A Comprehensive Survey on Vehicular Ad Hoc Networks (VANETs): Architectures, Methodologies, and Performance Analysis

Ranjana Jadhav[1], Khilesh Chaudhari[2], Rajiv Chaurasiya[3], Abhay Chikte[4], Yogiraj Chaukhande[5], Yogesh Bihani[6]

[1,2,3,4,5,6]*Department of Information Technology, Vishwakarma Institute of Technology, Pune, 411037, Maharashtra, India*

Abstract- Vehicular Ad Hoc Networks (VANETs) have emerged as a crucial technology in modern intelligent transportation systems (ITS). These networks facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, enabling applications in road safety, traffic optimization, and infotainment. However, the dynamic nature of VANETs introduces significant challenges in network stability, security, latency, and scalability. This survey provides an in-depth analysis of VANET architectures, key methodologies, emerging technologies, and recent advancements. We discuss cutting-edge approaches such as block-chain integration, AI-driven routing protocols, 5G-enabled architectures, and Software-Defined Networking (SDN)-based frameworks. The paper also highlights security threats and countermeasures, evaluating the effectiveness of trust management models and intrusion detection systems. Finally, we explore future research directions to enhance the performance, reliability, and scalability of VANETs.

Keywords: VANETs, Intelligent Transportation Systems (ITS), Vehicle-to-Vehicle Communication, Vehicle-to-Infrastructure Communication, Block-chain, 5G, Edge Computing, Software-Defined Networking, Cyber-security, Intrusion Detection Systems

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are a specialized form of Mobile Ad Hoc Networks (MANETs) designed to support intelligent transportation systems (ITS). They play a critical role in modern smart cities by facilitating real-time communication between vehicles, roadside infrastructure, and traffic management systems. With the rise of autonomous vehicles and connected car technologies, the importance of VANETs has grown significantly [1].

VANETs provide solutions for intelligent traffic management, accident prevention, and infotainment. However, their deployment comes with significant challenges, including security vulnerabilities, high mobility, frequent topology changes, and latency issues [2]. Various methodologies, including AI-driven routing, block-chain-based authentication, and 5G integration, have been proposed to address these challenges [3]. This paper presents a comprehensive survey of the latest advancements in VANETs, focusing on methodologies, security mechanisms, and emerging technologies.

Objectives:
This survey aims to:
1. Provide a comprehensive review of VANET architectures and communication models.
2. Analyze recent methodologies and emerging trends in VANET research.
3. Evaluate security mechanisms and intrusion detection techniques.
4. Discuss real-world applications and challenges in implementing VANETs.
5. Identify open research issues and future directions.

2. VANET ARCHITECTURES AND COMMUNICATION MODELS

2.1 Components of VANETs

VANETs consist of the following fundamental components:

- On-Board Units (OBUs): Communication devices installed in vehicles for exchanging data with other vehicles and infrastructure.
- Roadside Units (RSUs): Fixed communication nodes deployed along roadways to provide V2I connectivity.
- Application Units (AUs): Devices responsible for processing vehicular data and enabling user applications [4].

2.2 Communication Models in VANETs

VANET communication models include:

- Vehicle-to-Vehicle (V2V): Direct communication between vehicles without infrastructure support. Used for safety alerts and cooperative driving.
- Vehicle-to-Infrastructure (V2I): Communication between vehicles and RSUs, enabling centralized traffic control and internet access.
- Vehicle-to-Everything (V2X): An extension of V2V and V2I, incorporating communication with pedestrians, smart city sensors, and cloud networks [5].

3. LITERATURE REVIEW

Block-chain technology has emerged as a promising solution to enhance security and trust in Vehicular Ad-hoc Networks (VANETs). Traditional VANET architectures often rely on centralized authorities, which introduce vulnerabilities such as single points of failure and potential data breaches. The integration of block-chain in VANETs enables a decentralized framework that enhances security, trust, and data integrity. Various authentication techniques, including certificate-less authentication using elliptic curve cryptography and hierarchical block-chain-based authentication, have been proposed to mitigate security threats. Block-chain's fault tolerance ensures data consistency and prevents unauthorized tampering, making it an effective solution for vehicular communication networks. Additionally, the use of fog computing reduces latency, improving the efficiency of message dissemination among vehicles. Despite its advantages, block-chain-based VANETs face scalability challenges in high-density traffic environments, and processing delays due to complex block-chain operations can impact real-time decision-making.[3]

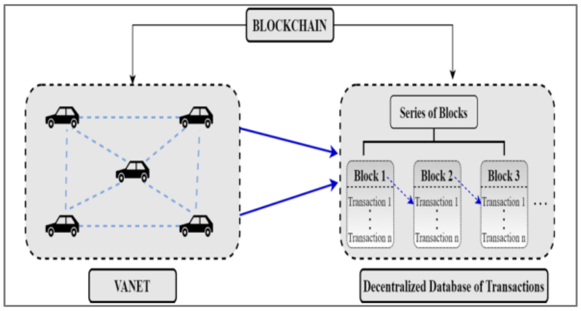

Figure 1: Blockchain based VANET architecture

The emergence of 5G technology has significantly improved VANET communication, offering ultra-low latency and high-speed data transfer capabilities. The integration of 5G into VANETs enhances both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, allowing seamless connectivity and real-time data exchange. However, security remains a major concern due to the openness and dynamic nature of vehicular networks. To address these challenges, a trust-based mutual authentication system combined with a Global Reputation Center (GRC) has been proposed. This framework evaluates the reputation of vehicular nodes based on their past behaviors, ensuring that only trusted entities participate in communication. The system effectively prevents security threats such as Sybil attacks, message spoofing, and unauthorized access. Furthermore, the 5G-enabled VANET paradigm enhances data confidentiality and location privacy, making it a more robust and scalable solution for intelligent transportation systems. Despite these advantages, the approach is computationally expensive, and large-scale deployments may introduce congestion and network instability.[5]

Ensuring trust and reliability in VANETs is crucial for secure communication and efficient traffic management. A multi-tier accreditation-based security framework has been introduced to enhance trustworthiness in vehicular networks. The proposed framework assigns trust ratings to vehicles based on multiple parameters, including processing time, packet loss rate, and prior behavior. Vehicles with higher trust ratings are prioritized for communication, while suspicious or potentially malicious vehicles are closely monitored. This approach effectively mitigates network disruptions caused by rogue vehicles and reduces the risk of malicious attacks such as data injection and denial-of-service (DoS) attacks. Additionally, the accreditation mechanism employs real-time monitoring and adaptive security policies to dynamically update trust scores, ensuring that VANETs remain resilient against evolving threats. The results demonstrate improved data packet transmission rates and reduced source-to-destination latency. However, the system's reliance on historical behavioral data raises concerns about trust manipulation and the need for continuous updates to prevent exploitation.[15]

The increasing complexity of VANETs has led to heightened concerns regarding cybersecurity, particularly in detecting and mitigating intrusion attempts. A machine learning-based approach utilizing a Random Forest classifier has been proposed to enhance network security. The system is designed to detect Distributed Denial-of-Service (DDoS) attacks and other anomalies by analyzing network traffic patterns in real-time. The Random Forest-based Network Intrusion Detection System (NIDS) improves classification accuracy and reduces false alarm rates compared to traditional intrusion detection methods. The two primary components of the system include a traffic gathering module and an attack detection module, which work together to identify and mitigate security threats effectively. This approach ensures the early detection of malicious activities, preventing potential disruptions in vehicular networks. While the model exhibits high accuracy and low false-positive rates, it requires extensive datasets for training and imposes computational overhead, which may impact its feasibility in real-time applications. These advancements in block-chain security, 5G-enabled trust management, multi-tier accreditation, and AI-driven intrusion detection collectively contribute to enhancing the security and reliability of VANETs. However, challenges such as computational overhead, scalability, and dynamic trust evaluation need to be addressed to enable widespread adoption and seamless integration into intelligent transportation systems.[11]

This paper introduces the SSMC-VANETs protocol, designed to enhance communication in VANETs by using a multi-hop clustering approach. The study evaluates performance through simulations in NS2 with SUMO-generated mobility data. The results indicate that SSMC-VANETs outperform MDEC-VANETs and COIM-VANETs in terms of energy efficiency, packet delivery ratio, end-to-end delay, and routing overhead, making it a more effective solution for managing vehicle-to-vehicle communication in high-speed environments.[2]

This research introduces the D-LAR protocol, which enhances energy efficiency and security in VANETs. The sleep scheduling algorithm helps in managing node activity states, reducing energy consumption and communication overhead. Simulation results show reduced collision attack detection delay and enhanced routing security, making D-LAR a suitable choice for secure and energy-efficient vehicular communication.[8]

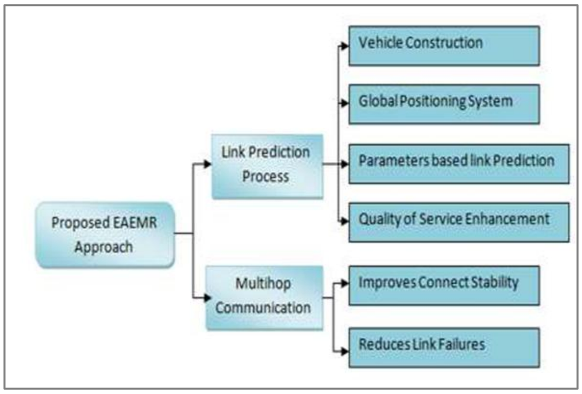
Proposed EAEMR Approach
Link Prediction Process
Multihop Communication
Vehicle Construction
Global Positioning System
Parameters based link Prediction
Quality of Service Enhancement
Improves Connect Stability
Reduces Link Failures

Figure 2: EAEMR Architecture

The EAEMR (Energy Aware Effective Multi-Hop Routing) model focuses on improving packet delivery ratio, energy efficiency, and reducing delay. By integrating Kalman filtering for link prediction and multi-hop communication, the protocol ensures better data transmission reliability. Results from NS2 simulations confirm that EAEMR achieves higher delivery rates and lower overhead compared to traditional routing models like MRGA-VANETs and LRMC-VANETs.[9]

This study presents W-GeoR, a weighted geographical routing protocol optimized for health monitoring applications in VANETs. It improves emergency data dissemination by selecting optimal next-hop nodes based on traffic mobility, inter-vehicle distances, speed, and link expiration time. Simulation results using SUMO and NS-3 show that W-GeoR significantly reduces packet loss and transmission delay, outperforming conventional routing approaches.[20]

Artificial Intelligence (AI) is increasingly being integrated into Vehicular Ad Hoc Networks (VANETs), giving rise to AI-enabled VANETs (AI-VANETs). However, ensuring cybersecurity in AI-VANETs remains a significant challenge. Traditional trust schemes rely solely on trust updates, making them vulnerable to long-term attacks. To address this, a human cognition-based trust update scheme (HC-TUS) is proposed, incorporating Ebbinghaus' forgetting theory to enhance trust evaluation. Simulation results demonstrate that HC-TUS enforces the "Hard to get, easy to lose" trust principle more effectively than BRSN and BTDS, while also detecting and mitigating collusion attacks more efficiently. Additionally, the study highlights open trust-related challenges in AI-VANETs.[4]

Artificial Intelligence (AI)-driven authentication mechanisms are essential for securing Vehicular Ad Hoc Networks (VANETs) while maintaining lightweight and privacy-preserving features. Traditional authentication methods either focus on security or efficiency but often rely on centralized authorities, making them vulnerable in infrastructure-less environments. This paper introduces an AI-based approach, ANFIS-GWO, which combines Adaptive Neuro-Fuzzy Inference System (ANFIS) with Grey Wolf Optimization (GWO) to enhance authentication in VANETs. The proposed method operates in two phases: GWO optimizes ANFIS parameters during training, and the model's performance is evaluated on a testing set. Simulation results indicate that ANFIS-GWO reduces computational, communication, and energy costs compared to existing authentication schemes, demonstrating its effectiveness for secure and efficient vehicular networks.[14]

Vehicular Ad-hoc Networks (VANETs) are a key component of Intelligent Transportation Systems (ITS), enabling secure data exchange among vehicles and infrastructure. However, their decentralized nature makes them vulnerable to cyberattacks, including position falsification. To address this, a Deep Learning-based Intrusion Detection System (DL-IDS) is proposed, leveraging a Multi-Layer Perceptron (MLP) algorithm with novel detection features such as RSSI aggregation and Time Difference of Arrival (TDoA). Trained on the VeReMi dataset, the DL-IDS can be deployed on a vehicle's Onboard Unit (OBU) for real-time detection. Experimental results demonstrate its superior accuracy and computational efficiency, outperforming existing models by 2-7% in detecting position falsification attacks and false emergency braking alerts.[16]

This paper explores the integration of Software Defined Networking with VANETs to improve network scalability, traffic control, and quality of service (QoS). The study compares different SDN-based VANET algorithms and highlights improvements in packet delivery, latency, and routing efficiency. The paper identifies key challenges such as network instability and proposes solutions leveraging centralized control mechanisms to optimize routing and data flow. The Whale Optimization Algorithm (WOA) optimizes cluster formation by considering communication range, node density, vehicle speed, and road conditions, reducing network instability and routing overhead while improving cluster optimization by 75% compared to ALO and GWO. The Canine Olfactory Route-Finding Algorithm (CORFA) minimizes latency by utilizing pre-cached routes stored in RSUs, eliminating the need for new route discovery and reducing delays in high-traffic areas. The Advanced Greedy Hybrid Bio-Inspired (AGHBI) Algorithm ensures congestion-free, shortest-path data transmission using greedy and hybrid optimization techniques, improving end-to-end delay and data delivery in dynamic traffic scenarios. These bio-inspired approaches, combined with SDN's centralized control, enable real-time traffic optimization, outperforming traditional VANET routing protocols. By leveraging nature-inspired techniques, the proposed methods significantly enhance routing efficiency, resource allocation, and congestion management, ensuring robust and reliable communication in dynamic vehicular environments.[6]

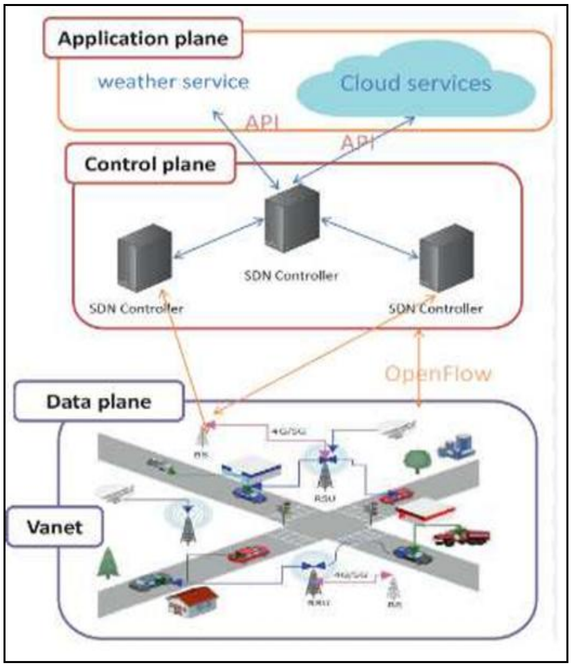

Fig. 3. SDN- VANET Architecture

This paper proposes a three-layer security architecture for VANETs, integrating block-chain and Mobile Edge Computing (MEC) to enhance data security and computational efficiency. The perception layer forms a block-chain network with vehicles and RSUs, where RSUs act as nodes for ledger updates and transaction validation, ensuring tamper-proof and traceable data storage. The edge computing layer leverages MEC to handle computationally intensive tasks, such as block-chain consensus mechanisms and video/image processing, reducing latency and network congestion. The service layer combines traditional cloud storage with block-chain, storing critical data like traffic accidents and violations on the block-chain for security, while general data is managed in the cloud for scalability. Block-chain ensures data integrity and traceability, while MEC offloads heavy computations from vehicles to edge servers, improving efficiency. This decentralized approach eliminates reliance on a central authority, addressing limitations like single points of failure and incomplete data security in existing systems. By integrating block-chain and MEC, the architecture provides a robust, scalable, and secure solution for VANETs, ensuring data consistency, reducing latency, and enhancing overall system resilience.[7]

The paper highlights the transformative role of Big Data and IoT in VANETs, enabling advanced traffic management, road safety, and real-time decision-making. Big Data, characterized by its volume, velocity, variety, and veracity, is generated from diverse sources like vehicle sensors, GPS, and traffic updates, facilitating traffic prediction, congestion management, and accident detection. IoT devices, including sensors, cameras, and GPS, enable seamless V2V and V2I communication, supporting smart traffic signals, accident alerts, and vehicle tracking. Data sources such as vehicle sensors, GPS, self-driving vehicle feeds, and real-time traffic updates provide critical insights for optimizing routes and improving safety. Machine learning and data analytics extract meaningful patterns from this vast data, enhancing traffic flow and reducing congestion. The integration of Big Data and IoT improves fuel efficiency, supports eco-friendly driving, and aids autonomous vehicles in safe navigation. Additionally, it fosters smart city development by enabling intelligent transportation systems. Overall, the synergy of Big Data and IoT in VANETs ensures enhanced traffic management, improved road safety, and efficient resource utilization, paving the way for smarter, safer, and more sustainable urban mobility. [19]

The study concludes that Network Dwelling Time (NDT) and Network Dwelling Distance (NDD) in Vehicle-to-RSU (V2R) communication cannot be determined purely through mathematical calculations, as real-world driving conditions, particularly speed variations, significantly impact these values. The experiments demonstrated that while vehicles do not maintain a constant speed, the average velocity within an RSU’s transmission range provides a reliable model for estimating NDD and NDT, with a minimal error margin of less than 0.03%. Additionally, the research highlights that vehicles near the edge of the RSU’s coverage are more likely to experience data loss due to connection instability. This finding suggests that optimizing RSU placement and transmission strategies can improve data reliability in V2R communication. Future work will focus on optimizing resource utilization by introducing proactive handover or overload control mechanisms to enhance V2R communication efficiency and reduce data loss. These improvements will contribute to a more stable and efficient vehicular communication network, ensuring better connectivity and data transmission for intelligent transportation systems.[18]

This research highlights the importance of connectivity probability in multi-way V2I communication networks, particularly in platoon-based VANETs. The study demonstrates that the presence of platoons significantly improves connection probability, making communication more reliable, especially in two-way V2I networks compared to single-way networks. Key factors such as traffic density, vehicle and RSU transmission range, RSU-to-RSU distance, and platoon ratio play a crucial role in determining network performance. Theoretical and simulated results confirm that integrating platoons enhances connectivity, which is essential for the advancement of Intelligent Transportation Systems (ITS). These findings provide valuable insights for government planners in designing future ITS solutions. Future work will focus on developing a connectivity routing protocol for platoon-based VANETs, ensuring secure and efficient communication within platoons, between platoon leaders and their members, and between vehicles and RSUs, further optimizing network performance.[17]

4. METHODOLOGIES IN VANETS

4.1 Block chain-Enabled VANETs

Block-chain technology has been introduced into VANETs to ensure decentralized and tamper-proof communication. Several studies have implemented:

- Certificate-less authentication schemes using elliptic curve cryptography for reducing key management complexity.
- Hierarchical block-chain architectures to enhance trust management and reduce latency.
- IoT and fog computing integration for improved scalability and fault tolerance.

Challenges: Block chain-based VANETs face processing delays and high computational costs, making real-time implementation difficult [6].

4.2 AI and Machine Learning for Routing Optimization

Machine learning (ML) and artificial intelligence (AI) have revolutionized VANET routing protocols. Notable AI-driven methodologies include:

- Reinforcement Learning-based routing for real-time adaptive decision-making.
- ANFIS-GWO (Adaptive Neuro-Fuzzy Inference System with Grey Wolf Optimization) algorithms for optimizing packet delivery.
- Deep Learning-based Intrusion Detection Systems (DL-IDS) for anomaly detection in vehicular networks.

Advantages: AI-based routing offers adaptive optimization, reducing congestion and improving QoS.

Limitations: High computational demands may hinder real-time processing in dynamic vehicular environments [7].

4.3 SDN in VANETs

SDN enables centralized network control, improving VANET scalability. SDN-driven solutions include:

- Multi-controller architectures for managing high-traffic loads.
- Bio-inspired optimization techniques (e.g., Whale Optimization Algorithm) for latency reduction.

- Anchor Bus-based routing frameworks to improve network stability.

Challenges: Requires real-world testing and infrastructure deployment for full-scale implementation [8].

4.4 5G and Edge Computing in VANETs

5G Integration has revolutionized VANETs, enabling ultra-low latency and high-speed connectivity. Techniques include:

- Trust-based mutual authentication model* for secure communication.
- Multi-hop relay techniques for extended coverage.
- Mobile Edge Computing (MEC) for offloading computational tasks.

Limitations: High computational overhead and dependency on advanced RSU infrastructure.

5. SECURITY CHALLENGES AND INTRUSION DETECTION IN VANETS

5.1 Threats in VANETs

VANETs are vulnerable to cyber threats such as:

- Sybil attacks: Malicious vehicles creating multiple identities.
- Gray-hole attacks: Selective packet dropping to disrupt communication.
- Position falsification attacks: Misleading location information for fraudulent purposes [9]

5.2 Intrusion Detection Mechanisms

Recent advancements in IDS include:

- Random Forest-based Intrusion Detection (NIDS) for real-time threat identification.
- Deep Learning-based Intrusion Detection Systems (DL-IDS) for position falsification attack mitigation [10].

6. COMPARATIVE ANALYSIS OF VANET TECHNIQUES

To provide an in-depth comparison of methodologies used in VANETs, we analyze key studies based on their methodologies, results, advantages, and limitations. Table 1 presents a comprehensive comparison of different approaches proposed in recent research.

Table 1: Comparison of Different VANET Methodologies

Category	Paper	Methodologies	Key Features	Results & Contributions	Limitations
Blockchain & Security in VANETs	[1]	Certificate-less authentication, Hierarchical block-chain based authentication	Fault tolerance, IoT-enabled security, Fog computing for reduced latency	Improved data integrity, decentralized trust management	Scalability issues in high-density regions, processing delays
	[7]	Trust-based authentication, Global Reputation Center (GRC)	5G integration, dynamic trust management, end-to-end security	Enhanced confidentiality, location privacy, attack resistance	High computational costs, network congestion risk
	[9]	Blockchain integration with Mobile Edge Computing (MEC)	Decentralized tamper-resistant storage, MEC for efficient processing	Improved security and lower latency in VANET communications	Instability in high-mobility environments
	[11]	Multi-tier trust rating system, malicious vehicle detection	Real-time trust assessment, rogue vehicle prevention	Enhanced security, lower latency in data transmission	Dependence on prior behavioral data, risk of trust manipulation
	[14]	Machine learning-based Network Intrusion Detection (NIDS)	AI-driven real-time anomaly detection, DDoS attack mitigation	High accuracy in threat detection, low false alarms	Requires extensive training data, computational overhead
AI & Optimization in VANETs	[3]	Trust modeling using AI algorithms	Adaptive security updates, AI-driven risk analysis	Improved detection of rogue nodes, enhanced network reliability	Requires dynamic adaptation for different traffic conditions
	[8]	AI-based path selection using trust evaluation	Optimized routing for secure data transmission	Reduced routing overhead, lower delay	High dependency on accurate trust scores
	[12]	Deep learning-based anomaly detection	Secure decentralized communication, position verification	Higher detection accuracy in VANET attacks	Potential false positives in dense networks

	[17]	AI-powered predictive analytics, Big Data integration	Real-time traffic optimization, intelligent routing	Improved traffic flow and reduced congestion	High data processing requirements
Routing & Communication in VANETs	[2]	Fuzzy logic-based cluster head selection	Stable clustering, reduced re-clustering frequency	91.46% packet delivery ratio, improved efficiency	Limited scalability, untested in urban environments
	[5]	Software-Defined Networking (SDN)	Centralized network management, bio-inspired optimization	Improved throughput, reduced latency	Requires real-world testing
	[6]	Location-based routing, energy-efficient sleep scheduling	Direction-aware path selection	Lower energy consumption, higher efficiency	Ignores urban signal obstructions
	[10]	GPS and AI-based link prediction	Dynamic route optimization, GPS-enabled accuracy	Reduced packet loss, improved transmission reliability	High computational complexity
	[18]	Weighted geographical routing	Emergency data transmission, health monitoring	Higher efficiency in post-disaster scenarios	Dependency on accurate GPS data
Performance Evaluation & Network Reliability	[4]	Survey-based analysis of VANETs	Identification of major challenges in VANETs	Clear taxonomy of VANET components	Lacks empirical validation
	[13]	Cluster-based message forwarding	Efficient traffic data propagation	Reduced network overhead, increased message delivery efficiency	Dependence on cluster head stability
	[15]	Multi-hop V2I connectivity analysis	Platoon-based vehicle networking	Improved road safety through better connectivity	Scalability concerns in low-density regions
	[16]	Simulation-based analysis	Impact of velocity on network dwelling time	Better RSU placement strategies	Challenges in maintaining connectivity at high speeds
Future Directions & Emerging Technologies	[9]	Blockchain-based security with edge computing	Enhanced security via distributed ledger	Improved scalability and efficiency	Computational resource constraints
	[4]	AI and SDN integration	Intelligent decision-making for VANETs	Improved automation and adaptability	High implementation costs
	[5]	Optimization algorithms for dynamic networking	Enhanced Quality of Service (QoS)	Increased network stability	Needs real-world validation
	[17]	IoT and big data analytics for real-time processing	Smarter transportation systems	Faster decision-making, improved data utilization	Privacy and security concerns

7. CONCLUSION

VANETs have evolved significantly over the years, offering solutions for intelligent transportation, road safety, and real-time vehicular communication. This survey has reviewed various methodologies, including block chain-based authentication, AI-driven routing optimization, multi-hop clustering, and SDN-based frameworks. While these techniques provide substantial improvements in security, efficiency, and scalability, several challenges remain. One of the primary concerns in VANETs is scalability in high-density regions. Existing clustering mechanisms and routing protocols struggle with high vehicle mobility and dynamic topologies [13]. Moreover, security and privacy remain critical issues, requiring robust encryption, trust models, and intrusion detection systems[14]. The integration of 5G and beyond (6G) technologies is expected to address some latency and connectivity challenges, but this also brings concerns regarding energy consumption and infrastructure costs [15].

REFERENCE

[1] Choudhary, P., & Singh, U. (2015). A Literature Review on Vehicular Ad-Hoc Network for Intelligent Transport. In *2nd International Conference on Computing for Sustainable Global Development* (pp. 1338–1341). IEEE. https://ieeexplore.ieee.org/document/7100480/

[2] Hamdi, M. M., Jassim, S. A., & Abdulhakeem, B. S. (2023). Successful Delivery Using Stable Multi-Hop Clustering Protocol for Energy Efficient Highway VANETs. *2023 7th International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*, 7(1), 1–6. https://ieeexplore.ieee.org/document/10304927/

[3] Tandon, R., Verma, A., & Gupta, P. K. (2022). Block-chain-enabled Vehicular Networks: A Review. *2022 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)*, 5(1), 1–5. https://ieeexplore.ieee.org/document/10029136/

[4] Fang, W., Zhu, C., Guizani, M., Rodrigues, J. J. P. C., & Zhang, W. (2023). HC-TUS: Human Cognition-Based Trust Update Scheme for AI-Enabled VANET. *IEEE Network*, 37(1), 123–129. DOI: 10.1109/MNET.011.2200245.

[5] Das, P., Ray, S., Sadhukhan, D., & Govil, M. C. (2022). 5G Enabled VANET Architecture Incorporating Security and Trust Management Mechanism. *Wireless Personal Communications*, 127(3), 2029–2050. DOI: 10.1007/s11277-022-09559-3.

[6] Ramesh, A., & Punniakodi, S. (2024). A Comprehensive Study on QoS Enhancement in SDN-Based VANET. In *2024 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1–6). DOI: 10.1109/ANTS.2024.9681234.

[7] Zhang, X., Li, R., & Cui, B. (2018). A Security Architecture of VANET Based on Block-chain and Mobile Edge Computing. *China Communications*, 15(7), 45–53. DOI: 10.1109/CC.2018.8456379.

[8] Chandramohan, K., Manikandan, A., Ramalingam, S., & Dhanapal, R. (2024). Performance Evaluation of VANET using Directional Location Aided Routing (D-LAR) Protocol with Sleep Scheduling Algorithm. *International Journal of Communication Systems*, 37(2), e5176. DOI: 10.1002/dac.5176.

[9] Kareem A. M. Al-sharhanee, Qaysar Salih Mahdi, Ahmed H. R. Alkhayyat, Fatima H. Alsalamy, & Nejood F. Abdulsattar. (2023). Experimental Analysis for Energy Aware Effective Multi Hop Routing in Vehicular Adhoc Networks. *6th International Conference on Engineering Technology and its Applications (IICETA)*, 6(1), 383–389. Link

[10] Samar Bayan, Utayba Mohammad, & Ahlam Al Mohammad. (2024). Position Falsification Attack Detection in Inter-Vehicle Networks Using Deep Learning. *IEEE International Conference on Electro Information Technology (eIT)*, 1(1), 1–6. Link

[11] Ghulam Mohi-ud-din, Zhiqiang Liu, Jiajun Chen, & Zhijun Lin. (2022). NIDS: Random Forest Based Novel Network Intrusion Detection System for Enhanced Cybersecurity in VANETs. *International Conference on Virtual Reality, Human-Computer Interaction and Artificial Intelligence (VRHCIAI)*, 1(1), 255–262. Link

[12] Index File (Referenced within SSMC-VANETs Paper (Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., & Zorzi, M. (2020). Toward 6G networks: Use cases and technologies. *IEEE Communications Magazine, 58*(3), 55-61.)

[13] Dutta, A., Campoverde, L. M. S., Tropea, M., & De Rango, F. (2024). A Comprehensive Review of Recent Developments in VANET for Traffic, Safety, and Remote Monitoring Applications. *Journal of Network and Systems Management*, 32(1), 1–25. DOI: 10.1007/s10922-023-09677-9.

[14] Balaji, V., Afsal, J., Santhosh, K. K., & Andreana, C. (2024). An Efficient and Secured Data Transmission in VANET Using LBK Interfaced AI-Optimized Routing Algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 15(1), 123–135. DOI: 10.1007/s12652-023-04056-7.

[15] Jyothi Na & Dr. Rekha Patil. (2023). A Multi-tier Accredit Based Security for Trustworthiness in VANETs Using Broadcasting Mechanism. *2nd International Conference on Electrical,*

Electronics, Information and Communication Technologies (ICEEICT), 2(1), 1–7. Link

[16] Sura Jasim Mohammed & Saad Talib Hasson. (2022). Modeling and Simulation of Data Dissemination in VANET Based on a Clustering Approach. *International Conference on Computer Science and Software Engineering (CSASE)*, 1(1), 54–61. Link

[17] Ahmed Waleed K. Al-Nasir & Dr. Foad Salem Mubarek. (2023). The Probability of Connectivity in the 2 Way / 2 Lane Platoon-Based V2I Communication Network. *15th International Conference on Developments in eSystems Engineering (DeSE)*, 1(1), 434–441. Link

[18] Nurshahrily Idura Ramli, Mohd Izani Mohamed Rawi, Mohd Faisal Ibrahim, Noorhayati Mohamed Noor, & Rosanita Adnan. (2023). The Influence of Velocity over Network Dwelling in VANET V2R Communication. *IEEE 16th Malaysia International Conference on Communication (MICC)*, 1(1), 91–98. Link

[19] Mahshad Mahmoudian, Yasin Kabalci, S. Mohammadali Zanjani, Ersan Kabalci, Hossein Shahinzadeh, & Farshad Ebrahimi. (2023). The Intelligent Mechanism for Data Collection and Data Mining in the Vehicular Ad-Hoc Networks (VANETs) Based on Big-Data-Driven. *5th Global Power, Energy and Communication Conference (GPECOM)*, 1(1), 495–502. Link

[20] Pawan Singh, Ram Shringar Raw, Suhel Ahmad Khan, Mazin Abed Mohammed, Ayman A. Aly, & Dac-Nhuong Le. (2022). W-GeoR: Weighted Geographical Routing for VANET's Health Monitoring Applications in Urban Traffic Networks. *IEEE Access*, 10(1), 38850–38860. Link