International Journal of Communication Systems

WILEY

RESEARCH ARTICLE

Optimizing Real-Time Vehicular Communications With a Cross-Layer Model for Energy-Efficient Clustering and Blockchain-Based Congestion Control

K. Satheshkumar[1] | S. Ramalingam[2] | A. Suresh Babu[3] | S. Murugesan[4]

[1]Department of ECE, Vivekanandha College of Engineering for Women, Tiruchengode, Tamil Nadu, India | [2]Department of ECE, Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu, India | [3]Department of ECE, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India | [4]Department of EEE, AMET University, Chennai, Tamil Nadu, India

Correspondence: K. Satheshkumar (satheshkumarphd25@gmail.com)

Received: 25 February 2025 | **Revised:** 8 January 2026 | **Accepted:** 20 July 2026

Keywords: clustering | optimization algorithms | routing | vehicular ad hoc networks

ABSTRACT

Vehicular ad hoc networks (VANETs) are essential components of intelligent transportation systems that facilitate real-time communication between vehicles (V2V) and between vehicles and infrastructure (V2I). Despite their importance, VANETs face challenges, such as high node mobility, energy limitations, security risks, and ever-changing network topologies. Existing clustering and routing algorithms often struggle to manage the instability caused by mobility, energy disparities, and secure congestion-free communication simultaneously. To address these challenges, this work introduced an integrated cross-layer framework featuring three innovative algorithms: mobility-aware black hole clustering (M-BHC), energy-aware piranha optimization algorithm (EPOA), and cross-layer multi-attribute blockchain routing with congestion control (CL-MABRC). The M-BHC algorithm enhances the stability of clusters and counters black-hole attacks by forming clusters dynamically based on real-time vehicle mobility patterns. EPOA optimizes the selection of cluster heads (CHs) by reducing energy consumption through a bio-inspired resource allocation strategy modeled on piranha predation behavior. CL-MABRC addresses network congestion and security using blockchain-based verification and cross-layer routing decisions informed by multi-attribute metrics. Extensive simulations were conducted with a setting of 100 veh/km^2. The proposed framework showed significant performance improvements over benchmark protocols, such as optimal security-aware cluster-based hybrid geographical and opportunistic routing (OSC-GOR), enhanced location-aided ant colony routing (ELAACR), trust-based multi-objective honey badger algorithm (TMOHBA), and robust cryptographic scheme for reliable data communication (RCSRC). It achieved a throughput of 99.89 Kbps, end-to-end delay of 3.9 ms, collision rate of 21.8%, energy consumption of 41.98%, and jitter of 0.05 ms. Together, the M-BHC, EPOA, and CL-MABRC algorithms create a robust, energy-efficient, and secure communication framework for VANETs, enhancing scalability, reliability, and real-time performance in transportation systems.

1 | Introduction

VANETs are becoming a key technology in existing intelligent transport systems and can enable vehicles to communicate dynamically with each other and with roadside facilities. This interconnectedness allows many applications, such as real-time traffic control, collision control, and dissemination of emergency information, which in actual sense results in better road safety and efficiency [1]. Nevertheless, VANETs, with their high mobility and dynamic topologies, pose serious challenges to the reliability, efficiency, and security of communication. Work on VANETs cuts across several key areas

© 2026 John Wiley & Sons Ltd.

All rights reserved, including rights for text and data mining and training of artificial intelligence technologies or similar technologies.

such as mobility management, energy efficiency, and security protocols [2]. These areas must be addressed to create a robust VANET infrastructure that can respond to the needs of modern transportation systems. Good mobility management can guarantee a smooth flow of information despite the high speed at which vehicles travel [3]. Energy-efficient protocols are essential because of the constraint sources of power in onboard units (OBUs), which require a strategy that increases the network lifespan. Furthermore, there is an urgent need to implement strong security measures to counteract malicious attacks that may interfere with the integrity and reliability of the network.

This study was motivated by the necessity to address the limitations of the available VANET solutions regarding dynamic network conditions, energy usage, and security risks. Conventional clustering and routing algorithms are not well adapted to the dynamic topology changes that are unique to vehicular scenarios, which cause an increase in communication overhead (OH) and reduce network performance [4, 5]. In addition, existing methods do not adequately address the power limitations of vehicle nodes or the complexity of developing security threats. Consequently, there is an urgent need to develop new frameworks that incorporate state-of-the-art algorithms to improve the stability of the clustering process, minimize energy consumption, and reinforce the security of VANETs [6].

The connected vehicle (CV) architecture, as shown in Figure 1, is an overall system that enables vehicles, infrastructure, and central management systems to interchange information. This illustration reveals the direction that modern transport systems are taking to create smarter and more interconnected roads. The highest architecture level is the central authority (CA), which is the brain of the system. CA is also associated with diverse applications and services that assist in managing and optimizing traffic flow, enhancing safety, and providing worthwhile services to the associated vehicles. The CA evaluates the information on the entire network and makes sound decisions to enhance transport efficiency. Roadside units (RSU) form the middle of the architecture and are antenna-like objects that are strategically positioned along

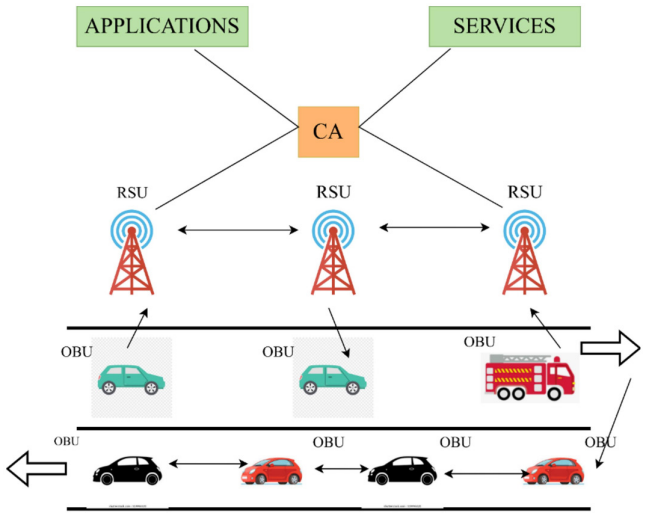


FIGURE 1 | Architecture of VANET.

the road. These RSUs are used to establish a connection between road vehicles and central authorities. They are indispensable elements of vehicle-to-infrastructure (V2I) connections, which allow the exchange of data in real time and provide essential traffic information. Diverse ground-level vehicles are equipped with OBUs. Such vehicles, including passenger vehicles and other vehicles, can receive and transmit information through OBUs. OBUs should allow vehicles to communicate with the RSUs above them and, theoretically, with other vehicles in their vicinity, creating a vehicle-to-vehicle (V2V) communication network.

This communication capability enables real-time updates on traffic, safety alerts, and emergency notifications. The entire system operates cohesively to create an intelligent transportation network that can monitor traffic conditions, manage traffic flow, respond efficiently to emergencies, and offer valuable services to CVs. The arrows in the diagram illustrate bidirectional communication channels, demonstrating how information flows seamlessly between all system components, thereby ensuring that all participants in the transportation network remain connected and informed. This study has significant potential to enhance the performance, scalability, and security of VANETs, which are essential elements of next-generation intelligent transportation systems. By developing solutions that effectively address mobility, energy consumption, and security, this study aims to promote the widespread adoption of VANETs, resulting in safer and more efficient road networks [7]. However, several challenges remain, as the high-speed movement of vehicles leads to frequent topology changes, complicating the maintenance of stable communication links and requiring the development of adaptive clustering mechanisms. Vehicular nodes often have limited power resources and require energy-aware protocols to prolong the network lifespan and ensure continuous operation. The open nature of VANETs renders them vulnerable to various attacks, such as black hole attacks, in which malicious nodes falsely advertise optimal paths to intercept data, compromising network integrity and user privacy [8–10].

Despite the availability of solutions, there are still difficulties in attaining optimal clustering and routing, which dynamically adjusts to network variations and is energy-efficient. Recent developments in VANETs have led to the proposal of different optimization algorithms to improve network performance. One study suggested a better ant colony optimization (ACO) algorithm, whereby fittest node clustering is used to optimize data routing. The other method integrates particle swarm optimization (PSO) with a sequential variable neighborhood search (SVNS) to develop a data dissemination protocol that optimizes the routing paths. Moreover, a hybrid Prairie dog optimization (PDO) algorithm was proposed to define consistent and stable cluster-based routing schemes [11–13]. In the context of highways, a path-routing protocol was developed, which is an optimal option that supports the efficient delivery of warning messages to vehicles. Hybrid deep neural network (DNN) and bidirectional long short-term memory (BiLSTM) models have been created to detect and prevent intrusion in the field of security, which have been trained on a trust-based clustering and routing scheme [14, 15]. In the fight against adversarial attacks, machine learning has been used to increase the security of VANETs. Moreover, machine learning models have been studied to forecast effective routing protocols based on feature information. Autonomous vehicle systems have also been proposed

to use secure routing protocols with the assistance of unmanned aerial vehicles (UAVs) [16, 17]. The CSKAS-VANET model was developed to prioritize stable clustering and authentication based on role-based access control and signcryption. Finally, a traffic control model using hybrid methods was created to predict congestion and rerouting to enhance the efficiency of the entire network [18, 19].

Despite extensive research on VANET optimization, clustering, and secure routing, existing approaches often address mobility, energy efficiency, congestion control, and security as separate problems, resulting in limited adaptability under highly dynamic traffic conditions. Frequent re-clustering, uneven energy consumption, and increased security OH remain critical challenges, particularly in real-time and dense vehicular environments. Moreover, the lack of tightly integrated cross-layer frameworks restricts the ability of current solutions to respond efficiently to simultaneous network dynamics and security threats. Motivated by these limitations, this work introduces a unified cross-layer framework that jointly incorporates mobility-aware clustering, energy-efficient optimization, and blockchain-assisted secure routing to achieve scalable, reliable, and real-time VANET communication. The M-BHC algorithm enhances cluster stability by forming clusters based on real-time analysis of vehicle mobility patterns. By dynamically adjusting cluster memberships in response to vehicular movements, M-BHC reduces the frequency of re-clustering and mitigates the risk of black-hole attacks by ensuring that data packets are routed through reliable nodes. The EPOA for CH selection optimizes energy consumption by emulating the predatory behavior of piranhas to select CHs with balanced energy loads. This approach ensures that CHs are chosen based on their residual energy and connectivity, distributing energy consumption evenly across the network and extending the overall network lifespan. The CL-MABRC protocol integrates blockchain technology into the routing process to enhance security and data integrity. By employing a cross-layer design, CL-MABRC utilizes multiple attributes such as link quality (LQ) and node trustworthiness for intelligent path selection. Additionally, it incorporates congestion control mechanisms to monitor network traffic in real time, dynamically adjusts routing paths to prevent bottlenecks, and ensures efficient data transmission. These ground-breaking algorithms solve the problems of VANETs by making real-time communication between vehicles scalable, energy-efficient, and safe.

The cross-layer design of VANETs is a strategic break design that violates the past layer differentiation of the network stack to allow more intelligent and coordinated decision making. Cross-layer models are used to maintain the exchange of contextual information between layers, such as mobility metrics of the physical layer, congestion and link status of the MAC layer, and routing decisions of the network layer, in highly dynamic vehicular networks, where the topology is changing at a very high rate and the reliability of communication is paramount. The holistic strategy contributes significantly to flexibility and enables routing protocols to make decisions that are informed by a combination of several parameters, including signal strength, node reliability, buffer occupancy, and latency. The proposed CL-MABRC algorithm, which integrates a cross-layer model, leads to more accurate and efficient routing decisions in a highly mobile environment with changing conditions of the network, which optimizes the quality of service (QoS) as well as minimizes the packet loss and delay. One of the fundamental issues in VANETs is energy efficiency, particularly because of the limited energy supply of OBUs and the growing need for sustainable communication. Re-clustering frequently because of node mobility results in the drainage of a lot of energy, which decreases the lifetime and performance of the network.

To overcome this, the proposed framework also integrates an energy-conscious CH selection framework using the enhanced piranha optimization algorithm (EPOA). This approach makes the cluster members balance their energy usage through the choice of cluster heads (CHs) according to the remaining energy, connection, and relative mobility. In addition, the M-BHC algorithm establishes stable clusters by predicting vehicular mobility, thereby minimizing cluster maintenance OHs. The inclusion of blockchain in VANETs is a major transformation in the control of data integrity, trust, and congestion issues. Blockchain technology has decentralized and tamper-resistant properties that enhance the reliability of route authentication and information sharing to ensure that malicious changes are reduced to a minimum. This is the CL-MABRC protocol, which utilizes a blockchain to verify routes through cryptographic hash verification and consensus processes to ensure the successful mitigation of route manipulation by malicious nodes. Moreover, the natural impossibility of changing the blockchain supports the safe assessment of trust among nodes, which works to create safer clusters and routes. Regarding congestion control, the protocol monitors live traffic and records and shares congestion information using a blockchain between trusted nodes to make advance changes to routes. The primary contributions of the works are as follows:

- Proposes an innovative cross-layer framework for VANETs that comprehensively incorporates clustering, routing, and security functions to enhance communication reliability and flexibility in highly dynamic vehicular contexts.
- Introduces an energy-aware clustering paradigm that significantly enhances cluster stability and lifetime by considering vehicle mobility patterns and energy distribution across nodes.
- Develops a decentralized, blockchain-supported routing mechanism that strengthens data authenticity, trust evaluation, and route integrity while ensuring efficient congestion control in high-density traffic scenarios.
- Provides a scalable and mobility-resilient communication model that dynamically adapts to frequent topology changes, reducing packet loss, routing delays, and re-clustering frequency.
- Contributes a comprehensive performance evaluation demonstrating substantial improvements over existing methods in terms of packet delivery ratio (PDR), end-to-end delay (EED), throughput, energy efficiency, and security robustness in VANET settings.

The remainder of this work is organized as follows. Section 2 discusses the related work. Section 3 describes the proposed work,

and Section 4 estimates its performance. Finally, Section 5 presents the conclusions and future work.

2 | Literature Survey

Kadam et al. propose that trust management procedures optimize CH and relay (data forwarder) selections for TACR operations. For clustering, this work derives the direct and indirect trust values for each vehicle. The ACO fitness function (FF) determines the hybrid trust value of each vehicle for these work projects. For optimal CH, the ACO algorithm prefers steady automobiles. These routing studies select forwarding relays and create trust-based access control mechanisms to ensure secure and dependable data transfer. This work used fuzzy logic to choose the optimal relay node and set access control rules based on trust. TACR boosts the throughput by 11.25% and the PDR by 8%. TACR reduces latency by 9.51% and OH by 12.32%. Because trust evaluation and clustering are complicated, the TACR approach may not scale well for large VANETs. It may also have trouble adapting to rapidly changing network topologies, which could compromise its performance [20].

Husnain et al. offer the intelligent, probability-based, and nature-inspired whale optimization algorithm (p-WOA), which forms vehicular communication clusters. The FF was developed using the probability for communication range, number of nodes, velocity, and highway routing, reducing unpredictability. The work found that VANETs that deploy ITS applications optimize their clusters by 75, cutting communication costs and routing OH and extending cluster life. Real-time performance may be affected by sophisticated bio-inspired cluster optimization schemes. They may also struggle to handle security issues or adapt to VANET dynamics [21].

Ali et al. created AOACNET, a secure, intelligent clustering system using AOA. AOA optimizes vehicle groupings. The performance values of each vehicle were used to prevent unauthentic nodes from joining the cluster during construction. Data transfer records determine the vehicle performance. A vehicle is punished (−1) to send a fake message and rewarded (+1) to send a legitimate message. According to the simulations, the proposed algorithm outperformed similar options by 25% in the defined optimization objectives. The arithmetic optimization–based secure intelligent clustering algorithm for VANET may not be able to handle real-time processing in networks that change significantly. Modern adversarial attacks may weaken security and expose users to sophisticated threats [22].

Ahmed et al. suggest using blockchain and VANETs to secure federated Q-learning. To secure traffic data, extended elliptic curve cryptography (EX-ECC) is first used. The federated Q-learning model trains the data and protects privacy. Blockchain storage using the IPFS technology improves VANET data security. The DPBFT consensus mechanism is used to validate the proposed blockchain system. Blockchain-enabled federated Q-learning can improve the VANET safety and performance. When running full simulations, the throughput (102,465.8 KB/s), communication OH (360.57 Mb), average latency (864.425 ms), communication time (19.51 s), encryption (0.98 ms), decryption (1.97 ms), consensus delay (50 ms), and validation delay (1.68 ms) are all taken into account. Blockchain transactions are expensive; hence, the blockchain-enabled federated Q-learning model may have scaling issues that impair the system performance. Federated learning may also cause difficulties in data privacy and coordination in decentralized systems [23].

Sarathkumar et al. use deep learning and the Coati optimization algorithm to improve VANET intrusion detection. ID-COADL categorizes VANET intrusions and secures them using a hyperparameter-tailored deep learning model. ID-COADL starts with min–max normalization to scale the input data uniformly. The ID-COADL deep belief network (DBN) model identifies intrusions. Finally, the COA can select DBN model hyperparameters to increase intrusion detection. The COATI optimization and deep learning for VANET intrusion detection may have high processing requirements, thereby limiting their real-time use. If the system cannot handle the dynamic nature of VANETs, it may delay attack detection and mitigation [24].

Suganyadevi et al. provide a meta-heuristic for HACOSMO that finds the shortest path depending on distance and traffic. According to HACOSMO, the routing OH ranges from 8% to 11% under IDBACOR, 10% to 14% under GRACO, 19% to 31% under OACO, and 24% to 37% under ACO for various vehicle numbers and speeds. The suggested strategy boosts throughput by 3%–7% over IDBACOR, 6%–8% over GRACO, 11%–15% over OACO, and 16%–25% over ACO. The swarm intelligence–inspired meta-heuristics multiple-constraint hybrid optimization VANET routing may be computationally demanding, restricting its capacity to scale for large networks. It may also be difficult to adapt to dynamic network topologies, which affects real-time performance and routing efficiency [25].

Divya et al. propose a clustered vehicle location technique for hybrid krill herd and bat optimization. Thus, the fitness-function-based hybrid krill-herd and bat optimization methods identify and stop attacks. This method also boosts communication security. The CVL protocol addresses the energy usage and packet delays. The adaptive-cluster-based vehicular routing protocol for secure communication may struggle to maintain cluster stability in dynamic VANETs. In addition, its security measures may not be sufficient to stop sophisticated cyber-attacks, jeopardizing network reliability [26].

Kheradmand et al. proposed TaLAR, a cluster-based, traffic-aware, low-latency routing scheme. CH nodes are selected using Harris Hawks Optimization (HHO) based on intracluster distance, link reliability, and vehicle relative speed. HHO chooses the optimum route between the source and destination CH nodes based on link dependability and inter-cluster distance. The Dijkstra algorithm and digital street map determine a traffic-aware and reliable path in the interconnection zone. Simulations showed that the proposed strategy improves PDR (22% and 19%), throughput (25% and 21%), and average EED (23% and 18%, respectively). VANET cluster-based routing schema with HHO may have computational complexity limits that limit real-time performance. Fast topology changes in VANET systems may affect cluster stability and routing [27].

Alam et al. introduced graph-based trust-enabled routing (GBTR) for VANETs. This approach evaluates the node

trustworthiness using direct, indirect, and contextual trust. The communication frequency, consistency, delay, and mobility with punishment/reward variables determine direct trust. Feedback trust, link reliability, and mobility factors determine indirect trust. Each node pair's contextual trust incorporates the location, time of day, weather, and traffic density. The trust scores from these evaluations determine the routing. Reliable routes are identified using route request/reply and maintenance mechanisms to improve network performance. The participants' trust levels were periodically updated using a trust update algorithm based on a lower reward and higher penalty. The simulations show that the proposed GBTR system outperforms traditional routing methods in terms of PDR%, DPR%, EED (ms), throughput (Kbps), and normalized routing load (packets/s). Secure graph-based trust-led graph-based trust evaluations are expensive to process; hence, VANET routing can be difficult. Dynamic large-scale VANET systems may suffer from poor trust accuracy and routing efficiency [28].

Sajithabegam et al. suggest improving dynamic adaptive cluster-based routing to reduce VANET suboptimal decisions. A central controller optimizes VANET clustering and routing using energy and distance-based clustering and dynamic adaptive cluster–based routing. EDBC builds clusters using energy and distance measurements between autos and RSUs. A fitness model chooses CHs from nodes with the highest fitness values, and LBFCM optimizes cluster formation. Merging LBFCM with the fitness model yields a CH with energy efficiency, stability, and dynamism. The shortest route is determined by the DACBR using network characteristics, including energy, communication, and traffic congestion. EDACR outperformed earlier methods in terms of throughput, network OH, PDR, and latency by 15%, 20%, 25%, and 30%, respectively. With a 10% packet loss reduction and 20% network lifespan enhancement, EDACR increases network stability. Software-defined vehicle networks may struggle to manage high computational demands for real-time clustering and routing decisions with energy- and distance-based optimized clustering and dynamic adaptive cluster-based routing. This approach may also struggle to maintain cluster stability and respond quickly to topology changes in dynamic network environments [29].

Punitha et al. proposed an optimal security-aware cluster-based hybrid geographical and opportunistic routing (OSC-GOR) for VANETs. This work obtains optimal clustering and energy efficiency via improved bald eagle optimization (IBEO). The trust scores from energy consumption and signal intensity determine CHs. Poplar optimization algorithms (POAs) perform better. An optimal min–max recurrent neural network (OMM-RNN) determines the next forwarder nodes for VANET data transfer. In high-mobility VANETs, the OSC-GOR may struggle to balance the security and routing efficiency. Its hybrid geographical and opportunistic routing strategy may increase computing costs, affecting large-scale real-time network performance [30].

Rakesh Kumar et al. offer the security metrics and authentication-based routing (SMART) protocol for VIoT networks to improve security and reduce OH. SMART produces hashes (digests) using the Merkle tree and encrypts them using elliptic curve cryptography to reduce OH. Integrating complete security metrics and authentication processes might increase computational and transmission OHs, limiting SMART protocol scalability. Its performance may also be affected by dynamic vehicle IoT systems with rapid topology changes and large node density [31].

Souissi et al. used two fuzzy inference systems, instant energy trust (IEN-Trust), and total energy trust (TEN-Trust), to assess the energy information quality in a fuzzy-based energy consumption trust (ECOTRUST) model. IEN-TRUST analyzes energy information for coherence with slope degree, speed, and acceleration rate, whereas TEN-TRUST compares nearby vehicles. The ECOTRUST paradigm may struggle to balance energy consumption optimization with trust assurance computational OHs. It may also be less useful in highly dynamic electric vehicle networks, where rapid topological changes may influence trust evaluation accuracy and energy efficiency [32].

Ramamoorthy et al.'s (2024) VANET enhanced location-aided ant colony routing (ELAACR) ensures transparent and secure data delivery. In Phase 1, location-aided key management (LAKM) was used, whereas in Phase 2, Ant Colony Routing (ACR) was used. The ACR and LAKM patterns ensure reliable communication. The LAKM method builds a secure network using group signatures and uses an ACR to find the fastest and most secure shortest path for data transfer. When compared with EHACORP and F-ANT, the proposed ELAACR has an average throughput (T) of 640 Kbps, packet loss rate (PLR) of 0.018%, PDR of 98.5%, OH of 0.157%, and EED of 0.16 s. ELAACR may be limited by the computational cost of the ACO technique, thereby impacting dynamic VANET real-time performance. Location information may also affect efficiency and security in circumstances of inaccurate or missing GPS data [33].

Mutalik et al. presented VANET routing security with the trust-based multi-objective honey badger algorithm (TMOHBA). Trust, EED, routing OH, energy, and distance are the cost functions used to optimize the TMOHBA. TMOHBA safe route finding improves data delivery and resilience to malicious attacks. Additionally, shortest-path discovery reduces latency and boosts VANET security. The PDR of TMOHBA for 10 malicious attacks is 90.6446%, which is greater than that of HEGSO and AODV-SP. Real-time routing in highly dynamic VANET systems may be problematic owing to the computational limits of the TMOHBA. Balancing trust, security, and routing efficiency in large-scale networks may also affect the performance [34].

Behura et al. crafted a multi-objective algorithm focused on optimizing the selection of CHs and securing communication in VANETs through a modified version of the enhanced station-to-station (e-STS) cryptographic protocol. This system utilizes isolation forest and autoencoder methodologies for accurate attack classification, bolstered by refined feature selection. It was designed to adjust to changing network topologies, markedly improving performance metrics, including accuracy (0.985%), recall (0.96%), F1 score (0.91%), and precision (0.872%). Furthermore, the technique enhances the PDR to 93%, elevates the cluster efficiency to 95%, augments the throughput to 10,199 kbps, and reduces the delay to 0.31 s. This method surpassed FASMO-DMN, MetaLearn, and

ACO-K-means in the MATLAB and SUMO simulations. The intricacy of these models may result in computational OH, thereby impeding real-time scalability in high-density traffic scenarios [35].

Mahesh et al. proposed an energy-efficient cluster-based routing (EECR) protocol that is augmented with fuzzy-TOPSIS (FT) in order to enhance communication of the VANETs. The protocol begins by choosing a CH using the hybrid shuffled shepherd Namib beetle optimization (HSS-NBO) algorithm. Subsequently, the routing is addressed through the jellyfish-beluga whale optimization (CJ-BWO) model, which considers factors such as security, trust, QoS, delay, and energy consumption. An intermediate node forwarding scheme is used to handle the region of nothingness, and in this case, the proxy agent RSU helps in recovering faults. This design ensures that both the reliability of the data and the energy usage are high. Nevertheless, various metaheuristic algorithms may elevate the computational requirements, which may impact the real-time scalability of the VANET dynamic environment [36].

Meera et al. suggested a hybrid algorithm named the Hippopotamus optimization algorithm–based energy-efficient stable cluster construction protocol (HHPOASCCP) to shape the clustering of vehicle nodes within VANETs. In this protocol, the equilibrium between exploration and exploitation in the HPOA is used to prevent local optima and find the most optimal cluster configurations globally. It is useful for selecting highly fit nodes to act as CHs and an efficient number of clusters to enhance energy efficiency. Simulations showed that the proposed model deployed 24.38% of nodes as CHs, decreased the clusters by 24.58, enhanced the efficiency in load balancing by 23.12, and saved 19.84% of energy consumption over traditional methods. Nevertheless, the model might be limited in highly mobile environments, where the stability of clustering can be influenced by frequent changes in topology, creating the need to reconfigure every node [37].

Ajaz et al. (2025) proposed cluster-based lion optimization routing protocol (CLORP) to optimize routing in the Internet of Vehicles (IoV). This protocol organizes stable groups and finds the best cluster leaders using the lion optimization Algorithm, which reduces the control message traffic and enhances AODV because gateway nodes are included. CLORP is used to improve the network by overcoming issues such as latency, the number of packets carried by the network, and routing OH in the dynamic topology. Improved AODV, CACOIOV, and other recent protocols have shown better results than AODV. However, it can also decelerate in high-mobility settings because of delays in re-clustering and adapting to topology changes [38].

Gopinath et al. proposed a cluster optimization strategy for VANETs, which uses a hybrid methodology involving flying foxes and enhanced whale algorithm (HFFEWA). In this method, highway paths, vehicle velocity, node density, and range of communication are used as a FF to minimize the randomness in cluster formation. The flying fox optimization algorithm (FFOA) was used to improve global exploration, whereas the enhanced whale algorithm (EWA) addressed the premature convergence problem, providing a balanced exploration and exploitation approach. Through simulations, it was found that the network life improved by 19.42% and the stable cluster formation improved by 32.18%, as well as an improved performance in the packet delivery rate, EED, and a decreased number of packet losses. Nonetheless, the bidirectional execution of these metaheuristic algorithms can lead to computational OH, which can affect real-time responsiveness in large-scale or high-rate vehicular contexts. Table 1 presents a significant literature review on VANET [41].

Dong et al. conducted an extensive assessment of authentication systems and attack detection approaches in vehicular ad hoc networks (VANETs), thoroughly evaluating threats, including Sybil, replay, impersonation, and black hole attacks. This study underscores the inadequacies of single-layer security measures in rapidly changing automotive contexts and stresses the necessity of cohesive authentication and intrusion detection systems [42]. Liu et al. conducted a comprehensive analysis of cross-layer authentication methodologies in wireless communication networks, emphasizing the enhancement of security and efficiency through information exchange across protocol layers. This work illustrated that cross-layer architectures enhance resilience to coordinated attacks and decrease authentication delay relative to conventional layered models [43].

2.1 | Problem Statement

Algorithms such as optimal security-aware clustering-geographical and opportunistic routing (OSC-GOR), ELAACR, TMOHBA, and robust cryptographic scheme for reliable data communication (RCSRC) have played a crucial role in enhancing the security, routing efficiency, and reliability of VANETs. However, these methods have limitations. OSC-GOR struggles to maintain capacity and durability under dynamic network conditions, whereas ELAACR faces challenges with energy efficiency and performance in high-traffic scenarios. Although TMOHBA employs sophisticated trust-based techniques, its high processing demand renders it unsuitable for devices with limited resources. Similarly, RCSRC offers robust security and reliability but incurs significant computational OHs during the security process, limiting its applicability in real-time scenarios. These limitations underscore the need for comprehensive and efficient strategies that balance security, performance, and adaptability in resource-constrained and highly dynamic environments.

2.2 | Novelty

Despite some significant breakthroughs in clustering and routing of VANETs, the existing solutions face difficulties with high-mobility environments, inefficient energy consumption management, or insufficient attempts to address security and congestion concerns.

- The proposed framework is innovative because of its overall cross-layer architecture, which adequately solves these critical problems with the coordinated action of advanced algorithms.

TABLE 1 | Summary of the existing clustering and routing algorithms in VANET.

Author(s) and year	Algorithm	Outcomes	Limitations	How proposed work overcomes the limitations	Points observed from existing works related to proposed work
Gayathri et al. (2024) [14]	CSKAS-VANET with RBMA and signcryption	Demonstrated improved cluster stability and secure communication with low computational requirements.	Lacks extensive testing under various mobility scenarios and potential attack conditions.	Proposed M-BHC and CL-MABRC algorithms are evaluated under dynamic mobility and attack models to ensure robustness.	Existing work highlights need for adaptable, mobility-aware clustering and secure communication.
Odiagbe et al. (2024) [15]	Hybridized framework for congestion prediction and rerouting	Achieved better traffic management by reducing congestion through real-time predictions and adaptive routing.	Scalability issues in larger network deployments remain unexplored.	Our approach employs EPOA and blockchain-integrated routing to ensure scalability and resilience in large-scale VANETs.	Adaptive routing and congestion management are critical to maintaining performance in dense traffic scenarios.
Kaur et al. (2023) [16]	Fr-Aro: Fuzzy clustering with hybrid optimization routing	Enhanced routing efficiency with reduced packet loss and extended network lifespan in VANETs.	Performance under heavy traffic loads and energy efficiency require further analysis.	The proposed CL-MABRC optimizes routing with cross-layer metrics and energy-aware decisions using EPOA.	Energy optimization and cross-layer design are essential for reliable VANET routing.
Monisha et al. (2023) [17]	Grasshopper optimization and modified key agreement	Improved relay selection in traffic-congested areas, ensuring higher security and reliability.	Increased computational overhead during the authentication process.	Our method ensures lightweight security using efficient blockchain validation mechanisms.	Secure relay and CH selection must balance overhead and computational complexity.
Qazi et al. (2024) [18]	Security-focused efficient routing algorithm	Enhanced security and routing performance in VANETs, protecting against various attacks.	Comparative analysis with existing methods is limited.	The proposed work includes comprehensive performance comparisons across 13 metrics with baseline algorithms.	Benchmarked evaluation helps establish practical utility and robustness.
Kaur et al. (2024) [19]	Jellyfish search and chimp optimization for SDN-VANET	Demonstrated effective attack detection and secure routing through adaptive optimization techniques.	Exhibits higher latency under rapidly changing network conditions.	CL-MABRC introduces congestion-aware adaptive routing and blockchain to reduce delay in dynamic topologies.	Optimization-based secure routing must also ensure low latency under topology variation.

(Continues)

TABLE 1 | (Continued)

Author(s) and year	Algorithm	Outcomes	Limitations	How proposed work overcomes the limitations	Points observed from existing works related to proposed work
Kadam et al. (2023) [20]	TACR: Trust-aware clustering-based routing	Ensured reliable communication by incorporating trust evaluation metrics into routing decisions.	Vulnerable to insider threats within the trust evaluation mechanism.	Blockchain-based route validation in CL-MABRC mitigates insider threats via decentralized trust models.	Insider threat resistance and trust validation are key gaps in conventional trust-based routing.
Ali et al. (2024) [39]	RCSRC: Cryptographic clustering for secure communication	Achieved secure and dependable data exchange with minimal packet loss.	High computational demands pose challenges for resource-constrained environments.	Our work utilizes lightweight yet effective clustering and routing models, ensuring energy-efficiency and security.	Security models must align with energy and resource constraints in VANETs.
Swamynathan et al. (2024) [40]	Blockchain and deep learning-based trusted routing	Delivered robust traffic prevention and enhanced network security through decentralized trust mechanisms.	Requires real-world implementation to evaluate scalability and performance.	Our simulations use realistic mobility models and varied scenarios to approximate real-world conditions.	Trust-based secure routing frameworks must prove scalability and practical applicability.

- Unlike traditional clustering algorithms, which rely on local or fixed parameters, the mobility-based hierarchical clustering (M-BHC) algorithm proposes a dynamic mobility prediction system. This method guarantees the long-term stability of the clusters, as the cluster memberships are adapted to changes in real time according to the predicted vehicle routes, which allows them to avoid frequent re-clustering.
- Unlike other traditional CH selection algorithms that do not consider changes in energy, the EPOA uses an energy-sensitive approach that uniformly distributes the communication load in the network. This innovation will enhance the lifetime of the network, particularly in energy-constrained conditions, such as those associated with VANETs.
- Cross-layer multi-attribute blockchain-enabled routing with congestion control (CL-MABRC) logic entails the combination of routing intelligence and security. Compared with current routing models, it takes into account and simultaneously considers the quality of links, level of trust, and congestion rates when applying blockchain in distributed trust verification. This is a cross-layer integration that is new for maintaining data integrity and network efficiency.
- In addition, the proposed system has a congestion-aware adjustment mechanism with real-time rerouting data that are dynamically adjusted according to the network load, maximizing throughput and minimizing latency. Traditional VANET routing protocols rarely accommodate this type of responsiveness.
- Finally, the incorporation of blockchain not only authenticates routing decisions but also prevents route tampering and black hole attacks in a decentralized manner, providing a secure-by-design approach that is not commonly found in previous work.

3 | Proposed Methodology

This work describes the suggested methodology, which combines three unique algorithms designed to overcome the fundamental difficulties in VANETs. The dynamic nature of VANETs, which includes high mobility, frequent topology changes, and congestion difficulties, requires improved clustering, CH selection, and secure routing. The proposed approach uses M-BHC, EPOA, and CL-MABRC to enable consistent communication, energy-efficient CH selection, and secure congestion-free routing, respectively. The M-BHC algorithm solves the instability induced by frequent clustering in high mobility settings. M-BHC automatically adjusts cluster membership based on vehicle mobility factors, such as speed, direction, and expected future positions, while maintaining stability and lowering communication OH. Meanwhile, the EPOA is suggested as an optimal CH selection algorithm that considers residual energy, network coverage, and node connection. This strategy ensures energy-efficient operations, which extend the lifespan of the network while ensuring a balanced load distribution. The CL-MABRC method integrates congestion-aware routing and secures blockchain validation. This cross-layer approach uses criteria such as network quality, vehicle mobility, and congestion levels to dynamically determine the best routes, whereas blockchain provides data integrity

and security. These techniques work together to create an appropriate network to address the main difficulties of VANETs, resulting in a scalable, reliable, and energy-efficient solution for vehicular communication networks. The following sections discuss the design and implementation of each algorithm.

Figure 2 illustrates the MBECR framework, which represents mobility-based black hole clustering with energy-aware congestion-controlled routing. The process begins with the formation of clusters using the M-BHC method. This is followed by the selection of an optimized CH through the EPOA, which considers various network attributes. In the final routing stage, the CL-MABRC is utilized to guarantee secure, congestion-aware, and efficient data transmission, and its performance is assessed using key metrics.

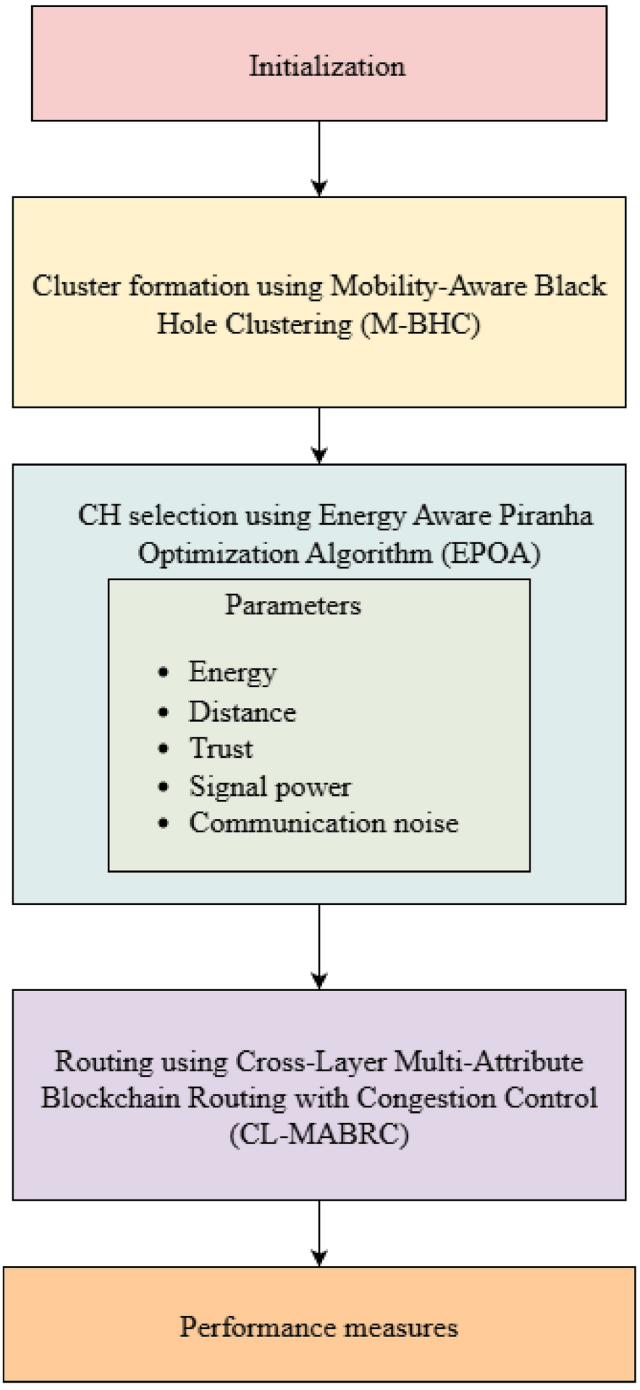


FIGURE 2 | Workflow of the proposed framework for VANET.

3.1 | Mobility-Aware Black Hole Clustering (M-BHC)

VANETs are dynamic networks established when vehicles communicate with one another and with the roadside infrastructure. Because of the high mobility of vehicles, the topology of VANETs changes quickly, posing routing and clustering challenges. Traditional clustering approaches struggle to maintain stable groups in changing environments. The M-BHC algorithm aims to alleviate this problem by incorporating mobility patterns into the clustering process. In classic BHC, a "black hole" is a vehicle that draws nearby vehicles based on its capabilities such as position, speed, and communication range. The black hole node serves as the cluster leader, coordinating routing and data transfer. However, because of the fast speed of vehicles and frequent topology changes in VANETs, utilizing a static clustering solution is wasteful. Consequently, mobility awareness was used to address these difficulties. The mobility-aware BHC algorithm improves on the classic BHC by considering vehicle movement. Mobility is represented by factors, such as speed, direction, and relative position, which are used to predict the future locations of vehicles. This prediction aids in identifying stable CHs and lowering the OH associated with frequent re-clustering. Figure 3 shows the M-BHC clustering diagram.

Clusters are formed from vehicles within the communication range of the CH. The range is calculated dynamically using the mobility estimate and available gearbox power. The mobility-aware BHC algorithm offers various advantages for VANETs. This approach lowers the OH associated with continual cluster reformation by considering vehicle movement patterns. It improves cluster stability by dynamically selecting the most appropriate vehicle as the CH, thus mitigating the impact of increased mobility. Furthermore, owing to stable CHs and fewer topology changes, the communication OH is reduced, thereby increasing the total network efficiency. The M-BHC

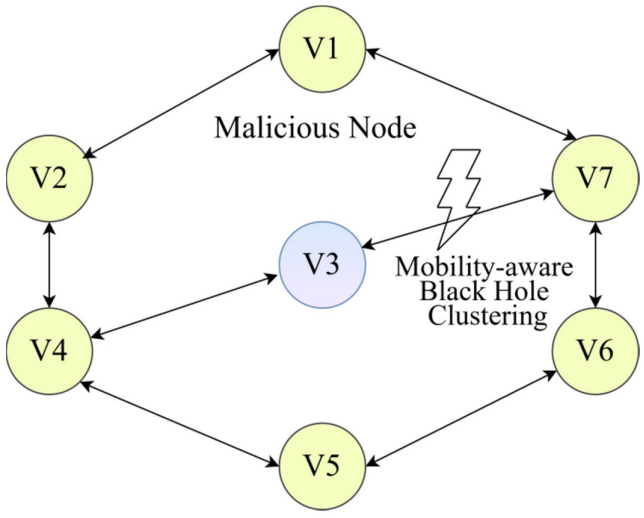


FIGURE 3 | M-BHC clustering algorithm.

algorithm provides a powerful clustering solution for highly dynamic VANET systems. By integrating mobility prediction with the conventional black hole concept, it accommodates the dynamically evolving topology of VANETs, thereby facilitating efficient clustering, stable communication, and minimal OH. This renders it a promising approach for real-time VANET applications, including traffic management and vehicle-to-vehicle communication.

The M-BHC method for VANETs is not based on a clear cluster selection. Instead, it uses mobility prediction, dynamic adjustment of communication ranges, and adaptive clustering to increase network stability and efficiency. This is referred to as mobility prediction, and it involves a simple motion model whereby the position of a vehicle in the future is forecasted. This is achieved by subtracting the product of the time step and average velocity at the current position of the vehicle. The mobility prediction (Equation 1) is as follows:

$$P_{pred} = P_{current} + \Delta_t \cdot V_{avg} \tag{1}$$

where P_{pred} denotes the expected position of the vehicle is, $P_{current}$ is the current position, Δ_t is the time step, and V_{avg} is the vehicle's average velocity. This prediction allows the system to predict the positions of vehicles in the near future, affording it the benefit of dynamism in an environment such as that of a VANET. The second critical concept is distance-based stability, which evaluates the relative stability of a vehicle concerning nearby traffic. The future positions are expected to affect vehicle stability. The Euclidean distance between two vehicles, V and $V_{neighbor}$, is based on the coordinates of the vehicles.

This estimated distance is necessary to cluster vehicles in groups with close proximity and relative mobility, which is essential for ensuring efficient communication in the network. The second notable characteristic of the M-BHC algorithm is the dynamic estimation of the communication range. In a highly mobile VANET, the communication range of vehicles should be set to their velocity and estimated location to ensure the best connection. The communication range is determined by the difference in speed between the vehicle and its surroundings. The communication range was calculated using Equation (2). In Equation (2), the communication range R_{comm} is dynamically adapted based on relative vehicle speeds to enhance the stability of cluster formation in high-mobility VANET environments. The parameters are determined as follows:

$$R_{comm} = R_{max} \cdot \left(1 - \frac{|\, V_{speed} - V_{avg} \,|}{V_{max}}\right) \tag{2}$$

- V_{speed}: This is the current (instantaneous) speed of the vehicle for which the communication range is being calculated. In this work, it is directly obtained from the random waypoint mobility model, where each vehicle selects a random destination and speed (within a defined range) and moves accordingly. The simulation framework tracks this speed in real time for each vehicle during mobility transitions.
- V_{avg}: This denotes the average speed of neighboring vehicles within the local vicinity (i.e., vehicles within the communication range or within a cluster). It is computed as follows:

$$V_{avg} = \frac{1}{N} \sum_{i=1}^{N} V_{speed}^{i} \tag{2a}$$

where N is the number of neighboring vehicles and V_{speed}^{i} is the speed of the ith vehicle. This value captures the collective mobility trend in the local region.

- V_{max}: This is the maximum allowable speed defined in the simulation environment, acting as normalization constant. It ensures that the computed speed deviation is scaled to a [0, 1] range for consistent control over range adaptation.R_{comm} refers to the dynamic communication range of a vehicle in the proposed M-BHC algorithm. It represents the effective distance within which a vehicle can reliably communicate with its neighboring nodes, and it varies based on the vehicle's mobility characteristics. Unlike a fixed communication radius, R_{comm} is adaptively calculated using the instantaneous speed of the vehicle V_{speed}, the average speed of all vehicles in the network V_{avg}, and the maximum allowed speed V_{max}. This adaptive adjustment helps maintain stable clustering in high-mobility VANET environments by dynamically resizing the communication range based on how similar a vehicle's speed is to the average speed in the network.

R_{max} is the greatest allowable communication range, V_{speed} is the vehicle's speed, V_{avg} is the average speed of adjacent vehicles, and $Vmax$ is the network's maximum speed. This equation guarantees that vehicles have a communication range appropriate for their motion, reducing excessive communication OH. This algorithm groups vehicles into clusters depending on their closeness to one another. The grouping requirement is that the distance between two vehicles, V and $V_{neighbour}$, is less than or equal to the communication range in Equation (3).

$$d\left(V, V_{neighbour}\right) \leq R_{comm} \tag{3}$$

where $d\left(V, V_{neighbour}\right)$ denotes the Euclidean distance between vehicle V and its neighboring vehicle $V_{neighbour}$, V denotes the current vehicle under consideration, $V_{neighbour}$ denotes the neighboring vehicle within the communication range, and R_{comm} dynamic communication range of vehicle V. If this criterion gets satisfied, each vehicle are considered members of the same cluster. This strategy aids in the effective organization of vehicles, minimizing the need for continual re-clustering as they travel. Because VANET vehicles are highly mobile, the clusters must be dynamically adjusted to suit variations in mobility. This adaptation is activated when the relative distance between a vehicle and the cluster centre reaches a predetermined threshold, δ_{adapt}. The adaption condition is phrased as follows in Equation (4):

$$d(V, ClusterCenter) > \delta_{adapt} \tag{4}$$

where $d(V, ClusterCenter)$ represents the distance between vehicle V and the cluster center, $ClusterCenter$ is the geometric center of the current vehicle cluster, and δ_{adapt} is the adaptive re-clustering threshold that triggers cluster reformation. This ensures that the

clustering structure remains relevant and efficient as vehicles move, reducing the communication OH caused by improperly fitted clusters. Finally, the relative speed of a vehicle and the group's average speed influences the group's stability. The stability score S_{group} for a vehicle group is determined using the distance to the group centre and the difference in speed between the vehicle and the group's average speed in Equation (5).

$$S_{group} = \frac{1}{1 + d\left(V, V_{group}\right) + \mid V_{speed} - V_{group\ speed} \mid} \tag{5}$$

where S_{group} denotes the stability score of the vehicle group, V_{group} denotes the representative vehicle or centroid of the cluster, $d\left(V, V_{group}\right)$ represents the distance between vehicle V and the group representative, V_{speed} denotes the instantaneous speed of vehicle V, and $V_{group\ speed}$ is the average speed of vehicles within the cluster. This equation plays a role in selecting the most stable grouping of vehicles, which is critical for reducing communication disruptions produced by vehicles with high relative mobility. The M-BHC method for VANETs uses these equations to dynamically change communication ranges, anticipate vehicle movements, and group vehicles based on mobility patterns. By avoiding explicit CH selection and focusing on mobility awareness, the method significantly decreases the OH of frequent re-clustering, resulting in more stable and efficient communication in the highly dynamic VANET environment. The algorithm 1 shows the pseudocode for M-BHC.

In the M-BHC algorithm, the predicted positions of vehicles are used when calculating the distances between the current vehicle, its neighbors, and the cluster centers. This is achieved through the mobility prediction model outlined in Equation (1), allowing the algorithm to proactively adjust clusters based on anticipated vehicle movement, thereby enhancing stability in dynamic VANET environments. Regarding the calculation of the communication range R_{comm}, the current model primarily considers relative speed to dynamically adjust the range, focusing on minimizing OH due to mobility. Although signal power and communication noise are not explicitly included, this simplification was made to reduce computational complexity and enable real-time execution in resource-constrained vehicular systems. Incorporating such physical-layer factors is indeed valuable and is noted as a potential extension in future work to further improve reliability. Lastly, although the current clustering mechanism does not explicitly limit the number of vehicles per cluster, it relies on adaptive re-clustering triggered by the threshold δ_{adapt} and stability score S_{group}, which naturally limits cluster size by reorganizing overly large or unstable clusters. However, we acknowledge that introducing a hard cap on cluster size could prevent communication congestion and will be considered in future enhancements of the M-BHC algorithm.

3.1.1 | Black Hole Attack Mitigation and Security Considerations in M-BHC

In the proposed M-BHC framework, black-hole-style malicious behavior is mitigated through mobility consistency enforcement rather than explicit cryptographic detection. Malicious vehicles in VANETs often attempt to attract traffic by advertising favorable metrics while failing to maintain stable spatial or mobility behavior. M-BHC limits such behavior by continuously evaluating real-time mobility patterns, relative distances, and group stability. Mobility prediction plays a central role in this process. Each vehicle's expected position is estimated using a motion model and compared with its observed movement. Vehicles that exhibit persistent deviations between predicted and actual mobility patterns are considered unstable and are excluded during adaptive re-clustering. This prevents malicious nodes from maintaining artificial cluster dominance. Distance-based clustering further restricts malicious influence. Vehicles are grouped only when the dynamic distance constraint is satisfied, and adaptive re-clustering is triggered when a node exceeds

ALGORITHM 1 | Mobility-aware black hole clustering.

```
Input:  (P_current), (V_speed), (V_avg), (Rmax), (Δ_t), (δ_adapt)
Output: Vehicle clusters
Initialize Vehicles.
    Set initial position P_current and V_speed
    Set initial communication range R_comm = Rmax
    Calculate predicted position P_pred based on current position and velocity:
    For each neighbouring vehicle V_neighbour
    Calculate the distance between V and V_neighbour
    Calculate R_comm dynamically based on speed and surrounding vehicles' speed
    If d(V, ClusterCenter) > δ_adapt, trigger re-clustering:
        Remove V from the current cluster
        Add V to a new cluster based on new positions and communication range.
    Calculate the stability score S_group for the vehicle group:
        If stability score S_group is high, keep V in the current group
        If stability score S_group is low, consider re-grouping V based on its stability score
    The vehicles are now grouped into stable clusters based on mobility awareness.
```

the stability threshold. Nodes that repeatedly violate these constraints are automatically isolated from clusters, thereby reducing their ability to attract or retain neighboring vehicles.

The group stability score integrates spatial proximity and relative speed similarity. Vehicles exhibiting abnormal speed deviations or unstable positioning receive lower stability scores and are gradually removed from cluster influence. Importantly, M-BHC avoids static cluster-head selection, reducing the attack surface associated with leader-centric black hole attacks. The framework also demonstrates inherent resilience to Sybil attacks. Since clustering decisions depend on physical mobility characteristics, multiple forged identities originating from the same location cannot simultaneously satisfy independent mobility and distance constraints. Overall, M-BHC provides an efficient, low- OH, mobility-driven mitigation mechanism that enhances clustering security in highly dynamic VANET environments.

3.2 | Energy-Aware Piranha Optimization Algorithm (EPOA) for CH Selection

VANETs have emerged as a crucial technology for enabling efficient communication within the transport systems. The dynamic topology, elevated mobility, and limited resources of VANETs present significant challenges to cluster formation and CH selection. The EPOA provides a novel and efficient CH selection mechanism that guarantees energy efficiency, stability, and scalability in VANETs. The algorithm reduces energy consumption during CH selection through a tripartite strategy: initially filtering CH candidates to decrease computational demands, prioritizing localized cluster formation to limit long-distance communication and conserve energy, and utilizing an energy-based fitness assessment that favors nodes with greater residual energy for CH positions. This comprehensive strategy ensures optimal energy use and increases the network longevity and overall efficiency. The EPOA is intended to handle the high dynamic and mobility topologies of VANETs. This technique ensures flexibility by partitioning the network into smaller, more manageable clusters, depending on geographic closeness. The EPOA was inspired by piranhas' collective predatory activity, which is recognized for its coordinated and efficient hunting techniques. This work is designed to optimize CH selection by balancing energy usage, communication OH, and cluster stability.

3.2.1 | Mathematical Model of EPOA

Localized group attack, bloodthirsty cluster attack, and scavenging foraging are EPOA patterns. Its main tasks are population initialization, evaluation, and parameter and agent location updates. Population candidate solutions can be expressed as follows using EPOA in Equation (6):

$$X = = \begin{bmatrix} x_{1,1} & \cdots & x_{1,2} \cdots & x_{1,D} \\ \vdots & \ddots & \vdots \ \iddots & \vdots \\ x_{2,1} & \cdots & x_{2,2} \cdots & x_{2,D} \\ \vdots & \iddots & \vdots \ \ddots & \vdots \\ x_{n,1} & \cdots & x_{n,2} \cdots & x_{n.D} \end{bmatrix} \tag{6}$$

$x_i = \left[x_{i1} x_{i2} \ \ldots \ x_{iD}\right]$ position vector representing piranhas.

Step 1: Initialize the position vectors of each individual in the piranha population using Equation (7).

$$x_i = lb_i + \beta_1 \times \left(ub_i - lb_i\right) \tag{7}$$

In the piranha candidate solution, x_i denotes the position of the i^{th} individual, whereas the upper and lower boundaries (ub_i *and* lb_i) of the piranha search in the habitat are represented accordingly. β_1 denotes a stochastic value inside the interval [0, 1].

Step 2: Specify the predation intensity parameter. Piranhas exhibit an acute ability to detect blood, with their responsiveness influenced by the blood concentration (F_i) as described in Equation (8) and the distance (d_i) as outlined in Equation (9) between the prey and the piranha. They are drawn to regions with higher blood concentrations; the more concentrated the blood, the faster they move, leading to the formulation in Equation (10).

$$F_i = \beta_2 \times \frac{Z_i}{4\pi d_i^2} \tag{8}$$

$$d_i = x_{prey} - x_i \tag{9}$$

$$Z_i = \left[x_i(t) - x_{i+1}(t)\right]^2 \tag{10}$$

where F_i represents the predation intensity parameter that pertains to the location of the i^{th} individual piranha, and the d_i distance represents the spatial separation between the i^{th} individual piranha and the prey (best solution). Z represents the source intensity, whereas Z_i denotes the intensity seen by the i^{th} search agent, which will fluctuate in real time as the agents persist in their pursuit, and is a β_2 random number ranging from 0 to 1.

Step 3: Nonlinear parametric control systems govern time-varying randomized processes, prevent premature population convergence, and smooth the transition from exploration to exploitation. Higher values of S let the search agent undertake an auditory-based global search and avoid getting stuck in a local optimum in the early and middle stages of PFOA, but as S changes, PFOA can converge faster in Equation (11).

$$S = C \cdot cos\left[\frac{\pi}{2} \otimes \left(\frac{t}{Max_{iter}}\right)\right]^4 \tag{11}$$

where Max_{iter} indicates the maximum iterations, S denotes the nonlinear control parameter, and C is a value-variable product.

Step 4: Reverse escape search. Flag E is applied in the reverse escape search to prevent the candidate population from becoming confined to a particular region and to enhance the solution by steering the search toward another location. This recurs throughout the search, providing the search agent with additional opportunities to meticulously examine the area in Equation (12).

$$E = \begin{cases} 1 & \beta_3 \leq 0.5 \\ -1 & \beta_3 > 0.5 \end{cases} \tag{12}$$

where E denotes the reverse escape flag used to alter the search direction, rand is a random number in the range [0,1], and β_3 represents a random number between 0 and 1.

Step 5: Update the proxy location formula.

1. The Localized Group Attack Pattern

2. The Bloodthirsty Cluster Assault Pattern

$$x_i(t+1) = \gamma_1 \sum_{k=1}^{pc} \frac{Lk(t) - xi(t)}{pc} - x_{prey}(t) \tag{13}$$

$$x_i(t+1) = \gamma_1 * e^{\gamma_2} * x_{pery}(t) + G * x_{pery}(t) * E * F_i + E * \beta_4 * S * F_i \tag{14}$$

It assaults prey several times its size as a social forager when in need of sustenance. Upon the entry of prey into their environment, a splash of water occurs, prompting the keenly sensitive piranhas to rapidly surround and bite the prey, beginning with the closest individual. Equation (13) represents localized group assault.where $x_i(t+1)$ is the new location of the search agents, pc is a randomly generated integer, and $Lk(t)$ is the fraction of local population attacks that are undertaken to commence the attack initially, where $L \in X$ and X represents the number of randomly produced piranhas. $x_i(t)$ represents the current agent's position, $x_{prey}(t)$ is the location of the best agent found in the previous iteration, and $\gamma 1$ is a random value uniformly distributed in [−2,2] that affects the piranha's trajectory.

Distant piranhas converge into the vicinity of an injured and bleeding victim, attacking with increased ferocity in response to the elevated blood concentration. Piranhas possess a distinct preference and olfactory sensitivity to blood. Viscous blood exhibits increased velocity. At this point, the blood content F_i, the distance d_i between piranhas and their prey, and the nonlinear cosine factor S, influenced by E, are significant. Piranhas can evade local optima and discover superior prey by altering their orientation (Equation 14).

where $x_i(t+1)$ denotes the new location of the search agent, $x_{pery}(t)$ denotes the location of the best agent found in the previous iteration, γ_1 is a random number uniformly distributed in [−2, 2], γ_2 is a random number uniformly distributed in [−1/2, 1/2], and β_4 is a random number between 0 and 1. The coefficient of piranhas' foraging ability, G, is an integer greater than or equal to 5. $\gamma_1 * e^{\gamma_2}$ has uniform dispersion, enabling dynamic adjustment and trade-offs between global and local search capabilities.

3. The Scavenging Foraging Patterns

Owing to its restricted vision, piranhas separate from the group while foraging in murky waters and nocturnally, swimming erratically as solitary entities, consuming carrion and seeds as delineated in Equation (15), employing vector analysis.

$$x_i(t+1) = \frac{1}{2}\left[e^{\gamma_2} * xC_1(t) - E * x_i(t)\right] \tag{15}$$

where $x_i(t+1)$ denotes the new position of the search agent, γ_2 is a random number evenly distributed in [−1,1], E is a variable that alters the direction of movement, $xC_1(t)$ denotes the position of the c1st agent randomly selected from the piranhas, $x_i(t)$ denotes i^{th} the position of the agent spontaneously selected from the agents, and C1≠i.4). The population growth of piranhas is constrained by their reproductive characteristics and natural predators. To maintain population diversity, the agent's survival rate (SR) is initially calculated using Equation (16). When the SR is below 1/4, the offspring population is generated using Equation (17):

$$SR(i) = \frac{fitness_{Max} - fitness(i)}{fitness_{Max} - fitness_{Min}} \tag{16}$$

$$x_i(t+1) = x_{prey}(t) + \frac{1}{2}\left\{\left[xC_1(t) - E * xC_2(t)\right] - \left[xC_2(t) - E * xC_3(t)\right]\right\} \tag{17}$$

where $x_i(t+1)$ is the new location of the searching agent, $x_{prey}(t)$ indicates the position of the optimal agent identified in the preceding iteration, E represents the parameter for altering the direction $xC_1(t), xC_2(t), xC_3(t)$, and C_1, C_2, C_3 denote the agent positions chosen at random from the piranhas with $C_1 \neq C_2 \neq C_3$, respectively. Algorithm 2 represents the EPOA pseudo-code. Figure 4 illustrates the flowchart for EPOA.

The EPOA technique gains a FF utilizing four input parameters distance to neighbors, energy for CH selection, trust level, and signal power, and communication noise. Distance to a neighbor: It can be relevant to choose CH with lesser distance between adjacent nodes. During the intracluster transmission system, power utilization of sensor to CH communication. Once the neighboring node distance is minimalized, then the energy of the intracluster broadcast can be minimized correspondingly. Objective 1: Minimizing

$$f_1 = \sum_{j=1}^{m} \frac{1}{l_j}\left(\sum_{i=1}^{l_j} dis\left(CH_j s_i\right)\right) \tag{18}$$

Trust factor (TF): Primarily, every single node states that TF is 1. The TF value can be decreased with an anomalous forecast system, but the node procedure is an abnormal task, and the nodes were termed as malicious nodes.

Objective 2: Maximizing

$$f_2 = \sum_{j=1}^{m} \frac{1}{m}\left(TF_j\right) \tag{19}$$

Energy: It is the energy count exhausted as CH to RE of CH. If the CH exploits a lesser energy process, the sensing, as well as broadcast procedure with greater RE, was gathered at a lower energy ratio. Thus, with a lower energy ratio, CH selective growth is more possible.Objective 3: Minimizing

$$f_3 = \sum_{j=1}^{m} \frac{E_c\left(CH_j\right)}{E_R\left(CH_j\right)} \tag{20}$$

Signal Power and Communication Noise: To enhance the reliability of wireless communication. Signal-to-noise ratio (SNR)

ALGORITHM 2 | Energy-Aware Piranha Optimization Algorithm (EPOA).

```
Initialize Parameters:
Set population size, maximum iterations (Max_iter).
Define upper(u_b) and lower (l_b) boundaries for the search space.
Initialize the position of each search agent using equation(7)
Evaluate Initial Population:
Calculate fitness of each agent based on the objective function.
Identify the position of the best agent (X_prey) and its fitness.
While t <Max_iter:
Update predation intensity parameter Fi for each agent using equation(10)
Update the non-linear control parameter S using equation (11)
Apply reverse escape search strategy using equation (12)
Update agent positions based on foraging patterns:
        Localized Group Attack Pattern using equation (13)
        Bloodthirsty Cluster Attack Pattern using equation (14)
        Scavenging Foraging Pattern using equation (15)
        Calculate survival rate SR
Reproduce offspring if SR ≤1/4 using equation (16)
Evaluate the fitness of all agents.
Update X_prey  with the position of the best agent
End While
The best solution X_prey and its fitness value
End
```

is now integrated into the FOA decision process. A higher SNR implies stronger signal quality and lower communication errors.

$$f_4 = \sum_{j=1}^{m} \left(\frac{P_{tx}(CH_j)}{P_{noise}(CH_j)} \right) \tag{21}$$

where m denotes the total number of clusters, l_j denotes the number of nodes in cluster j, $dis(CH_j, s_i)$ represents the distance between the CH and sensor node s_i in cluster j, $E_c(CH_j)$ is the energy consumed by CH j, $E_R(CH_j)$ is the residual energy of CH j, $P_{tx}(CH_j)$ denotes the transmission power of CH_j, and $P_{noise}(CH_j)$ represents an aggregate environmental and inter-node noise affecting CH_j.

The SNR value directly influences the reliability of data reception and packet delivery at the CH. Incorporating this into the objective function ensures that CHs are not only energy-efficient and trustworthy but also communicatively robust.

In the FOA system, a weighted linear combination of the objectives is minimized to determine optimal CHs:

$$\text{Minimize } F_{total} = \alpha_1 . f_1 + \alpha_2 . (1 - f_2) + \alpha_3 . f_3 + \alpha_4 . \left(\frac{1}{f_4} \right) \tag{22}$$

Subject to: $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$.

$$\alpha_2 \geq (\alpha_1 + \alpha_3 + \alpha_4)$$

$$0 < f_1, f_2, f_3, f_4 < 1$$

where $\alpha_1, \alpha_2, \alpha_3$, and α_4 denote the weighting coefficients and f_1, f_2, f_3, and f_4 represent the objective function. The proposed CH selection algorithm based on EPOA enhances communication efficiency in VANETs by employing numerous fitness criteria, such as energy, distance, throughput, trust, and entropy, while regulating the cluster size with explicitly set upper and lower membership thresholds. The maximum cluster size is limited to prevent communication bottlenecks, excessive interference inside the cluster, and rapid depletion of CH energy, whereas a minimum threshold guarantees that the CH contribution remains substantial and resource-efficient. In the fitness examination, prospective CHs who surpass or do not meet these thresholds are penalized, diminishing their likelihood of selection. These thresholds are dynamically modified based on the real-time vehicle density and movement patterns to ensure adaptability. This method guarantees that each CH maintains an ideal membership size, thus optimizing load distribution, reducing packet collisions, and improving routing stability in highly dynamic VANET situations.

3.2.2 | Comparative Analysis of Bio-Inspired Optimization Algorithms

Table 2 presents a comparative analysis of representative bio-inspired optimization algorithms in terms of exploration–exploitation balance, convergence speed, computational complexity, and suitability for VANET cluster-head selection. Traditional methods such as PSO, ACO, GA, and ABC exhibit

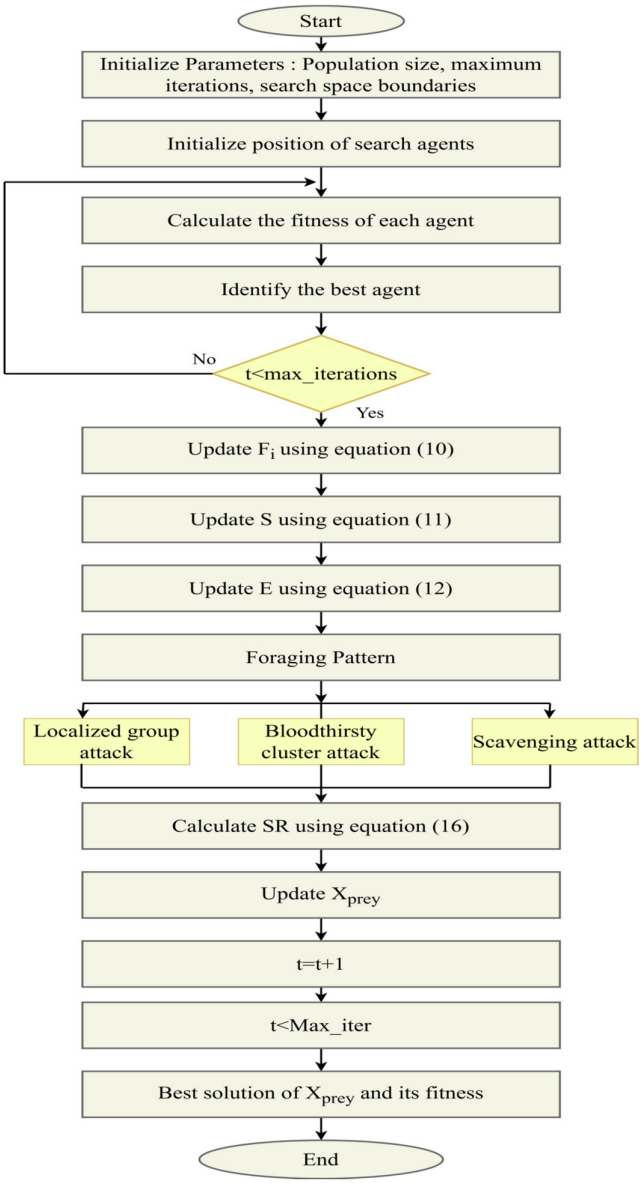


FIGURE 4 | Flowchart of EPOA.

limitations in dynamic vehicular environments due to premature convergence, slow iterative updates, or increased computational OH. In contrast, the proposed EPOA achieves a balanced exploration–exploitation trade-off with faster convergence and lower complexity. These characteristics make EPOA well suited for real-time, energy-efficient, and stable cluster-head selection in highly dynamic VANET scenarios.

3.3 | Cross-Layer Multi-Attribute Blockchain Routing With Congestion Control (CL-MABRC)

The CL-MABRC algorithm is a sophisticated routing approach intended for dynamic and resource-constrained networks, such as VANETs. The main innovation of CL-MABRC is its use of cross-layer optimization, multi-attribute decision-making, and blockchain technology to provide efficient, safe, and congestion-free routing, addressing the difficulties of high mobility, limited bandwidth, and security concerns in VANETs. CL-MABRC integrates many layers of the network stack (physical, data connection, network, and application) to optimize routing decisions. This cross-layer technique enables the algorithm to make real-time judgments using network state information such as the available bandwidth, vehicle speed, communication range, and congestion status. CL-MABRC improves the VANET data transmission efficiency by adjusting routing decisions to current network conditions across different levels. Traditional routing algorithms in VANETs frequently focus on a single measure such as the shortest path or hop count. However, CL-MABRC employs multi-attribute decision-making (MADM) to assess routes based on a variety of essential factors, such as vehicle speed, network quality, congestion state, security needs, and battery power. This ensures that routing decisions are made with a comprehensive view of the network, thereby increasing the reliability and efficiency of data transport in complex, rapidly changing VANET systems. Figure 5 depicts a block diagram of CL-MABRC.

CL-MABRC uses blockchain technology to deliver routing information that is decentralized, safe, and transparent. The

TABLE 2 | Comparative analysis of bio-inspired optimization algorithms for CH selection in VANET.

Algorithm	Exploration	Exploitation	Convergence speed	Computational complexity	Suitability for VANET CH selection
PSO (particle swarm optimization)	Moderate	Moderate	Medium	Low	May converge prematurely in dynamic VANETs
ACO (ant colony optimization)	High	Low	Slow	Medium	Iterative pheromone update slows real-time decision
GA (genetic algorithm)	High	Moderate	Medium	Medium-High	Crossover/mutation increases overhead for dynamic networks
ABC (artificial bee colony)	Moderate	Moderate	Medium	Medium	Balances search but may stagnate in large VANETs
EPOA (proposed)	High	High	Fast	Low	Rapid, adaptive, stable for real-time cluster-head selection

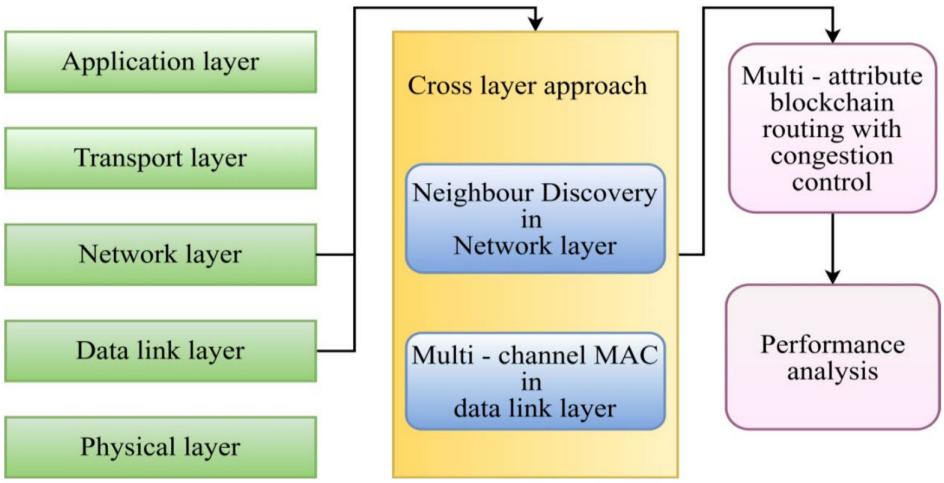


FIGURE 5 | Block diagram of CL-MABRC.

immutability of blockchain ensures that routing decisions are tamper-proof, lowering the danger of malevolent attacks, such as man-in-the-middle or Sybil attacks. The use of smart contracts allows for the automation of routing decisions, which improves routing efficiency and autonomy. CL-MABRC stands out for its capacity to dynamically manage network congestion. The program continuously detects network congestion and adapts the routing paths accordingly. This prevents packet loss and delays, resulting in optimal throughput. When congestion is detected, CL-MABRC dynamically finds alternate channels to reduce network congestion while ensuring reliable communication.

The CL-MABRC monitors each node's queue length and transmission delay to detect congestion. If the congestion level surpasses a certain threshold, the algorithm generates an alternate path using a modified version of Dijkstra's algorithm. The congestion detection formula is given by Equation (23).

$$Congestion\ Level = \frac{Queue\ Length}{Max\ Queue\ Length} + \frac{Transmission\ Delay}{Max\ Transmission\ Delay} \tag{23}$$

If the congestion level C_{level} exceeds a predetermined threshold C_{thresh}, the algorithm initiates a reroute. A variety of factors influence the routing decision, including LQ, vehicle speed, and congestion state. CL-MABRC employs a weighted sum method to compute a routing metric M_{route} for each path in Equation (24):

$$M_{route} = w_1 \cdot LQ + w_2 \cdot V_{speed} + w_3 \cdot \left(1 - C_{status}\right) \tag{24}$$

where M_{route} denotes the routing metric; w_1, w_2, and w_3 represent the weights allocated to each property; and LQ denotes the LQ. This multi-attribute metric ensures that the chosen method not only provides high connection quality but also considers vehicle mobility and congestion levels, resulting in improved overall network performance. Each routing choice is documented in a blockchain ledger to maintain transparency and avoid tampering. The blockchain validation process is expressed using Equation (25) as follows:

$$R_{validated} = H\left(P_{previous} \parallel P_{current} \parallel D_{timestamp} \parallel S_{signature}\right) \tag{25}$$

where $R_{validated}$ is the validated route in the blockchain ledger, $P_{previous}$ is the previous route's hash, $P_{current}$ is the current route's hash, $D_{timestamp}$ is the timestamp of the routing decision, and $S_{signature}$ is the cryptographic signature confirming the authenticity of the routing decision. The algorithm uses a dynamic congestion control factor C_{adjust} to adjust the routing paths based on realtime congestion levels. If the congestion exceeds a predefined threshold, the routing path is adjusted as follows using Equation (26):

$$C_{adjust} = \frac{C_{level}}{C_{thresh}} \cdot P_{alternative} \tag{26}$$

where $P_{alternative}$ represents the alternative route selected to avoid congestion, C_{level} represents the current measured congestion level of the active routing path, and C_{thresh} denotes the predefined congestion threshold beyond which route adaptation is triggered.

The CL-MABRC algorithm provides a unique approach for routing in VANETs. CL-MABRC enables efficient, safe, and stable routing in highly dynamic situations by combining cross-layer optimization, multi-attribute decision-making, blockchain, and congestion control. The algorithm's capacity to adapt to changing network conditions while retaining security and congestion-free operation makes it ideal for real-time applications, such as traffic management and V2V communication in modern VANETs. The CL-MABRC's usage of blockchain ensures openness and integrity in routing decisions, making it an advanced, future-proof solution for automotive networks. Algorithm 3 shows the pseudocode, and Figure 6 shows the flowchart of CL-MABRC.

3.4 | Proposed hybrid algorithm

Figure 7 shows a detailed flowchart depicting the integration of the M-BHC, EPOA, and CL-MABRC frameworks. Integration Architecture and Synergistic Operation: The integration of CL-MABRC with M-BHC and EPOA was achieved through a hierarchical cross-layer information-sharing mechanism that operated in three distinct phases. Phase 1 (Clustering

ALGORITHM 3 | Cross-Layer Multi-Attribute Blockchain Routing with Congestion Control (CL-MABRC).

```
Input: Vehicle positions and velocities, Available bandwidth and link quality (LQ), Queue
length and transmission delay, Congestion threshold (C_thresh), Routing attributes weights
(w1, w2, w3), Blockchain ledger for route validation
Output: Validated routing paths
Set initial positionP_current and velocity V_speed
  Set initial communication range R_comm based on vehicle's velocity
Set initial queue length and transmission delay.
For each road segment, initialize:  Link quality (LQ) and bandwidth information
Measure queue length (QL_V) and transmission delay (TD_V)
      Calculate congestion level C_level for V
  If C_level > C_thresh: Trigger congestion control and routing adaptation
  Calculate the routing metric M_route for each path
   Select the path with the highest M_routeas the preferred route
If congestion is detected, calculate alternative paths based on congestion level.
  Alternative Path = Calculate using dynamic routing metric and congestion control
    For each selected route:
  Generate route hash using the previous and current route information:
Record route hash in blockchain ledger for validation
   If congestion level C_level exceeds C_thresh, adjust the route
 Update route path to the new, congestion-free path
   Return the selected, validated routing path after considering congestion, link quality,
   and blockchain validation
       Repeat the Process
       For each time step Δt: Update vehicle positions, velocities, and network conditions
       Recalculate routing metrics and repeat congestion detection, multi-attribute
       decision-making, and blockchain validation
     End
```

Integration): M-BHC provides CL-MABRC with real-time data on the cluster topology, including cluster boundaries, mobility patterns from Equation (1), and black hole detection results. This enables the CL-MABRC to make routing decisions based on stable and secure cluster structures rather than individual vehicle positions. Phase 2 (CH Integration): EPOA supplies CL-MABRC with optimal CH information, such as energy levels, trust values, and multi-attribute fitness scores. CL-MABRC utilizes this information to prioritize routing paths through energy-efficient and trustworthy CHs, ensuring sustainable communication paths.

Cross-Layer Information Exchange Mechanism: The integration functions through a shared data structure that maintains (1) a cluster state matrix from M-BHC containing mobility vectors, cluster stability scores from Equation (5), and security status; (2) a CH performance vector from EPOA, including residual energy, fitness rankings, and SRs from Equation (16); and (3) a network condition matrix updated by CL-MABRC with congestion levels, blockchain verification status, and route quality metrics. This tri-directional information flow ensures that routing decisions in CL-MABRC are informed by both the clustering stability and energy optimization results. Optimal End-to-End Communication Delivery: This comprehensive framework achieves peak efficiency by employing adaptive route selection, where CL-MABRC modifies routing paths in response to M-BHC's predictions of cluster stability and EPOA's energy forecasts. It also proactively prevents congestion by utilizing M-BHC's mobility patterns to anticipate traffic bottlenecks and EPOA's energy distribution to evenly distribute the load among CHs. Additionally, it incorporates security-aware routing, with blockchain verification in CL-MABRC bolstered by M-BHC's black hole detection and EPOA's trust-based selection of CHs.

The proposed framework explicitly requires a set of initial parameters to initiate the clustering, optimization, and routing procedures. For the M-BHC algorithm, these include the initial vehicle positions $P_{current}$, instantaneous speeds V_{speed}, average neighborhood speed V_{avg}, maximum communication range R_{max}, time step Δ_t, and adaptive clustering threshold δ_{adapt}. For the EPOA-based CH selection, the residual energy of nodes, node connectivity, and cluster size distribution are required to guide the bio-inspired optimization. The CL-MABRC protocol additionally requires network topology information, LQ metrics, trust scores, and congestion thresholds to perform cross-layer route selection and blockchain verification. Multiple factors influence the final results, including node density, mobility patterns, initial energy allocation, and network load. Sensitivity to these factors was considered in the simulation design, and scenario-based variations were introduced to evaluate robustness. By defining these parameters upfront, the framework

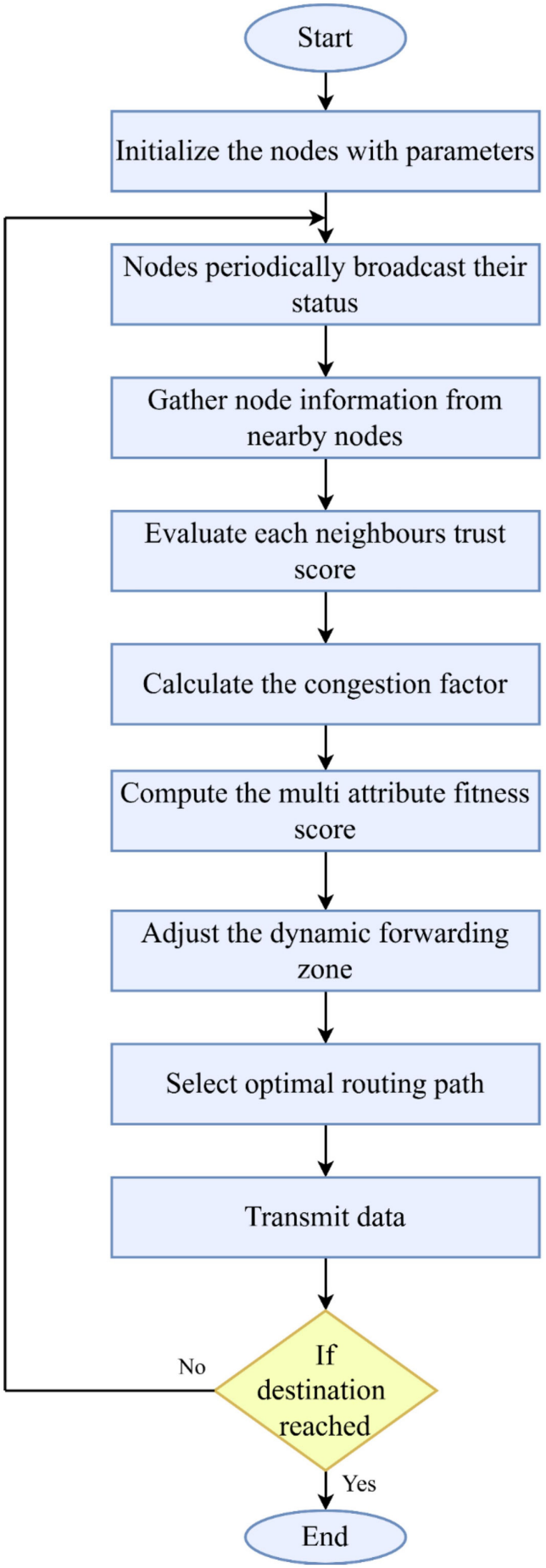


FIGURE 6 | Flowchart of CL-MABRC.

ensures reproducible, adaptive, and energy-efficient clustering and routing under diverse VANET conditions.

4 | Results and Discussion

The proposed method, which is implemented in MATLAB R2024a, simulates the VANET routing protocol with a secure route to provide user-specific composite services. The existing protocols—OSC-GOR [30], ELAACR [33], TMOHBA [44], and RCSRC [39]—were selected for comparison due to their close alignment with the key objectives and domains of the proposed approach. Specifically, these methods integrate security, clustering, trust management, and optimized routing, which are also the core focuses of our proposed M-BHC, EPOA, and CL-MABRC algorithms. The relation between the proposed and existing methods is outlined as follows:

- OSC-GOR: This method integrates security-aware clustering with geographical and opportunistic routing, similar to our M-BHC and CL-MABRC modules, which also emphasize mobility-aware clustering and cross-layer, secure routing. It serves as a baseline for assessing improvements in clustering stability and routing adaptability under dynamic VANET conditions.
- ELAACR: ELAACR utilizes location-based ACO for secure communication. This aligns with our use of position prediction and optimization techniques (EPOA) for efficient CH selection and adaptive routing. Comparing with ELAACR demonstrates how our model performs in both mobility-aware decisions and security-centric routing.
- TMOHBA: TMOHBA focuses on trust-based multi-objective optimization for secure routing. Our proposed framework incorporates multi-attribute trust evaluation and blockchain validation within CL-MABRC to further enhance routing reliability and security. Thus, TMOHBA is relevant for comparing trust-integrated security routing mechanisms.
- RCSRC: This cryptographic scheme focuses on secure cluster-based communication using cryptographic mechanisms. Our model similarly aims for secure data delivery but leverages blockchain for decentralized validation, providing a more scalable and tamper-resistant approach. Comparing with RCSRC highlights improvements in both security assurance and computational efficiency.

Not all existing methods such as OSC-GOR, ELAACR, TMOHBA, and RCSRC are readily available as pre-implemented modules or toolboxes in MATLAB. However, these protocols are algorithmically defined in the respective work publications, and their logic and workflows can be custom implemented in MATLAB using standard programming constructs, simulation parameters, and communication models. For the purpose of fair performance comparison, the algorithmic descriptions from the respective works were interpreted and implemented manually in MATLAB, ensuring

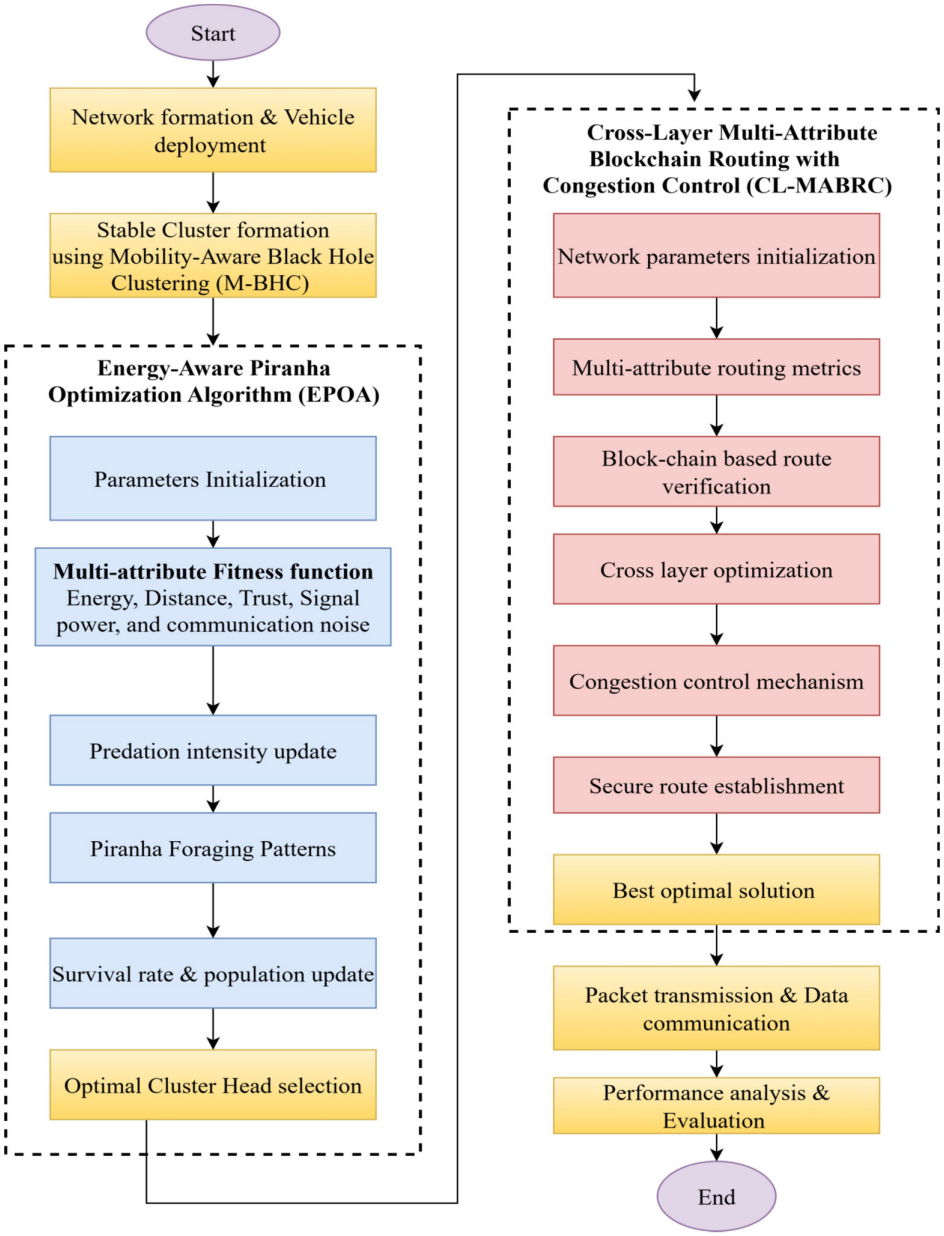


FIGURE 7 | Comprehensive flowchart of the integrated M-BHC, EPOA, and CL-MABRC framework.

that the comparison is based on equivalent simulation parameters, environmental settings, and performance metrics such as throughput, delay, energy consumption, and network security. Therefore, although pre-built MATLAB packages for these protocols may not exist, faithful MATLAB-based reproductions of these algorithms were created and validated to ensure accurate and meaningful comparisons with the proposed work.

The comparative evaluation in this study follows a two-level benchmarking strategy to ensure both rigorous quantitative validation and comprehensive state-of-the-art positioning. For simulation-level quantitative comparison, OSC-GOR, ELAACR, TMOHBA, and RCSRC were selected because they represent recent and well-established VANET routing and clustering approaches that can be consistently implemented and evaluated under identical simulation conditions. These methods collectively cover security-aware clustering, swarm-intelligence-based routing, trust-based multi-objective optimization, and cryptographic communication frameworks, which directly align with the core design objectives of the proposed M-BHC, EPOA, and CL-MABRC framework. Their algorithmic definitions, parameter settings, and operational assumptions enable fair, reproducible, and metric-consistent quantitative comparison within the same MATLAB-based simulation environment.

In addition to these baseline protocols, a broader set of recently published state-of-the-art VANET methods (2022–2025) is analyzed in Tables 4 and 5 to provide cross-study performance benchmarking. These methods include learning-based, federated, and dynamic load-balancing approaches that employ diverse experimental settings and network assumptions, making

direct simulation-level comparison impractical. Therefore, they are evaluated through literature-level comparison using reported performance metrics such as PDR, delay, and throughput. This dual-level comparison strategy ensures that the proposed framework is validated both through controlled quantitative simulations and through comprehensive benchmarking against contemporary VANET research trends.

4.1 | Simulation Parameters

The simulation parameters are shown in Table 3. MATLAB R2024a was chosen for implementation because of its strong simulation capabilities, built-in support for developing algorithms, and advanced visualization tools, which are ideal for the rapid prototyping and validation of new cross-layer and mobility-aware algorithms in VANET settings. The proposed CL-MABRC framework combines clustering, routing, congestion control, and blockchain validation, all of which require matrix-based processing, statistical analysis, and optimization routines. MATLAB provides optimized toolboxes, such as the communications toolbox and optimization toolbox, that efficiently facilitate these computations. Although specialized VANET simulators, such as NS-3 or OMNeT++, are commonly used for modeling low-level protocol stacks and testing large-scale deployments, MATLAB offers a more adaptable and modular platform for assessing algorithmic performance under controlled and reproducible conditions. Additionally, MATLAB R2024a features enhanced support for wireless communication models and dynamic mobility management, making it well suited for verifying the feasibility and effectiveness of the proposed method before integrating it into hardware-focused or discrete event-based environments.

During simulation, vehicle mobility traces were generated using the random waypoint mobility model, and network interactions were executed over discrete simulation time steps. Performance metrics such as throughput, PDR, EED, energy consumption, jitter, and collision rate were recorded at each time step based on successfully transmitted and received packets. For each simulation scenario, multiple independent runs were conducted with different random mobility seeds to mitigate stochastic bias, and the reported results represent the average values across these runs. Energy consumption was computed by accumulating the transmission and reception energy costs for each vehicle node over the simulation duration. Congestion and routing statistics were collected by monitoring queue occupancy, packet retransmissions, and path selection events. This systematic data collection process ensures repeatability, statistical stability, and fair performance comparison between the proposed CL-MABRC framework and benchmark protocols.

TABLE 3 | Simulation parameter setup.

Parameter	Value
Simulation area	1000 m × 1000 m
Mobility model	Random waypoint
MAC protocol	IEEE 802.11p
Routing protocol	CL-MABRC
Packet size	512 bytes
Energy model	Simple energy model
Energy initial value	100 J
Channel bandwidth	10 MHz

In the simulation, the parameter values were set to create a stable and repeatable testing environment. In dynamic networks such as VANETs, where node movement, topology, and communication conditions change quickly, setting key parameters (such as the simulation area, packet size, and initial energy) allows for the isolation and assessment of the proposed algorithms (e.g., M-BHC, EPOA, and CL-MABRC) under consistent baseline conditions. This method ensures that different models can be compared, supports fair benchmarking against existing protocols, and enables a systematic performance analysis (e.g., the effect of node speed or traffic density) by altering one factor at a time. Additionally, although core parameters are fixed for baseline tests, scenario-based variations (e.g., different vehicle speeds, node densities, or communication ranges) are introduced during the performance evaluation to showcase the adaptability and robustness of the proposed method in dynamic VANET conditions.

The initial energy of each vehicle node is set to 100 J in this study to represent a normalized communication energy budget allocated to on-board vehicular networking operations rather than the full vehicular battery capacity. Such an assumption is commonly adopted in VANET simulations to fairly evaluate and compare the energy efficiency of routing and clustering protocols under identical conditions. A similar initial energy configuration has been employed in recent VANET research, including the work on data dissemination using PSO, where an initial node energy of 100 J was used to analyze energy consumption and protocol performance in dynamic vehicular environments [45]. This energy level provides sufficient operational duration to observe meaningful energy depletion behavior while avoiding premature node failure. Therefore, the selected initial energy value ensures realistic performance evaluation, reproducibility, and consistency with established VANET simulation practices.

The initial allocation of 100 J of energy was adequate and suitable for this VANET simulation work. This amount is within the typical range used in VANET work, which is between 50 and 200 J, and is specifically designated for the operations of the communication subsystem, rather than the total vehicular power. Considering that standard VANET operations require 0.1 to 0.5 J per packet transmission and 0.05 to 0.2 J per reception, 100 J can support thousands of communication cycles over the course of the simulation. Crucially, the proposed EPOA algorithm is tailored for energy optimization, and the results confirm this adequacy by achieving extensive network performance (99.9% coverage efficiency, 99.89 Kbps throughput) while using only 41.98% of the available energy. This indicates that 100 J offers sufficient operational capacity while imposing meaningful energy constraints, allowing energy-aware algorithms to showcase their optimization capabilities against benchmark protocols. This makes it a suitable choice for assessing energy efficiency improvements of the framework in realistic VANET scenarios.

4.2 | Performance Metric Analysis Across Varying Vehicle Count

The selected performance metrics are chosen to comprehensively evaluate the proposed framework across reliability, efficiency, scalability, security, and real-time communication requirements of VANETs. Throughput, PDR, packet loss ratio (PLR), and EED quantify data transmission efficiency and timeliness under dynamic vehicular mobility. Collision rate, routing OH, and cluster OH measure medium access contention and control signaling efficiency, which are critical in dense networks. Energy consumption and computational complexity assess the sustainability and scalability of the proposed optimization and clustering mechanisms. Attack detection ratio and network security metrics evaluate the robustness of the blockchain-assisted and trust-aware security design. Coverage and bandwidth utilization reflect communication reach and spectrum efficiency, whereas jitter captures delay variation essential for real-time safety applications. Collectively, these metrics provide a holistic assessment of network performance and validate the effectiveness of the proposed cross-layer VANET framework.

4.2.1 | Throughput (Kbps)

$$Throughput = \frac{Total\ received\ data\ (in\ bits)}{Total\ time\ (in\ seconds)} \tag{27}$$

Throughput indicates how much data are successfully delivered over the network per unit time. It reflects the efficiency and speed of the network. Figure 8 shows the throughput performance. The proposed CL-MABRC algorithm shows higher throughput than existing approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. CL-MABRC enhances routing with cross-layer measurements and blockchain-based security, resulting in a congestion-free data flow. Collectively, these advances improve the throughput under dynamic network situations, exceeding the standard approaches. The CL-MABRC method boosts the THRO by 48.35 Kbps with 50 vehicles, whereas the OSC-GOR, ELAACR, TMOHBA, and RCSRC methods reduce it by 26.57, 31.21, 36.72, and 41.38 Kbps. The throughput results demonstrate that CL-MABRC consistently achieves higher data delivery rates under dynamic vehicular conditions. This improvement is primarily due to cross-layer routing decisions and blockchain-assisted congestion control, which prevent route failures and bottlenecks. Stable cluster formation further ensures uninterrupted data forwarding even at high vehicle densities.

4.2.2 | PDR (%)

$$PDR = \left(\frac{Packets\ received}{Packets\ sent}\right) \times 100 \tag{28}$$

PDR shows the percentage of successfully delivered packets out of the total sent. A higher PDR indicates better network reliability. The proposed algorithm, CL-MABRC, outperforms existing approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC in terms of PDR. The performance evaluation of the PDR is shown in Figure 9. CL-MABRC enhances routing by combining congestion control and blockchain security, resulting in efficient packet transmission even during peak traffic periods. These qualities contribute to a higher PDR than previous techniques, which suffer from increased packet loss owing to OH and restricted adaptability. The CL-MABRC approach improves the PDR by 62.78% with 50 vehicles, whereas OSC-GOR, ELAACR, TMOHBA, and RCSRC lower the THRO by 48.25%, 52.32%, 56.61%, and 62.78%, respectively. The proposed CL-MABRC achieves a higher PDR by maintaining stable routing paths and minimizing packet drops. Mobility-aware clustering and congestion-aware route selection reduce frequent link breaks, whereas blockchain-based verification prevents malicious route participation, ensuring reliable packet forwarding under varying traffic densities.

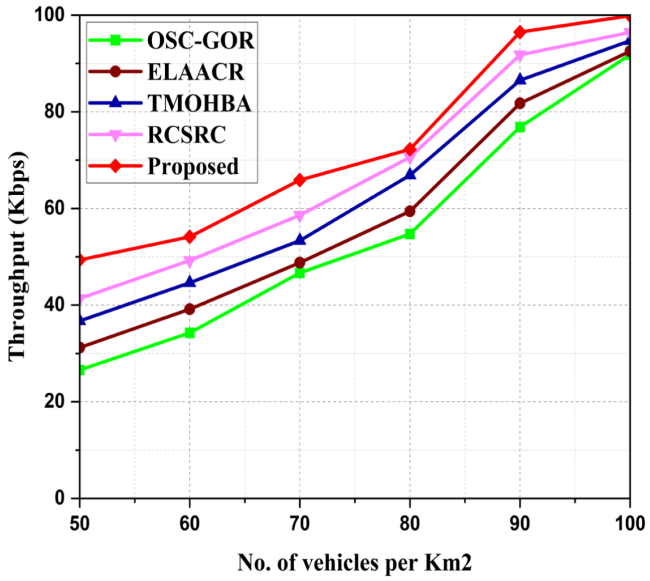


FIGURE 8 | Performance of throughput.

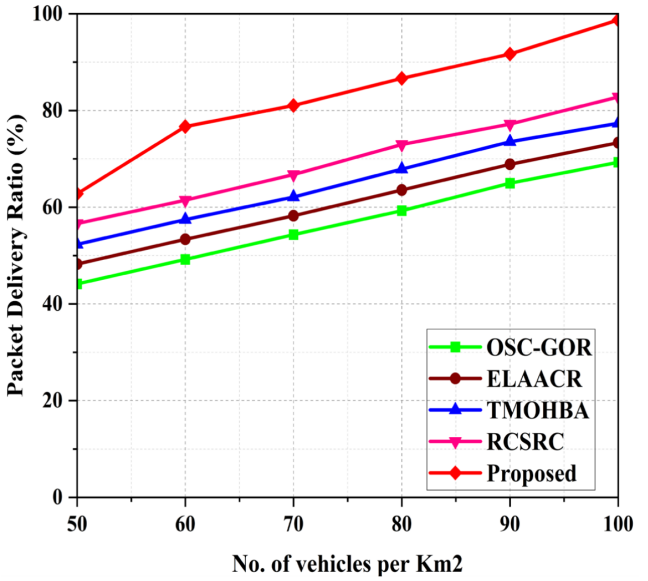


FIGURE 9 | Performance of PDR.

4.2.3 | PLR (%)

$$PLR = \left(\frac{Packets\ sent - Packets\ received}{Packets\ sent} \right) \times 100 \quad (29)$$

PLR quantifies the percentage of packets that never reached their destination. Lower values signify better performance. Figure 10 shows the performance of PLR. The proposed CL-MABRC algorithm shows a much lower PLR than existing approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. CL-MABRC decreases packet loss by combining congestion control and secure routing methods, ensuring consistent data transfer under changing traffic conditions of 1.1%. Existing techniques, however, experience increased packet loss as a result of re-clustering OH and congestion. The proposed strategies consistently increased the reliability of packet delivery. CL-MABRC significantly reduces packet loss by dynamically avoiding congested and unstable routes. The integration of cross-layer congestion feedback and secure route validation prevents buffer overflows and retransmissions. In contrast, conventional protocols experience higher packet loss due to frequent re-clustering and limited adaptability to mobility.

4.2.4 | EED (ms)

$$Average\ E2E\ Delay = \frac{\sum (Time\ received - Time\ sent)}{Total\ packets\ received} \quad (30)$$

E2E delay measures the average time taken for a packet to travel from source to destination. Lower delay is preferred for real-time applications. The proposed algorithm, CL-MABRC, has lower EEDs than OSC-GOR, ELAACR, TMOHBA, and RCSRC. CL-MABRC uses cross-layer measurements and congestion control to improve packet routing and minimize network congestion delays. Traditional methods, however, experience lengthier delays because of frequent clustering and congestion control inefficiencies. Together, the proposed techniques improve the speed and reliability of the data transit in dynamic VANET systems. The proposed CL-MABRC approach produced EEDs of 0.4 ms for 50 vehicle nodes. In contrast, existing routing algorithms, such as OSC-GOR, ELAACR, TMOHBA, and RCSRC, have achieved EEDs of 3.1, 2.8, 1.9, and 1.5 ms, respectively. Therefore, the performance in Figure 11 illustrates that when compared with alternative routing approaches, the proposed method has a lower delay. The EED is minimized in CL-MABRC due to efficient route selection and reduced control OH. Mobility-aware clustering stabilizes communication links, whereas congestion control avoids queuing delays. This combination ensures faster packet delivery, making the proposed framework suitable for real-time VANET applications.

4.2.5 | Collision Rate (%)

$$Collision\ Rate = \left(\frac{Number\ of\ Collided\ Packets}{Total\ Transmission\ Attempts} \right) \times 100 \quad (31)$$

For the evaluation of collision rate (Equation 31), the number of collided packets is obtained by tracking packets that fail to reach the intended receiver due to simultaneous transmissions or interference events within the simulation environment. The total transmission attempts correspond to all packets generated and transmitted by vehicles during the simulation runtime, including both successful and collided packets. Packet collision events are detected using the MAC layer model (IEEE 802.11p), which flags overlapping transmissions at receivers. Collision rate indicates how often packet collisions occur during transmission. A low collision rate suggests efficient channel utilization. The proposed algorithm CL-MABRC outperforms existing approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC in terms of the data broadcasting ratio. The congestion control and cross-layer measures of CL-MABRC reduce network congestion, allowing for more efficient data broadcasting. On the other hand, existing

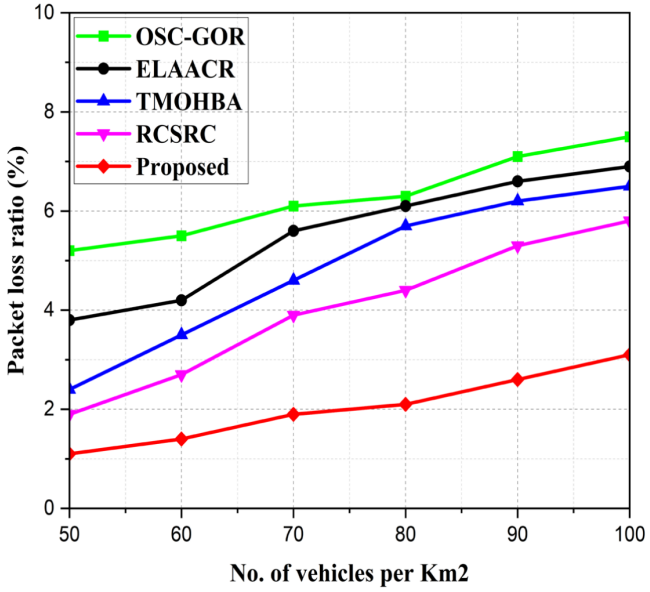


FIGURE 10 | Performance of PLR.

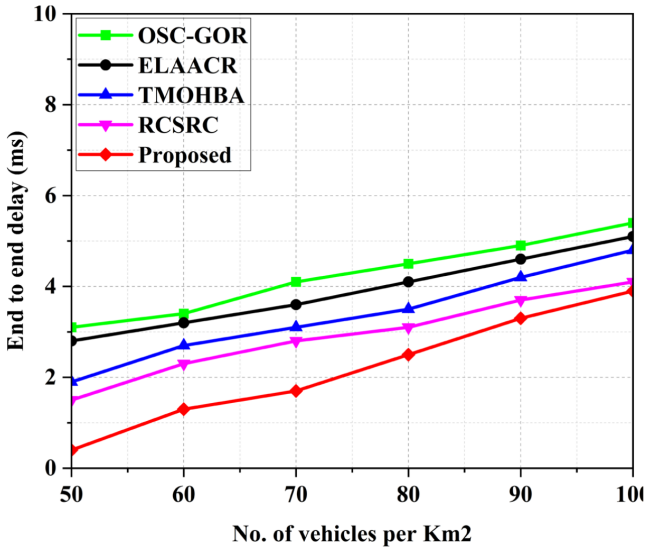


FIGURE 11 | Performance of end to end delay.

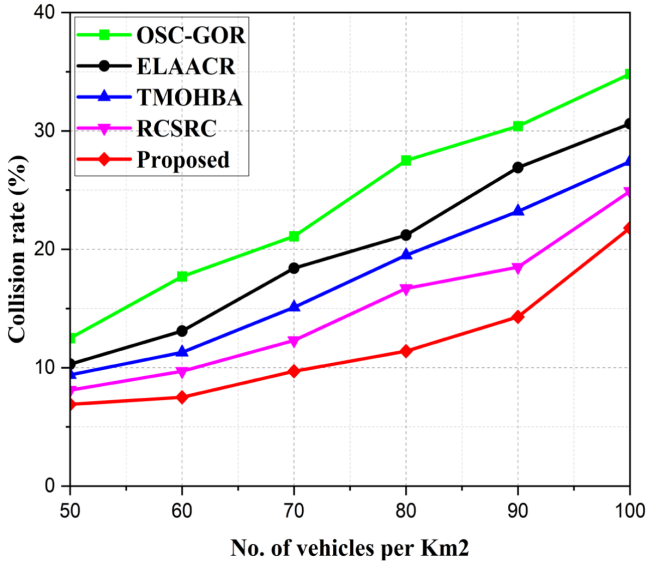


FIGURE 12 | Performance of collision rate.

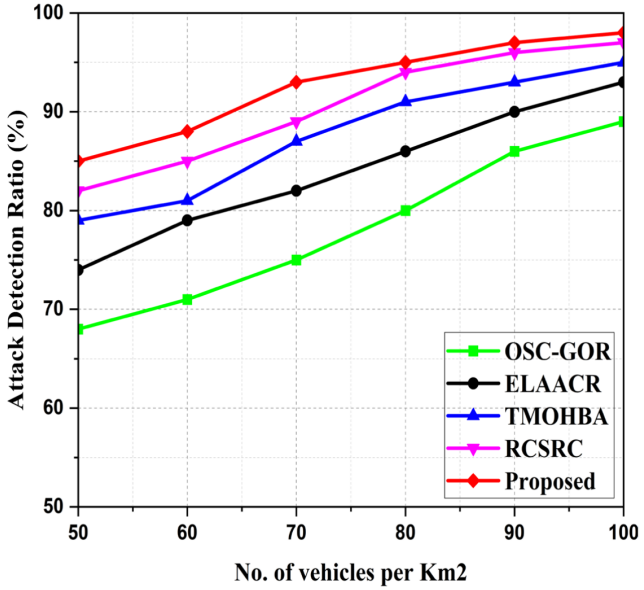


FIGURE 13 | Performance of attack detection ratio.

methods have limited scalability and adaptability, resulting in lower data broadcasting rates. The proposed methods significantly improve data broadcasting by combining the advantages of stability, energy efficiency, and congestion control. Existing routing algorithms, such as OSC-GOR, ELAACR, TMOHBA, and RCSRC, have achieved collision rates of 12.5%, 10.3%, 9.4%, and 8.1%, respectively. The proposed CL-MABRC achieved 6.9% for 50 vehicle nodes. Figure 12 shows the collision rate performance. The collision rate is notably lower in CL-MABRC because of controlled packet dissemination and congestion-aware transmission scheduling. Cross-layer coordination reduces simultaneous transmissions, whereas stable clusters limit unnecessary broadcasts. As a result, channel contention is minimized, leading to more efficient medium utilization than existing routing schemes.

4.2.6 | Attack Detection Ratio (%)

$$Attack\ Detection\ Ratio = \left(\frac{Number\ of\ Attacks\ Detected\ Correctly}{Total\ Number\ of\ Attacks\ Simulated}\right) \times 100 \tag{32}$$

For the attack detection ratio (Equation 32), the total number of attacks simulated is predefined in the scenario setup, encompassing black-hole, Sybil, or malicious routing attempts injected at controlled intervals. The number of attacks detected correctly is counted when the CL-MABRC protocol identifies and isolates these malicious nodes using blockchain-based verification and trust evaluation mechanisms, thereby allowing only legitimate data to be routed. Figure 13 shows how effectively the system detects attacks. A high ratio implies robust security detection mechanisms. The proposed algorithm, CL-MABRC, significantly increases the attack detection ratio over current approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. CL-MABRC improves security by leveraging blockchain-based trust mechanisms to identify threats such as packet spoofing and routing misbehavior. By contrast, the present algorithms are more vulnerable to undiscovered attacks, resulting in a lower detection rate. The proposed methods provide strong threat detection, resulting in increased security in dynamic VANET systems. Existing routing algorithms, such as OSC-GOR, ELAACR, TMOHBA, and RCSRC, have achieved attack detection ratios of 68%, 74%, 79%, and 82%, respectively. The proposed CL-MABRC achieves 85% accuracy for 50 vehicle nodes. Figure 13 shows the performance of the attack-detection ratio. CL-MABRC achieves a higher attack detection ratio by employing blockchain-based trust validation and secure route verification. Malicious nodes are rapidly identified and isolated, preventing participation in routing. This proactive security mechanism significantly improves detection accuracy compared with traditional protocols lacking decentralized verification.

4.2.7 | Routing OH (%)

$$Routing\ Overhead = \left(\frac{Routing\ control\ packets}{Total\ data\ packets\ received}\right) \times 100 \tag{33}$$

Routing OH represents the extra routing-related traffic in the network. Minimizing OH improves efficiency. The proposed algorithm, CL-MABRC, shows a significant reduction in routing OH compared with existing approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. CL-MABRC decreases congestion and improves routing efficiency by adding cross-layer measurements and blockchain security, thereby reducing the need for frequent route recalculations. Existing methods, on the other hand, suffer from higher OH owing to static or less adaptive routing strategies, resulting in inefficient communication. The novel CL-MABRC method had a routing OH of 21.4% for 50 vehicle nodes compared with 31.4%, 29.1%, 25.4%, and 23.7%, respectively. The graph shows that the CL-MABRC routing technique has a reduced routing OH compared with earlier strategies. Figure 14 shows the performance of the routing OH. The routing OH is reduced in CL-MABRC through adaptive route maintenance and cross-layer information sharing. By avoiding

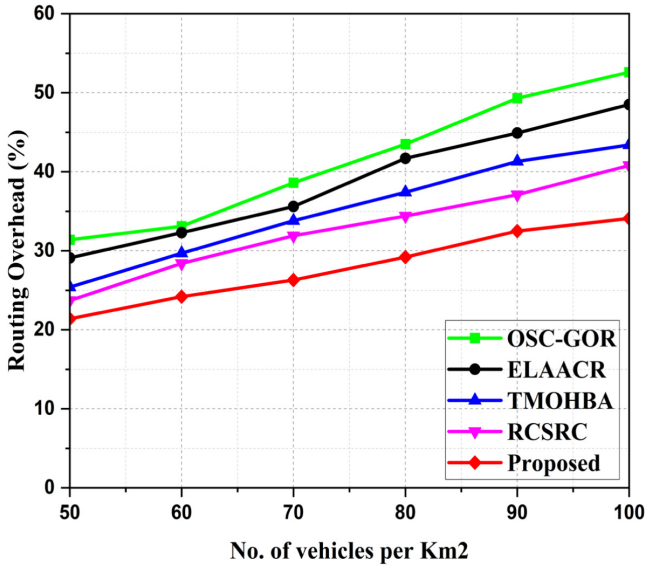


FIGURE 14 | Performance of routing overhead.

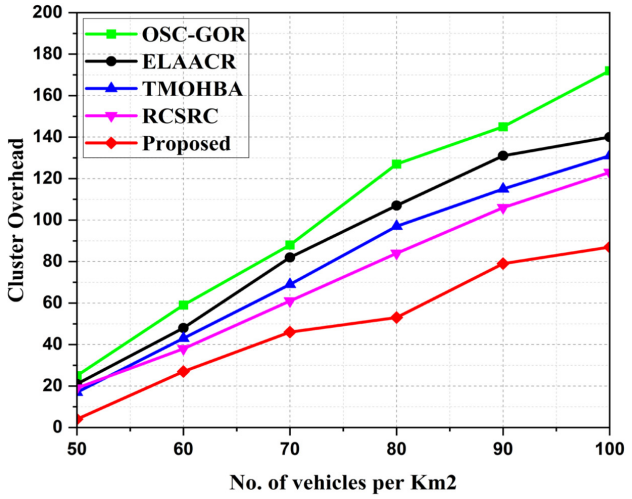


FIGURE 15 | Performance of cluster overhead.

frequent route rediscovery and unnecessary control packets, the protocol maintains efficient communication. This OH reduction directly contributes to improved scalability in dense vehicular environments.

4.2.8 | Cluster OH (%)

$$Cluster\ Overhead = \frac{Total\ Control\ Packets\ for\ Clustering}{Total\ Data\ Packets\ Transmitted} \tag{34}$$

Cluster OH in clustering-based VANET protocols, it shows the communication OH needed for forming and maintaining clusters. The proposed algorithm CL-MABRC greatly minimizes cluster OH when compared with existing approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. CL-MABRC decreases the control message OH by optimizing the routing and congestion management. Existing approaches, on the other hand, frequently suffer from excessive OH due to dynamic topology changes and high re-clustering frequency, resulting in increased communication costs and inefficiency. With 50 vehicles, CL-MABRC decreased the COH by 4, whereas OSC-GOR, ELAACR, TMOHBA, and RCSRC. M-BHC models increase COH by 25, 21, 17, and 19. Figure 15 shows the performance of the cluster OH. CL-MABRC minimizes cluster OH by employing mobility-aware clustering and energy-optimized CH selection. Stable clusters reduce re-clustering frequency and control message exchanges. In contrast, existing methods incur higher OH due to frequent topology changes and inefficient cluster maintenance mechanisms.

4.2.9 | Coverage (%)

$$Coverage = \left(\frac{Total\ Area\ Covered\ by\ Active\ Nodes}{Total\ Simulation\ Area}\right) \times 100 \tag{35}$$

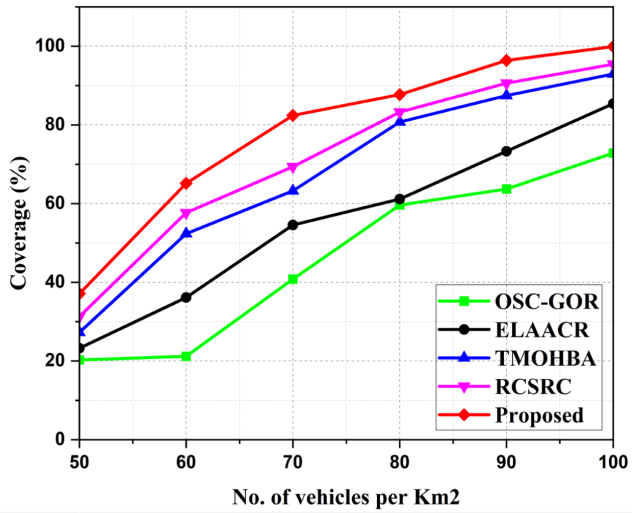


FIGURE 16 | Performance of coverage.

Coverage (Equation 35) is calculated by dividing the aggregate area effectively covered by active nodes, determined from the dynamic communication ranges of all vehicles, by the total simulation area. Coverage denotes how well the network nodes cover the simulation area. Higher coverage implies better reach and connectivity. The proposed CL-MABRC algorithm provides significantly better coverage than existing approaches, such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. CL-MABRC enhances coverage by optimizing across layers and controlling congestion, thereby preventing coverage gaps during peak traffic periods. Existing algorithms, however, have limited adaptability and significant transmission OH, making it difficult to maintain extensive coverage. The proposed methods improve coverage by responding to network dynamics and optimizing the use of available resources. The CL-MABRC method increased the COV by 37.11% with 50 vehicles, whereas the OSC-GOR, ELAACR, TMOHBA, and RCSRC models reduced it by 20.25%, 23.26%, 27.26%, and 31.29%, respectively. Figure 16 shows the coverage performance. The coverage performance of CL-MABRC is enhanced by effective resource utilization and congestion-aware routing. Cross-layer optimization prevents communication gaps

and ensures consistent connectivity across the simulation area. This adaptability allows the network to maintain higher coverage even under dynamic traffic conditions.

4.2.10 | Bandwidth (bps)

$$Bandwidth = \frac{Total\ data\ transmitted}{Transmission\ time} \tag{36}$$

Bandwidth is the maximum transmission capacity of a network channel. It affects the potential data transfer rate. The proposed algorithm, CL-MABRC, significantly enhances bandwidth utilization when compared with existing approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. The CL-MABRC incorporates cross-layer monitoring and congestion control to avoid bandwidth bottlenecks and improve communication. In contrast, conventional algorithms suffer from bandwidth inefficiencies owing to the excessive OH and less adaptable routing. The suggested methods effectively manage the bandwidth, resulting in improved overall network performance. The CL-MABRC method increases the bandwidth by 84 bps with 50 vehicles, whereas the OSC-GOR, ELAACR, TMOHBA, and RCSRC models decrease the bandwidth by 71, 74, 79, and 81 bps. Figure 17 shows the bandwidth performance. CL-MABRC improves bandwidth utilization by preventing congestion-induced bottlenecks and reducing redundant transmissions. Cross-layer monitoring enables efficient allocation of available bandwidth, whereas secure routing ensures only valid data flows consume network resources, leading to superior bandwidth efficiency compared with existing approaches.

4.2.11 | Energy Consumption (Joules)

$$Total\ Energy = \sum (Energy\ in\ TX + Energy\ in\ RX + Idle/Overhead\ energy) \tag{37}$$

Energy consumption represents the total energy consumed during the transmission, reception, and idle states. Important for energy-efficient routing in VANETs. The proposed CL-MABRC algorithm shows significant improvements in energy usage over existing approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. CL-MABRC decreases the energy consumption by combining congestion control and blockchain to enable energy-efficient routing. In contrast, conventional algorithms frequently consume more energy owing to the excessive control OH and suboptimal routing decisions. The CL-MABRC algorithm demonstrates an energy consumption of 9.18 J, whereas the traditional algorithms OSC-GOR, ELAACR, TMOHBA, and RCSRC consume 32.46, 27.09, 21.54, and 17.35 J, respectively. Figure 18 shows the performance of the energy consumed. Energy consumption is significantly reduced in CL-MABRC through energy-aware CH selection and optimized routing decisions. By limiting retransmissions, control OH, and unnecessary broadcasts, the framework conserves node energy, thereby extending network lifetime and improving sustainability in VANET deployments.

4.2.12 | Network Security (%)

$$Network\ Security = \left(\frac{Number\ of\ Secure\ Data\ Packets\ Transmitted}{Total\ Data\ Packets\ Transmitted}\right) \times 100 \tag{38}$$

Similarly, network security (Equation 38) is measured by counting the number of secure packets successfully transmitted through authenticated and verified paths relative to the total packets generated, ensuring that only data confirmed by the blockchain ledger contributes to the numerator. These mechanisms are tracked programmatically in MATLAB to provide precise and reproducible metric measurements. Network security indicates the proportion of transmitted data that remain secure. A higher percentage indicates greater resistance to attacks. The proposed CL-MABRC algorithm surpasses existing methods, such as OSC-GOR, ELAACR, TMOHBA, and

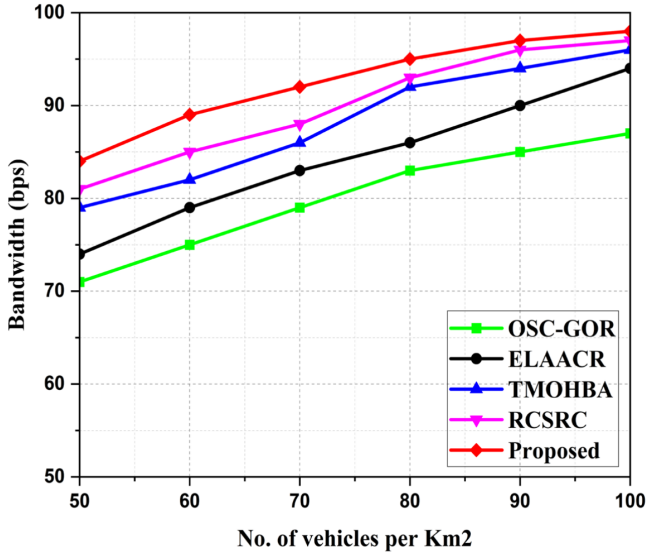


FIGURE 17 | Performance of bandwidth.

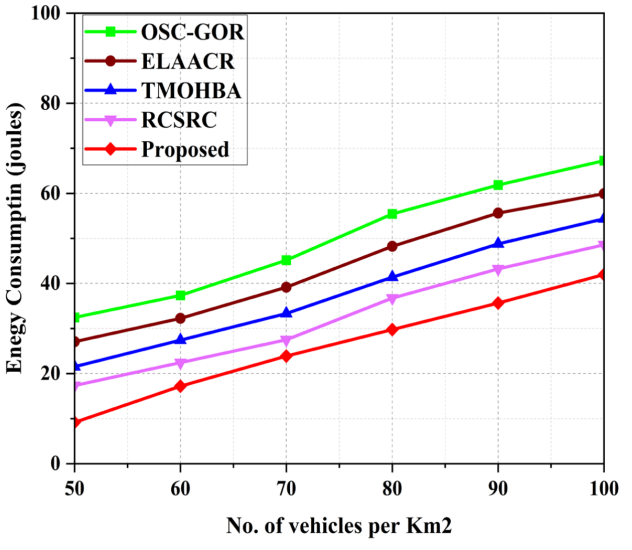


FIGURE 18 | Performance of energy consumption.

RCSRC, to enhance network security. CL-MABRC utilizes blockchain-based security protocols to block unauthorized access and ensure data integrity during transmissions. In contrast, current methods have inadequate security measures, making them more susceptible to threats, such as data tampering and unauthorized access. The proposed solutions provide robust protection against these risks and ensure secure communication within a VANET. With 50 vehicles, CL-MABRC increased network security by 95.5%, whereas OSC-GOR, ELAACR, TMOHBA, and RCSRC reduced it by 90.6%, 91.5%, 92.5%, and 94.9%, respectively. Figure 19 illustrates the network security performance. In the proposed method, network security (%) is determined using the given formula, where secure data packets are those successfully transmitted through authenticated, blockchain-validated routes. The CL-MABRC algorithm improves the data transmission security by integrating blockchain validation at the routing layer, inherently preventing unauthorized changes, ensuring route authenticity, and maintaining data integrity. Although the model does not simulate specific malicious attacks or employ intrusion detection systems, the use of trust evaluation, multi-attribute metrics, and decentralized blockchain validation aids in the secure delivery of data packets. Therefore, the network security percentage is a dependable measure of the capability of the protocol to ensure secure communication under dynamic VANET conditions.

ELAACR, which employs group signature-based LAKM and ACR, demonstrates relatively lower security owing to its limited adaptability in high-mobility VANET environments. Its static trust model and dependence on group signature authentication may not effectively address dynamic internal threats and real-time route manipulations. TMOHBA enhances ELAACR by incorporating trust and honey badger optimization but still lacks strong route validation. RCSRC, which utilizes robust cryptographic techniques and clustering, performs better in static conditions, but still does not match the proposed method.

The proposed CL-MABRC outperformed all others by integrating blockchain-based route validation, congestion-aware multi-attribute routing, and mobility-based clustering (M-BHC). This dynamic, cross-layer approach enables real-time validation of routing paths, ensuring secure packet transmission even in highly dynamic scenarios. This comprehensive security framework accounts for the superior network security performance across all vehicle densities.

CL-MABRC enhances network security by integrating blockchain-based authentication and route validation mechanisms. Only verified nodes and trusted routes participate in data transmission, ensuring data integrity and resistance to routing attacks. This decentralized security framework provides robust protection in highly dynamic VANET environments.

4.2.13 | Jitter (ms)

$$Jitter = Average\left(Delay_{i+1} - Delay_i\right) \tag{39}$$

Jitter measures the variability in packet delay, critical for applications like voice and video where consistent delivery is essential. The proposed algorithm, CL-MABRC, significantly increases jitter performance when compared with existing approaches such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. The CL-MABRC improves route stability by utilizing cross-layer metrics and congestion control, thereby minimizing delay variability. Existing algorithms, however, suffer from increased jitter owing to topology changes, congestion, and inefficient routing, resulting in less stable communication. The proposed solutions reduce jitter and improve real-time communications. The proposed technique had a low jitter value of 0.25 ms for 50 vehicle nodes, compared with existing methods such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. The M-BHC had jitter values of 0.67, 0.53, 0.47, and 0.35 ms, respectively. Figure 20 shows the jitter performance. The proposed

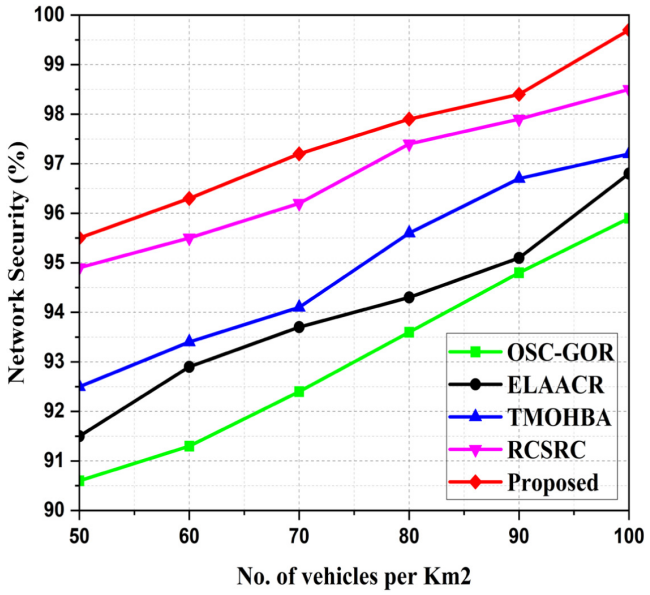


FIGURE 19 | Performance of network security.

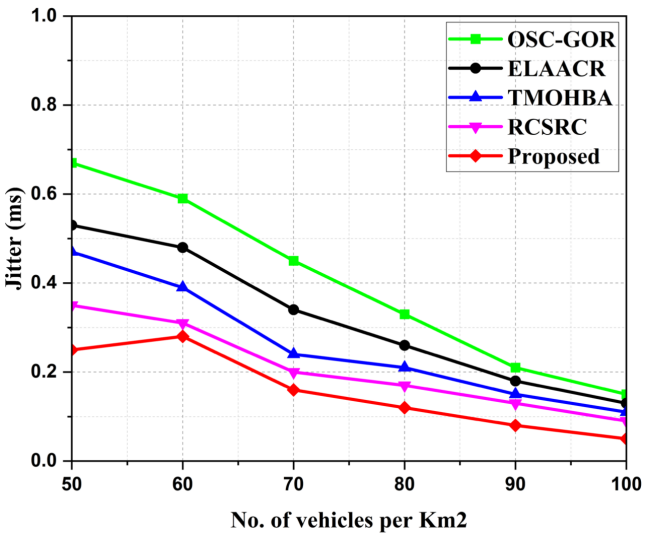


FIGURE 20 | Performance of jitter.

CL-MABRC exhibits lower jitter due to stable routing paths and reduced congestion variability. Mobility-aware clustering minimizes frequent route changes, whereas congestion control stabilizes packet transmission intervals. This results in consistent delay performance, which is essential for real-time multimedia and safety applications.

4.2.14 | Computational Complexity

Table 4 shows the computational complexity. The proposed CL-MABRC algorithm has a computational complexity of $O(nlogn)$, which is relatively efficient because it stores cross-layer attributes and blockchain data, allowing it to scale effectively in vast networks. OSC-GOR, with a computational complexity of $O(n^2)$, is ideal for smaller networks as it focusses on routing and security data. ELAACR and TMOHBA have higher computational complexity of $O(n^3)$ and $O(n^2)$, respectively, due to the storage requirements for ant colony pheromones, multi-objective optimization, and trust data. RCSRC has a computational complexity of $O(n^2)$, mostly for cryptographic and data transmission storage. The CL-MABRC algorithm strikes a balance between efficiency and scalability, exceeding existing approaches in terms of computational utilization for large-scale VANETs.

TABLE 4 | Computational complexity.

Algorithm	Computational complexity
OSC-GOR	$O(n^2)$
ELAACR	$O(n^3)$
TMOHBA	$O(n^2)$
RCSRC	$O(n^2)$
CL-MABRC	$O(nlogn)$

The overall computational complexity of the proposed CL-MABRC framework is derived by analyzing the dominant operations involved in clustering, optimization, and routing decisions. In the M-BHC module, vehicles perform neighbor discovery and distance computation based on predicted positions. By employing efficient neighbor indexing and localized clustering, these operations scale linearly with the number of vehicles, resulting in O(n) complexity. The EPOA-based cluster-head selection involves population initialization and fitness evaluation, where sorting or ranking of candidate solutions is required to identify optimal CHs. This step contributes O(n log n) complexity due to sorting operations. In the CL-MABRC routing phase, multi-attribute path selection relies on priority-based route evaluation and blockchain verification of selected routes, both of which operate on logarithmic lookup and validation mechanisms using distributed ledger indexing. Since no exhaustive path enumeration or global optimization is performed, the dominant complexity remains bounded by the sorting and priority-queue operations. Consequently, the overall computational complexity of CL-MABRC is O(n log n), which is lower than swarm-based and iterative routing protocols that require repeated global updates.

4.2.15 | State-of-the-Art Comparison

The state-of-the-art comparison in Table 5 examines the existing clustering and routing protocols in VANETs, emphasizing the challenges in managing high mobility, congestion, and security vulnerabilities. Conventional methods often face issues, such as frequent re-clustering, suboptimal CH selection, and

TABLE 5 | State of the art comparison.

Ref no	Author name	Algorithm	PDR (%)	End to end delay (s)	Throughput
[2]	Dhwani Desai et al. (2023)	Particle swarm optimization (PSO)–based time delay–based multipath routing (TMR) algorithm	98	0.5	6 Mbps
[4]	Akhilesh Bijalwan et al. (2023)	Dynamic aware transmission range parallel Euclidean distance (DA-TRPED)	94.21	—	27.23 Kbps
[20]	MV Kadam et al. (2023)	Trust aware clustering–based routing protocol (TACR)	8	—	11.25%
[23]	HA Ahmed et al.(2024)	Federated Q-learning by merging blockchain technology	—	—	102,465.8 KB/s
[27]	B Kheradmand et al. (2022)	Traffic-aware and low-latency routing schema (TaLAR)	22	23	25%
[33]	R Ramamoorthy et al. (2024)	Enhanced location-aided ant colony routing (ELAACR)	98.5	—	640 Kbps
	Proposed	Cross-layer multi-attribute blockchain routing with congestion control (CL-MABRC)	98.74	0.4	99.89 Kbps

TABLE 6 | Comparative evaluation of proposed CL-MABRC framework with recent state-of-the-art VANET routing and clustering techniques.

Ref no	Author name	Algorithm	PDR (%)	End to end delay
[46]	Bagirathan et al. (2025)	Ensemble long short-term memory (ELSTM)	81	0.17
[47]	Venkata Krishna Reddy et al. (2025)	Trust-enabled secure routing (TESR)	96	2.25 s
[48]	Chakravarthi Bachina et al. (2025)	Efficient stable cluster management model (ESCMM)	93	83.25
[49]	Sesham Anand et al. (2025)	Improvised ensemble deep learning framework	91.5	31.6
[50]	Anshu Devi et al. (2025)	Dynamic load balancing	83.3	7.60
	Proposed	Cross-layer multi-attribute blockchain routing with congestion control (CL-MABRC)	98.74%	0.4 s

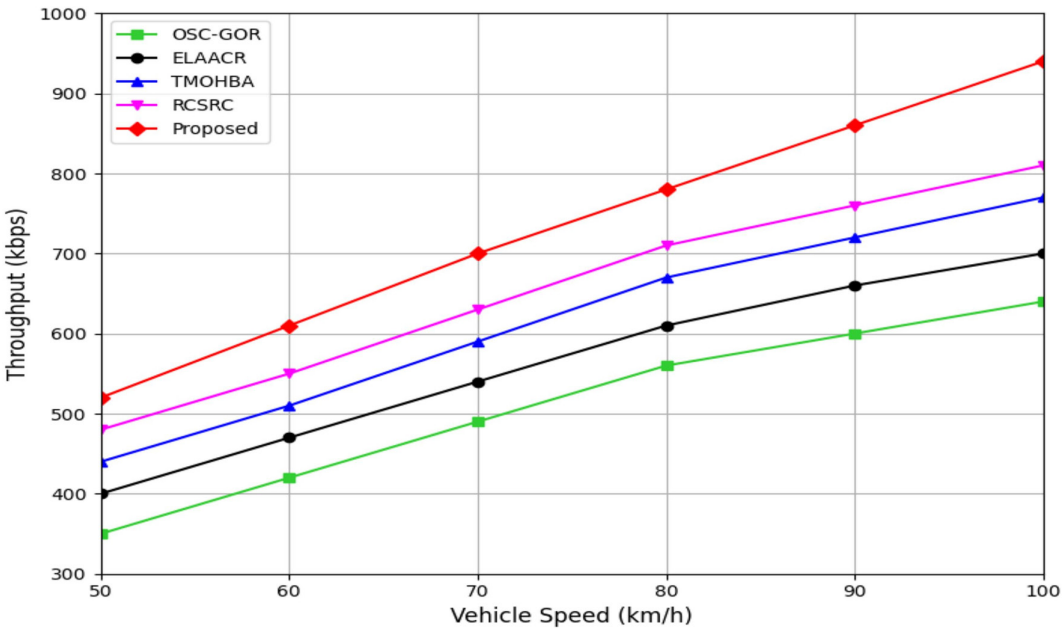


FIGURE 21 | Performance of throughput.

susceptibility to cyber threats. To overcome these limitations, this work introduces an advanced framework that incorporates M-BHC, EPOA, and CL-MABRC. This integrated approach enhances cluster stability, optimizes energy efficiency, strengthens security, and ensures reliable data transmission in dynamic vehicular networks.

4.2.16 | State-of-the-Art Comparison With Recent Algorithms

Table 6 presents a comparative evaluation of the proposed CL-MABRC framework with several recently published cutting-edge VANET clustering and routing algorithms. To evaluate communication reliability, latency, and data efficiency, key performance indicators, such as the PDR and EED, are examined. The findings clearly indicate that the CL-MABRC method outperforms the others, achieving the highest PDR at 98.74%, the lowest EED at 0.4 s, and the greatest throughput at 99.89 Kbps. Compared with methods such as ELSTM [46], TESR [47], and ESCMM [48], the proposed approach shows improved reliability and efficiency in dynamic vehicular environments. This confirms the robustness and real-time applicability of the proposed method for next-generation VANET systems.

4.3 | Performance Metric Analysis Across Varying Vehicle Speed

Figures 21–24 collectively depict how the proposed framework performs in comparison to existing methods—OSC-GOR, ELAACR, TMOHBA, and RCSRC—across different vehicle speeds ranging from 50 to 100 km/h. As shown in Figure 21, the proposed method consistently delivered the highest throughput, increasing from approximately 530 Kbps at 50 km/h to 960 Kbps

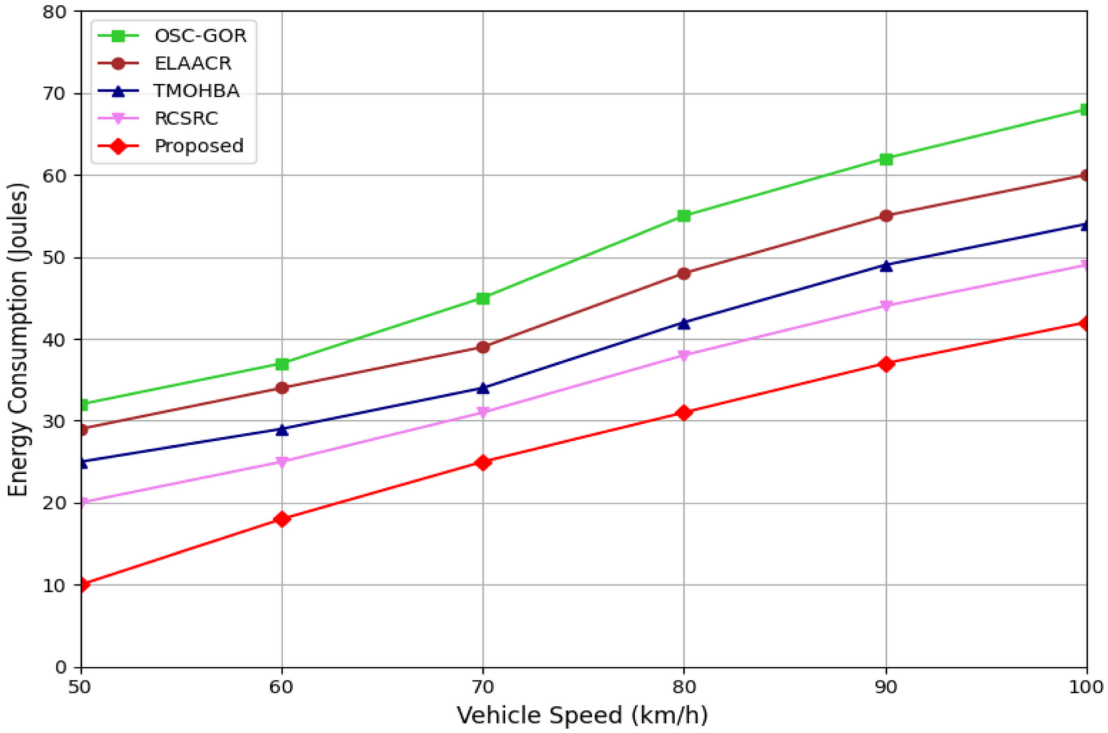


FIGURE 22 | Performance of energy consumption.

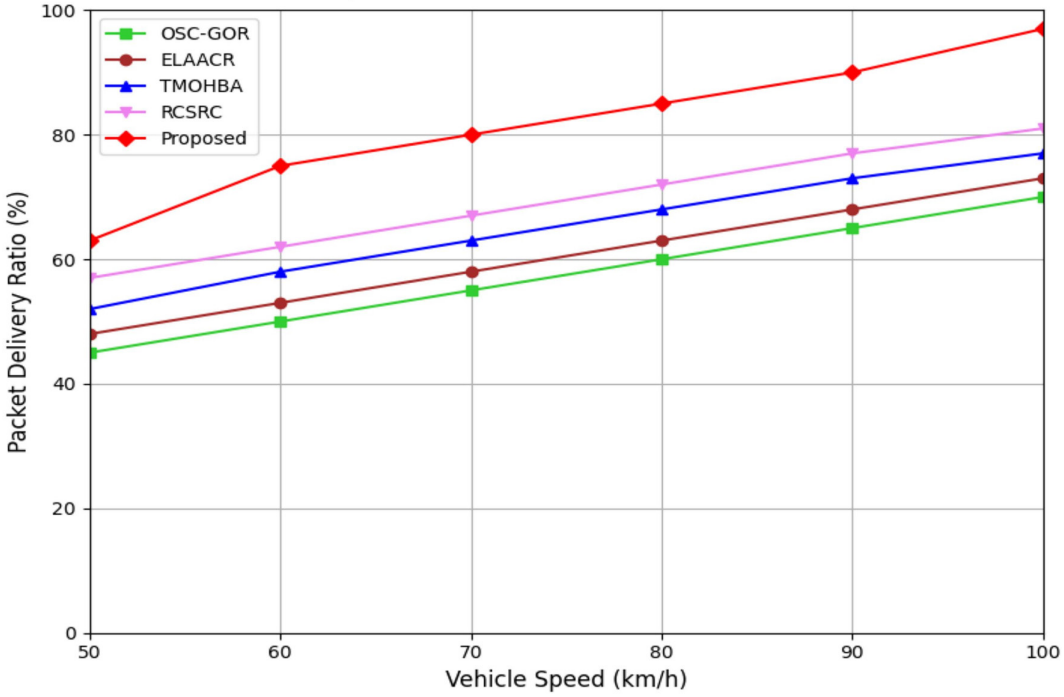


FIGURE 23 | Performance of packet delivery ratio.

at 100 km/h, surpassing OSC-GOR (370–680 Kbps), ELAACR (420–720 Kbps), and RCSRC (540–850 Kbps). Figure 22 shows the energy consumption, where the proposed method maintains the lowest energy usage, gradually increasing from 10 to 40 J as the speed increases, significantly outperforming OSC-GOR, which peaks at 78 J, and TMOHBA at 60 J. Figure 23 illustrates the PDR, with the proposed method achieving 96% at 100 km/h, starting from 63% at 50 km/h, compared with the lower values for OSC-GOR (45%–70%) and ELAACR (49%–74%). Lastly, Figure 24 shows that the proposed system also achieves the lowest EED, ranging from 0.5 ms at 20 km/h to 4.1 ms at 100 km/h, which is significantly lower than OSC-GOR (3.0–5.8 ms) and ELAACR (2.9–5.3 ms). These findings collectively confirm the superiority of the proposed framework in terms of communication efficiency, energy conservation, and reliability under varying mobility conditions in VANETs.

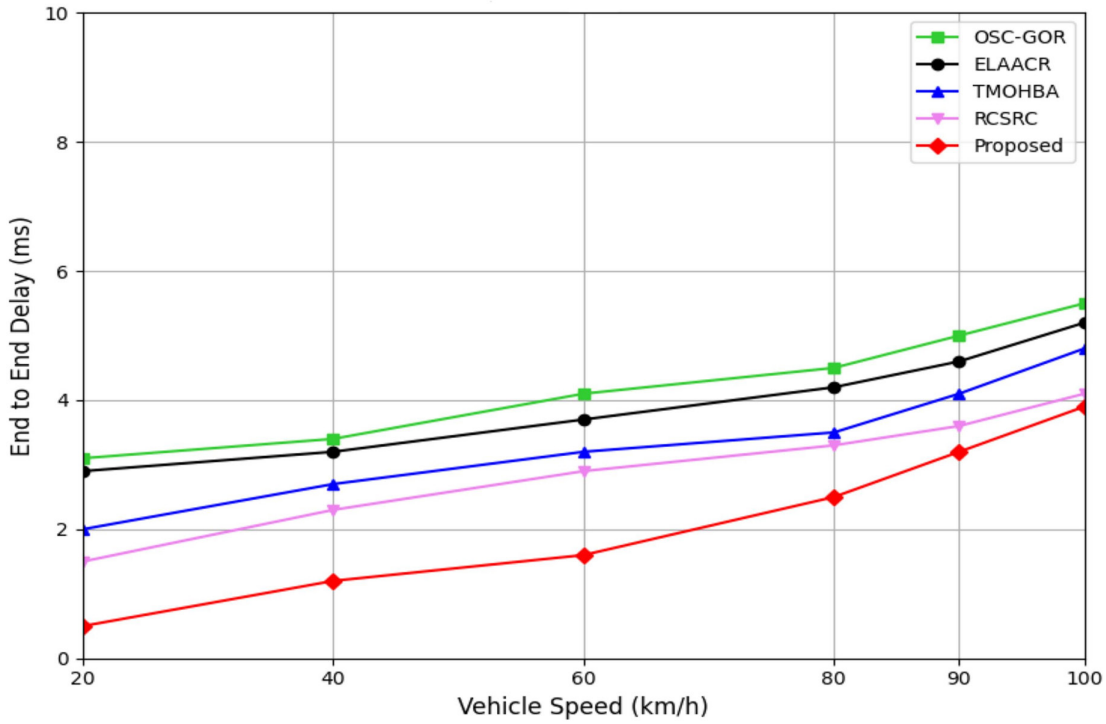


FIGURE 24 | Performance of end to end delay.

4.3.1 | Throughput (kbps)

4.3.2 | Energy Consumption (J)

4.3.3 | PDR (%)

4.3.4 | End-to-End Delay (ms)

4.4 | Qualitative and Quantitative Comparison With Traditional Approaches

Table 7 shows the qualitative comparison of proposed CL-MABRC with traditional VANET approaches. Traditional VANET routing and clustering approaches typically rely on static communication ranges, single-layer decision-making, and centralized or trust-only security mechanisms, which limits their adaptability under high mobility and dense traffic conditions. In contrast, the proposed framework introduces mobility-aware clustering, energy-efficient bio-inspired optimization, and blockchain-assisted cross-layer routing, enabling dynamic adaptation to network changes and enhanced security. Qualitatively, this integrated design reduces frequent re-clustering, balances energy consumption, and mitigates routing attacks more effectively than conventional schemes. Quantitatively, the proposed CL-MABRC framework demonstrates clear performance improvements over traditional methods, achieving higher throughput and PDR, along with lower EED, collision rate, routing OH, and energy consumption. Furthermore, improved attack detection ratio and network security metrics confirm the effectiveness of the blockchain-assisted trust model. These results collectively validate the superiority of the proposed plan over traditional VANET solutions from both conceptual and numerical perspectives.

4.5 | Practical Feasibility and Implementation Analysis

The experimental results demonstrate that the proposed framework is computationally feasible for real-time VANET deployment. The localized clustering of M-BHC and the intra-cluster optimization of EPOA significantly reduce global computation and control OH, enabling efficient execution even as network density increases. The observed low routing and clustering OH, along with reduced energy consumption, indicate that the proposed algorithms impose minimal processing burden on vehicular on-board units. Furthermore, the CL-MABRC protocol restricts blockchain operations to selected routing paths rather than network-wide consensus, limiting latency and storage OH. The O(n log n) computational complexity ensures scalability, whereas the stable throughput, low delay, and low jitter achieved in simulations confirm suitability for real-time safety and infotainment applications. These characteristics suggest that the proposed model can be practically implemented using existing vehicular communication hardware and software platforms.

5 | Discussion

5.1 | Blockchain OH and Security–Performance Trade-Off Analysis

The integration of blockchain in the proposed CL-MABRC framework enhances routing security by ensuring route authenticity, integrity, and resistance to tampering. However,

TABLE 7 | Qualitative comparison of proposed CL-MABRC with traditional VANET approaches.

Aspect	Traditional VANET approaches	Proposed CL-MABRC framework
Clustering strategy	Static or semi-static clustering based on position or ID	Mobility-aware dynamic clustering (M-BHC) using predicted positions
Routing decision	Single-layer routing based on topology or location	Cross-layer multi-attribute routing considering mobility, trust, and congestion
Energy management	No explicit energy optimization or uneven CH selection	Energy-aware CH selection using bio-inspired EPOA
Congestion handling	Reactive or fixed-threshold congestion control	Real-time adaptive congestion control integrated with routing
Security mechanism	Cryptographic or trust-based methods in isolation	Blockchain-assisted trust validation with attack detection
Scalability	Limited due to global control overhead	High scalability due to localized clustering and O(n log n) complexity
Throughput	Moderate	High (99.89 Kbps)
End-to-end delay	Higher due to frequent re-routing	Low (0.4 ms)
Packet delivery ratio	Moderate to high	High (98.74%)
Energy consumption	High and uneven	Reduced and balanced (41.98%)
Attack detection	Limited or reactive	High attack detection ratio with blockchain validation

this security improvement introduces additional OH, primarily in the form of computational processing and communication latency associated with block creation and validation. In the proposed design, blockchain operations are lightweight and event-driven, occurring only during route establishment or reconfiguration rather than during every packet transmission. This significantly limits consensus-related delays in real-time data forwarding. To minimize latency, the framework employs a permissioned blockchain model with a restricted set of validating nodes, such as CHs and RSUs. This approach avoids energy-intensive consensus mechanisms and reduces validation time compared with public blockchain systems. As a result, the blockchain-induced delay remains bounded and does not dominate end-to-end communication latency, as confirmed by the observed low delay and jitter values in the simulation results. A trade-off naturally exists between security and performance. Increasing the frequency of blockchain verification improves resistance to routing manipulation and replay attacks but may introduce additional processing delay. Conversely, reducing validation frequency enhances responsiveness but lowers security guarantees. The proposed CL-MABRC framework balances this trade-off by selectively invoking blockchain validation only for critical routing decisions, thereby achieving robust security without compromising real-time performance. This design makes the approach well suited for latency-sensitive VANET applications.

5.2 | Scalability Considerations of the Proposed Model

The scalability of the proposed framework is addressed through its modular and localized design, which limits global network dependencies as vehicle density increases. The M-BHC algorithm forms clusters based on local mobility patterns and adaptive communication ranges, ensuring that clustering decisions rely only on neighboring vehicles rather than the entire network. This localized clustering approach reduces control OH and prevents excessive re-clustering in dense scenarios. The EPOA-based CH selection operates within clusters, distributing computation and energy consumption and avoiding centralized optimization. Furthermore, the CL-MABRC routing protocol employs multi-attribute path selection and blockchain verification at the cluster level, restricting ledger interactions to selected routes instead of network-wide consensus. This hierarchical and cross-layer architecture ensures that increases in node density result in logarithmic growth of computational and communication OH. Consequently, the proposed model maintains stable throughput, low latency, and energy efficiency as network scale increases, making it suitable for large-scale and dense VANET deployments.

5.3 | Computational Complexity in Large-Scale Deployments

The proposed CL-MABRC framework is designed for scalability and practical feasibility in real-world, large-scale VANET deployments. The computational complexity of O(n log n) arises from the hierarchical, cluster-based processing: M-BHC performs localized mobility-aware clustering within neighborhoods rather than the entire network, whereas EPOA optimizes cluster-head selection within each cluster. Cross-layer routing and blockchain validation are applied only along selected paths, limiting ledger and verification OH. This hierarchical and localized approach ensures that computation grows sublinearly

with network size, avoiding bottlenecks in dense scenarios. Additionally, the lightweight bio-inspired optimization and localized blockchain operations reduce processing demands on vehicular onboard units, enabling real-time operation even in ultra-dense environments. Simulation results demonstrate low clustering and routing OH, confirming that the proposed framework can be deployed in large-scale VANETs without excessive computational burden or delay, making it suitable for practical vehicular communication systems.

5.4 | Limitations of the Proposed Framework

Although the proposed M-BHC, EPOA, and CL-MABRC framework demonstrates high performance in VANET scenarios, several limitations exist. The M-BHC clustering relies on accurate mobility prediction; sudden or erratic vehicle movements may reduce cluster stability and increase re-clustering OH. EPOA assumes that vehicles can provide accurate energy and connectivity information; discrepancies due to sensor errors or communication delays may affect CH selection. CL-MABRC employs blockchain-based validation, which introduces additional latency and storage OH under ultra-dense network conditions. Furthermore, extremely high vehicle densities or highly dynamic urban scenarios may challenge real-time computation, despite the O(n log n) complexity. Finally, the current model does not consider physical-layer interference or heterogeneous communication technologies. These limitations provide opportunities for future enhancements, such as incorporating adaptive mobility prediction, hybrid consensus mechanisms, and multi-radio integration.

6 | Conclusion

In this work, a detailed framework is introduced to boost VANET performance by incorporating three innovative algorithms: M-BHC, EPOA, and CL-MABRC. The findings demonstrate that the proposed framework effectively meets the primary goals outlined in this work, which include enhancing clustering stability in highly dynamic settings, optimizing the energy-efficient selection of CHs, and improving secure and congestion-aware routing. M-BHC adeptly creates stable clusters by utilizing real-time mobility data, whereas EPOA ensures optimal energy allocation in environments with limited resources. CL-MABRC integrates blockchain validation with cross-layer routing strategies to secure communication and dynamically manage congestion. Together, these strategies lead to notable performance improvements in terms of throughput (99.89 Kbps), EED (3.9 ms), energy consumption (41.98%), and network security (99.7%) compared with existing protocols such as OSC-GOR, ELAACR, TMOHBA, and RCSRC. However, this framework has certain limitations. The computational demands of blockchain validation can affect the scalability of the resource-constrained vehicular nodes. Additionally, the current model has been tested in simulated static traffic scenarios, which may not fully reflect the variability of real-world vehicular environments. Future work will aim to overcome these limitations by optimizing the energy usage of blockchain processes, expanding the framework to accommodate higher vehicle densities, and incorporating real-time traffic predictions using machine learning. Furthermore, deploying and evaluating the framework in real-world VANET settings with varied traffic and environmental conditions will offer more insight into its practical applicability. Integrating emerging technologies such as 6G, edge computing, and vehicular fog networks could further enhance the adaptability, scalability, and alignment of the framework with next-generation intelligent transportation systems. Although the current evaluation focuses on a traffic density of 100 vehicles/km^2, which represents moderate to high urban traffic conditions, ultradense vehicular scenarios introduce additional challenges such as severe channel contention, increased collision probability, and higher blockchain validation OH. Evaluating such conditions requires extensive large-scale simulations and parameter tuning to ensure fair comparison across protocols. Although these experiments are beyond the scope of the present study, the proposed cross-layer design and adaptive congestion-aware routing mechanism are inherently scalable, as they dynamically adjust clustering, routing, and congestion control based on local network conditions. A comprehensive evaluation under ultra-dense scenarios (e.g., ≥ 500 vehicles/km^2) will be conducted in future work to further validate scalability and robustness.

Funding

The authors have nothing to report.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

1. M. El-Dalahmeh, "An ECIES-Based Framework for Ensuring Security in VANET Using SDN and Fog Computing (Doctoral dissertation, Teesside University),".

2. D. Desai, H. El-Ocla, and S. Purohit, "Data Dissemination in VANETs Using Particle Swarm Optimization," *Sensors (Basel)* 23, no. 4 (2023): 2124.

3. R. Nasir, H. Ashraf, and N. Z. Jhanjhi, "Secure Authentication Mechanism for Cluster Based Vehicular Adhoc Network (VANET): A Survey," (2023), arXiv preprint arXiv:2312.12925.

4. A. Bijalwan, I. Hussain, K. C. Purohit, and M. A. Kumar, "Enhanced Ant Colony Optimization for Vehicular Ad Hoc Networks Using Fittest Node Clustering," *Sustainability* 15, no. 22 (2023): 15903.

5. M. A. Angel and T. Jaya, "An Enhanced Emperor Penguin Optimization Algorithm for Secure Energy Efficient Load Balancing in Wireless Sensor Networks," *Wireless Personal Communications* 125, no. 3 (2022): 2101–2127.

6. S. H. Gopalan, J. Ashok, A. Manikandan, and S. Ramalingam, "Data Dissemination Protocol for VANETs to Optimize the Routing Path Using Hybrid Particle Swarm Optimization With Sequential Variable Neighbourhood Search," *Telecommunication Systems* 84, no. 2 (2023): 153–165.

7. G. Nithyanandam, C. Ambiyaram, and S. Prabathkumar, "An Intelligent Hybrid Prairie Dog Optimization Algorithm-Based Stable Cluster Reliable Routing Scheme for VANETs," *International Journal of Communication Systems* 36, no. 14 (2023): e5549.

8. A. Kumar, A. K. Dubey, S. Ahuja, and V. Dutt, "Efficient Privacy Preserving Lightweight Cryptography for Multi-Hop Clustering in Internet of Vehicles Network," (2023).

9. M. A. Shah, F. Zeeshan Khan, G. Abbas, et al., "Optimal Path Routing Protocol for Warning Messages Dissemination for Highway VANET," *Sensors* 22, no. 18 (2022): 6839.

10. P. V. Sontakke and N. B. Chopade, "Hybrid DNN-BiLSTM-Aided Intrusion Detection and Trust-Clustering and Routing-Based Intrusion Prevention System in VANET," *Journal of Control and Decision* 12, no. 2 (2023): 1–18.

11. M. A. Habeeb, Y. L. Khaleel, and A. R. Abdulnabi, "Enhancing Security and Performance in Vehicular Adhoc Networks: A Machine Learning Approach to Combat Adversarial Attacks," *Mesopotamian Journal of Computer Science* 2024 (2024): 122–133.

12. P. Sehrawat and M. Chawla, "Prediction and Analysis of Machine Learning Models for Efficient Routing Protocol in VANET Using Feature Information," *Wireless Personal Communications* 136 (2024): 735–758.

13. A. D. Sree and K. Sharma, "Machine Learning Based Secure Routing Protocol With UAV-Assisted for Autonomous Vehicles," *International Journal of Sensors Wireless Communications and Control* 14, no. 1 (2024): 55–65.

14. M. Gayathri and C. Gomathy, "Design of CSKAS-VANET Model for Stable Clustering and Authentication Scheme Using RBMA and Signcryption," *Frontiers in Computer Science* 6 (2024): 1384515.

15. M. Odiagbe, O. Osanaiye, and O. Oshiga, "An Effective Traffic Management Framework for Congestion Prediction and Re-Routing Using Hybridized Techniques," *International Journal of Intelligent Transportation Systems Work* 22 (2024): 687–706.

16. G. Kaur and D. Kakkar, "Fr-Aro: Secure Interference Aware Fuzzy Based Clustering and Hybrid Optimization Driven Data Routing in VANETs," *Ad Hoc Networks* 151 (2023): 103298.

17. A. A. Monisha, T. R. Reshmi, and K. Murugan, "Secure Relay Selection Scheme for Traffic Congested Zone in VANET Using Grasshopper Optimization and Modified Authentication Key Agreement Algorithms," *Applied Intelligence* 53, no. 5 (2023): 5497–5518.

18. F. Qazi, S. A. Khan, F. Hanif, and D. E. S. Agha, "Efficient Routing Algorithm Towards the Security of Vehicular Ad-Hoc Network and Its Applications," *International Journal of Wireless Information Networks* 31, no. 1 (2024): 12–28.

19. U. Kaur, A. N. Mahajan, S. Kumar, and K. Dutta, "Jellyfish Search Chimp Optimization Enabled Routing and Attack Detection in SDN Based VANETs," *Wireless Personal Communications* 138, no. 2 (2024): 819–859.

20. M. V. Kadam, V. M. Vaze, and S. R. Todmal, "TACR: Trust Aware Clustering-Based Routing for Secure and Reliable VANET Communications," *Wireless Personal Communications* 132, no. 1 (2023): 305–328.

21. G. Husnain, S. Anwar, G. Sikander, A. Ali, and S. Lim, "A Bio-Inspired Cluster Optimization Schema for Efficient Routing in Vehicular Ad Hoc Networks (VANETs)," *Energies* 16, no. 3 (2023): 1456.

22. A. Ali, M. Assam, M. Alajmi, et al., "Arithmetic Optimization Based Secure Intelligent Clustering Algorithm for Vehicular Adhoc Network," *PLoS ONE* 19, no. 9 (2024): e0309920.

23. H. A. Ahmed, H. M. Jasim, A. N. Gatea, A. A. A. Al-Asadi, and H. A. A. Al-Asadi, "A Secure and Efficient Blockchain Enabled Federated Q-Learning Model for Vehicular Ad-Hoc Networks," *Scientific Reports* 14, no. 1 (2024): 31235.

24. K. Sarathkumar, P. Sudhakar, and A. C. Kanmani, "Enhancing Intrusion Detection Using Coati Optimization Algorithm With Deep Learning on Vehicular Adhoc Networks," *International Journal of Information Technology* 16 (2024): 3009–3018.

25. K. Suganyadevi and V. Nandalal, "Swarm Intelligence-Inspired Meta-Heuristics Hybrid Optimization for Multi-Constraint Routing in Vehicular Adhoc Networks," *IETE Journal of Research* 70, no. 1 (2024): 95–115.

26. N. S. Divya, V. Bobba, and R. Vatambeti, "An Adaptive Cluster Based Vehicular Routing Protocol for Secure Communication," *Wireless Personal Communications* 127 (2022): 1717–1736.

27. B. Kheradmand, A. Ghaffari, F. S. Gharehchopogh, and M. Masdari, "Cluster-Based Routing Schema Using Harris Hawks Optimization in the Vehicular Ad Hoc Networks," *Wireless Communications and Mobile Computing* 2022, no. 1 (2022): 1606317.

28. I. Alam, M. Manjul, V. Pathak, et al., "Efficient and Secure Graph-Based Trust-Enabled Routing in Vehicular Ad-Hoc Networks," *Mobile Networks and Applications* 29 (2024): 1732–1752.

29. A. Sajithabegam and T. Menakadevi, "An Enhanced Energy and Distance Based Optimized Clustering and Dynamic Adaptive Cluster-Based Routing in Software Defined Vehicular Network," *Telecommunication Systems* 87 (2024): 917–937.

30. A. Punitha and S. Raghupathi, "OSC-GOR: Optimal Security-Aware Cluster-Based Hybrid Geographical and Opportunistic Routing for Vehicular ad hoc Networks," *International Journal of Image and Graphics* 26 (2024): 2650023.

31. R. Kumar, S. K. Singh, D. K. Lobiyal, S. Kumar, and S. Jawla, "Security Metrics and Authentication-Based Routing (SMART) Protocol for Vehicular IoT Networks," *SN Computer Science* 5, no. 2 (2024): 236.

32. I. Souissi, R. Abidi, N. B. Azzouna, T. Berradia, and L. B. Said, "ECOTRUST: A Novel Model for Energy COnsumption TRUST Assurance in Electric Vehicular Networks," *Ad Hoc Networks* 149 (2023): 103246.

33. R. Ramamoorthy, "An Enhanced Location-Aided Ant Colony Routing for Secure Communication in Vehicular Ad Hoc Networks," *Human-Centric Intelligent Systems* 4, no. 1 (2024): 25–52.

34. P. Mutalik and V. C. Patil, "Trust Based Multi Objective Honey Badger Algorithm to Secure Routing in Vehicular Ad-Hoc Networks," *International Journal of Electrical and Computer Engineering (IJECE)* 13, no. 5 (2023): 2088.

35. A. Behura, A. Kumar, and P. K. Jain, "A Multi-Objective Approach for Secure Cluster Based Routing & Attack Classification in VANETs," *Peer-to-Peer Networking and Applications* 18, no. 3 (2025): 1–40.

36. R. K. Mahesh and S. S. Jawaligi, "Energy-Efficient Cluster-Based Routing in VANET Assisted by Hybrid Jellyfish and Beluga Optimisation and Fault Tolerance," *International Journal of Vehicle Autonomous Systems* 18, no. 1 (2025): 1–30.

37. V. Krishna Meera, C. Balasubramanian, and R. Praveen, "Hybrid Hippopotamus Optimization Algorithm–Based Energy-Efficient Stable Cluster Construction Protocol for Data Routing in VANETs," *International Journal of Communication Systems* 38, no. 13 (2025): e70171.

38. F. Ajaz, M. Naseem, J. V. N. Ramesh, M. Shabaz, and G. Ahamad, "Cluster Based Lion Optimization Routing Protocol for Internet of Vehicles (CLORP)," *Transactions on Emerging Telecommunications Technologies* 36, no. 3 (2025): e70089.

39. W. Ali, S. Z. Ninoria, G. Khan, and K. K. Gola, "Robust Cryptographic Scheme for Reliable Data Communication in VANET (RCSRC) Using Clustering Approach," *EURASIP Journal on Wireless Communications and Networking* 2024, no. 1 (2024): 1–26.

40. C. Swamynathan, R. Shanmugam, K. P. Mohan Kumar, and B. Subbiyan, "Traffic Prevention and Security Enhancement in VANET Using Deep Learning with Trusted Routing Aided Blockchain Technology," *Transactions on Emerging Telecommunications Technologies* 35, no. 11 (2024): e70004.

41. N. Gopinath, A. Chinnasamy, and T. S. Kumar, "Hybrid Flying Foxes and Enhanced Whale Algorithm-Based Cluster Optimization

Method for Efficient Stable Routing in Vehicular Ad Hoc Networks (VANETs)," *International Journal of Communication Systems* 38, no. 8 (2025): e70076.

42. S. Dong, H. Su, Y. Xia, et al., "A Comprehensive Survey on Authentication and Attack Detection Schemes That Threaten It in Vehicular Ad-Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems* 24, no. 12 (2023): 13573–13602.

43. X. Liu, J. Wang, S. Guo, and H. Wang, "A Survey on Cross-Layer Authentication in Wireless Communication Networks," *Journal of Networking and Network Applications* 4, no. 1 (2024): 21–30.

44. P. Mutalik and V. C. Patil, "Trust Based Multi Objective Honey Badger Algorithm to Secure Routing in Vehicular Ad-Hoc Networks," *International Journal of Electrical and Computer Engineering* (2088–8708) 13, no. 5 (2023): 5190–5197.

45. D. Desai, H. El-Ocla, and S. Purohit, "Data Dissemination in VANETs Using Particle Swarm Optimization," *Sensors* 23, no. 4 (2023): 2124.

46. K. Bagirathan, N. Saravanan, and K. Vijayabhaskar, "An Intelligent Recurrent Neural Network Driven Secured Routing Protocol for Vehicular Ad Hoc Networks," *Knowledge-Based Systems* 317 (2025): 113371.

47. M. V. K. Reddy, G. K. Kumar, P. V. Terlapu, D. Jayaram, and S. Samreen, "Trust Enabled Secure Routing in Vehicular Adhoc Networks," *International Arab Journal of Information Technology* 22, no. 3 (2025): 592–613.

48. C. Bachina, N. A. Kumar, S. Sheema, B. Al-Nassar, A. B. Amale, and S. Murugan, "Efficient Stable Cluster Management Model for NDN Heterogeneous Vehicular Ad Hoc Networks," 2025 International Conference on Frontier Technologies and Solutions (ICFTS), Chennai, India, (2025), 1–7, https://doi.org/10.1109/ICFTS62006.2025.11031987.

49. S. Anand and P. Nagarjuna, "Enhanced Ensemble Deep Learning Framework for Optimized Communication in Vehicular Ad Hoc Networks," *ICTACT Journal on Communication Technology* 16, no. 2 (2025): 3533–3538.

50. A. Devi, R. Kait, and V. Ranga, "Secure and Efficient Routing in Fog-Enabled VANETs: A Clustering-Based Approach,".