Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.079584

ARTICLE

Energy-Efficient and Load-Balanced Edge-Driven Vehicular Network Using Intelligent Task Offloading

Salahuddin[1], **Khalid Haseeb**[1,*], **Mansoor Nasir**[1], **NZ Jhanjhi**[2] and **Mamoona Humayun**[3]

[1]Department of Computer Science, Islamia College Peshawar, Peshawar, Pakistan
[2]School of Computer Science, Taylor's University, Subang Jaya, Selangor, Malaysia
[3]School of Computing, Engineering and the Built Environment, University of Roehampton, London, UK

*Corresponding Author: Khalid Haseeb. Email: khalid.haseeb@icp.edu.pk

Received: 24 January 2026; Accepted: 10 April 2026; Published: 08 May 2026

ABSTRACT: Intelligent Transportation System (ITS) interconnects smart technologies for the advancement in communication and autonomous decision making in vehicle interactions. It manages traffic control infrastructure, analyses road conditions, and supports cooperative awareness in a crucial environment. The sensors continuously collect real-time vehicle data, process it, and forward it to analysis servers to predict the behavior of Vehicular Ad hoc Networks (VANETs). Many approaches have been proposed to address research challenges in routing and improve communication for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) systems. However, due to dynamic topology, the network becomes disturbed and loses established connections, leading to instability in data transmission against unpredictable behavior of the network. This research presents a framework, referred to as Energy Efficient Load Balanced Edge-Driven Vehicular Networks (EELB-EVN), that aims to attain load-balanced communication across vehicles and the interconnected infrastructure, thereby preventing congestion and reducing computational cost. In addition, an Intelligent offloading technique is developed using the Analytical Hierarchy Process (AHP) to reduce the additional overhead on the devices, thus enabling energy-aware and latency-sensitive vehicular communication. Furthermore, trustworthiness strategies are explored to enhance reliability and ensure the credibility of information. The simulation tests revealed the significance of the proposed framework compared to related schemes in terms of energy consumption and latency by 20% to 25%, task success rate and network throughput by 30% to 40%, and computational complexity by 33% across dynamic vehicular scenarios.

KEYWORDS: Internet of Things; vehicular networks; edge computing; trustworthiness; energy efficiency

1 Introduction

In recent decades, the Internet of Things (IoT) has supported the integration of communication devices, vehicles, cloud platforms, and roadside units to form vehicular networks. It leads to processing and analyzing the collected data regarding traffic and environmental conditions to enable an intelligent transportation system with autonomous decision-making for road safety [1,2]. By exploring emerging wireless technologies integrated with cloud-level processing, it also enables vital functionalities that make VANETs more flexible in smart cities and automates the vehicle's interactions with manageable operational cost [3,4]. The use of artificial intelligence techniques enables the prediction of dynamic behavior of vehicles to assist the distributed learning practices [5,6]. Such strategies maintain collaborative processing with latency-aware transmission for Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) systems. In VANETS, edge computing provides the functionality of processing data and handling vehicle and RSU demands locally, rather than transmitting them to centralized analysis servers, thus efficiently utilizing resources and enabling decision-making for road safety and improving urban infrastructure [7,8]. Although many intelligent approaches have been proposed to address high mobility and rapid topology management in VANETs, they improve routing performance under critical conditions [9,10]. However, addressing latency and congestion-aware communication for dynamic channel modelling is a significant research challenge [11,12], thus effective load balancing prevents bottlenecks and a single point of failure in communication. Furthermore, securing the vehicular network against threats provides a trusted system for critical information sharing and maintains the integrity of IoT-ITS [13,14].

Although most of the existing approaches address the research challenge for vehicular networks for the management of dynamic topologies. However, rapid changes in vehicle positions lead to unbalanced load balancing between the RSUs and network edges, resulting in unpredictable communication gaps and routing holes. The higher frequency of session regeneration across vehicles results in additional communication costs and increased network delays. Thus, to achieve load balancing in the proposed approaches, the factor of timely delivery, along with latency-aware transmission, should be included. Furthermore, most recent approaches fail to detect malfunctioning devices in the presence of malicious devices, thereby compromising the efficiency of VANETs for network security and trustworthiness. This situation increases the likelihood of data leakage and unauthorized access to communication channels, thereby leading to message eavesdropping and misleading navigation systems. The main aim of this research is to introduce an energy-aware, load-balanced framework for vehicular networks that integrates intelligent offloading with edge computing. The three-layer architecture is developed to attain resource efficiency and optimize task offloading using the AHP-based Multi-Criteria Decision-Making method [15]. The vehicle tier generates task offloading decisions by exploring multi-level optimisation criteria. The Edge tier is an intermediate tier that distributes processing functionality and trust computation. Moreover, load balancing across vehicles is achieved through priority-based queuing mechanisms, providing effective, timely responses in a critical environment. Lastly, the cloud tier enables global data analytics, maintains trust, and regularly captures network behaviour for security purposes. The following are the significant contributions of our research study.

i. Develops an intelligent decision mechanism for task offloading along with trust-aware communication for vehicles. It optimizes the resources using multi-criterion computing and transfers the high-cost tasks towards the RSU rather than local vehicle-level processing.
ii. Adaptive load balancing with Trust-Weighted Distribution is developed to uniformly distribute network services across available RSUs, integrating security. In addition, based on network conditions, a priority-based scheduling scheme is proposed to handle multiple tasks on network edges.
iii. An energy-aware communication algorithm is designed, along with selected trusted paths, to optimise resource usage without malicious devices compromising security.

The rest of the paper is structured as follows. Section 2 presents a literature review and highlights the problem gap. The details of the proposed framework are discussed in Section 3. Section 4 elaborates on the experiments and the results discussion. In the end, a conclusion is provided in Section 5.

2 Related Work

ITS and IoT systems enabled the development of a smart system with effective communication and timely decision-making for real-time environments [16,17]. It provides traffic monitoring with RSU support and automates the sensing system to monitor road safety and support autonomous driving applications [18,19]. The evolution of edge technologies has also enabled significant growth in interaction with the physical environment and in maintaining the flow of information systems in complex mobile networks [20,21]. However, many existing applications are still exploring centralised architectures for vehicle traffic management, which impose additional complexity and computational overhead on the tiny, unpredictable devices [22,23]. Such schemes also face routing holes, data security issues, and single points of failure in large-scale IoT networks, thereby diminishing the quality of their vehicular services. The lack of load balancing not only degrades the performance in crucial infrastructure, but also minimizes the stability of the smart network with non-uniform resource utilization [24,25]. The authors [26] proposed a Harris Hawks Optimization-based clustering algorithm for VANETS (HHOCNET), which aims to increase energy efficiency by selecting cluster heads based on multiple parameters. In addition, as vehicles update their positions, the clusters are reformulated to maintain the network topology and enhance vehicle-to-vehicle interactions. The clustering overhead is reduced through HHO's intelligence, thereby decreasing the frequency of cluster head reselection, resource utilization and communication costs.

The study [27] introduces the Traffic-Aware Clustering-Based Routing Protocol (TACRP) for efficient and reliable data routing in VANETS and maintains the stability of the IoT network. It generates various clusters by exploring the traffic-aware information and vehicle mobility patterns, and later selects an optimal cluster head to establish intra and inter-cluster communication. Whenever network topology changes due to traffic, it re-selects cluster heads, reducing the frequency of route changes. Accordingly, providing a multi-hop routing mechanism enables the timely delivery of transportation data while supporting energy-efficient communication. The study [28] proposes a dynamic service-oriented approach for software-defined in-vehicle networks, extending SDN's application to support adaptive and service-oriented architectures. The proposed approach compares SDN-controlled service discovery with standard Ethernet switching, and the results show that SDN switching is superior in terms of adaptability, robustness, security, and Quality-of-Service. The study [29] has examined SDN-enabled vehicular networks from the perspective of platooning applications and has provided evidence for the theoretical foundations and practical implementations of SDN in controlling multiple onboard communication interfaces. The proposed solution makes it clear that SDN is a necessary component for developing safety, maintenance, and infotainment services for vehicle platoons. However, the majority of the approaches deal with the problems separately rather than offering a new solution with all the factors together, that is, energy, trust, security, and performance, being optimized.

Authors [30] propose a Distributed Ledger Technology (DLT)-assisted protocol, which aims to provide reliable and trustworthy communication in vehicular networks. In addition, a blockchain ledger enables transparent, verifiable data and effective communication between vehicles, facilitating authentic interactions. It prevents network threats and device or connected RSU misbehavior while reducing the computational overhead in a large-scale transportation system. The study [31] introduces the Secure Greedy Highway Routing Protocol (GHRP), a secure routing protocol that enhances data privacy and reliability in VANETS compared to existing approaches. In the first stage, the source, intermediate, and destination devices utilise hashing chains for authentication, while in the second stage, data security is achieved using one-way hashing. It also protects communication against black hole attacks, and its performance showed significant improvements in network metrics, particularly packet delivery rate, overhead, and average end-to-end delay. The study [32] introduces ECRDP, a hybrid clustering and routing scheme integrated with Density Peaks Clustering (DPC) and Particle Swarm Optimization (PSO), aiming to formulate the clusters and selection of optimal cluster heads. It proposed a fitness function for the chosen and appointment of suitable devices as a cluster heads by exploring features of DPC. The generated clusters are formulated based on the reliability of links between vehicles, thereby enhancing the stability of communication in a high-mobility urban environment. In addition, cluster heads are reselected to control and manage the dynamic topology of vehicular networks. Table 1 presents a comparative analysis of most of the existing approaches with our proposed framework.

Table 1: Feature comparison of existing schemes and proposed framework.

Feature	Existing Schemes	Proposed Framework
Network Management		
Dynamic topology	~	✓
Load balancing	~	✓
Communication gaps	~	✓
Routing holes	~	✓
Performance Optimization		
Latency-aware	×	✓
Energy efficiency	~	✓
Session optimization	×	✓
Trustworthiness		
Malicious detection	×	✓
Trust management	×	✓
Network security	~	✓
Intelligence		
Adaptive decisions	×	✓

✓: Supported ~: Partial ×: Not supported.

3 Proposed Methodology

This section explains the methodology of the EELB-EVN framework, which aims to develop a load-balanced, energy-efficient and trustworthy vehicular system. It enables multi-tier task offloading through an intelligent decision mechanism that maintains security and reliability against potential attacks.

3.1 System Model

In this section, the system model is elaborated on the interactions among vehicles, edges/RSUs, and bidirectional communication channels. Each vehicle V_i in the network is characterized using energy resource E_i, trust level Tr_i, location Lc_i, and existing load L_i, as given in Eq. (1). Fig. 1 depicts the network architecture of the proposed framework that comprised on different layers and their associate for the formulation of energy efficient and trusted communication.

$$V_i = \{E_i, L_i, Tr_i, Lc_i\} \tag{1}$$

At time t, vehicle V_i consumes energy E_{con} using Eq. (2).

$$E_{con}(V_i, t) = E_{idle} + E_{proc} \cdot L_i(t) + E_{\text{comm}} \cdot R_i(t) + E_{mov} \cdot V_{speed}(t) \tag{2}$$

where E_{idle}, E_{proc}, E_{comm}, and E_{mov} represent base, processing, communication, and movement energy consumption, respectively. Each RSU j acts as an edge with processing tasks C_j, queue length Q_j, Trust score Tr_j and current location L_j, as defined in Eq. (3).

$$R_j = \{C_j, Q_j, Tr_j, L_j\} \tag{3}$$

The communication links of the vehicular system for devices i and j can be determined using the straight-line distance metric $d(P_i, P_j)$, as given in Eq. (4).

$$d(P_i, P_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{4}$$

In addition, to distribute the tasks from vehicle V_i to RSU R_j, an offloading function can be established using Eq. (5), such that V_i should lie within the transmission range $Tran(R)$ of R_j.

$$L_{(V_i, RSU)} = \begin{cases} Active & \text{if } d(P_i, P_j) \leq Tran(R) \\ Inactive & otherwise \end{cases} \tag{5}$$

To load balancing and task forwarding for adjacent network edges is generated when both RSUs R_i and R_j fall in the same transmission range, and R_j is the neighbour of R_i, as given in Eq. (6).

$$L(R_i, R_j) = \begin{cases} \text{Active} & \text{if } d(P_i, P_j) \leq Tran(R) \text{ and } R_j \in N_i \\ \text{Inactive} & \text{otherwise} \end{cases} \tag{6}$$

In the proposed framework, the trust score for vehicle i is determined using Eq. (7) using a threshold limit θ.

$$\text{V(i)} \begin{cases} \text{trustworthy,} & T_i = \sum_{k=1}^{n} w_k p_{i,k} \geq \theta, \\ \text{untrustworthy,} & T_i < \theta, \end{cases} \tag{7}$$

where $p_{i,k}$ is the k-th normalized parameter of vehicle i in terms of packet reception rate and channel condition, w_k is its AHP-derived weight, n denotes the number of trust parameters, and the threshold is given by θ.

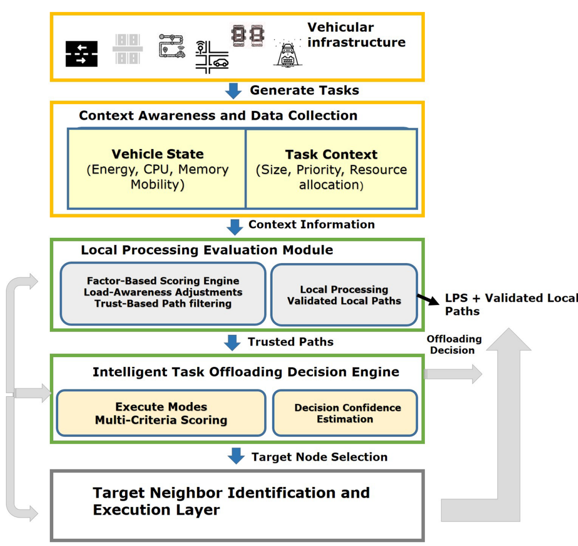


Figure 1: Network architectural flow of the proposed vehicular IoT-edge framework.

3.2 Intelligent Edge-Driven Decision Mechanism for Task Offloading

In this phase, task offloading is implemented using edge-level decision-making methods, providing an optimized and intelligent forwarding system for vehicular networks. The multi-criterion function consists of three parameters: k, i.e., energy, priority, and trust, which are utilized to compute the processing score. Firstly, the local processing score for vehicle i is computed to assess the suitability of processing tasks, as given in Eq. (8).

$$S_{\text{local}} = \left(\sum_{i=1}^{k} w_i^{\text{AHP}} \times f_i \right) \times P_{\text{penalty}} \times B_{\text{bonus}} \tag{8}$$

where w_i^{AHP} denotes the weighted contribution of the i factor using AHP or each parameter, $f_i \in [0,1]$ provides the normalized value, $P_{\text{penalty}} \in (0,1]$ and $B_{\text{bonus}} \geq 1$ are Bonus and Penalty values. Both functions provide dynamic adjustments to decision-making and enable more reliable task offloading services, as defined in Eqs. (9) and (10).

$$P_{\text{penalty}} = \prod_{k \in \{E,T,L\}} (1 - \alpha_k I_k) \tag{9}$$

$$B_{\text{bonus}} = \prod_{k \in \{E,T,L\}} (1 + \beta_k I_k) \tag{10}$$

where α_k denotes the weighted factor to control the particular impact of parameter, I_k is the indicator function, and $k \in \{E, T, L\}$ is various constraints in terms of energy, trust, and latency. Later, the RSU Offloading Score is computed, which is the most demanded function in the multi-criteria decision-making process. In ITS, network conditions are more dynamic, and device trust varies; thus, RSU accessibility is a critical factor in task offloading. The proposed framework determines the RSU offloading score S_{rsu} using Eq. (11). Fig. 2 shows the flowchart of the EELB-EVN framework for dynamic selection of AHP-based weights to support the decision-making system. Task offloading provides mechanisms for task execution, either locally or on the target device, to formulate routing paths that account for adaptive conditions and trust. In addition, the routes are dynamically updated by exploring updated multidimensional parameters and improving response time through time-sensitive task processing.

$$S_{rsu} = \left(\sum_{i=1}^{k} w_i^{\text{AHP}} \times f_i \right) \times P_{\text{network}} \times F_{\text{trust}} \tag{11}$$

where $P_{\text{network}} \in (0,1]$ denotes penalty for network condition and $F_{\text{trust}} \in [0,1]$ is trust parameter.

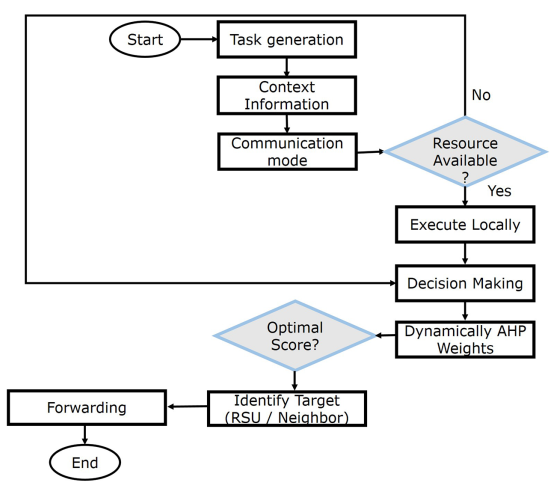


Figure 2: Procedural flow of the intelligent task offloading using dynamically AHP adjustment.

Energy-Aware Tasks Distributions and Allocation

This section presents the proposed energy-aware algorithm for lightweight communication and the mechanism for selecting trustworthiness routes in vehicular networks. The proposed framework minimizes the energy consumption by deciding the execution task i either locally or by offloading, as given in Eq. (12).

$$\min \sum_{i \in \{\text{local},\text{offload}\}} E_i \times x_i + E_{\text{transfer}} \tag{12}$$

where E_{local} denotes local processing energy consumption, $E_{offload}$ presents energy consumption for offloaded task execution, $E_{transfer}$ denotes the energy consumption in data forwarding, and $x_i \in \{0,1\}$ denotes variable for binary decision. In addition, the multi-hop route is selected for vehicular communication based on the highest trusted score using Eq. (13). Algorithm 1 governs the developed procedure of the proposed EELB-EVN framework to carry out the vehicular communication in a real-time environment with intelligent decision-making strategies. The AHP-based weighted distribution is explored to predict the target device for task offloading along the integration of edges, and enhances the efficiency of the vehicles with optimized performance in terms of resource consumption. Moreover, the trust is integrated to identify the more reliable edge devices to handle processing requests from the vehicles and to provide a fault-tolerant communication system.

$$\text{Trust}_{\text{path}} = \beta \cdot \max \begin{bmatrix} T_1 \\ T_2 \\ \vdots \\ T_n \end{bmatrix} \tag{13}$$

where max function identifies the highest trusted device and β denotes the trust influence in data transmission. Thus, the trusted and energy-efficient route r^* is formulated based on Eq. (14), and the trust level filter function is exploited in the identification of malicious vehicles, enhancing the reliable communication using Eq. (15). Fig. 3 shows the system design of the EELB-EVN framework along with all its development components.

$$p^* = \arg\min_{p \in P_{\text{tr}}} E_{\text{path}}(p) \tag{14}$$

$$P_{\text{tr}} = \{p : \forall i \in p, T_i \geq Thres\} \tag{15}$$

where P_{tr} is the set of candidate paths whose $T_i \geq thres$.

Algorithm 1: Energy-efficient and trust-aware task offloading decision

Input: VehicleState, Task, Network, Weights, PathNodes
Output: Mode, Confidence, Cost, Target
Initialize thresholds and scores;
for each $mode \in \{LOCAL, RSU, NEIGHBOR\}$ **do**
  Compute score using weighted factors (Energy, Complexity, Priority, Latency, Trust);
  Adjust score based on system load and normalize;
end
FilteredPath ← nodes in PathNodes with trust ≥ threshold;
Select Mode with highest score;
if *Mode* ≠ *LOCAL* **then**

(Continued)

Algorithm 1 (continued)

```
    Select Target from FilteredPath (high trust, low delay);
end
if scores are close then
    Prefer lower latency and higher trust;
end
Estimate Confidence and Cost (delay, energy);
return Mode, Confidence, Cost, Target
```

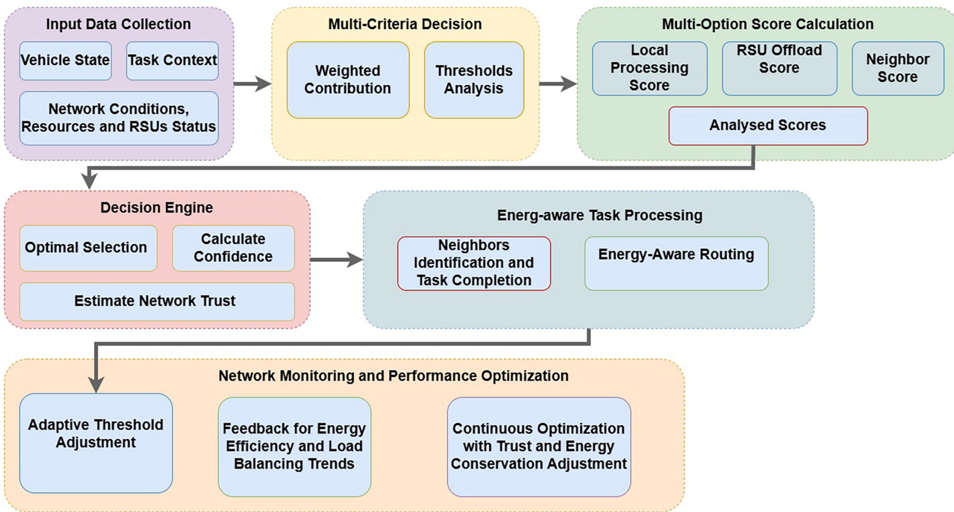


Figure 3: System design of the proposed edge-based IoT trusted framework for vehicular network.

4 Experimental Environment

This section explains the simulation configuration and analysis of performance metrics to assess the proposed EELB-EVN framework in Python 3.10+ with the integration of NS-3, SUMO for the simulated environment and mobility patterns. The analysis of the proposed EELB-EVN framework is measured against HHOCNET [26], ECRDP [32], and TACRP [27]. The vehicles range from 500 to 5000 for the construction of small-sized scenarios to larger ones. The number of RSUs is computed based on the vehicles, and a single RSU is assigned to 40–50 vehicles. RSUs serve as edge devices and handle task offloading. 30 tasks are generated per vehicle, and the simulation duration is determined by the total number of tasks. To estimate the level of trust and authentic vehicular communication, the number of malicious devices is estimated to range from 5% to 15%. A separate logging file is maintained to capture the vehicle traffic and track the vulnerable activities. The weighted contributions are analyzed using AHP to attain the reliability and consistency for vehicle communication. The proposed framework improves fault tolerance while increasing weighted trust values; however, it incurs slightly higher latency during device validation and trust maintenance. On the other hand, assigning higher weights to the latency parameter yields a rapid forwarding path when communicating with associated devices, and, ultimately, the highest weight is assigned to the energy factor, thereby enabling a longer network lifetime and establishing a robust network infrastructure. Accordingly, each parameter plays a vital role in developing a balanced multi-objective weighting strategy and in ensuring energy-efficient, intelligent decision-making in vehicular networks. Table 2 illustrates the parameters of the simulation configuration.

Table 2: Simulation parameters.

Parameter	Value
Initial energy	5 J
Mobile sensors	500–5000
RSU density	1 per 40–50 vehicles
Deployment	Random
Malicious devices	5%–15%
Sensing radius	5 m
Simulation runs	70
Communication protocol	IEEE 802.11p
Platform	Python 3.10+
Mobility model	SUMO
Network simulator	NS-3
Data size	512 bits
Benchmark schemes	TACRP, ECRDP, HHOCNET
Performance metrics	Energy, latency, success rate, throughput

Results Discussion

The scenario depicted in Fig. 4 presents the performance evaluation of energy consumption as the input varies from 500 to 5000. The proposed EELB-EVN framework consumes the least energy resource across vehicle densities among TACRP, ECRDP, and HHOCNET. This results from the early feasibility evaluation of local execution and the energy-aware scoring mechanism of EELB-EVN. The proposed EELB-EVN framework intelligently utilizes local resources and thus avoids the unnecessary processing for tasks offloading. Conversely, RSU-focused methods run the risk of overusing infrastructure nodes, thereby increasing energy consumption in vehicular transmissions. In addition, TACRP and HHOCNET lack energy-adaptive decision-making capabilities under increasing vehicular densities, therefore leading to inefficient network management, whereas EELB-EVN maintains energy-efficient performance, thus proving its scalability and also aptness for mobile, dense vehicular networks. Fig. 5 presents the performance analysis of energy consumption as vehicle mobility varies. As vehicle speeds increase, all methods show higher energy consumption due to increased communication, computation, and coordination overheads. Even so, the proposed EELB-EVN framework consumes less energy as compared to the existing approaches due to power-saving and nearly optimal load balancing while processing tasks and resource allocation. In addition, unlike baseline methods, the proposed EELB-EVN framework intelligently detects over-congested devices and, conversely, reduces unnecessary data transmission, thereby increasing energy efficiency and enabling a real-time vehicular system. The HHOCNET and TACRP approaches provide a moderate level of energy depletion; however, they are limited in efficient resource utilization. Similarly, the ECRDP approach leads to high network congestion due to the lack of a distributed communication paradigm in heterogeneous networks, thereby increasing energy consumption.

Fig. 6 illustrates the performance of network latency under the varying vehicles for the EELB-EVN approach and existing approaches. The results analysis revealed that the proposed EELB-EVN framework achieves the lowest network latency among all baseline approaches. This improvement can be attributed to the multi-criteria decision mechanism of the proposed EELB-EVN framework, which dynamically evaluates network conditions and ensures execution confidence through AHP weight adjustment. Unlike RSU-centric load balancing, the proposed EELB-EVN framework does not impose congestion at the boundaries of the vehicular system and selects the execution mode for effective processing of traffic with the least response time. Besides this, HHOCNETs that rely on static decision-making exhibit higher latency under dynamic traffic conditions. Fig. 7 demonstrates the evaluation of the proposed EELB-EVN framework and baseline approaches for network latency under varying mobility. Based on the results, it has been noticed that with the increase in the network load, power consumption also increases, because of the timely increase in demands for packet processing and transmission. However, the newly proposed EELB-EVN framework method does not budge under heavy network loads, as it optimizes energy use. Its power-aware scheduling and smart traffic engineering are the two main reasons behind this, and they work together to reduce bottlenecks and avoid unnecessary retransmissions. HHOCNET and TACRP produce energy patterns that fluctuate, thereby reflecting their dependence on load changes, whereas ECRDP postpones tasks in a worst-case scenario, as the very high traffic volume limits the performance of centralized RSUs.

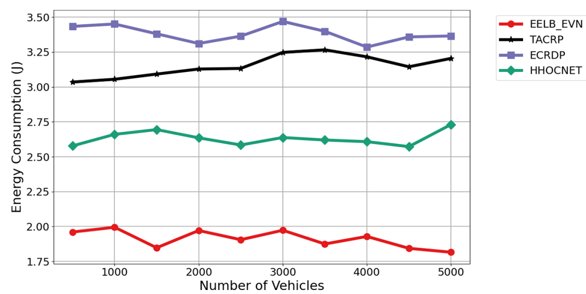


Figure 4: Performance impact of energy consumption for EELB-EVN, TACRP, ECRDP, and HHOCNET over varying vehicles.

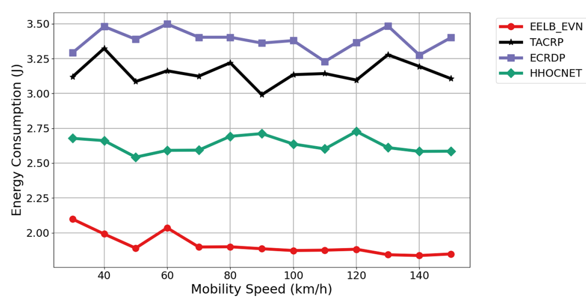


Figure 5: Performance impact of energy consumption for EELB-EVN, TACRP, ECRDP, and HHOCNET over varying speed.

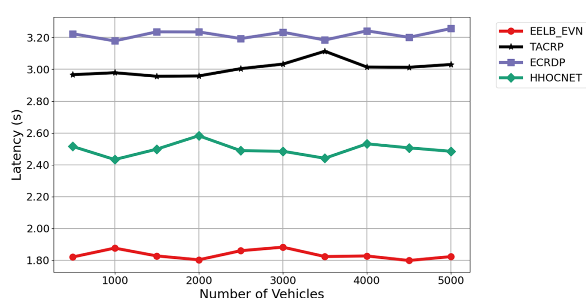


Figure 6: Performance impact of network latency for EELB-EVN, TACRP, ECRDP, and HHOCNET over varying vehicles.

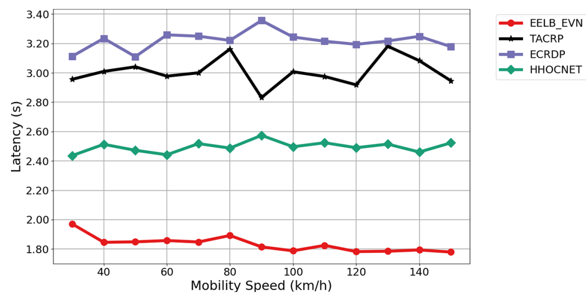


Figure 7: Performance impact of network latency for EELB-EVN, TACRP, ECRDP, and HHOCNET over varying speed.

Fig. 8 shows the performance evaluation of the proposed EELB-EVN framework across varying vehicles compared to existing approaches, in terms of task success rate. The results analysis demonstrates that the proposed EELB-EVN framework not only improves task success rates but also distributes a balanced load across network resources. This improvement is achieved through load-aware adaptation and trust-based route filtering mechanisms, which are the main building blocks of the proposed EELB-EVN framework for monitoring and regulating resource usage. As a result, it prevents certain RSUs or their neighbours from becoming overloaded and efficiently improves real-time data flow. On the other hand, TACRP, HHOCNET, and RSU focus on the lack of dynamic load awareness and are unable to optimally balance communication tasks. Fig. 9 illustrates the task success rate for the proposed EELB-EVN framework and existing approaches as a function of vehicle speed. Task contention and coordination complexity increase with dynamic topology, ultimately reducing success rates. However, the proposed EELB-EVN framework achieves the highest task success rate among baseline solutions for the vehicular system. This improvement is due to the optimised distribution of computational tasks between vehicles and edges to attain more robust long-run network connectivity. Moreover, unlike other baseline approaches, the proposed EELB-EVN framework ensures rapid task execution within a manageable response time and leads to efficient routing decisions by excluding bottlenecks during data transmission.

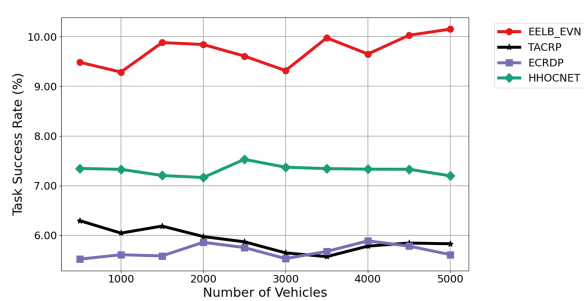


Figure 8: Performance impact of task success rate for EELB-EVN, TACRP, ECRDP, and HHOCNET over varying vehicles.

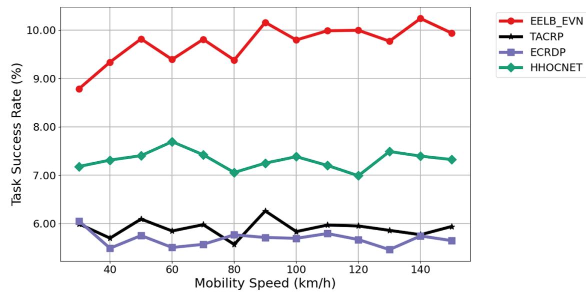
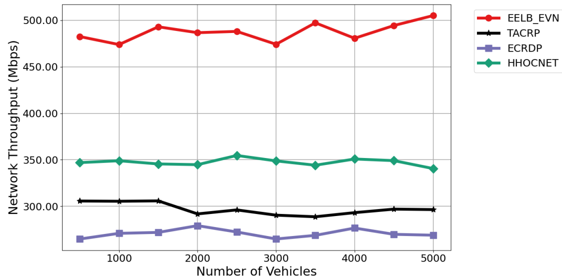
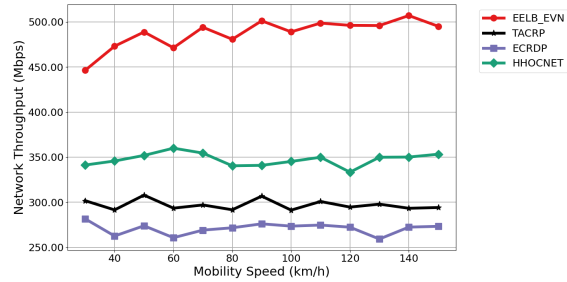


Figure 9: Performance impact of task success rate for EELB-EVN, TACRP, ECRDP, and HHOCNET over varying speed.

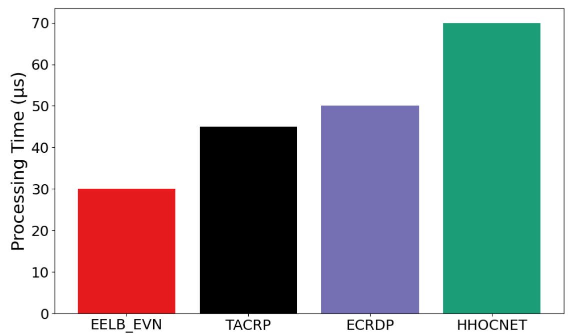
Fig. 10a illustrates the performance of the proposed EELB-EVN framework in terms of network throughput against baseline approaches. Based on the results, the proposed EELB-EVN framework enhances network throughput across varying vehicles by considering intelligent task offloading and controlling the contribution of each factor through dynamic weight adjustment. Moreover, the proposed EELB-EVN framework supports confidence-based decision-making, accounting for trust evaluation, energy feasibility, and system responsiveness for task execution. The existing methods, particularly HHOCNET and TACRP, are unable to support path filtering based on real-time computation and avoid the existing conditions while evaluating the device's trust. Furthermore, the success rates of RSU-based load balancing are also diminished by node congestion and computational overhead. In Fig. 10b, the performance of the proposed EELB-EVN framework is compared with benchmark approaches across varying vehicle speeds. Throughput usually increases effective device interaction and load balancing, but if resource management is inefficient, it can result in congestion and performance degradation. Based on the results, the EELB-EVN framework enhances network throughput under adaptive infrastructure and improves the traffic flowing among vehicles. Moreover, the consideration of intelligent decision-making criteria, effective bandwidth utilisation, and trust-aware data transmission enhances the network's ability to manage and process vehicular data. The routes are dynamically updated by exploring the latest device conditions and behavior, thereby improving data delivery performance in a critical environment for the transportation system. Fig. 10c illustrates the computational overheads in terms of processing time of the EELB-EVN framework and existing approaches over vehicular networks. It mainly depends on the varying vehicles, RSUs, and the decision-making algorithm, and is evaluated using AHP. In addition, detecting malicious activity requires complex infrastructure and imposes additional processing overhead on constrained devices. However, the EELB-EVN framework reduces processing time when evaluating local decisions compared to other solutions, owing to its edge-level decision-making policies, and achieves efficient load balancing while transporting vehicular data across unpredictable communication channels.



(a) Performance impact of network throughput over varying vehicles.



(b) Performance impact of network throughput over varying speed.



(c) Performance impact of processing time.

Figure 10: Performance comparison of EELB-EVN, TACRP, ECRDP, and HHOCNET under different evaluation metrics.

5 Conclusion

VANETs integrated with smart technologies have developed advanced, emerging protocols to facilitate and monitor ITS. Due to the high mobility and adaptive topologies, most existing approaches lead to link failures and introduce additional latency in the transmission of vehicular data and in traffic management. Furthermore, due to the unpredictable nature of ITS leads in networks, they are vulnerable to various threats, compromising network integrity. We proposed an energy-aware, load-balancing framework to address research challenges in routing and enhance trustworthiness in vehicular infrastructure. The adoption of AHP modelling to analyse the multiple factors in task offloading with the support of edge computing provides a reliable approach to uniform distribution of overhead on the devices, and decreases the probabilities of route dis-connectivity. Moreover, the trusted devices are assigned more priority for the formulation of paths and minimize the computational cost by preventing re-transmission of sensitive information for further processing and analysis. Unlike Deep Reinforcement learning (DRL), which requires significant computational overhead on constrained devices and imposes additional energy consumption on vehicular networks. The AHP offers a deterministic approach with lightweight, stable decision-making strategies that leverage multiple parameters in crucial network management. However, the proposed framework demands additional energy consumption as vehicle congestion increases during data capturing and forwarding, and it requires rapid task offloading services with associated resources. Over-congestion imposes additional resource consumption and ultimately reflects the stability of vehicular networks under dynamic topologies. In the future, we plan to integrate network slicing in our framework to process heterogeneous traffic separately and optimize the resources based on a particular application. In addition, the process of trust establishment, along with its maintenance in the presence of malfunctioning devices, needs to be explored.

Acknowledgement: The work was technically supported by the Department of Computer Science, Islamia College Peshawar, Peshawar, Pakistan. The authors are thankful for their support.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Conceptualization, Salahuddin, Khalid Haseeb; Formal analysis, Mansoor Nasir, Mamoona Humayun; Methodology, Salahuddin, Khalid Haseeb; Supervision, Khalid Haseeb, Mamoona Humayun; Validation, Mansoor Nasir, NZ Jhanjhi; Writing—original draft, Salahuddin, Mansoor Nasir; Writing—review & editing, Khalid Haseeb, NZ Jhanjhi. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: All data is available in the manuscript.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Dutta A, Samaniego Campoverde LM, Tropea M, De Rango F. A comprehensive review of recent developments in VANET for traffic, safety & remote monitoring applications. J Netw Syst Manag. 2024;32(4):73. doi:10.1007/s10922-024-09853-5.
2. Wang Y, Jiang J, Li S, Li R, Xu S, Wang J, et al. Decision-making driven by driver intelligence and environment reasoning for high-level autonomous vehicles: a survey. IEEE Trans Intell Transp Syst. 2023;24(10):10362–81. doi:10.1109/tits.2023.3275792.
3. Tripathy SS, Bebortta S, Mohammed MA, Deveci M, Marhoon HA, Martinek R. A secure mist-fog-assisted cooperative offloading framework for sustainable smart city development. Digital Commun Netw. 2026;12(1):165–79. doi:10.1016/j.dcan.2024.12.008.
4. Hazra A, Kalita A, Gurusamy M. Meeting the requirements of internet of things: the promise of edge computing. IEEE Internet Things J. 2023;11(5):7474–98. doi:10.1109/jiot.2023.3339492.
5. Mchergui A, Moulahi T, Zeadally S. Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs). Veh Commun. 2022;34(3):100403. doi:10.1016/j.vehcom.2021.100403.
6. Teixeira D, Ferreira J, Macedo J. Systematic literature review of AI/ML techniques applied to VANET routing. In: Future of Information and Communication Conference. Cham, Switzerland: Springer; 2022. p. 339–61.
7. Feng Z, Li K, Li B. A spectral clustering-based deployment strategy for roadside units in vehicular edge computing environments. Ad Hoc Netw. 2024;158(7):103483. doi:10.1016/j.adhoc.2024.103483.
8. Kalidoss L, Thouti S, Arunachalam R, Ramamurthy P. An efficient model of enhanced optimization and dilated-GRU based secured multi-access edge computing with blockchain for VANET sector. Expert Syst Appl. 2025;260(1):125275. doi:10.1016/j.eswa.2024.125275.
9. Behura A, Kumar A, Jain PK. A comparative performance analysis of vehicular routing protocols in intelligent transportation systems. Telecommun Syst. 2025;88(1):26. doi:10.1007/s11235-024-01243-1.
10. Upadhyay P, Marriboina V, Goyal SJ, Kumar S, El-Kenawy ESM, Ibrahim A, et al. An improved deep reinforcement learning routing technique for collision-free VANET. Sci Rep. 2023;13(1):21796. doi:10.1038/s41598-023-48956-y.
11. Liu T, Wang S, Dong Z, Li B, He T. From perception to computation: revisiting delay optimization for connected autonomous vehicles. ACM Comput Surv. 2025;57(8):1–45.
12. Song L, Hu X, Zhang G, Spachos P, Plataniotis KN, Wu H. Networking systems of AI: on the convergence of computing and communications. IEEE Internet Things J. 2022;9(20):20352–81.
13. Karthikeyan H, Usha G. A secured IoT-based intelligent transport system (IoT-ITS) framework based on cognitive science. Soft Comput. 2024;28(23):13929–39. doi:10.1007/s00500-023-08410-7.
14. Khanam S, Ahmedy IB, Idris MYI, Jaward MH, Sabri AQBM. A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE Access. 2020;8:219709–43. doi:10.1109/access.2020.3037359.

15. Vaidya OS, Kumar S. Analytic hierarchy process: an overview of applications. Eur J Oper Res. 2006;169(1):1–29.
16. Mahi MJN, Chaki S, Ahmed S, Biswas M, Kaiser MS, Islam MS, et al. A review on VANET research: perspective of recent emerging technologies. IEEE Access. 2022;10(2):65760–83. doi:10.1109/access.2022.3183605.
17. Zhang H, Li M. Towards an intelligent and automatic irrigation system based on internet of things with authentication feature in VANET. J Inf Secur Appl. 2025;88(4):103927. doi:10.1016/j.jisa.2024.103927.
18. Hasanujjaman M, Chowdhury MZ, Jang YM. Sensor fusion in autonomous vehicle with traffic surveillance camera system: detection, localization, and AI networking. Sensors. 2023;23(6):3335. doi:10.3390/s23063335.
19. Rawlley O, Gupta S. Artificial intelligence-empowered vision-based self driver assistance system for internet of autonomous vehicles. Trans Emerg Telecomm Technol. 2023;34(2):e4683. doi:10.1002/ett.4683.
20. Kong X, Wu Y, Wang H, Xia F. Edge computing for internet of everything: a survey. IEEE Internet Things J. 2022;9(23):23472–85. doi:10.1109/jiot.2022.3200431.
21. Sharma M, Tomar A, Hazra A. Edge computing for industry 5.0: fundamental, applications, and research challenges. IEEE Internet Things J. 2024;11(11):19070–93. doi:10.1109/jiot.2024.3359297.
22. Mostefaoui A, Merzoug MA, Haroun A, Nassar A, Dessables F. Big data architecture for connected vehicles: feedback and application examples from an automotive group. Fut Gener Comput Syst. 2022;134:374–87.
23. Ahmad Jan M, Adil M, Brik B, Harous S, Abbas S. Making sense of big data in intelligent transportation systems: current trends, challenges and future directions. ACM Comput Surv. 2025;57(8):1–43. doi:10.1145/3716371.
24. Khaledian N, Razzaghzadeh S, Haghbayan Z, Völp M. Hybrid Markov chain-based dynamic scheduling to improve load balancing performance in fog-cloud environment. Sustain Comput Inform Syst. 2025;45(1):101077. doi:10.1016/j.suscom.2024.101077.
25. Al-Mekhlafi ZG, Lashari SA, Al-Shareeda MA, Mohammed BA, Alshudukhi JS, Al-Dhlan KA, et al. Coherent taxonomy of vehicular ad hoc networks (VANETs)-enabled by fog computing: a review. IEEE Sensors J. 2024;24(19):29575–602. doi:10.1109/jsen.2024.3436612.
26. Ali A, Aadil F, Khan MF, Maqsood M, Lim S. Harris hawks optimization-based clustering algorithm for vehicular ad-hoc networks. IEEE Trans Intell Transp Syst. 2023;24(6):5822–41. doi:10.1109/tits.2023.3257484.
27. Habelalmateen MI, Ahmed AJ, Abbas AH, Rashid SA. TACRP: traffic-aware clustering-based routing protocol for vehicular ad-hoc networks. Designs. 2022;6(5):89.
28. Häckel T, Meyer P, Mueller M, Schmitt-Solbrig J, Korf F, Schmidt TC. Dynamic service-orientation for software-defined in-vehicle networks. In: 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring). Piscataway, NJ, USA: IEEE; 2023. p. 1–5.
29. Leon J, Aydeger A, Mercan S, Akkaya K. SDN-enabled vehicular networks: theory and practice within platooning applications. Veh Commun. 2023;39:100545.
30. Deng Z, Tang C, Li T, He D. A distributed ledger-assisted robust and trusted service protocol for VANETs. IEEE Internet Things J. 2024;11(24):40559–71. doi:10.1109/jiot.2024.3451303.
31. Khezri E, Zeinali E, Sargolzaey H. SGHRP: secure greedy highway routing protocol with authentication and increased privacy in vehicular ad hoc networks. PLoS One. 2023;18(4):e0282031.
32. Kandali K, Bennis L, El Bannay O, Bennis H. An intelligent machine learning based routing scheme for VANET. IEEE Access. 2022;10:74318–33. doi:10.1109/access.2022.3190964.