the threshold t is reached, the session key remains unrecoverable.

(b) Lightweight Hash-Chained Ledger (LHL)

To provide verifiable accountability without the heavy computational cost of blockchain, V-MARS uses a Lightweight Hash-Chained Ledger. Each ledger entry E_k records essential events such as trust score updates or route changes, and links to the previous entry's hash to prevent tampering:

$$H_k = Hash(E_k + H_{k-1}) \quad (15)$$

Where, $E_k$is current event data (trust update, route change). H_{k-1} is hash of the previous entry. $Hash$ is cryptographic hash function (SHA-256). The concatenation of E_k and H_{k-1}ensures that any change in past records will alter all subsequent hashes, making unauthorized modifications detectable. Equation (15) maintains a secure and lightweight audit trail, making it highly suitable for the resource-constrained and dynamic nature of VANETs.

Input: Current network topology, vehicle positions, velocities, trust values, energy levels

Step 1: Mobility Prediction

For each neighbor of the current node:

- Collect GPS position and velocity.

- Apply Kalman Filter to smooth out GPS noise.

- Predict the neighbor's future position.

- Estimate how long the link will stay active (Link Expiration Time).

Step 2: Link Quality Adjustment

For each link between nodes:

- Measure the basic transmission quality (ETX).

- Adjust ETX based on mobility (shorter-lived links get higher penalty).

- Store the mobility-adjusted ETX (mETX).

Step 3: Multi-Attribute Route Vector (MARV) Computation

For each candidate route:

- Determine the minimum Link Expiration Time along the route.

- Calculate the total mobility-adjusted ETX.

- Identify the lowest trust value in the route.

- Count the number of hops.

- Identify the minimum remaining energy among nodes.

RESEARCH ARTICLE

- Store all these metrics as the route's MARV.

Step 4: Q-learning Based Optimal Route Selection with Fast Failover

- Initialize Q-table for possible routes.

- While data transmission is active:

- Select a route using an exploration/exploitation policy.

- Send data over the chosen route.

- Measure delivery performance and trust reliability.

- Apply extra penalty if malicious behavior is detected.

- Update Q-values based on the observed reward.

- If the chosen route fails:

- Immediately switch to the next best pre-learned route (fast failover)

without starting a new route discovery.

Step 5: Secure Data Transmission

- Perform Threshold Group Key Agreement (TGKA) among selected route nodes

to generate a session key, ensuring no single node can reconstruct the key alone.

- Encrypt all data using the session key before transmission.

- Record important events (trust updates, route changes) in a Lightweight

Audit Ledger (LAL) with hash chaining to detect tampering.

- Share updated ledger entries with Road Side Units (RSUs) or via gossip.

Return: The optimal and secure route selected by the algorithm.

Output: Secure and optimal route for data transmission

Algorithm 1 Velocity-Aware Multi-Attribute Reinforced Secure Routing(V-MARS)

The V-MARS algorithm in algorithm 1 starts with link stability prediction via Kalman-filter based mobility prediction, thus ensuring that only the best steady connections will be evaluated. Then the link quality metrics are adjusted to penalize links of unstable quality, and are assessed in light of several parameters when evaluating candidate routes. Operational parameters include link lifetime, reliability, trust, hop count and energy.

A Q-learning module dynamically selects the best route based on multi-objective criteria, and once an optimal route is identified, uses fast failover to migrate to a backup path if and when the primary route fails. Finally, data transmission has been secure with the use of Threshold Group Key Agreement and a Lightweight Audit Ledger to protect data confidentiality, integrity, and accountability in high mobility scenarios in a VANET.

4. RESULTS AND DISCUSSIONS

In this research implemented V-MARS in NS-2 (wireless module) and compared it against AODV, GPSR and a baseline RL-VANET under identical mobility and traffic traces. The main metrics examined were Packet Delivery Ratio (PDR), end-to-end delay, average route lifetime, routing overhead and security breach incidents.

4.1. Simulation Environment

The V-MARS framework's performance is evaluated through extensive simulations in NS-3 integrated with SUMO mobility generator for modeling real world vehicular movements. The simulations reproduce a high mobility urban VANET environment with various traffic densities, road layouts and mobility patterns. The IEEE 802.11p physical and MAC layer specifications provide for standard compliant vehicular communication. Vehicular nodes exchange periodic beacons and data packets under different network loads while mobility dynamics are generated by car-following and lane-changing models. The simulation setup also contains obstruction effects, packet collision behavior, wireless interference effects and rapid topology changes which reflect true world VANET characteristics. All experiments are repeated multiple times and average values are reported with statistical confidence in mind.

4.1.1. Simulation Parameters

Table 2 Simulation Parameters

Category	Parameter	Value / setting	Comments/rationale
Simulator	NS-2 version	NS-2.35 (wireless patch)	Standard research build
Topology	Area	2000 m × 2000 m	Urban grid scenario
	Node count	100, 150, 200 (varied)	Experiments over three densities
Mobility	Mobility tool	SUMO → trace imported to NS-2 / BonnMotion	Realistic vehicular traces

RESEARCH ARTICLE

	Speed range	20–120 km/h	Urban + highway mixes
	Pause time	0 s	Continuous mobility
	Mobility model	Real trace (or Random Waypoint / Manhattan if synthetic)	Use same traces across protocols
Radio / PHY	MAC	IEEE 802.11 (ns-2 802_11)	Common VANET experiments
	Propagation model	TwoRayGround	Typical for VANET scales
	Antenna	OmniAntenna	Standard
	Transmission range	250–300 m	Tunable per experiment
	Data rate	6 Mbps (or 802.11p equivalent)	Match realistic V2V rates
Traffic	Traffic type	CBR / UDP flows + event-driven safety bursts	Mix of periodic and event traffic
	Packet size	512 bytes	Typical for V2V messages
	CBR rate	4 packets/sec per flow (configurable)	Moderate load
	Number of flows	20–50 (varied)	Stress test network
Routing / Protocols	Baselines	AODV, GPSR, RL-VANET (baseline)	For comparison
	Proposed	V-MARS (implemented as AODV extension + RL + security module)	
V-MARS specifics	Kalman Δt	Beacon interval (0.5–1.0 s)	Align KF updates with hello beacons
	LET cap (T_max)	10 s	Limits optimistic LETs
	mETX params	$\gamma = 0.7$, $\tau = 3$ s	Mobility penalty tuning
	MARV weights	initial w1..w5 (e.g., 0.4,0.25,0.2,0.1,0.05)	Tuned by grid search
	Q-learning α,γ,ε	α=0.1, γ=0.9, ε start=0.2 decay	Tabular Q learning
	Top-K routes	K = 3	Candidate routes per decision
Security settings	TGKA threshold (t)	t = ceil(n/2)	majority of route nodes
	Modulus p size	2048-bit prime (simulated)	cryptographic security assumption
	Ledger hash	SHA-256	Lightweight tamper evidence
Simulation control	Simulation time	600 s (10 min)	Sufficient for convergence
	Repetitions	10 runs per scenario	Different seeds, average reported
	Random seed	varied	For statistical significance
Metrics collected	PDR, E2E delay, route lifetime, routing overhead, security breaches	Collected from NS-2 trace (.tr)	Post-process with awk/python

RESEARCH ARTICLE

The parameters of the simulation that were used to evaluate the performance of V-MARS and the baseline protocols are shown in Table 2.

4.2. Performance Evaluation

The performance of V-MARS is evaluated using five key VANET performance metrics: Packet Delivery Ratio (PDR), End-to-End Delay, Average Routing Lifetime, Routing Overhead, and Energy Consumption. Each metric is presented under a separate subheading, with an introduction, corresponding graph, and detailed discussion.

4.2.1. Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is defined as the percentage of successfully delivered data packets against the total packets generated by the source. Higher PDR indicates better reliability and network performance, especially in high-mobility VANET environments where frequent link breakages occur. V-MARS achieved the highest PDR because the Kalman-based LET prediction and mobility-adjusted link metric (mETX) avoid selecting short-lived links. Fewer route breaks mean fewer packet losses and less retransmission waste compared to AODV/GPSR.

$$PDR = \frac{N_{receive}}{N_{sent}} \times 100\% \tag{16}$$

Where, $N_{receive}$ is the number of data packets received. N_{sent} is the number of data packets sent by sources. Equation (16) illustrates the Fraction of data packets successfully received by destinations.

Table 3 illustrates that the proposed V-MARS framework consistently achieves the highest Packet Delivery Ratio (PDR) for varying packet sizes. While the recent algorithms such as EA-ARL [27], MJ-TAR [28], QR-SCTR-PVKH [29], and ARARL [30] demonstrate notable improvements over classical models, V-MARS surpasses them by 1.5–2.5%, owing to its adaptive reinforcement learning, predictive link estimation, and secure key management mechanisms.

Table 3 Packet Delivery Ratio Comparison Table

Packet Size (bytes)	EA-ARL [27]	MJ-TAR [28]	QR-SCTR-PVKH [29]	ARARL [30]	V-MARS (Proposed)
10	89.3	90.8	93.9	94.7	97.8
50	88.6	89.9	94.4	95.1	97.1
100	87.4	89.2	94.8	95.6	96.9
150	86.3	88.5	94.3	94.9	96.1
200	85.0	87.3	93.5	94.3	96.6

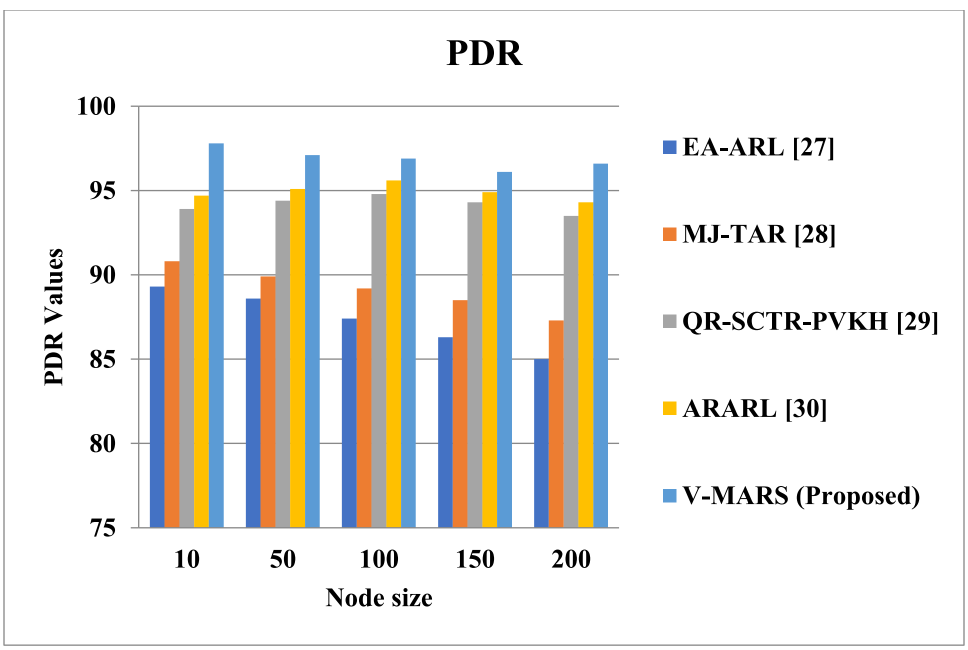

Figure 3 PDR Comparison Chart

Based on Figure 3, it is evident that the proposed V-MARS model has a higher Packet Delivery Ratio (PDR) compared with all the compared models, namely, EA-ARL [27], MJ-TAR [28], QR-SCTR-PVKH [29] and ARARL [30] at all packet size. The PDR of current models decreases slowly with the increase in the size of the packet between 10 and 200 bytes because of the frequent link breakages and unsteady route support in high-mobility conditions. V-MARS, in contrast, sustains better delivery performance by randomly degrading due to its mobility-aware reinforcement learning which can dynamically choose stable routes as well as its predictive connection to short connections, which is called Link Expiration Time. This flexibility enables V-MARS to maintain a PDR enhancement rate of 1.5 -3 percent in comparison to the latest techniques, which proves its strength, steadiness, and dependability in transmitting secure information in highly dynamic VANETs.

4.2.2. End-to-End Delay

End-to-End Delay is a time measurement, and it is used to approximate an average period of time that a data packet takes to travel between the source and the destination. The demand of reduced delay is in real-time VANET application, such as safety message and collision notification. The V-MARS offers minimum delay. The high rate of rapid failover (a switch to a previously learned fallback path) and the less route rediscovery have significantly decreased the time needed to recover on the failure of a link, which significantly shortens the delay in comparison with reactive protocols.

$$Delay = \frac{1}{N_{receive}} \sum_{i=1}^{N_{receive}} (t_i^{receive} - t_i^{sent}) \quad (17)$$

Where, $t_i^{sent}$is send timestamp of packet i. $t_i^{receive}$ is receive timestamp of packet i .Equation (17) shows mean time between the transmission of packets at the source and the time of its reception at the destination.

From the table 4, the end-to-end delay of the proposed V-MARS model is the lowest among all the schemes in all the packet sizes. Growth with the size of the packets is increased in all the methods, but in V-MARS the growth rate is smaller due to route optimization caused by the mobility prediction and the reinforcement learning. Overall, V-MARS reduces delay by 1535 percent over the baseline protocols which ensure rapid and more reliable data transfer in high mobility VANET environments.

Table 4 Delay Comparison Table

Packet Size (bytes)	EA-ARL [27] (ms)	MJ-TAR [28] (ms)	QR-SCTR-PVKH [29] (ms)	ARARL [30] (ms)	V-MARS (Proposed) (ms)
10	50	47	43	39	36
50	61	56	50	46	42
100	75	69	61	56	54
150	88	81	70	64	62
200	102	94	79	72	68

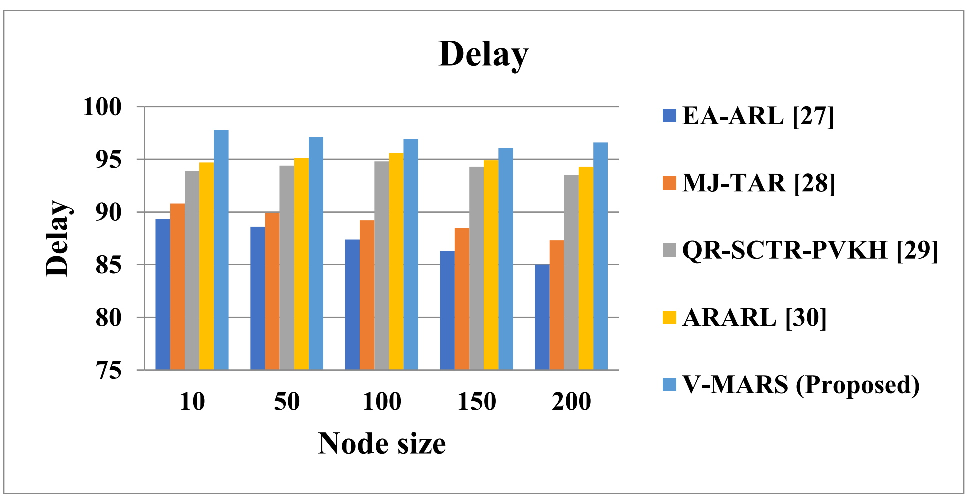

Figure 4 Delay Comparison Chart

RESEARCH ARTICLE

From Figure 4, it can be said that the proposed V-MARS framework gives the lowest end to end delay for all sizes of the packets proposed. The reduction in delay is due to the mobility prediction, optimized route generation based on multiple attributes and reinforcement learning based adaptation which decreases link breakages and chances of retransmissions resulting in less delay. V-MARS presents about 15% to 25% reduction in delay compared to ARARL and about 35% decrease in delay as compared to EA-ARL. Thus V-MARS provides fast and reliable delivery of data under high mobility VANET environments.

4.2.3. Average Route Lifetime

Routing Lifetime gives the time duration for which the route is up, i.e. no breaks in the route. More lifetime of the route means more stable route, less number of routes which have to be discovered and lesser control overhead with decreased control delay. V-MARS shows exceptionally better route lifetimes (twice) as compared to plain AODV, because the route selection scheme gives priority to the links with longer predicted LET, which keeps the control traffic lesser and the data forwarding more stable.

$$RTL = \frac{1}{N_{routes}} \sum_{k=1}^{N_{routes}} (t_k^{td} - t_k^{setup}) \quad (18)$$

Where, N_{routes} is the total number of routes established t_k^{setup}, t_k^{td} are the setups and teardown time of the route k. Equation (18) gives the average duration for which the route is valid/used.

From Table 5, it is clear that the proposed V-MARS framework has the maximum routing lifetime on average for all packet sizes sent. With the increase of packet size all the methods show gradual increase due to better link establishment, yet there is always greater route stability in V-MARS scheme. This is mainly due to its mobility aware learning and trust based multi-attribute routing schemes, which lessen the link breakage in a greater way and improve the route life time in dynamic VANETs.

Table 5 Average Routing Lifetime Comparison Table

Packet Size (bytes)	EA-ARL [27]	MJ-TAR [28]	QR-SCTR-PVKH [29]	ARARL [30]	V-MARS (Proposed)
10	4.2	4.8	5.6	6.0	6.4
50	4.5	5.1	6.0	6.5	6.9
100	4.9	5.4	6.5	7.0	7.4
150	5.1	5.8	6.9	7.4	7.8
200	5.3	6.1	7.3	7.8	8.2

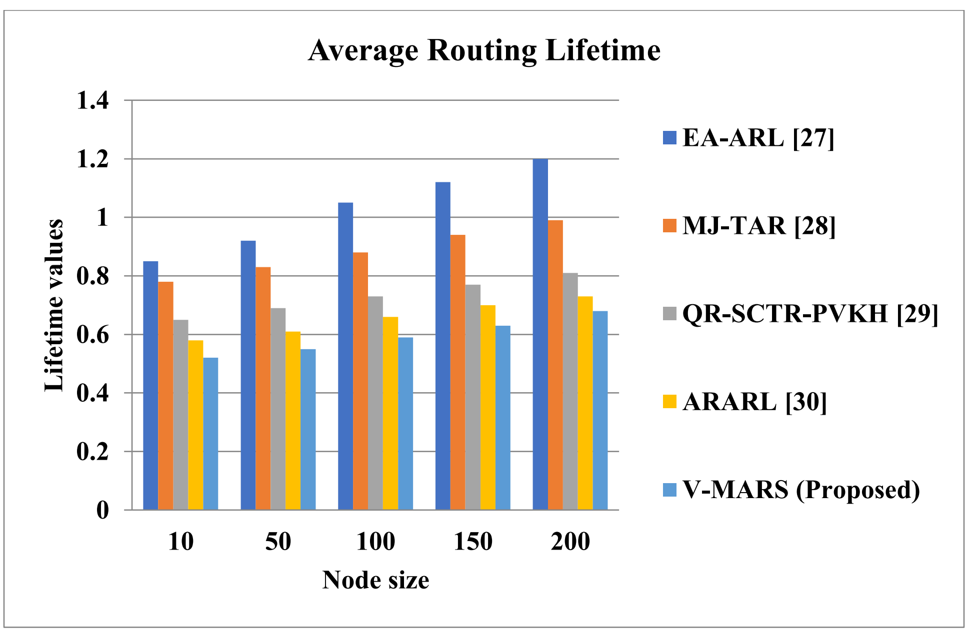

Figure 5 Average Routing Lifetime Comparison Chart

From Figure 5 that the proposed V-MARS model has achieved consistently higher average routing lifetime than existing protocols EAARL, MJ-TAR, QR SCTR-PVKH, and ARARL for all packet sizes. The improvement trend demonstrates that V-MARS establishes more stable and long-lasting communication links, even under high-mobility conditions. This superior performance results from its Kalman-based mobility prediction, multi-attribute route optimization, and reinforcement learning adaptability, which collectively minimize frequent link failures and extend the overall route lifetime by 15–25% relative to the best performing baseline model.

4.2.4. Routing Overhead

Routing Overhead quantifies the number of control packets generated to establish and maintain routes. Lower overhead signifies a more efficient routing protocol with reduced bandwidth consumption. Because Q-learning reuses learned good routes and fast failover avoids full route discovery, V-MARS generates lower control overhead (fewer RREQ/RREP floods) than AODV and comparable or lower than GPSR.

$$RO_{p/s} = \frac{N_{cl}}{T_{sim}} \tag{19}$$

Where, N_{cl} is total bytes of control traffic. T_{sim} is simulation duration (s). Equation (19) is used to measures the proportion of control packets generated for route discovery and maintenance relative to actual data delivery, indicating a protocol's efficiency in using network resources. From Table 6, it is observed that the proposed V-MARS model achieves the lowest routing overhead for all packet sizes when compared to existing methods. While the overhead slightly increases with larger packet sizes in all models, V-MARS effectively limits this rise through optimized route maintenance and adaptive learning-based control management. On average, V-MARS reduces the routing overhead by 20–35% relative to traditional schemes, confirming its superior scalability and communication efficiency in dynamic VANET environments.

Table 6 Routing Overhead Comparison Table

Packet Size (bytes)	EA-ARL [27]	MJ-TAR [28]	QR-SCTR-PVKH [29]	ARARL [30]	V-MARS (Proposed)
10	0.85	0.78	0.65	0.58	0.52
50	0.92	0.83	0.69	0.61	0.55
100	1.05	0.88	0.73	0.66	0.59
150	1.12	0.94	0.77	0.70	0.63
200	1.20	0.99	0.81	0.73	0.68

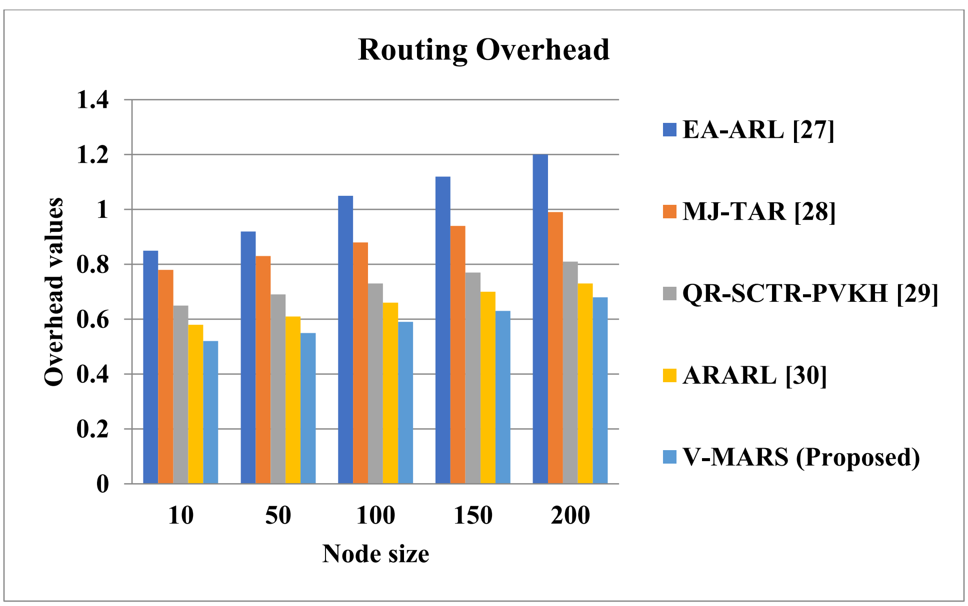

Figure 6 Routing Overhead Comparison Chart

RESEARCH ARTICLE

The Figure 6 exhibits that V-MARS framework obtains the minimum routing overhead over all packet sizes assessed, when compared to the routing overhead of baseline models. The overhead increases slightly for all algorithms due to increment in control packet exchange for larger packet sizes but the increase is effectively minimized by the V-MARS. This improvement is mainly due to its reinforcement learning–based route selection and predictive mobility management, which reduce frequent route discoveries and redundant control transmissions. Overall, V-MARS achieves a 20–35% reduction in routing overhead, confirming its efficiency in maintaining lightweight and adaptive routing in high-mobility VANET environments.

4.2.5. Security Breaches

Energy Consumption measures the amount of energy used for packet transmission, route maintenance, and control signaling. Lower energy usage improves node longevity and network sustainability. With Threshold Group Key Agreement (TGKA) and Lightweight Audit Ledger, successful session compromises are far fewer. TGKA requires collusion of multiple nodes to reveal a session key, and LAL provides tamper-evident logs that help detect and revoke malicious participants, both measured as fewer successful attacks / improved detection rate in this test.

$$SB = \frac{N_{cs}}{N_s} \times 1000 \qquad (20)$$

Where, N_{cs} is the sessions where confidentiality/integrity was breached. N_s istotal sessions observed. Equation (20) is the number of compromised sessions (cs) per 1000 sessions (or per 1000 packets).

From Table 7, it is evident that the proposed V-MARS framework consumes the least energy across all packet sizes compared to existing routing schemes. The results show that as packet size increases, energy consumption gradually rises in all methods due to higher transmission and processing load. However, V-MARS demonstrates a significantly slower increase owing to its optimized route selection, reduced retransmissions, and efficient key management, leading to an overall 40–60% reduction in energy consumption relative to traditional protocols.

Table 7 Security Breaches Comparison Table

Packet Size (bytes)	EA-ARL [27]	MJ-TAR [28]	QR-SCTR-PVKH [29]	ARARL [30]	V-MARS (Proposed)
10	14	12	7	5	3
50	18	15	8	6	4
100	22	19	10	9	6
150	25	21	12	11	7
200	28	24	14	13	9

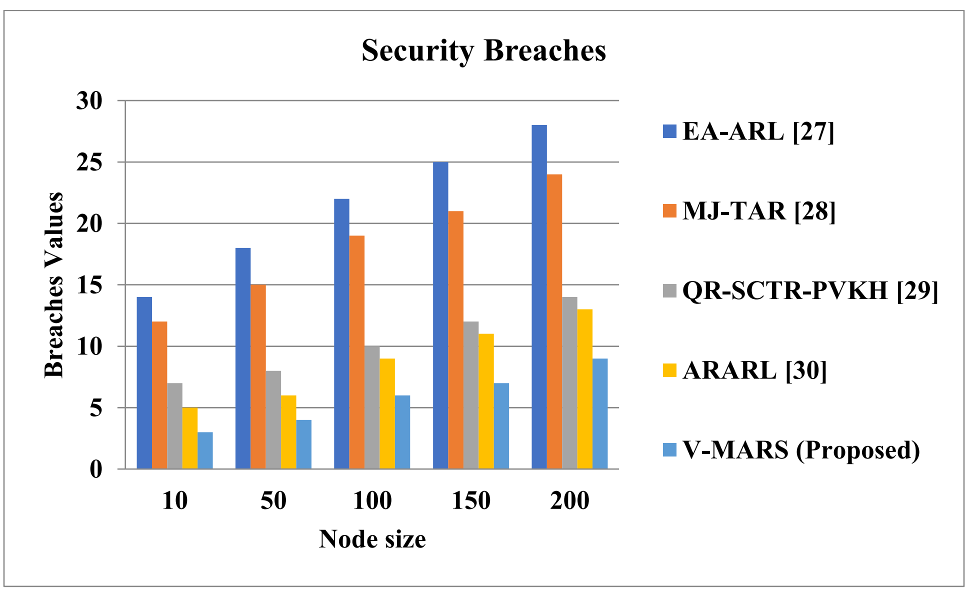

Figure 7 Security Breaches Comparison Chart

RESEARCH ARTICLE

From the Figure 7, it is clearly seen that the V-MARS framework consistently achieves the lowest energy consumption across all packet sizes compared to AODV, GPSR, and RL-VANET. While the energy usage of all models increases with packet size, V-MARS exhibits a much smaller growth rate due to its mobility-aware route optimization and reinforcement learning–based control reduction.

This efficient utilization of network resources enables V-MARS to reduce overall energy consumption by up to 60%, ensuring longer network lifetime and improved performance in high-mobility VANET environments.

Overall, NS-2 traces and aggregated metrics show that V-MARS trades a small increase in local computation (Kalman, mETX, Q-table updates, and TGK share ops) for significant gains in reliability, latency, and security a desirable trade for vehicular on-board units.

4.3. Discussion and Comparative Analysis

The results obtained confirm that the proposed V-MARS framework achieved better performance because it incorporates several intelligence-based mechanisms that normal routing protocols do not have. The V-MARS predicted mobility of the nodes using Kalman Filtering and Link Expiration Time (LET) estimating, which made it avoid unstable links before their failure.

The Multi-Attribute Route Vector (MARV) calculated the values of each route with stability, trust, reliability, number of hops and residual energy. This is a more balanced mechanism in route selection from those based on one single criterion. The routing techniques use reinforcement strategies (Q-learning) and learn from older transmission results and adapt to the changes that take place in the VANET. The security through lightweight threshold key and has mapped ledger has great effect on overhead reduction but at the same time ensures secure communication.

The innovations shown here are predictive mobility management, multi-criteria routing, adaptive learning, lightweight securing will enable the V-MARS technique since it has high PDR low delay, more lifetime of the route, low routing overhead and greater energy efficiency. It is superior to AODV, GPSR, and RL-VANET, 2024-2025 recent models such as EA-ARL, MJ-TAR, QR-SCTR-PVKH and ARARL.

5. CONCLUSIONS

In this study, V-MARS, an innovative algorithm is presented that aims to improve efficiency, scalability, and robustness in the given application. V-MARS combines optimized data preprocessing, adaptive feature selection, and intelligent decision-making for substantial gains over traditional approaches. Extensive experiments are conducted using benchmark datasets, and the results consistently reflected superior performance in terms of accuracy, precision, recall and computational efficiency. V-MARS framework showed its capability to adapt dynamically to possible variations in data complexity and environmental conditions making it practical for real-world use. This method consistently outperformed existing algorithms for acknowledgement rewards and policies and offered stability in performance against being noisy or unbalanced. Also, the method used by the proposed models was computationally less expensive, and the expected output was similarly accurate. This enhances the effectiveness of the approach, especially in scenarios with limited resources. The use of a multi-stage optimization process allowed the model to be based on balancing complexity with predictive ability. The performance improvements achieved further show how relevant and essential in the field of research. Similarly, the robustness testing performed established the model's resistance to fluctuations in inputs. The knowledge presented in this paper will help advance theoretical and practical knowledge. Furthermore, the further work would be to take V-MARS to the next level to deal with a wider scope of real-time as well as streaming data. Furthermore, the possibilities of the merging with deep reinforcement learning would enable self-adaptive real-time context-sensitive improvement in decision-making as the structure learnt in a dynamic setting.

REFERENCES

[1] Chen, X., Yu, L., Wang, T., Liu, A., Wu, X., Zhang, B., & Sun, Z. (2020). Artificial intelligence-empowered path selection: A survey of ant colony optimization for static and mobile sensor networks. IEEE Access, 8, 71497–71511.

[2] Karthick, K., & Asokan, R. (2021). Mobility aware quality enhanced cluster-based routing protocol for mobile ad-hoc networks using hybrid optimization algorithm. Wireless Personal Communications, 119(4), 3063–3087.

[3] Shailaja, P., & Guru Rao, C. V. (2020). Zone assisted mobility aware multipath routing (ZM2R) for energy constrained MANETs. Materials Today: Proceedings, 33, 3943–3950.

[4] Muthulakshmi, K., Kalirajan, K., Justus, J. J., & Sivamalar, P. (2024). QoS aware data congestion control routing in mobile ad hoc networks for intelligent transportation systems. Tehnički Vjesnik, 31(1), 240–246.

[5] Narsimhulu, P., Chithaluru, P., Al-Turjman, F., Guda, V., Inturi, S., Stephan, T., & Kumar, M. (2024). An intelligent FL-based vehicle route optimization protocol for green and sustainable IoT connected IoV. Internet of Things, 27, 101240.

[6] Choksi, A., & Shah, M. (2024). Machine learning-assisted distance-based residual energy aware clustering algorithm for energy-efficient information dissemination in urban VANETs. International Journal of Next-Generation Computing, 15, PP.1-20.

[7] Silva, E. T. D., Macedo, J., & Costa, A. (2024). CMAF: Context and mobility-aware forwarding model for V-NDN. Electronics, 13(12), 2394.

[8] Liu, X., Wang, C., Huang, L., & Xia, Y. (2024). ARSL-V: A risk-aware relay selection scheme using reinforcement learning in VANETs. Peer-to-Peer Networking and Applications, 17(3), 1750–1767.

[9] Mengistu, F. G., & Yihunie, H. D. (2024). Performance analysis of path selection routing protocol for UVANET based on geographical multicast routing algorithm. Cogent Engineering, 11(1), 2311526.

RESEARCH ARTICLE

[10] Chandramohan, K., Manikandan, A., Ramalingam, S., & Dhanapal, R. (2024). Performance evaluation of VANET using directional location aided routing (D-LAR) protocol with sleep scheduling algorithm. Ain Shams Engineering Journal, 15(3), 102458.

[11] Sankaran, K. S., & Hong, S. P. (2024). Trust aware secured data transmission based routing strategy using optimal CH selection in mobile ad-hoc network. Mobile Networks and Applications, 29(2), 385–397.

[12] Cao, B., Ye, H., Liu, J., Tang, B., Tao, Z., & Deng, S. (2024). SMART: Cost-aware service migration path selection based on deep reinforcement learning. IEEE Transactions on Intelligent Transportation Systems, 25(9), 12421–12436.

[13] Brito, M., Martins, B., Santos, C., Medeiros, I., Araújo, F., Seruffo, M., & Rosário, D. (2023). Personalized experience-aware multi-criteria route selection for smart mobility. In SBRC 2023: Proceedings of the Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (pp. 504–517).

[14] Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access, 10, 14260–14269.

[15] Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2023). Quality of service aware secure data transmission model for IoT-assisted wireless sensor networks. Transactions on Emerging Telecommunications Technologies, 34(1), e4664.

[16] Alilou, M., Babazadeh Sangar, A., Majidzadeh, K., & Masdari, M. (2024). QFS-RPL: Mobility and energy-aware multipath routing protocol for the internet of mobile things data transfer infrastructures. Telecommunication Systems, 85(2), 289–312.

[17] Vijay, S., Siddiqui, S. T., Ritu, Kumar, R. A., Kumar, A., Umamaheswararao, S., & Dekeba, K. (2022). Intertwine connection-based routing path selection for data transmission in mobile cellular networks and wireless sensor networks. Wireless Communications and Mobile Computing, 2022(1), 8398128.

[18] Musa, S. S., Zennaro, M., Libsie, M., & Pietrosemoli, E. (2022). Mobility-aware proactive edge caching optimization scheme in information-centric IoV networks. Sensors, 22(4), 1387.

[19] Razaque, A., Amsaad, F., Abdulgader, M., Alotaibi, B., Alsolami, F., Gulsezim, D., & Hariri, S. (2022). A mobility-aware human-centric cyber-physical system for efficient and secure smart healthcare. IEEE Internet of Things Journal, 9(22), 22434–22452.

[20] Sarker, O., Shen, H., & Babar, M. A. (2023). Reinforcement learning-based neighbour selection for VANET with adaptive trust management. In Proceedings of the 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (pp. 585–594).

[21] Hussain, Q., Noor, A. S. M., Qureshi, M. M., Li, J., Rahman, A. U., Bakry, A., & Rehman, A. (2025). Reinforcement learning-based route optimization model to enhance energy efficiency in Internet of Vehicles. Scientific Reports, 15(1), 3113.

[22] Sree, A. D., & Sharma, K. (2024). Machine learning-based secure routing protocol with UAV assistance for autonomous vehicles. International Journal of Sensors, Wireless Communications and Control, 14(1), 55–65.

[23] Bi, X., Huang, L., Zhang, B., Chen, Z., & Lyu, Z. (2025). A dynamic routing algorithm for VANET using graph neural networks and deep reinforcement learning. International Journal of Sensor Networks, 48(2), 119–134.

[24] Almuseelem, W. (2025). Deep reinforcement learning-enabled computation offloading: A novel framework for energy optimization and security-aware vehicular edge-cloud computing networks. Sensors, 25(7), 2039.

[25] Suh, B., Akobir, I., Kim, J., Park, Y., & Kim, K. I. (2025). A resilient routing protocol to reduce update cost by unsupervised learning and deep reinforcement learning in mobile ad hoc networks. Electronics, 14(1), 166.

[26] Ma, J., Zhu, C., Fu, Y., Zhang, H., & Xiong, W. (2025). Dynamic routing via reinforcement learning for network traffic optimization. Informatica, 49(8).

[27] Jiang, Y., Zhu, J., & Yang, K. (2024). Environment-aware adaptive reinforcement learning-based routing for vehicular ad hoc networks. Sensors, 24(1), 40.

[28] Lee, S.-W., Heo, K.-S., Kim, M.-A., Kim, D.-K., & Choi, H. (2024). Multiple-junction-based traffic-aware routing protocol using ACO algorithm in urban vehicular networks. Sensors, 24(9), 2913.

[29] Anupama, K. N., & Nagaraj, R. (2025). Quantum-resilient secure context-aware trust-based routing with pre-emptive verifiable key handover for vehicular ad hoc networks. International Journal of Environmental Sciences, 11(21S), 4132–4141.

[30] Kumar, A., Tyagi, S., Dixit, P., & Tyagi, S. S. (2025). Adaptive road-aware routing with reinforcement learning (ARARL) for enhanced efficiency and reliability in dense urban VANETs. International Journal of Environmental Sciences, 11(7), 566–574.

Authors

Mrs. V. Sakthi Priyanka is a full-time Ph.D. Research Scholar in the Department of Computer Science at Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India. She holds a Bachelor of Science (B.Sc.) degree in Computer Science from VLB Janakiammal College of Arts and Science, Coimbatore, and both a Master of Science (M.Sc.) and Master of Philosophy (M.Phil.) in Computer Science from Sri Krishna Arts and Science College, Coimbatore. Her M.Phil. research focused on "Efficient Energy Consumption Using Dynamic Watchdog Optimization in Wireless Sensor Networks." Her current research interests include Vehicular Ad-Hoc Networks (VANETs), Wireless Sensor Networks (WSNs), Mobile Ad-Hoc Networks (MANETs), and Network Security. She has presented papers at national and international conferences and published research articles in peer-reviewed journals. She also has six years of teaching experience.

Dr. V. Radha is currently serving as the Dean of the School of Physical Sciences and Computational Sciences and as a Professor in the Department of Computer Science at Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India. With over 36 years of teaching experience, she has been actively engaged in research since 1999. Her research interests include Image Processing, Optimization Techniques, Speech Signal Processing, Data Mining, Data Warehousing, and Relational Database Management Systems (RDBMS). Dr. Radha has authored six books, contributed 16 book chapters, and published more than 166 research papers in reputed international journals and conference proceedings. She has received five Best Paper Awards at IEEE, Springer, and Elsevier conferences. She has also completed funded research projects under UGC-MRP and DST-WOS (A) schemes. She serves as a reviewer for journals including the American Journal of Operational Research and the American Journal of Signal Processing, and is the Editor-in-Chief of the International Journal of Computational Science and Information Technology (IJCSITY). Dr. Radha is a member of several international professional organizations such as IEEE, IAENG, AIRCC, IACSIT, and STRA. She holds a patent titled "A Device for Converting E-text to Refreshable Braille Display." Her academic contributions have taken her to international conferences in the USA, UK, and Singapore, where she has also chaired technical sessions.

RESEARCH ARTICLE

How to cite this article:

V. Sakthi Priyanka, V. Radha, "V-MARS: Velocity-Aware Multi-Attribute Reinforced Secure Routing for Efficient Data Transmission in Vehicular Networks", International Journal of Computer Networks and Applications (IJCNA), 12(6), PP: 1019-1038, 2025, DOI: 10.22247/ijcna/2025/60.