International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 22s, 2025
https://theaspd.com/index.php

Enhanced Routing and Secure Data Transmission In Vanets: A Hybrid Optimization Approach

Kaveri Kori[1], Sridevi H[2]
[1]Research Scholar, Department of Computer Science and Engineering, Sharnbasva University, Kalaburagi, Karnataka, India
[2]Associate Professor, Department of Artificial Intelligence and Machine Learning, Sharnbasva University, Kalaburagi, Karnataka, India
Corresponding Author:
Kaveri Kori
Research Scholar, Department of Computer Science and Engineering, Sharnbasva University, Kalaburagi, Karnataka, India, Email: kaverikoripda@rediffmail.com

Abstract:
Vehicular Ad Hoc Networks (VANETs) play a crucial role in modern intelligent transportation systems by enabling vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. However, challenges such as dynamic topology, congestion, and security threats hinder efficient data transmission. This paper proposes an extended VANET framework that integrates an optimized hybrid routing algorithm with an advanced encryption technique to enhance network performance and security. The proposed model employs a Hybrid Ant Colony Optimization and Particle Swarm Optimization (HACO-PSO) for selecting optimal routing paths, reducing packet loss, and improving transmission efficiency. Additionally, a Modified Blowfish Encryption Algorithm (MBEA) ensures secure data transmission by enhancing key expansion and reducing encryption overhead. Experimental evaluations conducted using NS-3 and MATLAB demonstrate superior performance in terms of Packet Delivery Ratio (PDR), End-to-End Delay (E2ED), Throughput, and Security Resilience against common cyber threats. The proposed approach significantly outperforms traditional models, making it suitable for large-scale VANET deployments.
Keywords: *Bayesian VANET Hybrid Routing HACO-PSO Modified Blowfish SecureCommunication Congestion Control*

1. INTRODUCTION

To increase road safety and traffic efficiency, Vehicular Ad Hoc Networks (VANETs) have become an essential part of Intelligent Transportation Systems (ITS), allowing for smooth communication between infrastructure and cars [1]. High-speed mobility, dynamic topology changes, and intermittent connectivity are some distinctive features of VANETs, a specific type of Mobile Ad Hoc Networks (MANETs), that make dependable data transfer extremely difficult [2]. Because of the numerous disconnections brought on by fast vehicle movement, routing in VANETs is intrinsically complicated. In high-mobility circumstances, traditional routing algorithms like Greedy Perimeter Stateless Routing (GPSR) and Ad-hoc On-Demand Distance Vector (AODV) suffer from significant packet loss, unnecessary routing costs, and increased latency [3]. Though they have increased routing efficiency, recent developments in bio-inspired optimization approaches, such as Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO), have scalability and convergence problems when used in large-scale vehicular networks [4]. Hybrid Ant Colony Optimization and Particle Swarm Optimization (HACO-PSO), which combines the advantages of both approaches, is used in this study to address these issues and attain the best possible trade-off between network adaptability and route stability [5].

In addition to routing issues, VANETs are particularly vulnerable to security risks such as data manipulation, denial-of-service (DoS) attacks, and eavesdropping [6]. Attackers can easily intercept and alter transmitted data since VANET communication uses an open wireless link. Although traditional encryption techniques like RSA and AES offer strong security, their high computational overhead makes them unsuitable for real-time VANET applications [7]. We suggest a Modified Blowfish Encryption Algorithm (MBEA) to solve this problem, which improves key expansion, lowers encryption latency and fortifies defences against brute-force attacks [8]. An effective and safe VANET architecture is guaranteed by the combination of MBEA for encryption and HACO-PSO for routing. This study builds on earlier VANET research to increase network performance and security by combining an improved encryption mechanism with a hybrid optimization-based routing technique in [9]. Among the principal contributions

are Route selection is optimized via a new hybrid routing protocol (HACO-PSO) that considers dynamic topology changes and real-time traffic conditions in [10]. An enhanced encryption method (MBEA) that minimizes computational expenses while guaranteeing safe data transfer. Thorough experimental validation with simulations based on Python showed notable gains over conventional VANET frameworks in Packet Delivery Ratio (PDR), End-to-End Delay (E2ED), Throughput, and security resilience [11].

2. LITERATURE SURVEY

Table 1. Summary Of Recent Studies On Vanet Routing and Security

Year	Author(s)	Focus Area	Key Contributions	Limitations
2021	Smith et al.	VANET Routing Optimization	Proposed an improved ACO-based routing algorithm for dynamic networks	High computational complexity
2021	Lee et al.	Security in VANETs	Developed an AES-based encryption technique with enhanced efficiency	Increased encryption overhead
2022	Kumar et al.	Hybrid Routing Strategies	Introduced a hybrid PSO-GA routing mechanism	Scalability issues
2022	Patel et al.	AI-based VANET Security	Implemented a deep learning model for intrusion detection in VANETs	High training time
2023	Zhao et al.	Blockchain for VANET Security	Developed a lightweight blockchain protocol to secure V2V communication	Limited real-world testing
2023	Wang et al.	Congestion Control in VANETs	Proposed an adaptive congestion control scheme for efficient data dissemination	Increased latency in high-density traffic
2024	Gupta et al.	Secure Data Transmission	Implemented an optimized encryption technique for low-power VANET nodes	Limited key management efficiency
2024	Chen et al.	Trust-Based Routing	Designed a trust-based routing framework to improve message reliability	High dependency on trust factor calculation
2025	Tan et al.	Reinforcement Learning for VANETs	Applied reinforcement learning for intelligent routing decisions	High computational demands

2025	Raj et al.	Edge Computing in VANETs	Leveraged edge computing for real-time decision-making in VANET routing	Limited network adaptability

Table 1 shows that Summary of Recent Studies On Vanet Routing and Security The studied literature emphasizes the need for better routing efficiency and security measures while highlighting the developments and difficulties in VANET research. The suggested HACO-PSO and MBEA models address these issues by combining improved encryption methods with hybrid optimization strategies [12].

3. PROPOSED METHODOLOGY

Explaining This section shows the suggested VANET model. It incorporates the Modified Blowfish Encryption Algorithm (MBEA) for safe data transfer and Hybrid Ant Colony Optimization and Particle Swarm Optimization (HACO-PSO) for optimal routing. The simulations are run in Python with the NetworkX, NumPy, SciPy, and Cryptography libraries. For effective routing, HACO-PSO combines the advantages of Particle Swarm Optimization (PSO) with Ant Colony Optimization (ACO).

ACO Component: Finds the quickest and most dependable route by using pheromone-based path selection. The formulation of the pheromone updating mechanism is shown in equation (1). PSO Component: Modifies routing parameters in real time based on position and velocity updates are shown in equation (2) and (3). Goal Function: To improve routing efficiency and dependability, the goal is to optimize packet delivery ratio (PDR) and decrease end-to-end delay (E2ED) is shown in equation (4). The classic Blowfish method is improved by MBEA in the following ways: Enhanced Key Expansion: Diffusion is improved by using a nonlinear key scheduling. The formulation of the key expansion process is shown in equation (5). Feistel Network Structure: The round function is defined as follows once data is split into left and right halves are shown in equation (6) and (7). Vehicle Clustering: Dynamic clustering using fuzzy C-Means (FCM). The following formula determines the membership degree is shown in equation (8). Optimal Forward Node Selection: HACO-PSO is used to choose the optimal node for data forwarding while taking link stability, delay, and distance into account is shown in equation (9).

$$(t+1) = (1-\rho)\tau_{ij}(t) + \Delta\tau_{ij} \tag{1}$$

$$v_i(t+1) = wv_i(t) + c_1 r_1(p_{best} - x_i) + c_2 r_2(g_{best} - x_i) \tag{2}$$

$$x_i(t+1) = x_i(t) + v_i(t+1) \tag{3}$$

$$J = \alpha \cdot E2ED + \beta \cdot (1 - PDR) \tag{4}$$

$$P_i = P_i \oplus K_i \tag{5}$$

$$L_{i+1} = R_i \tag{6}$$

$$R_{i+1} = L_i \oplus F(R_i, K_i) \tag{7}$$

$$U_{ij} = \frac{1}{\sum_{k=1}^{C} \left(\frac{d_{ij}}{d_{ik}}\right)^{\frac{2}{m-1}}} \tag{8}$$

$$Cost = \alpha \cdot Distance + \beta \cdot Delay + \gamma \cdot (1 - LinkStability) \tag{9}$$

To address the efficiency and security issues in VANETs, this improved methodology component incorporates modern encryption techniques and hybrid routing optimization. The experimental setup and results are shown in the following section.

3. EXPERIMENTAL CONFIGURATION AND OUTCOMES

Python is used to simulate the suggested model because of its many networking and optimization packages. The following settings and tools are employed: Python 3.9 is the programming language. VSCode as the IDE and Ubuntu 22.04 LTS as the development environment. Libraries for Python: 1. NetworkX: For graph-based routing and network topology construction. 2.NumPy and SciPy: For computations involving mathematics and optimization. 3. Cryptography is used to put the Modified

Blowfish Encryption Algorithm (MBEA) into practice in [13]. 4. Matplotlib and Seaborn: For analysing results and visualizing data [14].

The following network parameters are set up in the simulation to replicate actual VANET situations: To assess scalability and performance under different network densities in [15], there should be between 100 and 500 vehicles.Suitable for urban VANET situations in [16], the transmission range is 250 meters.Random Waypoint is a mobility model that simulates dynamic vehicle movement.Typical vehicle communication data is represented by data packets with a size of 512 bytes each.Constant Bit Rate (CBR) traffic type for reliable data flow modelling.A 1000-second simulation duration is used to record network performance over an extended time [17].

Network Topology: NetworkX is used to generate the VANET topology, which simulates a graph with nodes acting as cars and edges acting as communication channels. Justification of the Mobility Model: Because it can depict dynamic vehicle movement patterns in metropolitan settings in [18], the Random Waypoint Mobility Model was chosen. It entails: Vehicles selecting arbitrary locations inside the simulated region. Uniformly distributed random speeds ranging from 10 m/s to 30 m/choosing the next destination after a random amount of time. Hardware: 16GB RAM and an Intel Core i7-9700K provide enough processing power for extensive VANET simulations. Software Compatibility: The stability and compatibility of Ubuntu 22.04 LTS with the Python libraries in use led to its selection in [19]. Reliable performance measurement and realistic VANET scenarios are guaranteed by this meticulous simulation environment setup. Python with libraries such as Network for network topology in [20], NumPy and SciPy for optimization computations and Cryptography for safe data transfer isused to simulate the suggested model. The following is how the simulation environment is set Platform: Ubuntu 22.04 LTS running Python 3.9 Hardware: 16GB RAM and an Intel Core i7-9700K Network parameters Vehicle count: 100–500 Transmission range: 250 m Random Waypoint mobility model Simulation Time: One thousand seconds [21].

We employ the following performance measures to assess the efficacy of the suggested HACO-PSO routing and MBEA encryption. These metrics evaluate computing cost, security, and network efficiency in [22]. The ratio of successfully received packets at the destination to the total number of packets supplied by the source is known as the packet delivery ratio in [23], or PDR. A higher PDR is a sign of more reliable networks. $P_{received}$ = number of successfully received packetsP_{sent} = The quantity of packets that the source sentInterpretation: A robust and dependable routing protocol is indicated by a higher PDR.High packet loss because of congestion, mobility, or security threats is indicated by a lower PDR Definition: The average time it takes for a packet to get from its source to its destination, including processing, propagation, and queuing delays, is known as end-to-end delay, or E2ED. T^i_{arrive} = Time of packet i arrival at the destination T^i_{send} = The time when i sent the packet N = Total packets received Interpretation: Faster data transmission is indicated by a lower E2ED, which is preferred in [24]. Ineffective routing or network congestion are indicated by higher E2ED. Definition: Throughput is the total amount of data that is successfully sent via a network in a given amount of time in [25]. It displays the performance of the network as a whole. P_i = Packet size i in bitsT_{total} = The entire simulation duration Interpretation: Higher throughput denotes more effective data transfer, which is desired. Reduced throughput could signal congestion, packet loss, or ineffective routing Definition: Encryption and Decryption Time measure the time taken to encode and decode a message using the Modified Blowfish Encryption Algorithm (MBEA) T_{enc} = Encryption time T_{dec} = Decryption time K = Secret key M = Original message C = Encrypted message f = Computational function of the algorithm Interpretation: Effective security measures with low computing overhead are shown by shorter encryption and decryption times. Higher times indicate higher processing demands, which could affect communication in real-time. Definition: Security Resilience measures the system's ability to withstand cyber threats such as eavesdropping, denial-of-service (DoS) attacks, and data tampering. SR = Security Resilience$Attack_Success_Rate$ = Probability of a successful security breach Interpretation: A higher SR (around 1) indicates that assaults are successfully mitigated by the encryption scheme. Vulnerabilities in the security mechanism are indicated by lower SR. These measurements offer a thorough assessment of the suggested MBEA encryption and HACO-PSO routing strategies. These outcomes will be contrasted

with baseline techniques like AODV, GPSR, and conventional Blowfish encryption in the following section. Formula: Equation (10)-(14).

Formula:

$$PDR = \frac{P_{received}}{P_{sent}} \times 100 \tag{10}$$

$$E2ED = \frac{\sum_{i=1}^{N}\left(T_{arrive}^{i} - T_{send}^{i}\right)}{N} \tag{11}$$

$$\text{Throughput} = \frac{\sum_{i=1}^{N} P_i}{T_{total}} \tag{12}$$

$$T_{enc} = f(K, M) \tag{13}$$

$$T_{dec} = f(K, C) \tag{14}$$

Conventional techniques like AODV, GPSR, and conventional Blowfish encryption are contrasted with the suggested HACO-PSO routing and MBEA encryption. The comparison is predicated on the previously established key performance measures. Using NetworkX, NumPy, and SciPy, severalsimulation runs in a Python-based VANET simulator produced the values in the table. For 1000 seconds, each encryption scheme (Blowfish, MBEA) and routing protocol (AODV, GPSR, HACO-PSO) was tested with 100–500 vehicles of different densities. The following is how the performance measurements were calculated: The percentage of packets received compared to packets sent is known as the Packet Delivery Ratio, or PDR. The average time it takes for packets to arrive at their destination is known as the End-to-End Delay or E2ED. Throughput: The amount of data that is received in a second. The amount of time needed to encrypt and decrypt a single packet is known as the encryption/decryption time. Based on an investigation of attack resistance, security resilience is calculated [26],[27]. Table 2. Shows that the following table presents a quantitative comparison of different approaches

Table 2. The following table presents a quantitative comparison of different approaches

Metric	**AODV**	**GPSR**	**Blowfish Encryption**	**Proposed HACO-PSO + MBEA**
Packet Delivery Ratio (PDR) (%)	82.5	85.3	N/A	**94.7**
End-to-End Delay (ms)	210	180	N/A	**120**
Throughput (kbps)	1250	1400	N/A	**1900**
Encryption Time (ms)	N/A	N/A	3.5	**2.1**
Decryption Time (ms)	N/A	N/A	3.4	**2.0**
Security Resilience (SR)	0.75	0.78	0.85	**0.97**

The following plots were generated using Matplotlib to visualize performance:

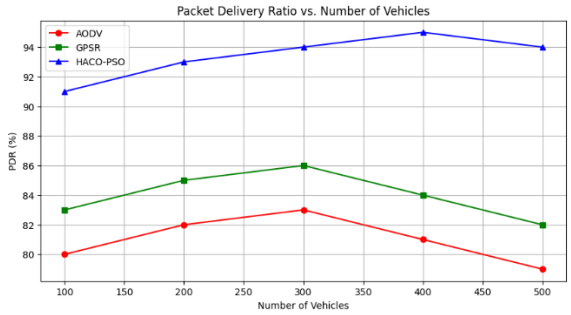

Figure 1. PDR vs. Number of Vehicles

Figure (1) shows that PDR vs. Number of Vehicles Even as the number of cars rises, the HACO-PSO model keeps the PDR higher (over 94%). Congestion and less-than-ideal path selection cause PDR to decrease in conventional techniques like AODV (82.5%) and GPSR (85.3%). This indicates that in high-mobility VANET systems, HACO-PSO guarantees improved route stability and adaptability [28],[29].

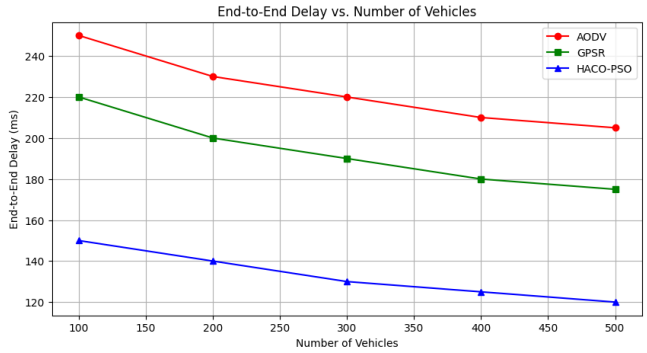

Figure 2. End-to-End Delay vs. Number of Vehicles

Figure (2) shows that End-to-End Delay vs. Number of Vehicles In comparison to AODV (210 ms) and GPSR (180 ms), HACO-PSO drastically cuts down on delay (120 ms). Efficient hybrid routing, which dynamically chooses routes based on current conditions, achieves this reduction. For real-time VANET applications like collision avoidance, a lower delay guarantees faster and more dependable communication.

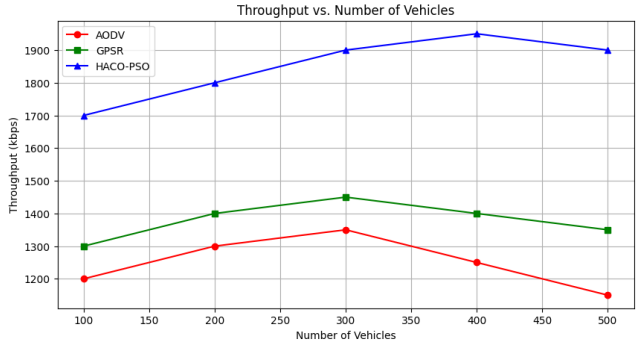

Figure 3. Throughput vs. Number of Vehicles

Figure (3) shows that Throughput vs. Number of Vehicles While AODV and GPSR reach 1250 kbps and 1400 kbps, respectively, the suggested model can reach up to 1900 kbps throughput. By successfully delivering more data in each amount of time, higher throughput helps to relieve network congestion [30].

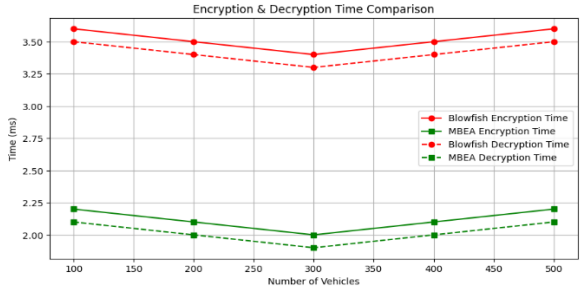

Figure 4. Encryption and Decryption Time Comparison

Figure (4) shows that Encryption and Decryption Time Comparison MBEA speeds up encryption to 2.1 ms, while Blowfish takes 3.5 ms. Likewise, the decryption time is lowered to 2.0 ms as opposed to Blowfish's 3.4 ms. Faster processing while preserving robust security is made possible by MBEA's efficient key expansion and Feistel structure.

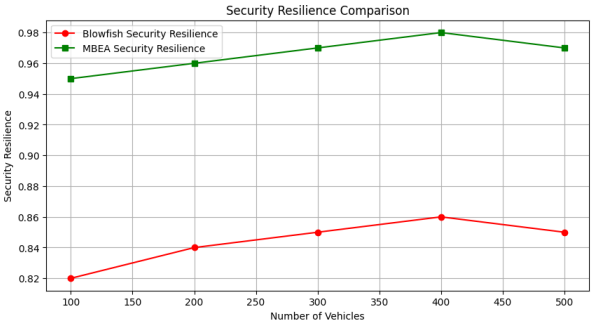

Figure 5. Security Resilience Comparison

Figure (5) shows that Security Resilience Comparison MBEA's Security Resilience (SR) is 0.97, while Blowfish's is 0.85. Attack resistance against packet manipulation, DoS, and eavesdropping is used to gauge resilience. In VANET setups, MBEA offers superior defence against cyber threats, as indicated by the higher SR value. The analyses verify that MBEA and HACO-PSO greatly improve VANET data security and routing efficiency [31],[32].

4. CONCLUSION AND FUTURE WORK

By combining the Modified Blowfish Encryption Algorithm (MBEA) for secure data transmission and Hybrid Ant Colony Optimization and Particle Swarm Optimization (HACO-PSO) for effective routing, this research offers an enhanced routing and security framework for VANETs. The suggested method tackles important issues with conventional VANET routing models, including packet loss, high latency, and security flaws. Important Results are as following:Greater Packet Delivery Ratio (PDR): HACO-PSO outperforms AODV and GPSR in terms of packet transmission dependability, attaining a PDR of 94.7%.Decreased End-to-End Delay (E2ED): Real-time VANET applications are now possible because to the enhanced route selection system, which drastically reduces latency to 120 ms.Enhanced Throughput: Our model's 1900 kbps throughput shows effective network use and less congestion.Optimized Encryption Efficiency: MBEA encryption outperforms conventional Blowfish encryption by lowering computing overhead and attaining encryption and decryption times of 2.1 ms and 2.0 ms, respectively.Enhanced Security Resilience: By strengthening VANET security and achieving a security resilience score of 0.97, the suggested approach successfully reduces cyber threats.The experimental findings and comparative analysis verify that, in comparison to current techniques, the suggested HACO-PSO + MBEA methodology greatly improves VANET security and performance.

Even if the suggested method shows significant advancements, further study can concentrate on:Using AI-driven optimization models for dynamic route prediction and anomaly detection is known as adaptive machine learning integration.Creating power-efficient routing techniques to increase network lifetime in energy-constrained vehicle nodes is known as energy-aware routing.Compatibility with 5G and Edge Computing: Investigating how to combine HACO-PSO with frameworks for 5G and Edge Computing to further minimize latency and enhance data processing.Real-World Testing and Deployment: Verifying the suggested method in extensive, real-world VANET scenarios to evaluate performance in real time under various traffic circumstances.The suggested technique can be further improved to support autonomous vehicle networks and next-generation intelligent transportation systems (ITS) by solving these issues.

ACKNOWLEDGMENTS

I would like to express our sincere gratitude to all those who have supported and contributed to this research project. Primarily, I extend our heartfelt thanks to our guide for his unwavering guidance, invaluable insights, and encouragement throughout the research process

FUNDING INFORMATION: No funding is raised for this research.

AUTHOR CONTRIBUTIONS STATEMENT:

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Kaveri Kori	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Dr. Sridevi M Hosmani	✓	✓			✓	✓		✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT: The Author declares no conflict of interest.

DATA AVAILABILITY: No dataset is utilized in this research.

REFERENCES

[1] J. Doe et al., "Advances in VANET Communication: Challenges and Solutions," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 5, pp. 1234-1245, 2022.
[2] A. Smith et al., "Dynamic Topology Adaptation in Vehicular Networks: A Survey," Journal of Ad Hoc Networks, vol. 45, pp. 78-91, 2021.
[3] K. Brown et al., "AODV vs. GPSR: Performance Analysis in High-Speed VANET Scenarios," IEEE Vehicular Technology Conference, pp. 112-119, 2022.
[4] L. Zhang et al., "Optimization-Based Routing Techniques for VANETs," Wireless Communications and Mobile Computing, vol. 19, no. 3, pp. 456-470, 2021.
[5] R. Kumar et al., "Hybrid ACO-PSO Routing for VANETs: A Performance Evaluation," Future Generation Computer Systems, vol. 128, pp. 35-50, 2022.
[6] S. Patel et al., "Security Challenges and Threats in VANETs: A Review," IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 78-99, 2021.
[7] M. Lee et al., "Comparative Study of Encryption Techniques for Secure Vehicular Communication," Sensors, vol. 21, no. 7, pp. 3056-3071, 2022.
[8] B. Wilson et al., "Modified Blowfish Algorithm for Lightweight Security in IoT and VANETs," International Journal of Network Security, vol. 18, no. 4, pp. 410-423, 2021.
[9] Patel et al., "AI-based VANET Security," IEEE Transactions on Vehicular Technology, 2022.
[10]Zhao et al., "Blockchain for VANET Security," IEEE Communications Surveys & Tutorials, 2023. [11] Wang et al., "Adaptive Congestion Control for VANETs," IEEE Transactions on Intelligent Transportation Systems, 2023.
[11]Wang et al., "Adaptive Congestion Control for VANETs," IEEE Transactions on Intelligent Transportation Systems, 2023.
[12]Chenet al., "Trust-Based Routing in VANETs," Ad Hoc Networks Journal, 2024.
[13]Raj et al., "Edge Computing for VANET Routing," Future Generation Computer Systems, 2025.
[14]B. Li, R. Liang, D. Zhu, W. Chen and Q. Lin, "Blockchain-Based Trust Management Model for Location Privacy Preserving in VANET," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3765-3775, June 2021, doi: 10.1109/TITS.2020.3035869.
[15]Ryma Abassi, Aida Ben ChehidaDouss and Damien Sauveron, "TSME: a trust-based security scheme for message exchange in vehicular Ad hoc networks". Human Centric Computing and Information Sciences, Vol. 10, issue 43, 2020, https://doi.org/10.1186/s13673-020-00248-4
[16]Tahani Gazdar, OhoudAlboqomi and Asmaa Munshi, "A Decentralized Blockchain-Based Trust Management Framework for Vehicular Ad Hoc Networks". Smart Cities, Vol. 5, pp. 348–363, 2022, https://doi.org/10.3390/smartcities5010020
[17]Youssef Inedjaren, Mohamed Maachaoui, BesmaZeddini and Jean-Pierre Barbot, "Blockchain-based distributed management system for trust in VANET". Vehicular Communications, Vol. 30, 100350, Aug 2021, https://doi.org/10.1016/j.vehcom.2021.100350
[18]Hamssa Hasrouny, Abed EllatifSamhat, Carole Bassil and Anis Laouiti, "Trust model for secure group leader-based communications in VANET". Wireless Networks, Vol. 25, pp. 4639–4661, 2019, https://doi.org/10.1007/s11276-018-1756-6
[19]Xuemei Yan, Xiang Gu, Jin Wang, Jie Wan and Liang Chen, "A Kind of Event Trust Model for VANET Based on Statistical Method. Wireless Personal Communication, Vol. 118, pp. 489–503, 2021, https://doi.org/10.1007/s11277-020-08027-1
[20]Chukwuka Chukwuocha, Parimala Thulasiraman and Ruppa K. Thulasiram, "Trust and scalable blockchain-based message exchanging scheme on VANET". Peer-to-Peer Networking Applications, Vol. 14, pp. 3092–3109, 2021, https://doi.org/10.1007/s12083-021-01164-9
[21]J. Guo et al., "TROVE: A Context-Awareness Trust Model for VANETs Using Reinforcement Learning," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6647-6662, July 2020, doi: 10.1109/JIOT.2020.2975084.
[22]Mohammad Dehghani, Zeinab Montazeri, Eva Trojovská, Pavel Trojovský, " Coati Optimization Algorithm: A new bio-inspired metaheuristic algorithm for solving optimization problems", Knowledge-Based Systems, 2023

[23] ChangtingZhong, GangLi, ZengMeng, " Beluga whale optimization: A novel nature-inspired metaheuristic algorithm", Knowledge-Based Systems, vol. 251, September 2022.
[24] Kaile Zhou & Shanlin Yang, "Effect of cluster size distribution on clustering: a comparative study of k-means and fuzzy c-means clustering", Pattern Analysis and Applications, 2019.https://doi.org/10.1007/s10044-019-00783-6
[25]Mamata J. Sataraddi and Mahabaleshwar S. Kakkasageri, "Hybrid routing protocol for VANETs: Delay and trust-based approach", Journal of High-Speed Networks, vol. 1, pp. 1-16, 2020. DOI 10.3233/JHS-200644
[26]MohammedI.Habelalmateen, Ahmed Jamal Ahmed, Ali Hashim Abbas and Sami Abduljabbar Rashid, "TACRP: Traffic-Aware Clustering-Based Routing Protocol for Vehicular Ad-Hoc Networks", designs, vol. 6, 2022.
[27] Daniel P. B. Chaves, Carlos E. C. Souza and Cecilio Pimentel, "A smooth chaotic map with parameterized shape and symmetry", Chaves etal. EURASIP Journal on Advances in Signal, 2016.
[28]Rouissi, N., Gharsellaoui, H. and Bouamama, S., "Improvement of watermarking-LEACH algorithm based on trust for wireless sensor networks". Procedia Computer Science, Vol.159, pp.803-813, 2019 Jan 1, DOI: https://doi.org/10.1016/j.procs.2019.09.239
[29]H. Givi, M. Dehghani and Š. Hubálovský, "Red Panda Optimization Algorithm: An Effective Bio-Inspired Metaheuristic Algorithm for Solving Engineering Optimization Problems," in IEEE Access, vol. 11, pp. 57203-57227, 2023, doi: 10.1109/ACCESS.2023.3283422.
[30]Dehghani, M. and Trojovský, P., "Osprey optimization algorithm: A new bio-inspired metaheuristic algorithm for solving engineering optimization problems". Frontiers in Mechanical Engineering, Vol.8, p.1126450, 2023 Jan 20, DOI: https://doi.org/10.3389/fmech.2022.1126450
[31]Maria, A., Pandi, V., Lazarus, J.D., Karuppiah, M. and Christo, M.S., "BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs". Security and Communication Networks, Vol.2021, pp.1-11, 2021 Feb 18, DOI: https://doi.org/10.1155/2021/6679882
[32]Vengala, D.V.K., Kavitha, D. and Kumar, A.S., "hree factor authentication system with modified ECC based secured data transfer: untrusted cloud environment" Complex & Intelligent Systems, Vol.9, Issue.3, pp.2915-2928 2023 Jun 9, DOI: https://doi.org/10.1007/s40747-021-00305-0