Iranian Journal of Science and Technology, Transactions of Electrical Engineering
https://doi.org/10.1007/s40998-026-01150-y

RESEARCH PAPER

Energy Efficient Trust-Aware Aqua Raptor Optimization Algorithm (TA-ARO) for Secure Routing in VANETs

K. Satheshkumar[1] · S. Ramalingam[2] · A. Suresh Babu[3] · R. Sarojini[4]

Received: 2 January 2025 / Accepted: 15 June 2026
© The Author(s), under exclusive licence to Shiraz University 2026

Abstract
Vehicular ad hoc networks (VANETs) play a vital role in enabling intelligent transportation systems; however, their high dynamic topology and limited resources are significant challenges to energy-efficient and secure communication. To address these issues, an energy-efficient and trust-aware clustering and routing framework, termed FCKOA-TA-AROA has been proposed and it employs Optimized Fuzzy C-Means (OFCM) clustering to form stable vehicle groups, while the Modified Kookaburra Optimization Algorithm (MKOA) selects optimal cluster heads based on energy and mobility characteristics. Secure and efficient routing is achieved using a Trust-Aware Aqua Raptor Optimization Algorithm (TA-AROA) by incorporating trust evaluation and energy-aware path selection. In addition, homomorphic encryption is utilized to protect trust-related information during data transmission. Simulation results indicate that the proposed framework substantially outperforms the existing routing schemes in terms of energy efficiency, security, and communication reliability by making it a promising solution for secure VANET communications. Specifically, the proposed algorithm achieves superior performance compared to the Graph-Based Trust-Enabled Routing (GBTR), Bionic Remora Optimization Algorithm (BROA), Adaptive Binary Bird Swarm Optimization integrated with Adaptive Golden Eagle Optimization (ABBSOA-AGEOA), and Falcon Optimization Algorithm-based Energy Efficient Communication Protocol for Cluster-based Routing (FOA-EECPCR). The simulation results demonstrate that the proposed method attains the throughput of 99 Kbps, packet delivery ratio of 88%, and energy consumption of 42 J, outperforming all compared schemes across all key metrics.

Keywords Vehicular ad hoc networks · Clustering · Routing · Optimized fuzzy C-Means · Kookaburra Optimization Algorithm · Aqua Raptor Optimization Algorithm

1 Introduction

Vehicle ad hoc networks (VANET) are the part of Intelligent Transportation Systems (ITS) that allow the vehicles and the infrastructure to share information and data in real time (Ul Hassan 2024; Hussein et al. 2024). The applications that they facilitate include autonomous driving, traffic management, and emergency services which are essential for providing better road safety and effective transportation control. VANETs help to ensure high traffic efficiency and reduce the risk of accidents by allowing the vehicles to exchange information quickly with road infrastructure (Saoud et al. 2024; Al-Mekhlafi et al. 2024; Alam et al. 2024).

However, the VANETs face significant challenges, owing to the fast mobility of nodes, dynamic network topologies, and limited energy sources, despite their promising address to these challenges. These factors complicate the reliability

✉ K. Satheshkumar
satheshkumarece@vcew.ac.in

S. Ramalingam
ramalingam.s@sece.ac.in

A. Suresh Babu
sureshbabu.a@kce.ac.in

R. Sarojini
sarojiniraju18@gmail.com

[1] Department of ECE, Vivekanandha College of Engineering for Women, Tiruchengode, Tamilnadu, India

[2] Department of ECE, Sri Eshwar College of Engineering, Coimbatore, Tamilnadu, India

[3] Department of ECE, Karpagam College of Engineering, Coimbatore, Tamilnadu, India

[4] Department of ECE, Government College of Engineering, Bodinayakkanur, Tamilnadu, India

Published online: 13 July 2026

of communication protocols and lead to the possibility of data loss or transmission delays (Swamynathan et al. 2024). Furthermore, VANETs may also be exploited by security attacks, including malicious nodes, malicious data, and unauthorized access, which compromise the network integrity and security. For building successful clustering and routing protocols to these networks, the realizations of low latency, energy efficiency, scalability and high security at the same time are still major challenges (Barve and Patheja 2024; Choksi and Shah 2024).

Many clustering and routing algorithms have been designed to address these issues, including GBTR, BROA, ABBSOA-AGEOA, FOA-EECPCR, and swarm intelligence (Ant Colony Optimization, PSO, and grey wolf optimization) (Karne and Sreeja 2024). Moreover, Q-Learning and Deep Q-Networks (DQN), Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNN) have been applied and they rely on machine learning to dynamically control routing decisions based on traffic characteristics and predict mobility (Liu et al. 2024; Darney et al. 2024; Wang et al. 2024a). Although these strategies make the system more energy-efficient, optimized, and predictive, they are associated with several limitations. Conventional algorithms include the problems of poor CH selection, poor load balancing, and high routing overheads of dense networks or high dynamic networks. Swarm intelligence techniques work slowly to converge or trap themselves in local optima and usually they do not have built-in trust or security protection. Machine learning models are expensive to train, require large volumes of data, are costly to compute, and are difficult to apply in real-time VANET settings. These issues explain the need of an all-inclusive framework that can manage energy efficiency, secure routing, and scaling cluster management. Current techniques are not effective in supporting the integrated requirements of energy efficiency, security, reliability, and scalability in dynamic VANET environments. An integrated model that integrates high-level clustering, bio-inspiration, trust-sensitive routing, and encryption which are needed to provide secure, energy-efficient, and reliable communication in ITS (AlMarshoud et al. 2024; Kn and Nagaraj 2025; Mohammed et al. 2024).

The present work provides a hybrid framework that addresses the existing gaps by incorporating multiple sophisticated techniques. It employs Optimized Fuzzy C-Means (OFCM) for effective and streamlined clustering, Modified Kookaburra Optimization Algorithm (MKOA) for energy-efficient and reliable selection of CHs, and Trust-Aware Aqua Raptor Optimization Algorithm (TA-ARO) for secure and adaptable routing. Moreover, Modified Homomorphic Encryption (MHE) has been utilized to guarantee data security and safety of vehicle-to-everything communication. The harmonious balance of the framework through the combination of these techniques yields energy efficiency, scalability, and security, making it suitable for dynamic vehicular applications. The proposed solution enhances the performance of the network by increasing the packet delivery ratio as well as energy efficiency, and defending against malicious attacks with low latency. This framework eliminates the limitations of current algorithms and provides a holistic and real-time VANET solution through clustering, bio-inspired optimization, trust-based routing, and encryption.

At the candidate node level, a nonlinear adaptive control parameter is used in the MKOA to vary the position of the candidate node with reference to the global optimum and the position of its local neighbors. This enables a more flexible trade-off between exploration and exploitation. This type of design ensures that the choice of CHs is not affected by the fast movement of the vehicles, since the MKOA can redress the cluster structures with in a brief period, when the vehicles shift lanes, speed, and direction. The MKOA is robust, unlike PSO, which tends to lose stability on many occasions owing to the topology change mechanism as a result of the velocity update and that causes wastage of energy and the reformation of cluster regularly. In the case of routing, the TA-ARO has been chosen because its multiphase pursuit-diving search possesses an integrated surface-randomized exploration with depth-based exploitation. The protocol operates this mechanism to find optimum routes by refining candidate routes iteratively using a trust-weighted fitness evaluation that integrates energy efficiency and malicious node avoidance. This adaptive depth-based exploitation allows TA-ARO to rapidly converge to achieve trustworthy routes in changing VANET conditions. Compared to GA, the operators of the crossover-mutation of GA are expensive for calculating large-scale route optimization, and the use of pheromones and the evaporation by ACO create a latency that is less sensitive to topological changes in real time. The proposed framework uses biologically inspired operators which include MKOAs adaptive cooperative hunt model and TA-AROs pursuit dive mechanism to balance its energy usage, faster converge, to offer lower routing overhead, and withstand attacks for outperforming other metaheuristic algorithms of PSO, GA, and ACO in VANETs.

The significant contributions of this work are as follows:

- To achieve dynamic and precise vehicle groups with the help of the OFCM clustering, minimize intra-cluster distances, and adjust the size of a cluster according to the mobility patterns.
- To choose CHs that are energy-efficient and stable and by considering the residual energy, mobility, and connection stability that support cluster longevity and minimize overhead, MKOA has been applied.

- To develop a safe and dependable routing plan using TAROA. The trust model is used to determine the behavior of the node to stop malicious attacks and ensure that the data intact during transmission.
- To apply clustering and to select CH as well as routing algorithms to balance energy efficiency and network performance in dynamic VANET systems in order to improve the packet delivery ratio, throughput, bandwidth, and network security.
- To optimize the computation efficiency of the clustering and routing algorithms by using lightweight algorithms, such as OFCM and bio-inspired algorithms to ensure that the protocol is used in real-time VANETs.

The rest of this work is structured as follows. In Sect. 2, a detailed framework of current VANET clustering as well as routing technologies is presented. Section 3 describes the design of the proposed secure clustering and routing protocol, which includes trust management and security mechanisms. In Sect. 4, the simulation setup, performance measures, and evaluation outcomes are described, and the proposed methodology is compared with the state-of-the-art methodologies. Finally, Sect. 5 concludes the work by summarizing the main findings, limitations and the future research directions.

2 Literature Survey

Ali et al. (2024a) have introduced a secure intelligent clustering algorithm (AOSICA) for VANETs. The algorithm applies mathematical optimization in clustering and security precautions to reduce the assaults in order to address the VANET energy efficiency and security challenges. It improves the stability of clusters, optimizes CH, and ensures the transmission of network information. Nonetheless, this work has some weaknesses. AOSICA enhances clustering performance and security but not scalability in dynamic large-scale VANETs. The optimization of arithmetic can add the complexity of computation of real-time implementations and limit their applicability in low-latency contexts. As the suggested security techniques have not been thoroughly tested against advanced attacks such as DDoS or Sybil attacks, they may become more robust.

Umale et al. (2024) have developed a novel IoV routing and data transfer approach by using an improved deep learning energy predictor model. In this work, the energy consumption of IoV nodes is predicted to optimize routing and data security. Deep-learning architecture takes the advantage of real-time vehicle data to optimize routing, conserve energy, and enhance network results. The protocol is robust for IoV applications because it is ensured that the security measures are in place to protect the transmission of data. Despite its strengths, this strategy has flaws. Deep learning models increase computing complexity and hence, rendering them unsuitable for resource-constrained applications. This work also ignores VANETs' high mobility and changeable topology of VANETs, and subsequently, they can affect routing and clustering stability. Security frameworks without trust-based procedures can also improve malicious node detection and mitigation.

Jia et al. (2024) have described a safe fog computing authentication and trust detection framework for VANETs and it uses an adaptive deep neural network (DNN) and data methods to protect privacy. This technique secures data transfer and protects vehicular users' privacy while maintaining a trust-based authentication scheme for dependable vehicle-fog node communication. The framework uses an adaptive DNN to detect and mitigate threats in real time, thereby improving the network security and trustworthiness. Although effective, this procedure has drawbacks. Deep neural networks may have considerable computational overhead in resource-constrained VANETs. Although the framework guarantees anonymity, it ignores its usefulness in large-scale VANETs with significant mobility, as dynamic topology changes may influence the accuracy and adaptability of the DNN models. The absence of a comprehensive energy-efficient mechanism in the suggested system could lead to energy waste, particularly in high-vehicle-density scenarios.

Ali et al. (2024b) have introduced a federated learning-based, privacy-aware location prediction model for the IoVT to improve privacy and vehicle position prediction. Decentralized data processing using federated learning retains sensitive location data on local vehicles rather than a central server. This privacy-preserving technique improves the IoVT security in autonomous driving and traffic management. Collaborative learning enhances vehicle positioning without compromising user privacy in the location-prediction model. Although helpful, this strategy has numerous drawbacks. First, frequent vehicle updates and synchronizations may cause network congestion and communication overhead in federated learning. Second, the model's success depends on the local data quality and quantity, which may vary among vehicles, causing prediction inaccuracies. In resource-constrained circumstances, federated learning computation may deplete a vehicle's battery and hence, its energy efficiency decreases. Finally, the effects of high mobility and dynamic network conditions on location prediction accuracy and stability remain unknown.

Saemi et al. (2024) have proposed balancing roadside unit loads to improve VANET real-time data transmission services. This work optimizes the vehicle-RSU connection to improve data transmission in dynamic and mobile

situations. This technique decreases congestion, latency, and VANET data transfer throughput by balancing the RSU loads. This solution also covers RSU resource utilization and vehicle-to-infrastructure communications. This method has some limitations. In high dynamic settings, the load balancing algorithm may not be fully adaptive to rapid changes in the vehicular network architecture, thereby affecting its efficiency. Second, the work does not examine energy efficiency, which is crucial in VANETs, especially for vehicles with limited battery resources. Third, although the approach improves data transmission quality, it lacks security methods, such as data integrity or malicious node protection, which are necessary for VANET connections. Finally, the effect of high-density vehicular traffic on solution scalability has not been fully studied.

Qi et al. (2024) have proposed a hybrid trust-based emergency message dissemination model for VANETs to increase the reliability and efficiency of critical message transmission. The framework evaluates the trustworthiness of vehicles involved in message distribution using direct and indirect trust methods, ensuring that dependable nodes forward messages. Using trust models and adaptive message forwarding algorithms, the framework improves VANET safety by enhancing emergency message delivery accuracy and speed. However, the model has significant drawbacks. First, trust-based systems may be vulnerable, if malicious nodes modify trust metrics or conduct faulty trust computations, resulting in inefficient Message Propagation (MP). The model only addresses emergency message distribution, not energy efficiency, which is critical in VANETs, particularly in high-traffic or long-duration circumstances. In large, dense networks where vehicular mobility is high, the concept might not be able to be trusted, and the messages are distributed efficiently; thus, there is no large-scale work on scalability. Finally, traffic jams and congestion in networks can also affect the system performance.

Wang et al. (2024) have provided an Attribute-Based Access Control (ABAC) privacy-preservation strategy of sharing data on VANETs and it involves intrusion detection and hiding policies. The proposed approach ensures that only authorized vehicles have access to specified data while simultaneously protecting users' privacy using attribute-based access rules. Furthermore, the use of an intrusion detection system improves data transmission security by detecting and mitigating hostile attempts to access the data. The policy-hiding technique improves privacy by concealing the access control policies from unauthorized parties. Although this approach enhances data security and privacy, it has some drawbacks. First, the computational burden associated with attribute-based encryption and policy management may result in longer processing time, particularly in resource-constrained vehicles. Second, the efficiency of an intrusion detection system is strongly reliant on the validity of the threat model, and false positives or negatives can undermine its dependability.

Memon et al. (2024) have offered a dynamic pseudonym trust-based approach for protection against attack scenarios in Internet of Vehicle Ad-Hoc Networks (IoVANETs). To protect user privacy, the model employs dynamic pseudonyms, and a trust-based method assesses the reliability of vehicles in the network. This method helps to prevent identity-based attacks, such as Sybil attacks, by continually changing vehicle pseudonyms, making it harder for malevolent entities to follow or target specific vehicles. The trust mechanism ensures that only trustworthy vehicles participate in communication, thereby the network's security and integrity are improved. Despite the fact that the concept is characterized by substantial security and privacy advantages, it is limited in several ways. First, the dynamic pseudonym-shifting process introduces extra overheads in communication because regular updates are necessary to achieve pseudonym security. This may result in network congestion and delays, especially when there are high vehicle densities. Second, the model can be manipulated through trust by advanced adversaries who can mimic trusted actions. Moreover, not all large and high mobile networks can be covered by this method, and it may affect the model performance when applied in actual IoV conditions.

Rajakumar et al. (2024) have assessed clustering-based routing protocols in VANETs. This work discusses the scalability, energy efficiency, and improvement of packet delivery and routing systems using clustering-based systems. To analyze the strengths and weaknesses of the VANET protocol, this work examines CH selection, intra cluster communication, and inter cluster routing. Protocols based on clustering can enhance the efficiency of the network by minimizing the cost of communication and spreading the load among the vehicles. However, this work has significant flaws. First, in high dynamic VANETs, where vehicle placements and network architecture change rapidly and as a result, many clustering-based protocols struggle to establish stable clusters and raise costs. Second, although energy economy is crucial, the protocols evaluated do not always account for the limited resources of vehicles, especially in large networks. Owing to network congestion and communication delays, clustering-based methods may not scale well in intensive vehicle traffic scenarios. Finally, this work does not cover malicious-attack security measures, which are essential for VANET communication reliability and safety.

El-Gayar et al. (2024) have proposed a smart collaborative intrusion detection system (IDS) for vehicular networks that uses an ensemble machine learning model to detect and mitigate security issues. The system uses numerous machine

learning algorithms to create a robust model that can detect many VANET attack scenarios, including DoS and Sybil attacks. Multiple models work together to improve the detection accuracy and reduce false positives in the ensemble approach. The collaborative IDS allows the vehicles to share danger data, thereby network security is improved in real time. Although the suggested method enhances security, it has drawbacks. Ensemble machine learning approaches may increase computing complexity, which is difficult in resource-constrained vehicle applications. Second, continual data exchange between the vehicles may raise privacy concerns and increase network traffic. The system is effective at recognizing a variety of assaults, but it does not solve the challenges caused by the increasing mobility of VANET vehicles and they may affect the timeliness and accuracy of attack detection.

Setia et al. (2024) have presented a machine learning-driven VANET cloud environment DDoS detection method to improve vehicular network security and reliability. Machine learning algorithms are used to recognize DDoS attacks based on the network traffic patterns. The combination of cloud-based resources enables scalable and efficient detection of large-scale threats and secures vehicular communication networks in real time. However, this technique has several disadvantages. First, the quality of training data is a factor that determines whether the model is efficient and it may be challenging to acquire in dynamic VANET settings. Second, the machine learning models are resource-intensive and computationally complex, which means that they cannot be used in vehicles with limited processing ability. This methodology might fail to identify VANET security risks, including Sybil or impersonation attacks, because it is based on DDoS.

Magdalin et al. (2024) have suggested energy-efficient and secure V2X (Vehicle-to-Everything) communication based on optimized DBSCAN, RLA-ODV, and homomartino-based encryption. Reinforcement learning enhances vehicle clustering and routing, reduces energy consumption, and improves communication security. The Homomartino algorithm safeguards data privacy, during the communication process in V2X. This solution is attractive for energy efficiency and security, but it has limitations. In large VANET s with high mobility and dynamic topologies, the DBSCAN clustering algorithm may have difficulty in scaling. Second, the computational complexity of the suggested encryption method may impede communication, particularly in resource-constrained vehicles. The work does not completely examine the impact of dynamic vehicular network changes on routing decisions and clustering stability, but it does examine energy efficiency.

Krishnan et al. (2024) have presented a QoS-based adaptive multi-constrained energy-efficient routing technology for VANETs. While preserving excellent QoS, the protocol optimizes the routing options by considering energy, latency, and dependability. The protocol can adapt to changing network circumstances and choose the most efficient data transmission methods. This technique reduces energy usage while guaranteeing reliable communication for real-time navigation and traffic control. Although beneficial, this strategy has drawbacks. First, the multiconstrained structure of the protocol complicates the routing decisions, which can increase the computational cost, particularly in low-power vehicles. The protocol covers energy efficiency and QoS; however, it does not address how high-density vehicular traffic and network congestion affect the routing performance. However, malicious attacks, which are crucial in VANET systems, are not included in this work. Finally, further testing is necessary to ensure the scalability of the protocol in large-scale networks with high mobility and performance in dynamic contexts.

Putta et al. (2026) have structured a hybrid adaptive network-based node authentication and optimal routing framework to improve security and communication efficiency in VANET environments. The authentication process employs a Hybrid Adaptive Network (HAN) model integrating Conditional Random Field (CRF) and Ridge classifiers, with parameter tuning performed using the Updated Random Attribute-based Circle-Inspired Optimization (URA-CIO) algorithm. Following authentication, optimal routing is established based on multiple criteria, including residual energy, throughput, packet delivery ratio, delay, and path availability. The proposed framework has achieved an authentication accuracy of 92% by outperforming several conventional approaches while ensuring secure and reliable vehicular communications.

Vaissnave et al. (2026) have designed an advanced deep learning-based threat detection framework to enhance security in Internet of Things (IoT) networks. The model integrates attention mechanisms with deep learning techniques to effectively learn spatial and temporal traffic characteristics while addressing data imbalance and feature selection challenges. The proposed approach has been evaluated using the IoT-23 and N-BaIoT datasets, which contain diverse IoT traffic and botnet attack scenarios. Experimental results have demonstrated superior threat detection performance by achieving accuracy rates of 99.93% and 99.86%, respectively. The study highlights the effectiveness of attention-driven feature learning for improving network security and reducing misclassification rates.

Table 1 provides an overview of recent clustering and routing strategies suggested for VANETs along with their algorithms, results, and drawbacks. The examined studies include a variety of methods, such as trust-based models, privacy-preserving access control, machine learning-based

Table 1 Summary of the existing clustering and routing techniques in VANET

Reference No	Author(s) & Year	Algorithm	Outcomes	Limitations
[20]	Saemi et al. (2024)	Load balancing on roadside units	Improved real-time data transmission quality in VANETs	Does not address energy efficiency of RSUs and impact on latency in highly dynamic environments
[21]	Qi et al. (2024)	Hybrid-trust-based model	Enhanced emergency message dissemination in VANETs	Delay in high-mobility scenarios; vulnerability to trust-related attacks
[22]	Wang et al. (2024)	Privacy-preserving attribute-based access control with intrusion detection	Improved data privacy and security for VANET data sharing	Computational overhead and scalability issues in dense networks
[23]	Memon et al. (2024)	Dynamic pseudonyms trust-based model	Enhanced attack protection in IoV networks	Pseudonym update overhead and limited scalability in large networks
[24]	Rajakumar et al. (2024)	Clustering-based routing protocols	Evaluation of routing protocols for performance in VANETs	Focus on simulation and it lacks energy efficiency and security analysis
[25]	El-Gayar et al. (2024)	Ensemble machine learning-based IDS	Improved intrusion detection for securing vehicular networks	Computational complexity and it lacks evaluation of advanced attack types
[26]	Setia et al. (2024)	Machine learning-driven DDoS detection	Improved DDoS attack detection in VANET cloud environments	High computational overhead and limited exploration of other attack types
[27]	Magdalin and Kumarasabapathy (2024)	Optimized DBSCAN, RLA-ODV routing, homomartino encryption	Energy-efficient and secure V2X communication	High computational cost and DBSCAN struggles with scalability in dynamic networks
[28]	Krishnan et al. (2024)	Adaptive multi-constrained energy-efficient routing	Improved energy efficiency and QoS in VANETs	Limited security analysis and scalability in high-density networks is not fully explored
[31]	Anjali et al. (2024)	Attack prevention techniques in VANETs	Improved security by preventing attacks in VANETs	Limited scope and lacks detailed evaluation in real-world scenarios
[32]	Wang et al. (2024)	Trust evaluation-based group message forwarding	Secure message forwarding in VANETs with trust evaluation	Trust evaluation may lead to delays and lacks analysis of advanced attacks
[33]	Alotaibi et al. (2024)	Falcon Optimization Algorithm	Energy-efficient communication protocol for VANETs	Limited exploration of dynamic network conditions and security implications
[34]	Alsalem AO. (2024)	Secure authentication and privacy-preserving techniques	Improved authentication and privacy in VANETs	Focus on theory and lacks real-world validation and scalability analysis

intrusion detection, and bio-inspired optimization techniques. Although these methods show advancements in security, energy efficiency, and service quality, they often encounter issues with scalability, computational demands, and adaptability in high dynamic vehicular environments. These challenges highlight the necessity of more comprehensive and integrated solutions, which are impetus for the framework to be designed and it has been proposed in the present work.

3 Proposed Methodology

In the proposed framework, the four core components—Optimized Fuzzy C-Means (OFCM) clustering, Modified Kookaburra Optimization Algorithm (MKOA)–based cluster head (CH) selection, Trust-Aware Aqua Raptor Optimization Algorithm (TA-AROA) routing, and Modified Homomorphic Encryption (MHE)—operate in a tightly coupled and sequential manner to support real-time VANET communication. Initially, OFCM dynamically groups the vehicles into clusters by considering the mobility characteristics such as relative velocity, inter-vehicle distance, and communication link stability, ensuring adaptive clustering under high mobility conditions. Within each cluster, MKOA is then applied to select an optimal CH by optimizing an objective function that accounts for residual energy, node connectivity, mobility stability, and trustworthiness, thereby g frequent CH re-elections are reduced and cluster longevity improved.

Once CHs are established, TA-AROA performs secure and energy-aware routing between the source and the destination clusters. Trust values are continuously evaluated based on packet forwarding behavior, historical reliability, and interaction consistency, and they are incorporated with the routing fitness function along with energy consumption and delay metrics. This enables TA-AROA to identify optimal multi-hop paths that avoid malicious or unreliable nodes while maintaining high routing efficiency. During data transmission, MHE is employed to encrypt trust and the reliability messages are exchanged between vehicles and CHs for ensuring data confidentiality and integrity without exposing sensitive trust information. The encrypted data are securely transmitted and stored in the cloud server for supporting verification and future trust updates. The entire framework operates iteratively and adaptively by allowing real-time

updates of clusters, CH roles, trust values, and routing paths in response to network topology changes. This integrated design ensures seamless information flow between clustering, CH selection, trust evaluation, and secure routing and they result in a robust, energy-efficient, and attack-resilient VANET communication system.

Figure 1 illustrates the basic architecture of VANETs. In such a network, the infrastructure-less half uses ad hoc vehicles, and the infrastructure-oriented half uses roadside units. Each vehicle is equipped with an on-board unit (OBU) and sensors that are used to collect and analyze data in the form of messages. These messages are sent to other automobiles or RSUs for vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication. The vehicles have one or more application units. AUs use supplier apps through OBU connections. However, AUs deploy RSUs at the traffic signals, parking lots and roadside locations. The RSUs have two network devices: one for dedicated short-range radio transmission and one for infrastructure component communication. AUs from several vehicles can access the Internet via an RSU or another server.

3.1 Cluster Formation Using Optimized Fuzzy C-Means Clustering

In this section, an optimized fuzzy c-means-based centralized clustering technique has been proposed to partition the network into an appropriate number of clusters. This approach assumes that the BS node is aware of the network architecture. The BS node connects all CHs and employs FCM method to determine cluster centroids as well assigns SNs to clusters $(fC_1, C_2 \ldots C_{cg})$ using SN data. Each node has a degree of membership (u_{ab}) for a cluster c_b instead of being a complete member. The FCM algorithm iteratively minimizes the following objective function on a small scale:

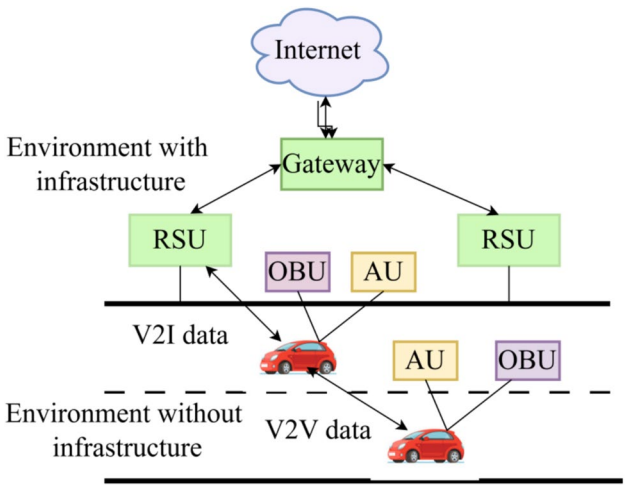


Fig. 1 Basic architecture of VANETs

$$\sum_{a=1}^{c}\sum_{b=1}^{N} u_{ab}^{m} d_{ab}^{2} \tag{1}$$

where u_{ab} represents the cluster membership of sensor node SNb's, and d_{ab} denotes its distance from the center point of cluster Ca. The fuzziness parameter is m > 1. FCM-based clustering is influenced by the number of clusters (c) and the number of sensor nodes. The main activities during clustering include:

1. Selecting the fuzzy cluster number c.
2. Randomly initializing c cluster centers.
3. Creating the membership matrix using sensor node data.

$$u_{ab} = \frac{1}{\sum_{K=1}^{c}\left(\frac{d_{ab}}{d_{kb}}\right)^{\frac{2}{m-1}}} \tag{2}$$

4. Calculate the cluster's center with

$$c_b = \frac{\sum_{a=1}^{N} u_{ab}^{m} n_a}{\sum_{a=1}^{N} u_{ab}^{m}} \tag{3}$$

5. Steps 3 and 4 should be performed until all nodes' membership values converge and it is expressed as:

$$max\left\{U_{ab}^{I+1} - U_{ab}^{I}\right\} < \beta \tag{4}$$

where U_{ab}^{I} is the membership matrix for the i^{th} iteration, and b is the termination indicator, which is in the range from 0 to 1. When the algorithm converges, each node is assigned with the cluster for which it has the highest membership value. After constructing the VANET topology, the protocol operates in rounds, with each round divided into the previously described CH selection and data transmission phases.

3.2 CH Selection Using Modified Kookaburra Optimization Algorithm

This section covers the conceptual framework and the theoretical underpinnings of the proposed MKOA approach, followed by a description of the mathematical models used in its application to address the optimization issues. Dacelo, a ground kingfisher species from the Coraciiform and Alcedininae families, is native to New Guinea and Australia. Arid savannas, wet forests, water-edge places, and suburban areas with tall trees are the habitats of this species. This bird emits a laugh that serves as a warning to enemies not to approach its territory. Kookaburras are blue, brown, or white, and their head feathers and the dark brown patch behind their eyes give them an angry appearance. Figure 2

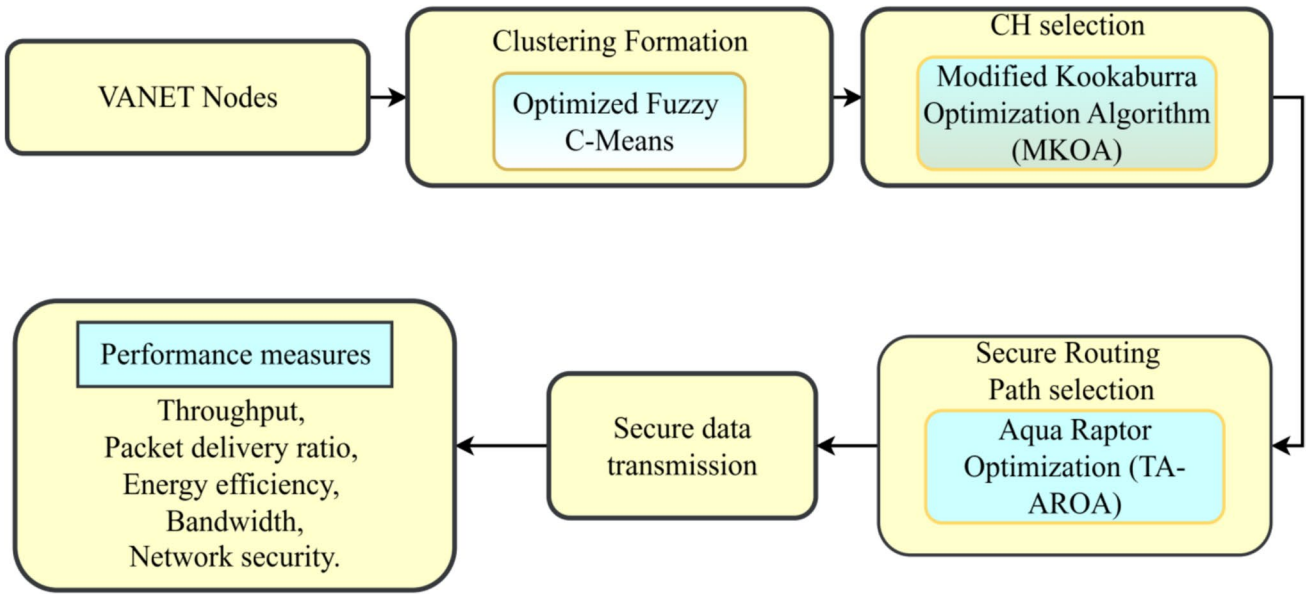


Fig. 2 Block diagram of VANET

depicts the overall block diagram of a VANET. The MKOA is a bio-inspired optimization technique that mimics the foraging behavior of kookaburras, a bird species known for its distinctive hunting style. MKOA can be applied to optimize important network procedures in VANETs (CH selection, routing, and resource management).Since it uses the natural hunting behavior of kookaburras to search the network space effectively, the algorithm is particularly appropriate for dynamic and energy-limited VANET situations. The MKOA dynamically selects the most appropriate CHs by simulating the search process for the optimal prey as well as for balancing energy consumption, load distribution, and communication efficiency. The modularity and elasticity of the MKOA make it an ideal choice for handling dynamic topologies and mobility trends in VANETs. The optimization method helps to optimize the system performance of the general network, energy efficiency, data delivery rates, and reduction of communication overhead in VANET systems, such as autonomous driving and traffic management.

3.2.1 Inspiration of MKOA

Kookaburras eat mice, insects, snakes, frogs, small reptiles and birds. Kookaburras use their beaks for diving and hunting. The bird plunges with its mouth open, catches the food, and then returns to a tree branch to hit and kill the prey. It takes the victim, breaks it, and eats it. This organism kills its victim by striking it against a tree in a unique way, a strategy that is crucial to the ecosystem. Thus, the clever behaviors of kookaburras have evolved into effective strategies for using the derived MKOA.

3.2.2 Algorithm Initialization

The population-based optimizer MKOA randomly searches a problem-solving space during an iterative process of problem optimization. The MKOA population places each kookaburra in the problem-solving space, assigns decision variable values based on their positions and thereby, vector-modelable candidate solutions are formed for problem resolution. Equation (5) depicts the MKOA population matrix, and Eq. (6) randomly allocates each place for kookaburras to begin MKOA implementation.

$$A = \begin{bmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_N \end{bmatrix}_{N\times m} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,d} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i,1} & \cdots & a_{i,d} & \cdots & a_{i,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{N,1} & \cdots & a_{N,d} & \cdots & a_{N,m} \end{bmatrix}_{N\times m} \tag{5}$$

$$a_{i,d} = lb_d + r \cdot (ub_d - lb_d) \tag{6}$$

where, X is the MKOA population matrix, A_i is the i^{th} kookaburra (candidate solution), $a_{i,d}$ is its d^{th} dimension in the search space (decision variable), N is the number of kookaburras, m is the number of decision variables, rrr is a random number in the interval [0,1], and lb_d and ub_d are the lower and upper bounds of the d^{th} decision variable, respectively. Since every position of the kookaburra is a potential solution to its problem, there may be an evaluation for each objective function. As mentioned previously, Eq. (7) shows how to vectorize the evaluated values of the objective function of the problem.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(A_1) \\ \vdots \\ F(A_i) \\ \vdots \\ F(A_N) \end{bmatrix}_{N\times 1} \quad (7)$$

F denotes the vector of the evaluated objective functions, and F_i denotes the i^{th} kookaburra-based objective function. The objective function values are the best way to estimate the potential solutions and population members. The best and worst objective function values represent the best and worst members, respectively. Each iteration changes the position of the kookaburras in the issue-solving space and prompts a reevaluation of the problem's goal function as well as an update to the best member of the population based on a comparison of the new values.

3.2.3 Mathematical Modeling of MKOA

Based on the simulations of natural kookaburra actions, the proposed MKOA method iteratively improves potential solutions in two steps: exploration and exploitation. The discussion of the MKOA population update mechanism continues in the search space.

3.2.4 Phase 1: Hunting Strategy (Exploration)

Kookaburras consume small birds, reptiles, insects, mice and frogs. Although its legs are weak, its robust neck aids in hunting. The Kookaburra's ability to select and attack its prey results in significant displacement. This method combines a global search with exploration, which involves scanning the problem-solving space to avoid the local optimal area and finding a large optimal area. Like each kookaburra, the MKOA design uses the prey location of other kookaburras with a higher goal function value to imitate the hunting techniques. Equation (8) determines the prey set of each kookaburra by comparing the values of the objective function.

$$CP_i = \ A_k : F_k \ < F_i \ \ and \ \ K \ \neq \ i, \quad (8)$$

Where i = 1, 2, …, N and k ∈ 1, 2, …, N. CP_i is the set of candidate prey for i^{th} kookaburra, A_k is the kookaburra with a better objective function value than the i^{th} kookaburra, and F_k is the objective function value.The MKOA design implies that each kookaburra randomly assaults a target. Equation (9) models the progress of the kookaburra's hunting method toward the prey to calculate its new position. Equation (10) states that the new position replaces the old one, if the target function improves.

$$a_{i,d}^{P1} = a_{i,d} + r \cdot SCP_{i,d} - I \cdot a_{i,d}, \quad (9)$$

where i = 1, 2, …, N, and d = 1, 2, …, m

$$A_i = \begin{cases} A_i^{P2}, & F_i^{P2} < F_i \\ A_i, & else \end{cases} \quad (10)$$

where, A_i^{P1} is the new suggested position of the i^{th} kookaburra based on the first phase of MKOA, A_i,d^{p1} is its d^{th} dimension, F_i^{P1} is its objective function value, r is a random number with a normal distribution in the range of [0,1], $SCP_{i,d}$ is the d^{th} dimension of the selected prey for the i^{th} kookaburra, I is a random number from the set {1,2}, N is the number of kookaburras, and m is the number of decision variables.

3.2.5 Phase 2: Ensuring That the Prey is Killed (Exploitation)

A distinctive behavior of kookaburras is their way of ensuring their prey is no longer alive. Once they catch their prey, they transport it to a tree and repeatedly smash it against a branch or trunk until it is completely lifeless. Kookaburras' stance changes slightly while approaching the hunting place. This local search-exploitation technique can produce better results closer to the previously solved problems and interesting places. Equation (11) determines a random position to mimic kookaburras' movement near the hunting area. This displacement should occur randomly in a radius of $u_{bd} - l_{bd}$ around each kookaburra's center. The radius of this neighborhood is initially set to the maximum value, but it is reduced throughout the successive iterations to improve local search for better solutions. If the new position calculated for each kookaburra enhances the goal function in Eq. (12), it replaces the old position.

$$a_{i,d}^{P2} = a_{i,d} + 1 - 2r \cdot \frac{u_{bd} - l_{bd}}{t} \quad (11)$$

where i = 1, 2, …, N, d = 1, 2, …,m, and t = 1, 2, …, T

$$A_i = \begin{cases} A_i^{P2}, & F_i^{P2} < F_i \\ A_i, & else \end{cases} \quad (12)$$

where, A_i^{P2} is the new suggested position of the i^{th} kookaburra based on the second phase of MKOA, F_i^{P2} is its objective function value, t is the iteration counter of the algorithm, and T is the maximum number of iterations. Equation (8) (Prey Set Identification): This equation identifies the set of potential solutions (candidate cluster heads) that perform better than the current solution. Regarding VANET, it implies the selection of more stably connected

vehicles and those with more residual energy as leaders. Equations (9)–(10) (Exploration–Hunting Strategy): These equations offer the position of a kookaburra (candidate solution) towards a prey with a higher performance. This is practically equivalent to vehicles dynamically adapting their CH candidacy to vehicles with more favorable mobility and link stability in their neighborhood so that the search space is explored globally. Equations (11)-(12) (Exploitation -Killing Prey): These equations also optimize the current best solution by performing smaller local modifications. In practice, this means fine-tuning of the CH selection process by comparing the nearby nodes with the similar characteristics, so that the final chosen CH balances energy efficiency and connectivity stability.

3.2.6 Repetition Process and Pseudocode of MKOA

KOA's initial iteration ends with upgrading all kookaburra spots from the first and second stages. After each iteration, the best solution is adjusted and saved. The changing coordinates and the objective function values determine the next iteration of the algorithm. The algorithm updates the kookaburra positions until the last iteration based on the Eqs. (8)–(12). Finally, the MKOA suggests the best potential solution for the algorithm. Algorithm 1 shows MKOA's implementation stages in pseudocode. OFCM clustering reduces the distance between the nodes within a cluster and ensures that the vehicles in VANETs are placed in the right category so that, dynamic and adaptable clusters can be formed. The OFCM maps vehicles with different membership clusters to cope with mobility and variation in VANETs. MKOA selects the cluster head for maximum efficiency and stability. MKOA optimizes the selection of CH by considering residual energy, mobility, and connection stability to sustain the cluster lifetime and reduce re-clusters. This combination makes the clusters energy-efficient, robust, and resistant to VANET challenges, including high mobility and frequently changing topologies. An efficient, scalable, and cost-effective clustering algorithm based on the use of OFCM and MKOA enhances the reliability of vehicles through connections and the network and it conserves energy.

Start MKOA
Initialize the problem details: define variables, objective function, and constraints.
Set population size (N) and maximum iterations (T).
Randomly generate the initial population matrix using Equation (6).
Evaluate the objective function values for the initial population.
For t=1 to T:
For i=1 to N:
Phase 1: Exploration (Hunting Strategy)
Identify the set of potential preys using Equation (8).
Randomly select a prey for the i^{th}MKOA agent.
Calculate the new position of the i^{th}MKOA agent using Equation (9).
Update the position of the i^{th}MKOA agent using Equation (10).
Phase 2: Exploitation (Killing the Prey)
Determine the new position of the i^{th}MKOA agent using Equation (11).
Update the agent's position using Equation (12).
End For
Store the best solution found so far.
End For
Output the best quasi-optimal solution achieved by MKOA.
End MKOA

Algorithm 1 Pseudocode of MKOA

3.2.7 Objective Function for MKOA-Based Cluster Head (CH) Selection

In the proposed framework, each candidate solution A_i in MKOA represents a potential cluster head configuration. The objective function $F(A_i)$ evaluates the suitability of a vehicle to act as a CH by jointly considering energy efficiency, mobility stability, and communication reliability. The objective function is formulated as:

$$F(A_i) = w_1 . \frac{E_i}{E_{max}} + w_2 . \frac{1}{V_i + \in} + w_3 . L_i \tag{13}$$

Where:

- E_i denotes the residual energy of vehicle i,
- V_i represents the relative mobility (speed variation) of vehicle i,
- L_i indicates the link stability which is computed based on the predicted link duration with neighboring vehicles,
- w_1, w_2, w_3 are weighting coefficients satisfying $w_1 + w_2 + w_3 = 1$, and.
- $\in$ is a small constant to avoid division by zero.

Optimization Goal: The MKOA maximizes $F(A_i) = w_1$, thereby selecting cluster heads that:

- possess higher residual energy (longer CH lifetime),
- exhibit lower mobility variation (greater topological stability), and
- maintain stronger and longer-lasting communication links.

Thus, MKOA exploration and exploitation phases (Eqs. 8–12) correspond to globally searching for stable CH candidates and locally refining CH selection, respectively, under dynamic VANET conditions.

3.3 Routing Path Selection Using Trust-Aware Aqua Raptor Optimization Algorithm

The Aqua Raptor Optimization Algorithm, which is used in VANETs, optimizes routing by replicating the hunting and movement behaviors of a raptor in water. Vehicles in VANETs serve as mobile nodes that dynamically create networks to share information. The issues that routing in such a network should overcome, include high mobility, frequent changes in topology, and real-time delivery of data. AROA attempts to solve these problems by taking inspiration from raptor behavior, where nodes (vehicles) are considered as hunters, in search of the best routes (prey). The algorithm chooses the most appropriate routing paths depending on the mobility of the nodes, stability of links, level of congestion, and delays in transmission. Nodes constantly reconsider their environment, revise their routing decisions, and select routes that reduce latency and maximize the success of data packet delivery.

In AROA routing, nodes are grouped into clusters to decrease the overhead of the network and enhance its scaling. The criteria used for selecting CHs are the connectivity of their nodes, stability, and remaining energy. These CHs are coordinators that effectively control intra- and inter-cluster communications. The process of determining the routing path involves an iterative process in which the best route is determined by assessing the fitness of every possible route based on optimization functions established based on raptor hunting strategies.

3.3.1 Inspiration of Aqua Raptor

Aqua raptors, also referred to as fish, river, and sea hawks, are nocturnal predators that consume a wide variety of fish species. Aqua Raptor's brilliant natural behavior of grabbing fish and bringing them to an appropriate consuming region can be used to design a new optimization algorithm. These intelligent Aqua Raptor actions are mathematically modeled to produce the AROA technique, which is outlined below.

3.3.2 Mathematical Modelling

This subsection describes how to update Aqua Raptor positions during exploration and exploitation using natural behavior simulations.

3.3.3 Initialization

In the proposed AROA population-based technique, a repetition-based mechanism may find a suitable solution based on the problem-solving power of its population members. As an AROA member, Aqua Raptor uses its search space location to estimate problem variables. As a vector, each aqua raptor represents one alternative answer. A matrix can represent the AROA population, which contains all Aqua Raptors as in Eq. 14. Equation (15) randomly distributes Aqua Raptors in the search space at the start of the AROA deployment.

$$A = \begin{bmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_N \end{bmatrix}_{N \times m} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,j} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{i,1} & \cdots & a_{i,j} & \cdots & a_{i,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{N,1} & \cdots & a_{N,j} & \cdots & a_{N,m} \end{bmatrix}_{N \times m} \tag{14}$$

$$a_{i,j} = lb_j + r_{i,j} \cdot (ub_j - lb_j), i = 1,2,\ldots,N, j = 1,2,\ldots,m \tag{15}$$

where X represents the population matrix of Aqua Raptor locations, A_i represents the j^{th} candidate solution, $a_{i,j}$ represents its j^{th} dimension (problem variable), N represents the number of Aqua Raptors, m represents the number of problem variables, $r_{i,j}$ represents random numbers in the range [0,1], and lb_j and ub_j represent the lower and upper bounds. The principal objective function in the Equations can be evaluated, since each Aqua Raptor may solve its assigned task. Equation (16) allows the vectors to represent the problem's objective function values.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(A_1) \\ \vdots \\ F(A_i) \\ \vdots \\ F(A_N) \end{bmatrix}_{N\times 1} \tag{16}$$

where F_i represents the calculated objective function value for the i^{th} aqua raptor and F is the vector of the objective function values. The alternative solutions are judged based on their objective function values. The best element represents the best value of the objective function, whereas the worst member represents the worst value. The search space position of the Aqua Raptors changes with each iteration, necessitating a change in the best candidate solution.

3.3.4 Phase 1: Identifying Positions and Hunting for Fish, also Known as Exploration

Aqua Raptors, ferocious hunters with exceptional eyesight, specialize in underwater fishing. After finding and attacking the fish, they dive underwater to chase it down. Initial AROA population updates are based on Aqua Raptor's natural behavior simulations. Simulating the Aqua Raptor's attack on fish changes its position in the search region and it helps the AROA to find the optimal spot as well as to avoid local optima. For each AROA design Aqua Raptor, this work has considered other Aqua Raptors with higher objective function values as subsea fish. The Aqua Raptor fish sets are calculated using Eq. (17).

$$FP_i = \{X_k | k \in \{1, 2, ..., N\} \wedge F_k < F_i\} \cup \{X_{best}\} \tag{17}$$

Where FP_i is the fish position set for the i^{th} Aqua Raptor and X_{best} is the best Aqua Raptor solution. This fish is randomly struck by the Aqua Raptor. Equation (19) simulates the matched Aqua Raptor's movement toward the fish to set its new position. Equation (20) states that the Aqua Raptor will move, if the objective function grows.

$$a_{i,j}^{P_1} = a_{i,j} + r_{i,j} \quad (SF_{i,j} - I_{i,j} \quad a_{i,j}) \tag{18}$$

$$a_{i,j}^{P_1} = \begin{Bmatrix} a_{i,j}^{P_1},\ lbj & \leq & a_{i,j}^{P_1} \leq ubj \\ lbj,\ a_{i,j}^{P_1} & < & lbj \\ ubj,\ a_{i,j}^{P_1} & > & ubj \end{Bmatrix} \tag{19}$$

$$A_i = \begin{cases} A_i^{P1}, & F_i^{P1} < F_i \\ A_i & else \end{cases} \tag{20}$$

where A_i^{P1} is the i^{th} Aqua Raptor's new position based on the first phase of AROA,$a_{i,j}$ is its j^{th} dimension, F_i^{P1} is its fitness function, SF_i is the fish selected for i^{th} osprey, $SF_{i,j}$ is the j^{th} dimension, $r_{i,j}$ are random numbers in the interval [0,1] and $I_{i,j}$ are random numbers from the set {1,2}.

3.3.5 Phase 2: Vehiclerying the Fish to an Appropriate Place Position (Exploitation)

The Aqua Raptor delivers the captured fish to a suitable eating area. This real-world behavior is simulated for the second population update stage of AROA. Modeling the fish movement leads to the modest adjustments that have established the Aqua Raptor's location in the search space, improved the AROA's local search capability and caused convergence towards better solutions near the identified solutions. Equation (22) assigns each population member a new random "suitable position for eating fish" under the AROA design. This has approximated the aquatic raptor behavior. Equation (23) replaces the connected element's old location, if the objective function increases in this new position.

$$a_{i,j}^{P2} = a_{i,j} + \frac{lbj + r\cdot(ubj - lbj)}{t}, \quad i = 1, 2, \ldots, N, j = 1, 2, \ldots, m, t = 1, 2, \ldots, T, \tag{21}$$

$$a_{i,j}^{P2} = \begin{Bmatrix} a_{i,j}^{P2}, & lbj & \leq & a_{i,j}^{P2} \leq ubj \\ lbj, & a_{i,j}^{P2} & < & lbj \\ ub, & a_{i,j}^{P2} & > & ubj \end{Bmatrix} \tag{22}$$

$$A_i = A_i^{P2} \begin{cases} , & F_i^{P2} < F_i \\ A_i & else \end{cases} \tag{23}$$

where A_i^{P2} is the i^{th} Aqua Raptor's new position based on the second phase of the AROA, $a_{i,j}^{P2}$ is the j^{th} dimension, F_i^{P2} is its fitness function, r_{ij} are random numbers in the interval [0,1], t is the iteration counter of the method, and T is the total number of iterations.

The flowchart in Fig. 3 of TAROA in VANETs illustrates the step-by-step process of integrating trust evaluation with optimization techniques for secure and efficient routing.

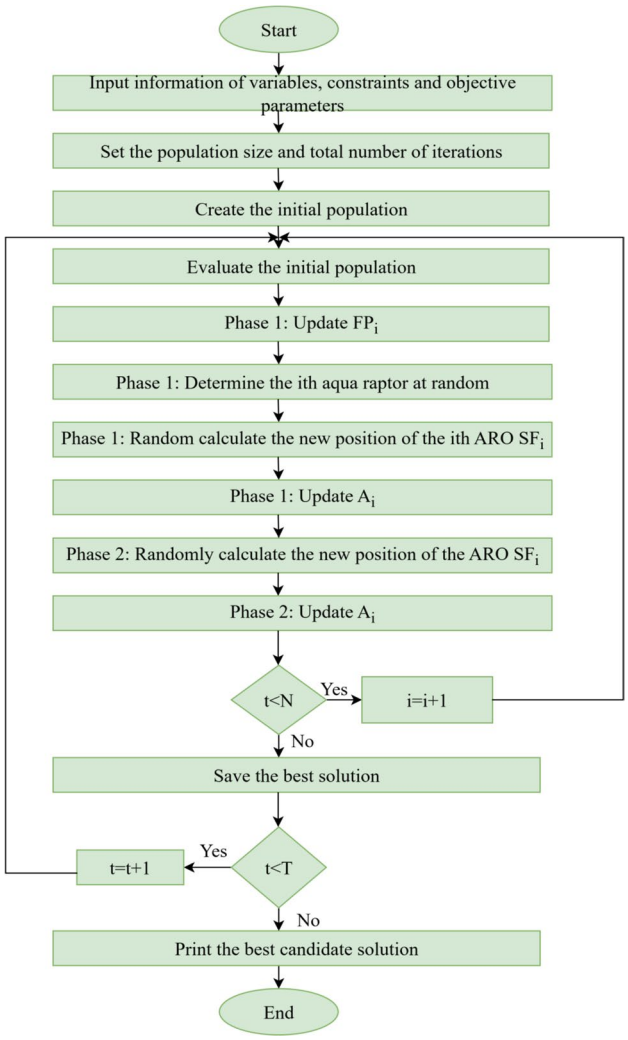


Fig. 3 Flow chart of TA- AROA method

The algorithm begins by collecting and analyzing data from vehicular nodes, including their movement patterns, energy levels and trustworthiness. The trust values of each node are calculated using several criteria, including previous behavior, reliability, and network interactions. The AROA is then used to choose the best path to use in transmitting the data and it is based on the nodes that have high trust scores as well they use minimum energy. The flowchart assists in the choice of CHs and the creation of safe communication channels and data packet routing over the trustful nodes. Finally, the algorithm is dynamically adjusted to network changes. It guarantees secure, reliable, and energy-efficient communication within VANETs and it consistently updates the trust metrics by considering the changing network state. The initial AROA is performed by rearranging all the Aqua Raptor in the first and second stages. The objective function values for updating the top candidate solution are compared. The model is further iterated to obtain the modified Aqua Raptor positions until Eqs. (13–22) are achieved. After the algorithm is run, the problem is solved using the best candidate solution obtained between the iterations.

3.3.6 Objective Function for TA-AROA-Based Routing Path Selection

During the TA-AROA routing phase, every Aqua Raptor is a potential multi hop routing path between a source and a destination. The routing objective function is given as

$$F(R_j) = \alpha.T_j + \beta.\frac{1}{D_j} + \gamma.\frac{1}{PLR_j} + \delta.\frac{1}{E_j} \tag{24}$$

where:

- T_j is the aggregated trust value of nodes along route jjj,
- D_j denotes the end-to-end delay,
- PLR_j represents the packet loss rate,
- E_j is the energy consumption along the route, and
- α, β, γ, δ are weighting parameters for controlling routing priorities.

Optimization Goal:

TA-AROA maximizes $F(R_j)$ to identify routing paths that:

- traverse highly trusted vehicles,
- minimize latency and packet loss,
- reduce energy expenditure, and
- ensure reliable data delivery under high mobility.

The exploration phase of AROA identifies promising routing regions, while the exploitation phase refines the paths near optimal solutions, enabling fast convergence and adaptability to frequent topology changes in VANETs.

3.3.7 Practical Interpretation

In summary, the objective functions $F(A_i)$ and $F(R_j)$ are not the abstract mathematical entities, but explicit performance evaluators that guide MKOA and TA-AROA toward:

- stable and energy-efficient cluster head selection, and
- secure, low-delay, and trustworthy routing path optimization.

This explicit formulation bridges the gap between the mathematical models and their real-world VANET implementation by eliminating ambiguity and ensuring algorithm transparency.

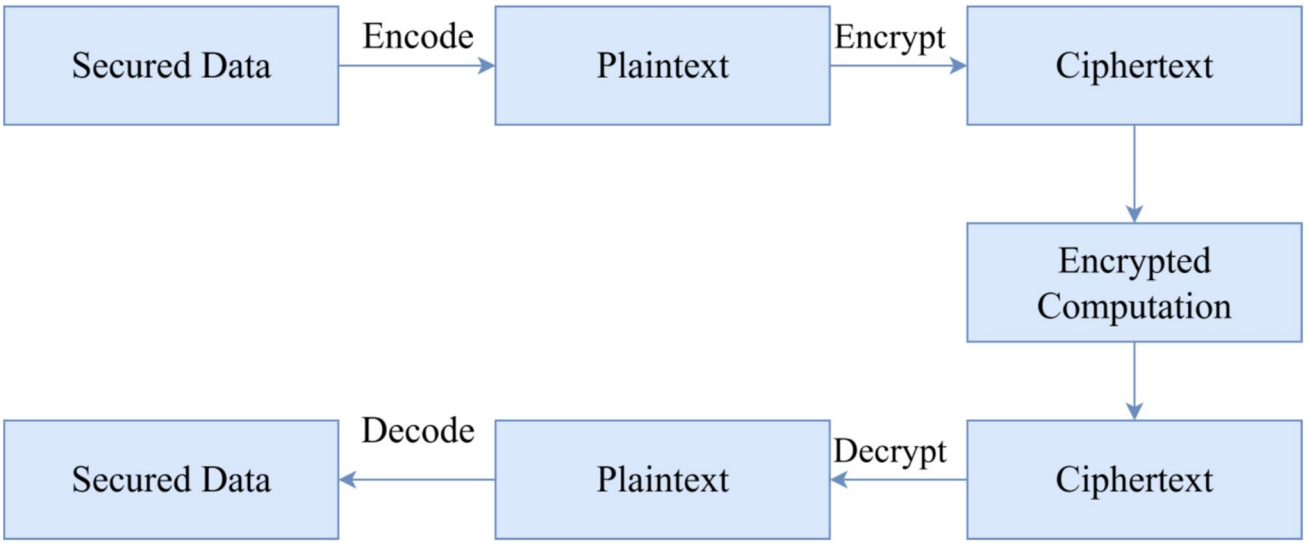


Fig. 4 The process flow of the modified homomorphic encryption algorithm

3.4 Modified Homomorphic Encryption

Encryption algorithms are an essential aspect of contemporary cryptography, whereby data are secured by converting information into an unreadable form unless they are decrypted with the necessary decryption key. These types of algorithms are used globally in various applications, such as secure communication, data secrecy, and information security, to transform plaintext into cipher text by employing highly complex mathematical functions. In contrast, symmetric cryptography requires the same key for encryption and decryption. This category of encryption comprises five basic components of the system. The algorithm requires an unencrypted text, which is a primary data or message that is supposed to be encrypted. Here, the plaintext is subjected to two basic operations, namely, substitution and transformation, which determine the encryption scheme and provide security to the final cipher text (Kaur and Kakkar 2025; Yousefi et al. 2024).

The process flow of the Modified Homomorphic Encryption algorithm is depicted in Fig. 4.An algorithm starts with a secret key that is given as an input, and it determines the type of rotations and changes that are performed during the encryption process. The outcome of the operations is cipher text, which is the encrypted data that are directly affected by both the secret key and the plaintext. Both encryption and decryption are complementary processes that should be performed together to recover the data correctly. The algorithm also works during the decryption process, where it employs the secret key and ciphertext to reconstitute the original plaintext. In this work, the developed Modified Homomorphic Encryption (MHE) is based on the Paillier additive homomorphic scheme, which provides homomorphic addition and scalar multiplication. In the conventional Paillier scheme, the encryption of a message m with a public key (n,g) is as follows:

$$C = E(m) = g^m.r^n(modn^2) \tag{25}$$

where $r \in Z_n^*$ is a random value, n=$p.q$ is the RSA modulus, and g is a generator. Decryption is performed with the private key λ=lcm (p-1, q-1):

$$m = \frac{L\left(C^{\lambda} \mod n^2\right)}{\left(g^{\lambda} \mod n^2\right)} (\mod n) \tag{26}$$

With L(x)=$\frac{x-1}{n}$

The suggested change proposes two improvements.

1. Key-dependent rotation matrix transformation of the plaintext prior to encryption, which minimizes the size of the ciphertext and eliminates the chosen plaintext attack. This step is modeled as

$$m' = R_k(m) \quad m.\theta(\mathrm{mod}n), \theta = f(x) \tag{27}$$

Where f(k) is a rotation factor that is determined based on the secret key k.

2. Adaptive randomization during cipher text generation, where instead of a single random r, a time-varying nonce ρ_t is used:

$$C' = g^{m\prime}.\rho_t^n(\mathrm{mod}n^2) \tag{28}$$

This adjustment makes VANET communication more resilient to replay and the traffic analysis attacks through predictability. The MHE is computationally lightweight, unlike the traditional fully homomorphic encryption schemes, such as BGV or CKKS, which are computationally expensive and impractical in resource-constrained VANET nodes. This enables secure aggregation of trust values, residual energy, and routing metrics without plaintext exposure and allows expeditious encryption/decryption compatible with real-time vehicular conditions.

3.4.1 Trust Evaluation Mechanism

The proposed framework uses a lightweight modified homomorphic encryption scheme to secure trust values transferred along the routing and formation of clusters to guarantee the confidentiality and integrity of trust information. The encrypted trust scores enable intermediate and cluster nodes to perform aggregation and comparison operations with the encrypted trust scores without disclosing the actual values of the trusts and avoiding the attacks of trust manipulation and eavesdropping. This protocol guarantees that the vehicles with malicious intent do not have the ability to learn or modify trust estimation but still incur low computational costs that are applicable to high dynamic VANETs. The result is that secure trust-directed routing choices are obtained and they do not affect energy efficiency or real-time communication demands.

In the proposed FCKOA-TA-AROA framework, trust quantifies the reliability and cooperative behavior of vehicles during data forwarding and cluster participation. Trust is computed based on directly observable node behaviors, including packet forwarding behavior, packet drop tendency, transmission delay consistency, and mobility stability. These parameters collectively capture whether a vehicle reliably participates in routing without exhibiting selfish or malicious actions.

The trust score of vehicle i is calculated as a normalized weighted sum:

$$T_i = w_1.PFR_i + w_2.(1 - PDR_i) + w_3.(1 - D_i) + w_4.MS_i \quad (29)$$

Table 2 Simulation parameter setup

Parameter	Value
Simulation area	1000 m × 1000 m
Number of vehicles	500 nodes
Mobility model	Random waypoint (synthetic mobility)
Vehicle speed	20 m/s
Packet size	512 bytes
MAC protocol	IEEE 802.11p
Simulator Tool	MATLAB R2024a

Where PFR_i denotes packet forwarding ratio, PDR_i represents packet drop rate, D_i is delay deviation, MS_i indicates mobility stability, and $\sum w_i = 1$. The trust value is periodically updated using recent observations to reflect dynamic node behavior. Vehicles with trust values below a predefined threshold are excluded from the cluster head selection and routing decisions, thereby malicious or unreliable nodes are prevented in participating data transmission.

4 Results and Discussions

Using MATLAB R2024a, the proposed method has been implemented to simulate a VANET routing protocol that establishes secure routes for delivering user-specific composite services. Table 2 lists the simulation parameters. The model is selected as an artificial but popular simulation of vehicle motion in the first VANET experiments, in which nodes choose a destination randomly, it is assumed to be within the simulation area, move at a specified speed (20 m/s), and stop before selecting a new waypoint. Although fine-grained mobility and traffic control are achieved through the use of dedicated VANET simulators, such as NS-3 or Veins (OMNeT++with SUMO), it is aimed to assess the network-layer performance of the suggested clustering, trust-aware routing, and encryption mechanisms under controlled and repeating mobility patterns. The implementation of optimization algorithms (FCKOA, MKOA, TA-AROA) and integration of cryptographic modules (MHE) in the MATLAB environment provide the ability to maintain similarity in the design of the simulation and computational analysis.

The algorithms that are compared with the proposed FCKOA-TA-AROA algorithm are well-defined as follows: GBTR is the Graph-Based Trust-Enabled Routing scheme that uses graph theory to make trust-based routing decisions; BROA is the Bionic remora optimization algorithm that applies nature-inspired optimization techniques to make routing decisions; ABBSOA-AGEOA is the name of the Adaptive Binary Bird Swarm Optimization Algorithm that incorporates the Adaptive Golden Eagle Optimization Algorithm to make routing decisions and FOA-EECPCR is the Falcon Optimization Algorithm-based Energy Efficient Communication Protocol for Cluster-based Routing that combines falcon optimization with energy-aware clustering mechanisms. The state-of-the-art algorithms are used as a broad benchmark to confirm the high performance of the proposed algorithm in different network conditions as well as vehicle densities.

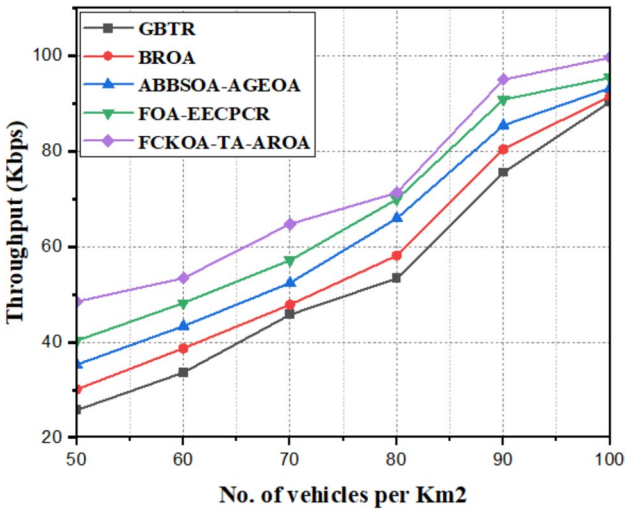


Fig. 5 Performance of throughput (Kbps)

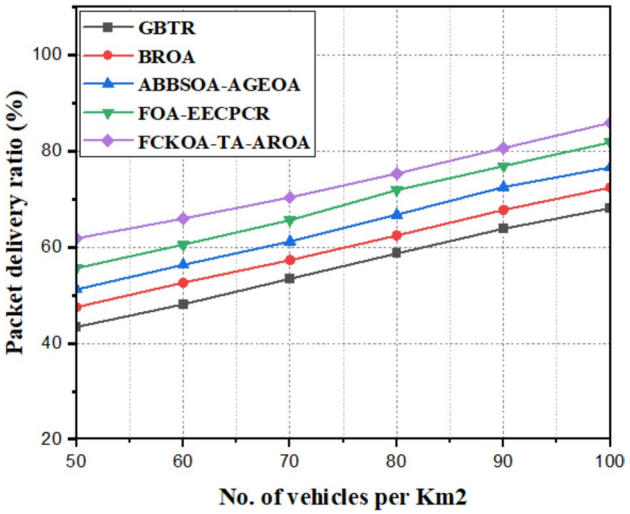


Fig. 6 Performance of PDR (%)

4.1 Performance Evaluation Based on Vehicle Density (Vehicles per Km^2)

The proposed FCKOA-TA-AROA algorithm is tested for different vehicle densities as indicated by the number of vehicles per square kilometer. The analysis is carried out with the comparison of benchmark algorithms, such as GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, and traffic densities of 50, 60, 70, 80, 90, and 100 vehicles/km^2. The analysis considers several performance parameters, including throughput (Kbps), packet delivery ratio (%), energy efficiency (%), bandwidth (bps), network security (%), attack detection rate (%), transmission delay (ms), routing overhead (%), cluster overhead (%), and coverage percentage (%). Detailed descriptions of each metric are provided in the subsequent discussion to demonstrate the adaptability of the proposed protocol for varying traffic densities.

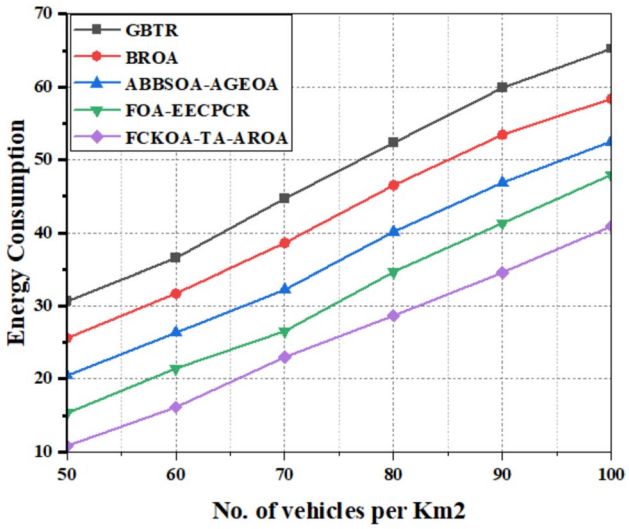


Fig. 7 Performance of energy consumption (J)

4.1.1 Throughput (Kbps)

Energy-efficient trust-aware clustering and routing protocols are compared with GBTR, BROA, ABBSOA-AGEOA, FOA-EECPCR, and FCKOA-TA-AROA. GBTR uses trust-based routing to deliver packets reliably; however, crowded networks increase energy usage. BROA and ABBSOA optimize CH selection and routing pathways using bio-inspired methods to increase throughput, whereas AGEAO dynamically addresses packet loss. Falcon-inspired cluster-based routing optimizes the throughput of FOA-EECP. Figure 5 shows the throughput performance. The proposed FCKOA-TA-AROA method enhances the throughput by 48.53 Kbps with 50 vehicles, whereas the GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR methods reduce it by 25.75, 30.12, 35.27, and 40.33 Kbps, respectively.

4.1.2 Packet Delivery Ratio (%)

The PDR is a key measure of VANET routing protocol efficiency and dependability of VANET routing protocols. The ratio of successfully delivered data packets to source node packets is calculated. Energy-efficient clustering and routing techniques indicate a greater PDR and better network performance. The equation ofthe PDR is as follows:

$$PDR = \frac{Total\ number\ of\ packets\ received\ at\ destination}{Total\ number\ of\ packets\ sent\ by\ source} \times 100 \quad (30)$$

Fuzzy clustering and trust-aware optimization reduce packet loss, improve route stability, and optimize energy

usage in dynamic VANET systems to increase the PDR. Figure 6 shows the PDR performance. The FCKOA-TA-AROA method enhances PDR by 61.87% with 50 vehicles, whereas GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR reduce THRO by 43.41, 47.52, 51.23, and 55.65%, respectively.

4.1.3 Energy Consumption (J)

Figure 7 illustrates the comparison of energy consumption (measured in joules, J) of the proposed FCKOA-TA-AROA algorithm with the existing routing algorithms. Energy consumption refers to the amount of energy expended by each node during packet transmission and it contributes to the overall energy usage of the network. The FCKOA-TA-AROA algorithm has used an energy consumption of 10.81 J whereas the traditional algorithms such as GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR have consumed 20.64, 25.61, 20.45, and 15.32 J, respectively. The graph indicates that the suggested protocol uses less energy to operate than the traditional routing methods and it explains its ability to consume less energy to operate.

4.1.4 Bandwidth (bps)

VANET energy-efficient clustering and routing methods rely on bandwidth to transmit data with the maximum efficiency as well as to enhance network performance. Network throughput depends on the channel bandwidth, which is the maximum rate of data transfer. In bits per second (bps), the following equation is used:

$$B = \frac{C}{T} \tag{31}$$

where B is the bandwidth, C is the data transferred (in bits), and T is the transmission time (s).

Maximum bandwidth utilization saves energy, maintains constant communication, and enhances routing protocols, including GBTR, BROA, ABBSOA-AGEOA, FOA-EECPCR, and the proposed FCKOA-TA-AROA, when mobile VANETs have high mobility. Figure 8 shows that the bandwidth performance and it is augmented by 82 bps when using the FCKOA-TA-AROA, and that of the GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR models are 70, 73, 76, and 79 bps, respectively.

4.1.5 Network Security (%)

Energy-efficient routing and clustering protocols of VANET provide network security to the data to achieve data confidentiality, integrity, and availability, as well as to save

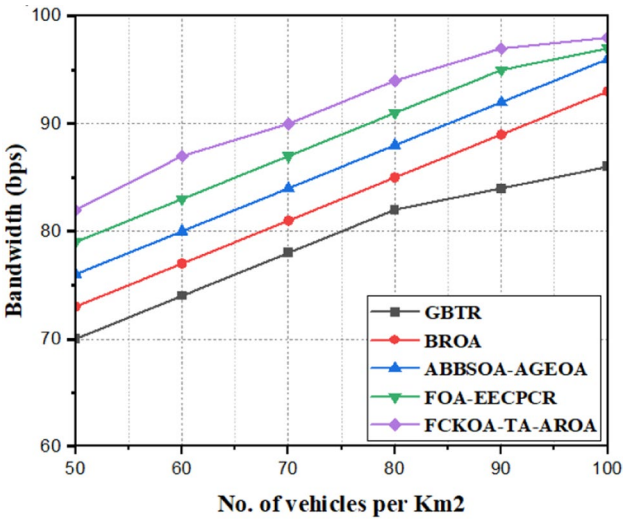


Fig. 8 Performance of bandwidth (bps)

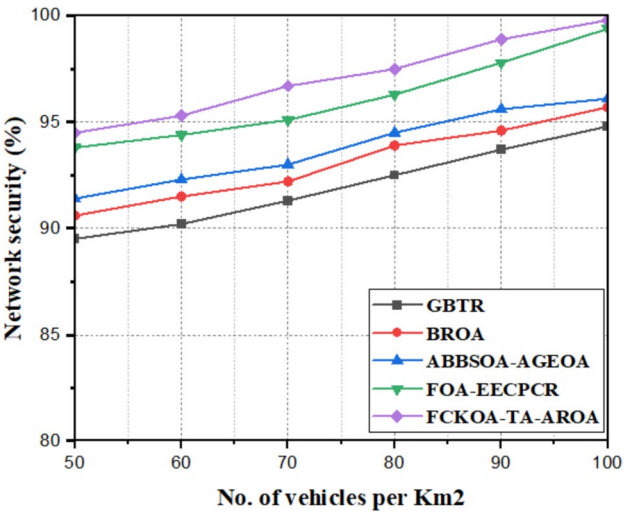


Fig. 9 Performance of network security (%)

energy. Securing communication between the vehicles through trust-aware protocols and encryption is extremely important to prevent unauthorized access or malicious attacks. The trust model of algorithms such as GBTR and FCKOA-TA-AROA uses the assessment of trust along with nodes that have acted properly in the past, and only trusted nodes are used to route the data. The following equation involves the use of trust (T) and energy usage (E) to determine the security of the network:

$$S = \frac{T.E}{T + E} \tag{32}$$

Where S is security, T is node trust, and E is energy usage. This equation assigns routing work to the trusted nodes that consume less energy as a priority to ensure a balance

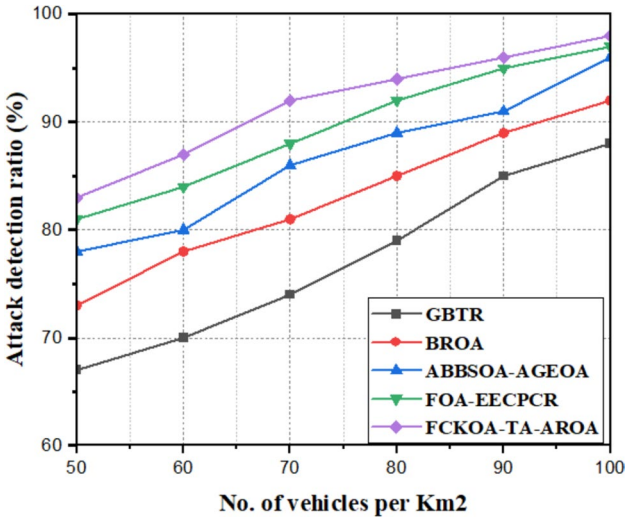


Fig. 10 Performance of ADR (%)

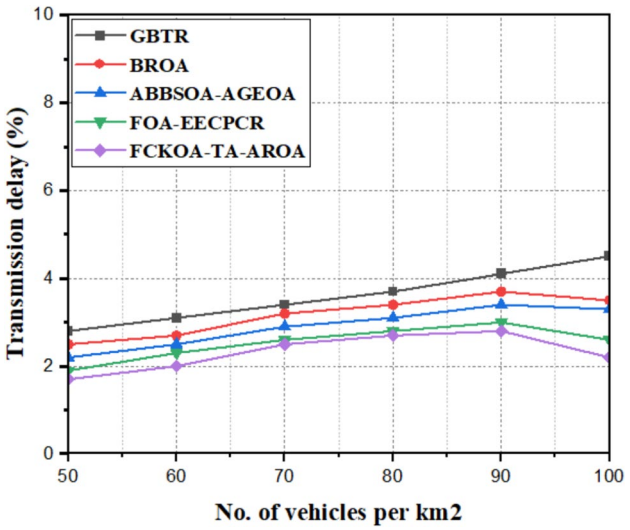


Fig. 11 Performance of transmission delay (%)

between security and energy efficiency. Figure 9 depicts the network security performance. FCKOA-TA-AROA increases the network security of 50 vehicles by 94.5 percent, as compared to GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, which reduce it by 89.5, 90.6, 91.4%, and 93.8%, respectively.

4.1.6 Attack Detection Ratio (%)

The ADR is a key performance indicator of the ability of VANET security processes to identify hazardous actions. The ratio of successfully detected attacks to network attacks is measured. The ADR formula is:

$$ADR = \frac{Number\ of\ Attacks\ Detected}{Total\ number\ of\ actual\ attacks} \times 100 \qquad (33)$$

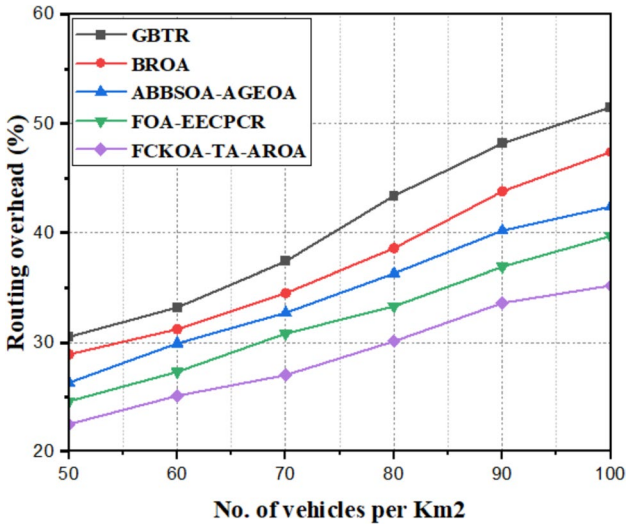


Fig. 12 Performance of Routing overhead (%)

A higher ADR indicates better assault detection. This measure evaluates the capacity of the FCKOA-TA-AROA algorithm to detect and mitigate security risks, thereby boosting network trust and reliability. Figure 10 illustrates the ADR performance. The FCKOA-TA-AROA method improves attack detection by 83% with 50 vehicles, whereas the GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR models reduce it by 67, 73, 78, 81%, respectively.

4.1.7 Transmission Delay (%)

The transmission delay of FCKOA-TA-AROA is compared with GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR in Fig. 11. The packet count and network transmission capacity affect the transmission delay. The FCKOA-TA-AROA method has achieved 1.7 ms transmission latency for 50 vehicle nodes. The transmission delays of the previous routing algorithms, namely GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, are 2.8, 2.5, 2.2, and 1.9 ms, respectively. Thus, the graph shows that the proposed routing strategy has a shorter transmission time than the others.

4.1.8 Routing Overhead (%)

The routing overhead is the total number of packets sent during the simulation. Fraction of source-generated packets is forwarded. Cloud data security can be improved by full encryption key control. Figure 12 presents the routing overhead (%) comparison of GBTR, BROA, ABBSOA-AGEOA, FOA-EECPCR, and FCKOA-TA-AROA. The proposed FCKOA-TA-AROA method depicts a routing overhead of 22.5%for 50 vehicle nodes, compared to 30.5, 28.9, 26.3, and 24.6% of the existing techniques. The graph

shows that the FCKOA-TA-AROA routing technique possesses reduced routing overhead compared to the existing strategies.

4.1.9 Cluster Overhead

Cluster overhead refers to the total communication and control cost incurred during cluster formation, cluster maintenance, and cluster head (CH) re-election processes in the VANET. In this work, cluster overhead is defined as the aggregate number of control packets exchanged per clustering cycle, including beacon messages, cluster join requests, CH advertisements, trust updates, and re-clustering notifications. Since the focus is on relative protocol efficiency rather than the absolute signaling size, the metric is represented as a normalized unitless value which enables fair comparison among different routing schemes under identical network conditions. Cluster overhead can be expressed as:

$$Cluster\ Overhead = \sum_{i=1}^{N} (M_{beacon} + M_{join} + M_{CH} + M_{update}) \quad (34)$$

Where N denotes the number of vehicles per km^2, M_{beacon}, M_{join}, M_{CH}, and M_{update} represent the control messages exchanged for neighborhood discovery, cluster affiliation, cluster head selection, and trust/maintenance updates, respectively. A higher cluster overhead indicates frequent re-clustering, excessive control signaling, and unstable cluster structures, which directly contribute to increased energy consumption and reduced network scalability.

Figure 13 shows the performance of the proposed FCKOA-TA-AROA cluster overheads compared to the existing algorithms with varying numbers of vehicles. In the case of 50 vehicles, the proposed model halves the cluster overhead by five, as compared to 28, 23, 18, and 20 of GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, respectively. These results reveal that FCKOA-TA-AROA will be very useful in reducing the maintenance overhead in clusters, and hence, it becomes very easy in making the process of scaling and enhancing the efficiency of a network in dynamic VANET settings.

4.1.10 Coverage (%)

Figure 14 represents the comparison of coverage performance of the proposed FCKOA-TA-AROA algorithm with that of the existing algorithms at various vehicle counts. The data show that the coverage of GBTR and BROA is lower, and ABBSOA-AGEOA also has lower numbers. Although through FOA-EECPCR, a reasonable similarity in the coverage levels is achieved compared to the proposed model, it

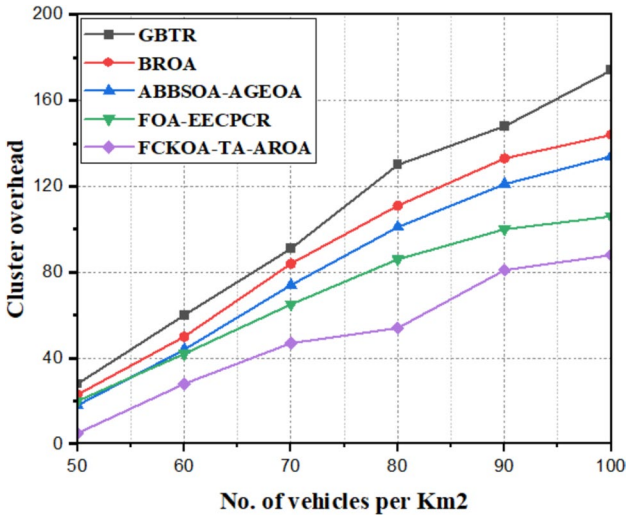


Fig. 13 Performance of cluster overhead

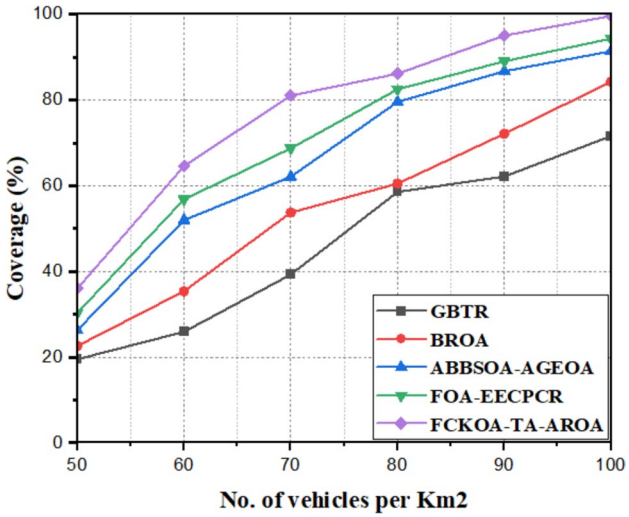


Fig. 14 Performance of coverage

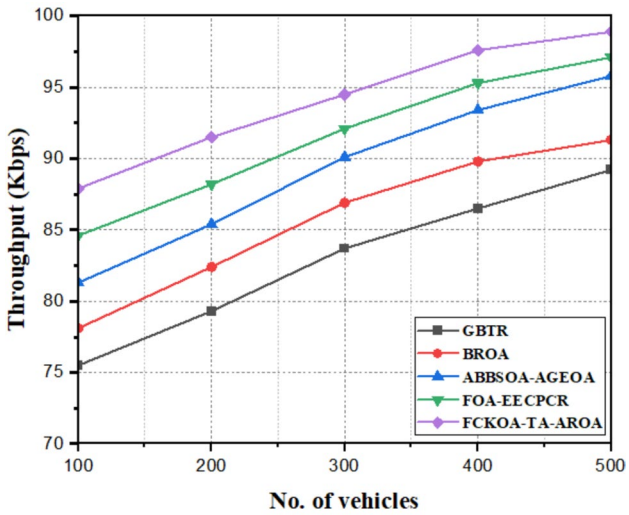


Fig. 15 Performance of throughput

is always lower. Conversely, FCKOA-TA-AROA presents the highest coverage with an improvement of 36.01%, when the number of vehicles is 50.Meanwhile, the GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPR have dropped by 19.52, 22.62, 26.31, and 30.31%, respectively. These findings highlight the superior scalability and reliability of the proposed approach in maintaining network coverage during dynamic VANET scenarios.

4.2 Performance Evaluation Based on Network Size (Number of Vehicles)

The overall performance of the proposed FCKOA-TA-AROA algorithm has been evaluated against four current algorithms, namely GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, with n sizes of 100, 200, 300, 400, and 500 nodes, respectively. Several performance indicators are compared, including throughput (Kbps), packet delivery ratio (%), bandwidth (bps), network security (%), attack detection rate (%), transmission delay (ms), cluster overhead (%), and coverage (%).The performance metrics are presented in the respective Figures and discussed below to highlight the effectiveness of the proposed approach.

4.2.1 Throughput (Kbps)

Figure 15 depicts the throughput performance. The proposed FCKOA-TA-AROA approach portrays a throughput of 98.9 kbps with 500 vehicle nodes. Conversely, the existing routing algorithms, including GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, have provided the throughput values of 89.2, 91.3, 95.8, and 97.1 kbps, respectively. The graph shows that the proposed methodology has a better throughput than the other routing methods.

4.2.2 Packet Delivery Ratio (%)

The performance of the PDR is shown in Fig. 16. The obtained PDRs of the existing routing algorithms, such as GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, are 85.31, 88.34, 91.36, and 94.78%, respectively; however, the proposed FCKOA-TA-AROA method has shown 98.39% with 500 vehicle nodes. From the PDR perspective, the proposed technique is better than the other known routing techniques. This variation in the PDR indicates higher reliability of FCKOA-TA-AROA in the reliable transmission of packets in the network. Although GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR have exhibit a progressive fall in PDR, indicating varied degrees of packet loss and decreasing routing efficiency, FCKOA-TA-AROA has a better success rate in packet delivery.

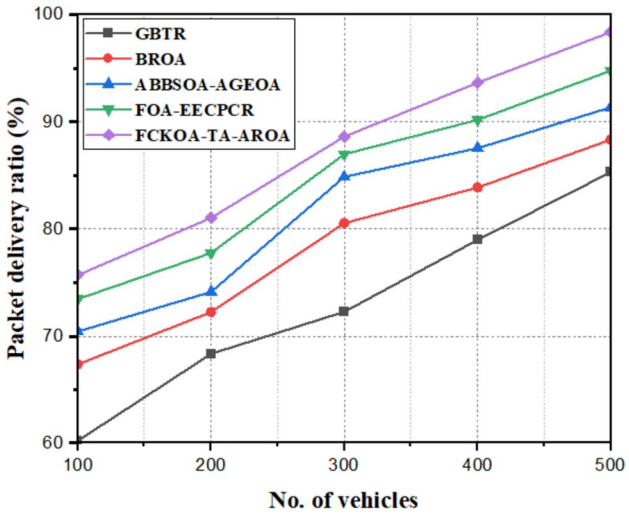


Fig. 16 Performance of PDR

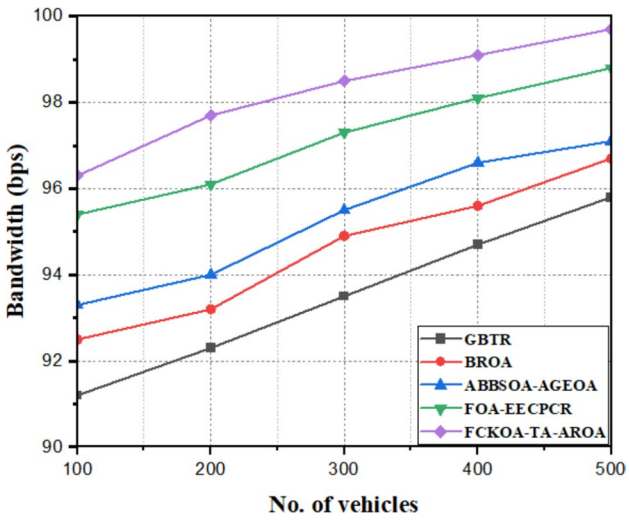


Fig. 17 Performance of bandwidth

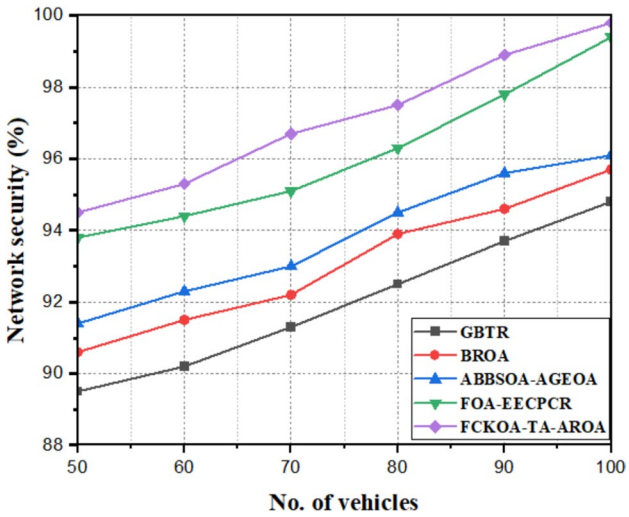


Fig. 18 Performance of network security

4.2.3 Bandwidth (bps)

Optimizing bandwidth usage lowers energy consumption, assures continuous communication, and enhances routing protocols of GBTR, BROA, ABBSOA-AGEOA, FOA-EECPCR, and the planned FCKOA-TA-AROA, particularly in high-mobility VANETs. Figure 17 shows the bandwidth performance. The FCKOA-TA-AROA technique enhances the bandwidth by 99 bps with 500 nodes, but the GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR models reduce the bandwidth by 88, 94, 96, and 98 bps, respectively.

4.2.4 Network Security (%)

Network security in energy-efficient VANET clustering and routing protocols maintains data confidentiality, integrity, and availability, while conserving energy. Vehicle communication must be secured by using trust-aware protocols and encryption to avoid unauthorized access or malicious assaults. Figure 18 shows the performance of network security. The trust model assigns trust values to nodes in algorithms such as GBTR and FCKOA-TA-AROA based on their previous behavior and it guarantees only trustworthy nodes route. FCKOA-TA-AROA improves network security by 99.7% for 500 nodes, while GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR reduce it by 95.8, 96.7, 97.1, and 98.8%, respectively.

4.2.5 Attack Detection Rate (%)

Figure 19 shows the ADR performance. The graph illustrates that the proposed FCKOA-TA-AROA approach outperforms the other routing algorithms in terms of the attack detection rate. The FCKOA-TA-AROA technique improves attack detection by 97% with 500 nodes, but the GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR models reduce it by 89, 93, 95, and 96%, respectively. This is due to the fact that the technique is able to identify and offer remedies to potential security risks in the network.

4.2.6 Transmission Delay (%)

The transmission delay performance is shown in Fig. 20. The proposed FCKOA-TA-AROA system has recorded a transmission delay of 2.7 ms on 500 vehicle nodes. Comparatively, the transmission delays of the existing routing algorithms, including GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, are 4.2, 3.8, 3.5, and 3.1 ms, respectively. The graph indicates that the proposed methodology has a lower propagation delay than the other routing strategies.

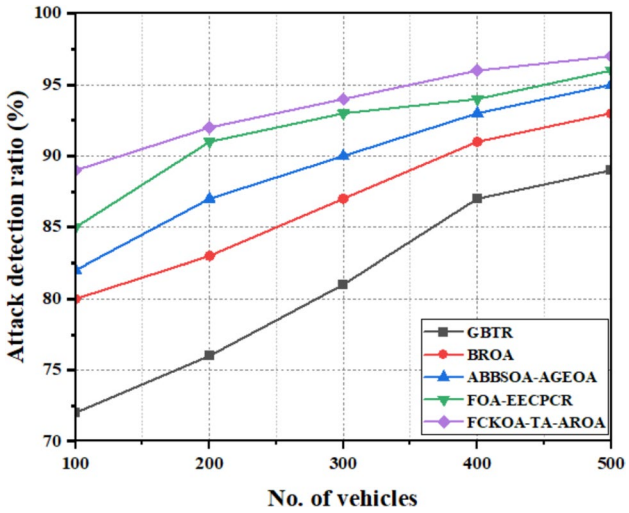


Fig. 19 Performance of ADR

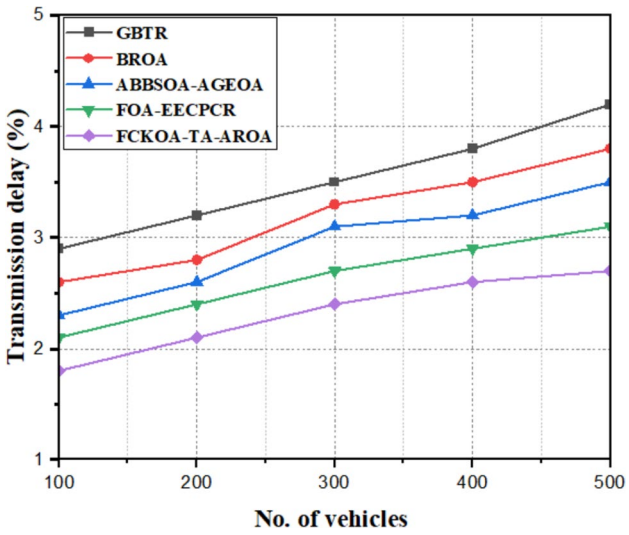


Fig. 20 Performance of transmission delay

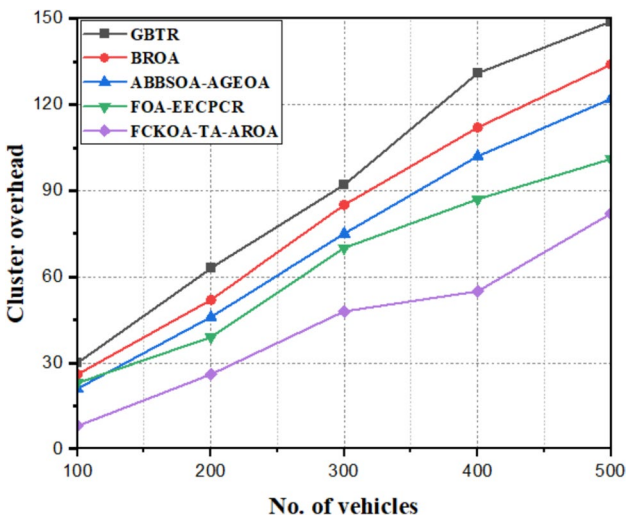


Fig. 21 Performance of cluster overhead

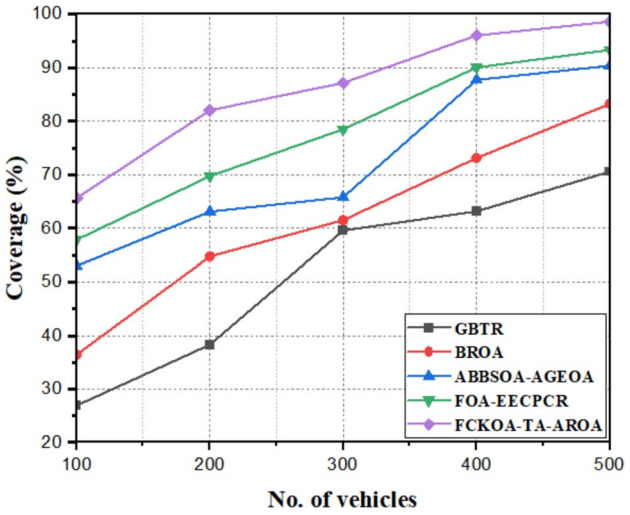


Fig. 22 Performance of coverage

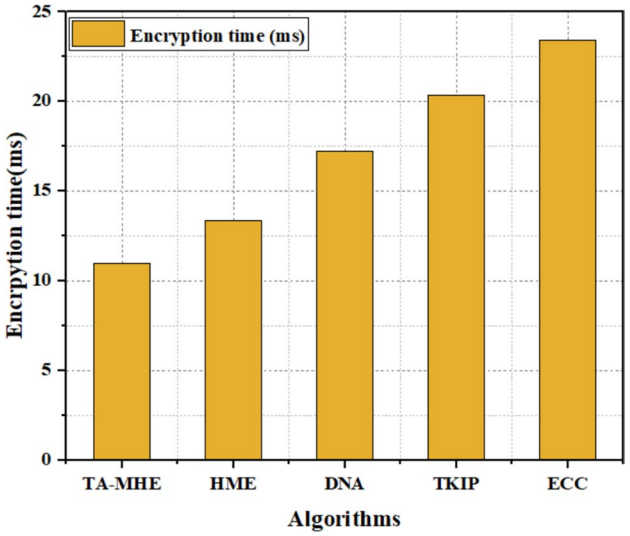


Fig. 23 Performance of the encryption time (ms)

4.2.7 Cluster Overhead

Figure 21 shows the cluster overhead of FCKOA-TA-AROA model for varying numbers of vehicles. FCKOA-TA-AROA ensures that COH is minimized to 82, when the number of vehicle nodes is 500, but GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR cause cluster overheads of 149, 134, 122, and 101, respectively. These results show that the advanced model is useful in reducing the overhead of the clusters. It consequently minimizes the maintenance expenses as well as improves scalability and such a reduction in the cluster overhead guarantees efficient cluster management, even under the conditions of high vehicle density and dynamic VANET situations.

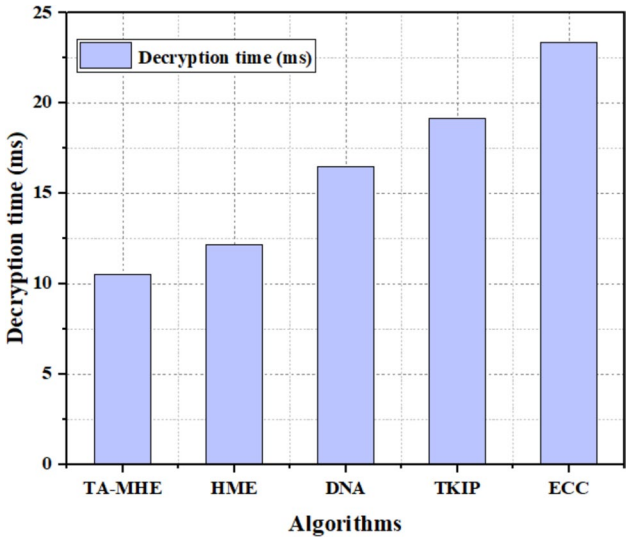


Fig. 24 Performance of the decryption times (ms)

4.2.8 Coverage (%)

Figure 22 illustrates the coverage of different routing algorithms with different values of the number of vehicles. The FCKOA-TA-AROA algorithm always has the best coverage, exceeding 95%, when the network is extended to 500 vehicles. Competitive results are also achieved by FOA-EECPCR and ABBSOA-AGEOA, but the levels of coverage of BROA and GBTR are relatively low. Overall, the suggested model has proved to be highly scalable and robust in achieving high network coverage under changing VANET conditions. The ABBSOA-AGEOA method also has yielded low coverage values. The coverage value given by FOA-EECPCR is more accurate than that of FCKOA-TA-AROA, which has produced the maximum value of all methods. The FCKOA-TA-AROA technique has increased the coverage by 98.62% with 500 vehicle nodes, whereas the GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR models have decreased the coverage by 70.58, 83.24, 90.39, and 93.34%, respectively.

4.3 Performance Evaluation of Encryption and Decryption Time

4.3.1 Encryption Time (ms)

The encryption time is the processing time required to encrypt the data. A comparison of the encryption time (ms) of the proposed TA-MHE algorithm with that of existing algorithms, that is, HME, DNA, TKIP, and ECC, is shown in Fig. 23. This comparison indicates that TA-MHE is more efficient in vehiclerying out the encryption processes, thereby making the data encryption faster. Encryption takes 10.98 ms to complete with the proposed TA-MHE algorithm,

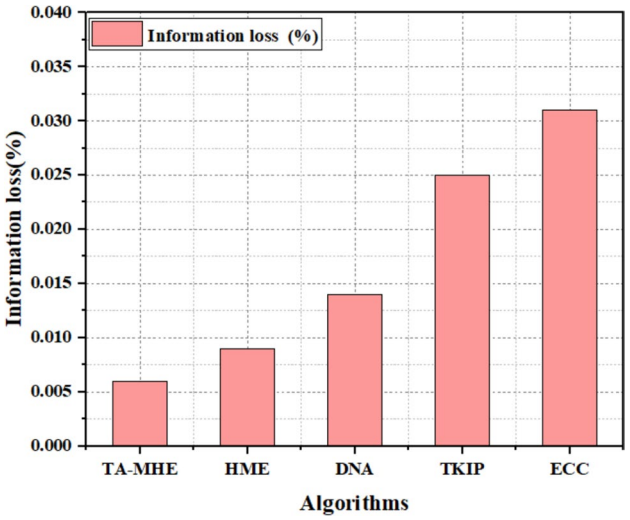


Fig. 25 Performance of the information loss (%)

which means that the algorithm is not as time-consuming as other existing cryptography algorithms. In addition, the encryption of TA-MHE proves that it is more efficient and is therefore suitable for applications that require high processing. The decryption time concept is associated with the rate of processing data to be decrypted. The longer the data size, the more time it takes to decode.

4.3.2 Decryption Time

Figure 24 presents the decryption time (ms) comparison of the proposed FCKOA-TA-AROA algorithm and the existing techniques GBTR, BROA, ABBSOA-AGEOA and FOA-EECPCR. The results indicate that the proposed FCKOA-TA-AROA algorithm requires less time than the other available algorithms, with a decryption time of 10.52 ms. The reduced latency time of FCKOA-TA-AROA should be mentioned, particularly because of the high-speed access to the data and data processing methods, which enhance the overall system performance and responsiveness.

4.4 Information Loss (%)

Figure 25 demonstrates the loss of information (in %) between the proposed TA-MHE algorithm and the existing cryptographic approach. The information loss is 0.006 bits. The significantly reduced loss of information in TA-MHE validates its effectiveness in data encryption and decryption with minimal loss. In contrast, the greater loss of information associated with HME, DNA, TKIP, and ECC implies that these methods can harm the quality of data to a larger extent, thereby affecting the applicability and reliability of the encrypted data. The graph above clearly shows that the proposed TA-MHE has fewer information losses and is a superior model compared to other cryptographic methods.

4.5 Computational Complexity

As indicated in Table 3 of computational complexity, although the FCKOA-TA-AROA approach increases computational complexity with fuzzy logic and multi-optimization, it offers more accurate clustering and routing and possibly enhances the efficiency of VANET. The computational complexity of FCKOA-TA-AROA, listed as O

Table 3 Computational complexity comparison of VANET routing algorithms

Algorithm	Computational complexity	Description/Justification
GBTR	$O(V^2)$	Simple greedy-based routing; low computational cost but limited in cluster stability and security
BROA	$O(N \cdot M)$	Bio-inspired routing; scales linearly with nodes (N) and number of iterations or candidate solutions (M)
ABBSOA-AGEOA	$O(N^2)$	Swarm-based optimization; quadratic scaling due to population interactions for path optimization
FOA-EECPCR	$O(N \cdot k)$	Fuzzy clustering combined with FOA; scales with number of nodes (N) and clusters (k)
FCKOA-TA-AROA	$O(N \cdot M \cdot k)$	Combines three layers: OFCM clustering (O (N·k)), MKOA CH selection (O(N·M)), and TA-ARO routing (O(N·P)). Although higher than simpler methods, it remains polynomial and scalable. Parallel/distributed execution further reduces practical runtime. The added complexity is justified by improvements in cluster stability, energy efficiency, secure routing, and attack resilience

Table 4 State of the art comparison

Ref No	Author name (Year)	Algorithm	PDR (%)	Energy consumption (J)	Throughput (kbps)
[8]	Choksi (2024)	Dynamic clustering algorithm (DCA)	-	68	72.5
[14]	Anupama et al. (2024)	AN2-TAS2FS	83	-	81.3
[27]	Magdalin et al. (2023)	DBSCAN	85.6	52.77	65.4
[33]	Alotaibi (2024)	FOA-EECPCR	81.58	55	79.6
[37]	Kadam (2023)	TACR	80.2	-	74.8
[38]	Babu (2024)	BROA	86	-	78.7
Proposed		**FCKOA-TA-AROA**	**88**	**42**	**99**

(N·M·k), represents the combined per-iteration cost of cluster formation (OFCM), CH selection (MKOA), and routing optimization (TA-ARO). Although the framework involves multiple optimization layers, each layer scales linearly or near-linearly with the number of nodes, candidate CHs, and clusters, rather than quadratically with N^2 or cubically with N^3. Moreover, many operations, such as trust evaluation, cluster formation, and CH selection, can be performed in parallel or distributed across vehicles and they significantly reduce the practical run time. The FCKOA-TA-AROA has a higher theoretical complexity than the simpler methods (GBTR, BROA, FOA-EECPCR), and the performance gains in energy efficiency, secure routing, and cluster stability justify the additional computational cost. Moreover, the polynomial complexity remains scalable for realistic VANET deployments.

4.6 State of the Art Comparison

Table 4 presents a comparative evaluation of the proposed FCKOA-TA-AROA algorithm against the existing leading techniques, focusing on PDR, energy consumption, and throughputin the performance evaluation based on Vehicle Density (Vehicles per Km^2). Moderate performance is shown by the dynamic clustering algorithm (DCA) (Choksi and Shah 2024) and DBSCAN (Magdalin and Kumarasabapathy 2024), whereby DBSCAN hasa PDR of 85.6% and a throughput of 65.4 kbps, but with a higher power consumption (52.77 J).FOA-EECPCR (Anjali et al. 2024) and TACR (Kaur and Kakkar 2025) have improved the throughput but have issues with energy efficiency and delivery ratio. Similarly, AN2-TAS2FS (Kn and Nagaraj 2025) and BROA (Yousefi et al. 2024) have provided enhanced trust and security by yielding higher PDR values of 83% and 86%, respectively. Conversely, the proposed FCKOA-TA-AROA depicts the best PDR of 88%, balanced energy consumption of 42 J, and stable throughput of 99 kbps. Thus, the proposed algorithm outperforms the benchmark algorithms.

4.7 Statistical Analysis

To robustly verify the statistical significance of the proposed experimental outcomes, a detailed statistical analysis of all the performance metrics is performed by employing 20 independent simulation runs for each network configuration. Table 5 displays the statistical validation, including the mean values, standard deviation, 95% interval, and p-values of the paired t-tests of the proposed FCKOA-TA-AROA with all the benchmark algorithms (GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR).The findings indicate that the proposed approach has produced statistically significant improvements in all the measures considered, and the p-values of the results are consistently less than 0.001, which proves that the changes in the performance are not caused by chance but they represent the actual algorithmic superiority of the proposed method. In Packet Delivery Ratio, FCKOA-TA-AROA provides a mean of 80.24% (50–100 nodes) and 89.67% (100–500 nodes) with a small confidence intervaland it is better than the top competing algorithm, FOA-EECPCR, by 4.92% and 4.43%, respectively. Similarly, for the Attack Detection Rate, the proposed approach has attained 92.47% (50–100 nodes) and

Table 5 Statistical validation of performance metrics across comparative algorithms

Metric	Algorithm	Mean±SD	95% CI	p-value
PDR (%) (50–100 nodes)	FCKOA-TA-AROA	80.24±2.15	[78.09, 82.39]	–
	FOA-EECPCR	75.32±2.48	[72.84, 77.80]	<0.001
	ABBSOA-AGEOA	71.85±2.92	[68.93, 74.77]	<0.001
	BROA	67.21±3.15	[64.06, 70.36]	<0.001
	GBTR	62.48±3.41	[59.07, 65.89]	<0.001
PDR (%) (100–500 nodes)	FCKOA-TA-AROA	89.67±1.82	[87.85, 91.49]	–
	FOA-EECPCR	85.24±2.21	[83.03, 87.45]	<0.001
	ABBSOA-AGEOA	82.15±2.56	[79.59, 84.71]	<0.001
	BROA	78.92±2.89	[76.03, 81.81]	<0.001
	GBTR	74.35±3.12	[71.23, 77.47]	<0.001
ADR (%) (50–100 nodes)	FCKOA-TA-AROA	92.47±1.68	[90.79, 94.15]	–
	FOA-EECPCR	88.35±2.12	[86.23, 90.47]	<0.001
	ABBSOA-AGEOA	84.52±2.45	[82.07, 86.97]	<0.001
	BROA	80.28±2.81	[77.47, 83.09]	<0.001
	GBTR	75.64±3.18	[72.46, 78.82]	<0.001
ADR (%) (100–500 nodes)	FCKOA-TA-AROA	95.83±1.45	[94.38, 97.28]	–
	FOA-EECPCR	91.52±1.87	[89.65, 93.39]	<0.001
	ABBSOA-AGEOA	87.64±2.34	[85.30, 89.98]	<0.001
	BROA	83.21±2.68	[80.53, 85.89]	<0.001
	GBTR	78.45±3.01	[75.44, 81.46]	<0.001

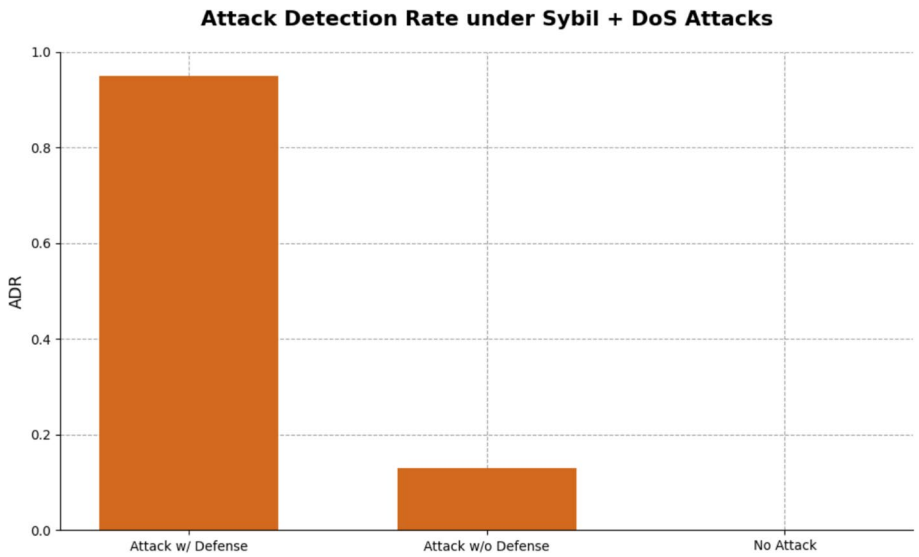


Fig. 26 ADR under sybil and DoS attacks in VANETs

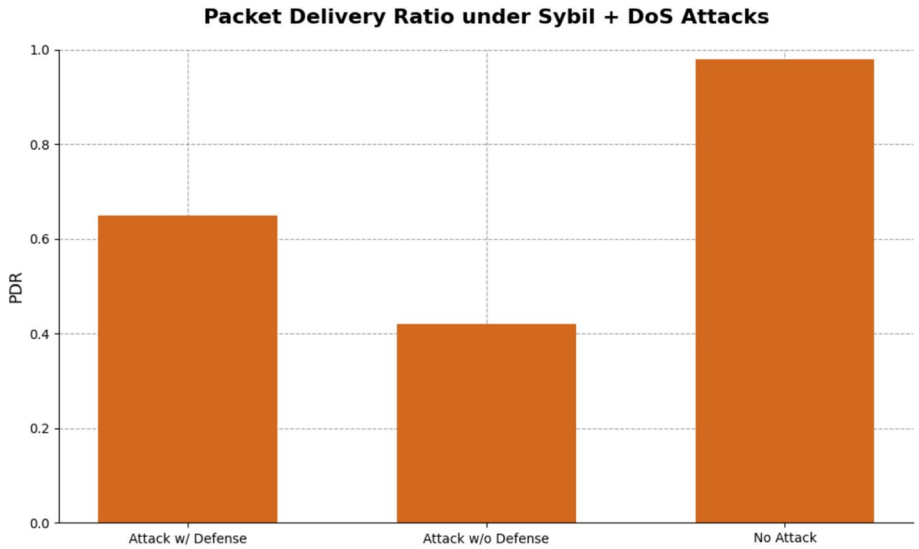


Fig. 27 PDR under sybil and DoS attacks in VANETs

95.83% (100–500 nodes), which are 4.12% and 4.31% better than FOA-EECPCR, respectively, with high statistical significance. The high degree of consistent narrowness of the confidence intervals of all metrics demonstrates high reliability and reproducibility of the proposed solution, and the significant difference in the mean values with low standard deviations proves high level of robustness and stability of the FCKOA-TA-AROA at various levels of network density and operating conditions, which in turn prove the effectiveness of the solution on secure and efficient VANET routing applications.

4.8 Adversarial Dataset and Evaluation

To evaluate the strength of the suggested FCKOA-TA-AROA framework under adversarial conditions, a synthetic adversarial dataset has been developed in MATLAB. This is achieved by simulating the Sybil and DoS attack conditions within a VANET setting. The dataset consists of 100 vehicle nodes, 5% of which is malicious attackers. Normal vehicles transmit one packet in each time step whereas DoS attackers transmit packets ten times as frequently which lead to congestion and flooding of the channels. In the case of Sybil attacks, every malicious node generates multiple identities (Sybil factor = 10) and sends fake beacons to interfere with trust management. The simulation is performed with 200 time steps, and each experiment is performed ten times independently to guarantee statistical reliability.

The evaluation is focused on two major adversarial indicators: the Packet Delivery Ratio (PDR) and the Attack Detection Rate (ADR). PDR is used to determine the percentage of packets that are delivered and the number of packets that are sent, which denote how attacks can affect communication reliability. ADR determines the rate of

Table 6 Comparative analysis of routing, swarm intelligence, and machine learning approaches in VANETs

Algorithm	Key features	Advantages	Limitations
GBTR	Graph-based trust routing	Simple, moderate security	Moderate energy efficiency and PDR
BROA	Bio-inspired path optimization	Good exploration, moderate convergence	Higher energy consumption and routing overhead
ABBSOA-AGEOA	Hybrid clustering and routing	Improves stability	Moderate computational complexity
FOA-EECPCR	Energy-aware clustering & routing	Fast convergence	Lower network security & coverage
ACO-VANET	Ant-inspired path selection	Good for shortest-path routing	Can converge slowly in dynamic networks
PSO-VANET	Particle-based optimal path	Low computational cost	Prone to local optima
GWO-VANET	Grey wolf hunting strategy for routing	Good exploration–exploitation balance	Moderate computational complexity
Q-Learning VANET Routing	Adaptive path selection	Adapts to dynamic topology	Requires training and slower convergence
DQN-Based Routing	Deep Q-network for adaptive routing	Handles high mobility	High computational cost and large training data are required
LSTM-VANET	Predicts vehicle mobility for routing	Improves reliability	Needs historical data and high training cost
CNN-Routing	Extracts spatial traffic features	High routing accuracy	Computationally intensive
Proposed FCKOA-TA-AROA	OFCM clustering + MKOA-based CH selection + TA-ARO trust-aware routing with homomorphic encryption	High PDR, energy efficiency, network security, low delay, high attack detection	Slightly higher computational cost than the simple heuristics

malignant operations that a defense mechanism can recognize and isolate. Three cases are considered: (i) baseline condition, that is, no attack; (ii) attack; and (iii) attack under the proposed TA-AROA + TA-MHE defense. The results show that the suggested defense is very effective in the detection of most of the lost PDR and nearly 95 of the ADR, and it is, therefore, effective against the Sybil and DoS attacks in small-scale VANETs.

Figure 26 shows the ADR of the FCKOA-TA-AROA structure under the Sybil and DOS attacks. Three cases are contrasted: a control where there is no attack, an attack where there is no defense, and an attack where there is TA-AROA + TA-MHE defense mechanism. The results suggest that the proposed framework is effective in detecting and separating most malicious nodes, with an ADR of approximately 95%, which is a good indicator of high protection against such threats. Figure 27 shows the PDR performance of the FCKOA-TA-AROA framework in comparison with the same nature of attacks. The scenarios that are compared are the baseline, an attack without defense, and an attack with TA-AROA + TA-MHE defense only. The suggested approach is able to retrieve the majority of lost packets in the case of attacks. It highlights the increased reliability and resiliency of communication in adversarial settings.

In spite of the fact that the experiments currently focus on attacks on Sybil and DoS, the FCKOA-TA-AROA framework is inherently resistant to more complex attacks, due to its layered design.The trust-aware routing system is a routing system that continuously evaluates the behavior of the nodes, black holes and gray holes, and colluding nodes are counteracted by allocating them a low trust score, thus ensuring that they are not selected as CHs or routing nodes. The path selection used by TA-ARO considers energy and trust, and homomorphic encryption ensures that the data integrity and effects of wormhole and selective manipulation of packets on the network are reduced. Dynamic routing also helps overcome the outcomes of jamming because it avoids congested or damaged routes. As a whole, optimized clustering, trust evaluation, secure routing, and encryption measures offer high levels of protection against different advanced cyber threats.

4.9 Causal Analysis of Optimization Mechanisms

The performance gains achieved by the proposed framework are the result of a direct mapping between bio-inspired behaviors and concrete networking operations, rather than the metaphorical inspiration alone. In the Modified Kookaburra Optimization Algorithm (MKOA), the cooperative hunting behavior is modeled as collaborative evaluation of candidate cluster heads, where multiple fitness factors—residual energy, relative mobility, and link stability—are jointly optimized. This coordinated selection process avoids isolated or short-lived cluster head choices, thereby significantly re-clustering frequency and control message exchanges are reduced. As a result, unnecessary energy expenditure caused by frequent cluster maintenance is minimized and it leads to improved energy efficiency and prolonged network lifetime. Similarly, in the Trust-Aware Aqua Raptor Optimization Algorithm (TA-AROA), the pursuit-diving strategy is translated into rapid trust-guided route refinement, where routing paths are continuously adjusted to exclude low-trust or suspicious nodes. This aggressive elimination of unreliable nodes during route construction

prevents packet dropping, selective forwarding, and trust manipulation attacks at early stages. Consequently, data packets are consistently forwarded through high-trust paths and they directly contribute to high packet delivery ratio as well as 99.8% network security rate is achieved. Thus, the biological behaviors are explicitly reflected in algorithmic decision-making and it establishes a clear causal link between optimization strategy and network performance improvements.

5 Discussion

5.1 Comparative Discussion of Machine Learning and Swarm Intelligence Approaches

In Table 6, Comparative Analyses of Routing, Swarm Intelligence, and Machine Learning Approaches in VANETs have been presented. The relative evaluation of machine learning and swarm intelligence techniques shows the exceptional advantages of the proposed FCKOA-TA-AROA in VANET. Traditional routing protocols, including GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, provide middle-range delivery of packets and energy saving but lack adaptive trust and cryptographic capabilities. Swarm intelligence algorithms (e.g., ACO, PSO, GWO) are based on probabilistic exploration and collective search methods of locating paths; however, convergence also depends on the density of networks, and there are no inherent means of dealing with malicious nodes or safe data delivery. Routing machine learning methods (e.g., Q-learning and DQN) are adaptive to topology and they respond to changes in the topology via reinforcement feedback; however, deep models (e.g., LSTM and CNN) can use both temporal and spatial patterns in traffic to make better predictions. Moreover, these approaches require large amounts of training data and hence, they are slow in inference. Further, they require large amounts of computing power, which makes them impractical in vehicular networks in real time. On the other hand, the suggested FCKOA-TA-AROA model incorporates optimized fuzzy grouping to maintain consistency, MKOA-driven CH selection to obtain energy equilibrium, and a trustful optimization algorithm with homomorphic encryption to ensure secure routing. Such a design shows low computational overhead, high packet delivery ratio, lower delay, better energy consumption, and well-rebuilt attack resistance. Hence, the scalability and security requirements of the hybrid are better than the current ML and swarm intelligence methods.

The comparative assessment presented in Table 6 is intended to provide a qualitative and methodological comparison of representative routing, swarm intelligence, and machine learning–based approaches in VANET environments. The comparison is conducted under a unified simulation framework to ensure fairness and reproducibility. All algorithms are evaluated using the same VANET simulation environment, mobility model, traffic density, and communication parameters and they are consistent with the experimental setup described in Section X. Performance comparison focuses on commonly adopted VANET metrics, including packet delivery ratio (PDR), end-to-end delay, throughput, routing overhead, energy consumption, and network security indicators such as attack detection rate and trust reliability. For machine learning–based approaches, the evaluation considers training overhead, convergence behavior, and adaptability to dynamic topology, while swarm intelligence–based methods are assessed based on convergence efficiency, routing stability, and computational complexity. Where explicit quantitative results are not directly reproduced under identical conditions, the comparative attributes are derived from the performance characteristics reported in the corresponding literature. This ensures that the comparison in Table 6 reflects a fair, transparent, and reproducible evaluation of algorithmic strengths and limitations within a consistent VANET simulation context.

The FCKOA-TA-AROA architecture is created such that it can be distributed and processed in parallel by allowing local clusters to be formed, CH to be selected, and routing to be done based on trust within each individual cluster rather than being centrally executed across the entire network. The design is such that it does not result in computational and communication load growing exponentially with the number of vehicles involved. Moreover, the OFCM clustering algorithm dynamically adjusts the size of the cluster according to the density of the nodes, MKOA selects the optimal CHs in each cluster, and TA-ARO provides better routing in locality by successfully distributing the workload in the network. Thus, in highly congested urban networks with thousands of vehicles, the framework incurs a computationally tractable level of complexity, the routing overhead is minimized, and it is highly energy conscious as well as provides secure and reliable communication.

A similar simulation will be conducted in the future research with large-scale urban traffic data to analyze the performance of a very dense VANET. The implicit solution of this work concerns the mobility of vehicles and network congestion through OFCM clustering and the routing mechanism using TA-ARO, which is dynamically adjusted to the forms of node mobility and the intensity of the traffic. The clustering algorithm considers the change in vehicle speed, lane changes, and inter-vehicle distances to create stable clusters, and the routing algorithm considers energy and trust to prevent congested or unreliable routes. As an example, the framework can be used with realistic mobility models, such as the Intelligent Driver Model (IDM) or simulated

SUMO traces, and the effects of congestion can be measured using a metric such as the average utilization of a link or length of a packet queue. The models and the congestion-aware metrics can be integrated with future extensions to assess the efficiency of the routing mechanisms and network performance in different traffic situations.

5.2 Mobility Model Selection

In this work, the Random Waypoint (RWP) mobility model has been employed to evaluate the proposed FCKOA-TA-AROA framework under high dynamic and topology-independent vehicular movement conditions. Although RWP does not explicitly model road constraints, traffic signals, or vehicular regulations, it is widely adopted in VANET and MANET researches for analyzing the fundamental behavior of routing, clustering, and trust mechanisms under frequent topology changes and unpredictable node mobility. The primary objective of this work is to assess robustness, adaptability, and energy efficiency of the proposed optimization-based routing framework rather than to model city-specific traffic dynamics. Moreover, the use of RWP enables a controlled and reproducible evaluation environment that facilitates fair comparison with the existing optimization- and trust-based VANET routing schemes reported in the literature where many of which adopt similar synthetic mobility settings. To ensure transparency, this limitation has been explicitly acknowledged, and as the future work, the proposed framework can be extended to realistic road-aware mobility models and traffic simulators to further validate its applicability in real-world vehicular environments.

6 Conclusion

An integrated energy-efficient and secure clustering and routing framework, FCKOA-TA-AROA, has been presented for vehicular ad hoc networks. By combining OFCM-based clustering, MKOA-driven cluster head selection, and TA-AROA-based trust-aware routing, the proposed approach effectively enhances energy efficiency, network stability, and security in highly dynamic VANET environments. The inclusion of lightweight homomorphic encryption further ensures the confidentiality and integrity of trust information, during data transmission. Comprehensive simulation results confirm that the proposed framework consistently outperforms the existing benchmark methods across key performance metrics. Compared to GBTR, BROA, ABBSOA-AGEOA, and FOA-EECPCR, the proposed algorithm improves PDR by 15.33%, 11.43%, 7.69%, and 3.82%, respectively, during the performance evaluation based on the network size (number of vehicles). Furthermore, a large-scale analysis with 500 nodes has confirmed the superior performance of the proposed model compared to the baseline algorithms. At the outset, the FCKOA-TA-AROA framework offers a robust, energy-efficient, and secure solution for VANETs, and it ensures reliable V2X communication while enhancing network stability as well as resilience to security threats.

7 Future Scope

Although the main emphasis of the proposed method is on the algorithmic structure and performance dimensions of secure clustering and routing, it is acknowledged that the ethical, regulatory, and deployment factors are equally crucial for the successful implementation of VANET-based ITS. Ensuring adherence to data privacy regulations, such as the GDPR and CCPA, can be achieved by incorporating privacy-preserving techniques, such as anonymization, pseudonymization, and homomorphic encryption, with sensitive vehicular information. From a regulatory standpoint, standards such as IEEE 1609 (WAVE), ETSI ITS-G5, and the evolving 5G/6G V2X guidelines offer directives for authentication, message integrity, and spectrum utilization and with which, the TA-ARO framework can be modified to comply with. Ethical issues involve balancing security and user privacy and they prevent unauthorized monitoring as well as maintaining transparency in trust management. Deployment in real-world scenarios also necessitates addressing the interoperability with current infrastructure, scalability under high-density traffic conditions, and adherence to national transportation safety regulations. Consequently, future research may focus on assessing TA-ARO within these regulatory frameworks, integrating privacy-by-design principles, and addressing practical deployment issues to ensure technological effectiveness and societal acceptance. Although MATLAB provides a flexible environment for evaluating clustering, routing, and optimization algorithms, it does not fully capture realistic vehicular traffic dynamics. In addition, the Random Waypoint mobility model may not accurately represent real-world road constraints, traffic signals, and lane-changing behaviors. Future work may validate the proposed framework using integrated vehicular network simulators such as NS-3, Veins, and SUMO under realistic urban traffic scenarios.

Author Contribution The first author should be that person who contributed most to the work, including writing of the manuscript. The sequence of authors should be determined by the relative overall contributions to the manuscript.

Funding This research has received no external funding.

Data Availability No datasets were generated or analysed during the current study.

Declarations The authors declare that this manuscript is original, has not been published previously, and is not under considered for publication elsewhere.

Competing Interests The authors declare no competing interests.

References

Alam I, Manjul M, Pathak V, Mala V, Mangal A, Thakur HK, Sharma DK (2024) Efficient and secure graph-based trust-enabled routing in vehicular ad-hoc networks. Mob Netw Appl. https://doi.org/10.1007/s11036-023-02274-9

Ali W, Din IU, Almogren A, Rodrigues JJ (2024b) Federated learning-based privacy-aware location prediction model for internet of vehicular things. IEEE Trans Veh Technol. https://doi.org/10.1109/tvt.2024.3368439

Ali A, Assam M, Alajmi M, Ghadi YY, Indira S, Akhmediyarova A, Alkahtani HK (2024a) Arithmetic optimization based secure intelligent clustering algorithm for vehicular adhoc network. PLoS ONE 19(9):e0309920

AlMarshoud M, SabirKiraz M, Al-Bayatti AH (2024) Security, privacy, and decentralized trust management in VANETs: a review of current research and future directions. ACM Comput Surv 56(10):1–39

Al-Mekhlafi ZG, Al-Shareeda MA, Mohammed BA, Alayba AM, Saleh AMS, Al-Reshidi HA, Almekhlafi K (2024) Integrating safety in VANETs: a taxonomy and systematic review of VEINS models. IEEE Access. https://doi.org/10.1109/access.2024.3476512

Alotaibi Y, Rajasekar B, Jayalakshmi R, Rajendran S (2024) Falcon optimization algorithm-based energy efficient communication protocol for cluster-based vehicular networks. Comput Mater Contin. https://doi.org/10.32604/cmc.2024.047608

Alsalem AO. (2024). Secure authentication and privacy-preserving techniques in vehicular AD-HOC networks (Doctoral dissertation, Purdue University Graduate School)

Anjali T, Goyal R, Balaji GN. (2024). Prevention of attacks in vehicular adhoc networks. In 2024 IEEE international students' conference on electrical, electronics and computer science (SCEECS) (pp. 1–8). IEEE.

Babu D, Rao TS (2024) A secure routing protocol using trust-based clustering and bionic intelligence algorithm for UAV-assisted vehicular ad hoc networks. Trans Emerg Telecommun Technol 35(5):e4977

Barve A, Patheja PS. (2024). A Clustering approach for attack detection and data transmission in vehicular ad-hoc networks. Adhoc& Sensor Wirel Networks, 58.

Choksi A, Shah M (2024) Machine learning based centralized dynamic clustering algorithm for energy efficient routing in vehicular ad hoc networks. Trans Emerg Telecommun Technol 35(1):e4914

Darney PE, Vallileka N, Manoj S, Fernando AV, Krishnan RS, Prasath SR. (2024). Hybrid Fault Prediction and Recovery Framework for VANETs using AI and Federated IoT. In 2024 International Conference on Inventive Computation Technologies (ICICT) (pp. 1854–1860). IEEE.

El-Gayar MM, Alrslani FA, El-Sappagh S (2024) Smart collaborative intrusion detection system for securing vehicular networks using ensemble machine learning model. Information 15(10):583

Hussein NH, Koh JS, Yaw CT, Tiong SK, Benedict F, Yusaf T, Kadirgama K, Hong TC (2024) SDN-based VANET routing: A comprehensive survey on architectures, protocols, analysis, and future challenges. IEEE Access. 17(13):126801–126861

Jia J, Kumarasamy SS, Pokkuluri KS, Kumar KS, Priyanka TP, Wang F (2024) A robust authentication and trust detection with privacy preservation of data for fog computing in VANET using adaptive deep neural network. IEEE Access. https://doi.org/10.1109/access.2024.3486811

Kadam MV, Vaze VM, Todmal SR (2023) TACR: Trust aware clustering-based routing for secure and reliable VANET communications. Wireless Pers Commun 132(1):305–328

KARNE, R. K., & SREEJA, T. (2024). Efficient Cluster-Based Routing Protocol for VANET Traffic Forecasting with Hybrid Optimization Algorithm. J Inf Sci Eng. 40(6).

Kaur G, Kakkar D (2025) A secure lightweight authentication model with interference aware routing and attack detection approach in VANET. Clust Comput 28(2):109

Kn A, Nagaraj R (2025) Secure vehicle-to-vehicle communication using routing protocol based on trust authentication secure sugeno fuzzy inference system scheme. Recent Patents on Engineering 19(1):E230224227390

Krishnan R, Kalimuthu VK, Jeyaseelan WRS, Venkatachalam B (2024) QoS based adaptive multi-constrained energy efficient routing for vehicular ad hoc networks. Tehničkivjesnik 31(5):1570–1575

Liu J, Zhao H, Han P, Gui G, Ohtsuki T, Sari H, Adachi F (2024) An ensemble learning-based fault detection method for vehicular ad hoc networks in intelligent transportation systems. IEEE Trans Veh Technol. https://doi.org/10.1109/tvt.2024.3502698

Magdalin IP, Kumarasabapathy N (2024) Optimized DBSCAN with RLA-ODV routing and encryption based on homomartino algorithm for energy efficient and secure V2X communication. Opt Quant Electron 56(11):1785

Memon I, Shaikh RA, Shaikh H (2024) Dynamic pseudonyms trust-based model to protect attack scenario for internet of vehicle ad-hoc networks. Multime Tools Appl 83(5):13395–13426

Mohammed BA, Al-Shareeda MA, Alsadhan AA, Al-Mekhlafi ZG, Sallam AA, Al-Qatab BA, Alayba AM (2024) Service based VEINS framework for vehicular ad-hoc network (VANET): a systematic review of state-of-the-art. Peer-to-Peer Netw Appl. https://doi.org/10.1007/s12083-024-01692-0

Putta NR, Kumar YR, Nirupama P et al (2026) An efficient hybrid adaptive network-based node authentication and optimal routing mechanism for enhancing security in VANET environment. Iran J SciTechnol Trans ElectrEng. https://doi.org/10.1007/s40998-026-01050-1

Qi J, Zheng N, Xu M, Chen P, Li W (2024) A hybrid-trust-based emergency message dissemination model for vehicular ad hoc networks. J Inf Secur Appl 81:103699

Rajakumar R, Suresh T, Sekar K. (2024). analyzing the efficacy of clustering-based routing protocols in vehicular Ad Hoc networks: a performance evaluation. In Congress on Control, Robotics, and Mechatronics (pp. 257–269). Singapore: Springer Nature Singapore.

Saemi B, Halataei F, Ahmadi R, Ashkaran A, Mirkamali S, Hosseinabadi AAR (2024) Improving the quality of real-time data transmission service in VANETS by balancing the load on road side units. Clust Comput. https://doi.org/10.1007/s10586-024-04317-6

Saoud B, Shayea I, Yahya AE, Shamsan ZA, Alhammadi A, Alawad MA, Alkhrijah Y (2024) Artificial intelligence, internet of things and 6G methodologies in the context of vehicular ad-hoc networks (VANETs): survey. ICT Express. https://doi.org/10.1016/j.icte.2024.05.008

Setia H, Chhabra A, Singh SK, Kumar S, Sharma S, Arya V, Wu J (2024) Securing the road ahead: machine learning-driven DDoS attack detection in VANET cloud environments. Cyber Secur Appl 2:100037

Swamynathan C, Shanmugam R, Mohan Kumar KP, Subbiyan B (2024) Traffic Prevention and Security Enhancement in VANET Using Deep Learning With Trusted Routing Aided Blockchain Technology. Trans Emerg Telecommun Technol 35(11):e70004

Ul Hassan M, Al-Awady AA, Ali A, Sifatullah Akram M, Iqbal MM, Abdelrahman Ali YA (2024) ANN-based intelligent secure routing protocol in vehicular ad hoc networks (VANETs) using enhanced aodv. Sensors 24(3):818

Umale BR, More NN (2024) Energy efficient routing and secured data transmission in the IoV: improved deep learning model for energy prediction. Multimed Tools Appl. https://doi.org/10.1007/s11042-024-18172-5

Vaissnave V, Baskaran G, Mana SC et al (2026) Enhancing iot network security through an advanced deep learning-powered threat detection system. Iran J SciTechnol Trans ElectrEng. https://doi.org/10.1007/s40998-026-01043-0

Wang Y, Gao H, Xiang Z, Al-Dulaimi A (2024a) Reliable routing for V2X networks: a joint perspective of trust-prediction and attack-resistance. IEEE Internet Things J. https://doi.org/10.1109/jiot.2024.3468472

Wang Z, Wang J, Liu Y, Yang X, Qi F, Song W (2024b) Privacy-preserving attribute-based access control scheme with intrusion detection and policy hiding for data sharing in VANET. IEEE Internet Things J. https://doi.org/10.1109/jiot.2024.3384753

Wang L, Hao H, Wang C, Han X (2024c) VANETs group message secure forwarding with trust evaluation. Digital Communications and Networks. https://doi.org/10.1016/j.dcan.2024.11.007

Yousefi D, Farhad F, Abed M, Gavidel S. (2024). Presenting a new approach in security in inter-vehicle networks (VANET). arXiv preprint arXiv:2411.19002.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.