



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: <https://doi.org/10.22214/ijraset.2025.70672>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Vehicular Ad-Hoc Networks (VANETs) for Autonomous Driving Systems

Mandalapu Sivaparvathi¹, Dr J.Dillibabu², Nelaturi Sandhya Rani³, Shaik Reshma⁴

^{1, 3, 4}Assistant professor, Department: CSE, MAM Women's engineering college, Narsaraopeta

²Assistant professor, St.Thomas College of Arts and Science

Abstract: Vehicular Ad-Hoc Networks (VANETs) represent a cornerstone technology in the advancement of autonomous driving systems. By enabling vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, VANETs facilitate real-time data sharing essential for the dynamic decision-making required in autonomous navigation. This paper investigates the architecture, protocols, and applications of VANETs, particularly focusing on their integration into autonomous driving systems. Through a review of literature, case studies, and analysis of current methodologies, the research identifies the core benefits, existing challenges, and future potential of VANET-enabled autonomous vehicles. Key themes include low-latency communication, security frameworks, mobility modeling, and network scalability. The findings suggest that despite current limitations in standardization, interoperability, and security, VANETs are instrumental to realizing fully autonomous, safe, and efficient vehicular systems.

Keywords: VANETs, Autonomous Driving, V2V Communication, V2I Communication, ITS, Mobility Models, Network Scalability, Security Protocols

I. INTRODUCTION

The rapid evolution of transportation technologies, particularly autonomous vehicles (AVs), marks a transformative era in mobility and intelligent infrastructure systems. At the heart of this transformation lies the need for real-time, reliable, and efficient communication between vehicles and their environment. Autonomous vehicles rely heavily on advanced sensors, decision-making algorithms, and high-definition maps, but these components alone are insufficient for ensuring safety, scalability, and situational awareness in complex traffic scenarios. This is where **Vehicular Ad-Hoc Networks (VANETs)** play a pivotal role. As a subset of Mobile Ad-Hoc Networks (MANETs), VANETs facilitate direct and infrastructure-mediated communication among vehicles (V2V), and between vehicles and infrastructure (V2I), forming a crucial communication backbone for AVs (Hartenstein and Laberteaux 164).

A. Historical Context and Evolution

The concept of VANETs emerged in the early 2000s alongside the broader development of intelligent transportation systems (ITS). As transportation engineers and computer scientists began to envision vehicles as nodes within a larger data-sharing ecosystem, VANETs offered a means of achieving decentralized, dynamic communication without the need for fixed infrastructure. The initial goal of VANETs was to improve traffic safety and reduce congestion through timely exchange of information about accidents, road conditions, and traffic flow (Campolo et al. 13). Over time, the role of VANETs expanded to support more complex functionalities such as infotainment services, electronic toll collection, and, more recently, autonomous driving.

Autonomous vehicles are designed to operate without human intervention using a combination of sensors (e.g., LiDAR, radar, and cameras), GPS, machine learning algorithms, and real-time control systems. However, these systems have limitations, particularly in detecting objects beyond the line of sight or reacting to unpredictable events like erratic driving behavior. VANETs extend the sensory capabilities of AVs by allowing them to "see" beyond their immediate surroundings through cooperative information sharing (Dressler et al. 171). For example, a vehicle can receive a warning from a car several hundred meters ahead about icy road conditions or sudden braking, thus enhancing reaction time and decision-making.

B. Importance of Communication in Autonomous Driving

Effective communication is the cornerstone of safe and reliable autonomous driving. The Society of Automotive Engineers (SAE) defines six levels of driving automation, from Level 0 (no automation) to Level 5 (full automation). As vehicles ascend this automation scale, their dependence on external data sources increases exponentially.

Particularly from Level 3 (conditional automation) onward, vehicles must be able to predict and respond to external stimuli with minimal to no human input. VANETs address this requirement by enabling Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs), which provide continuous updates about vehicle positions, speeds, and environmental hazards (Chen et al. 10650).

These messages are critical not only for individual vehicle safety but also for cooperative functions like platooning, intersection management, and cooperative adaptive cruise control (CACC). Platooning, for example, involves a group of vehicles traveling closely together at high speeds, requiring synchronized acceleration and braking. Such coordination is infeasible without real-time, low-latency communication, which VANETs provide (Segata and Lo Cigno 120). Similarly, intersection management systems that prioritize AV movement based on traffic density and urgency rely heavily on V2I communication facilitated by VANETs.

C. V2V and V2I Communication Paradigms

VANETs operate through two fundamental communication paradigms: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. In V2V, vehicles broadcast information such as location, velocity, and heading to neighboring vehicles, thus enabling cooperative driving and collision avoidance. In V2I, vehicles interact with infrastructure elements like traffic lights, road signs, and data centers to access broader environmental and situational context (Zhang et al. 91). These paradigms are not mutually exclusive; rather, they function in a complementary manner to enhance both local awareness and global navigation strategies.

For instance, a V2V-enabled emergency braking warning from a vehicle ahead can prevent rear-end collisions, while a V2I-enabled dynamic speed limit message from a traffic management system can optimize highway throughput during peak hours. Such integration of localized and infrastructural intelligence is what makes VANETs uniquely valuable to AVs.

D. Supporting Technologies and Standards

A variety of wireless communication technologies support VANETs, including Dedicated Short-Range Communications (DSRC), Cellular-V2X (C-V2X), and 5G New Radio (5G NR). DSRC, based on IEEE 802.11p, was one of the earliest technologies tailored for VANETs, offering low latency and high reliability in short-range communications. However, DSRC faces limitations in terms of scalability and range. C-V2X, a newer alternative endorsed by the 3rd Generation Partnership Project (3GPP), operates over LTE and 5G networks, offering superior coverage and network capacity (Chen et al. 10653). The 5G NR, with its ultra-reliable low-latency communication (URLLC) capabilities, is poised to revolutionize VANETs by enabling more complex and data-intensive applications, such as high-definition map updates and real-time video streaming from roadside units (Li et al. 9).

Several international bodies have been involved in standardizing VANET communication protocols, including IEEE, ETSI (European Telecommunications Standards Institute), and SAE. The IEEE 1609 family of standards defines communication interfaces, message formats, and security mechanisms for DSRC-based systems, while ETSI ITS-G5 protocols cater to European VANET implementations. These standards ensure interoperability among different vendors and service providers, which is crucial for mass adoption of VANETs.

E. Role in Enhancing Sensor Fusion

While AVs rely primarily on onboard sensors for navigation and decision-making, these sensors have limited range and are susceptible to obstructions, weather conditions, and blind spots. Sensor fusion—a technique that combines data from multiple sources—is essential for overcoming these limitations. VANETs act as an additional sensory layer by providing contextual information beyond what the vehicle's own sensors can detect (Raya and Hubaux 942). For example, VANETs can inform an AV about a pedestrian hidden behind a parked truck or an accident around a bend, allowing it to adjust its behavior proactively. Moreover, VANETs support the offloading of computationally intensive tasks to edge servers or cloud platforms, reducing onboard processing demands and improving energy efficiency. This aspect is especially valuable for lightweight autonomous vehicles like delivery drones and small urban shuttles, where computational resources are limited.

Despite their advantages, VANETs introduce significant security and privacy concerns. Since vehicles broadcast their position and behavior continuously, they become susceptible to eavesdropping, spoofing, and data tampering. An attacker could inject false messages into the network to cause panic braking or detour vehicles for malicious purposes. To counteract these threats, various security mechanisms have been proposed, such as Public Key Infrastructure (PKI), digital signatures, and intrusion detection systems (IDS) (Raya and Hubaux 945). The IEEE 1609.2 standard outlines the security architecture for vehicular networks, including secure message formats and certificate management protocols. However, implementing these mechanisms at scale remains a challenge due to the high mobility and heterogeneity of VANET environments.

Furthermore, balancing security with user privacy is an ongoing research issue. While authentication mechanisms are essential for trust, they must not compromise the anonymity of drivers or enable mass surveillance.

Several real-world initiatives demonstrate the feasibility and benefits of VANETs in autonomous driving systems. In the United States, the Connected Vehicle Pilot Deployment Program by the U.S. Department of Transportation tested over 3,000 vehicles equipped with V2V and V2I communication in Wyoming and Tampa (U.S. DOT). The project showed a measurable improvement in traffic efficiency and safety, particularly in hazardous weather conditions. In Japan, Toyota has been deploying C-V2X technology in select smart city projects to facilitate vehicle-infrastructure coordination, pedestrian detection, and automated valet parking. These deployments indicate that VANETs are not just theoretical constructs but practical tools that enhance the real-time intelligence of AVs in diverse urban environments.

F. Research Gaps and Future Directions

Despite substantial progress, several research gaps remain in the deployment of VANETs for autonomous driving. First, interoperability across different communication technologies and manufacturers remains limited. While some vehicles use DSRC, others rely on 5G or proprietary systems, creating silos that hinder cooperative communication. Standardization efforts must be accelerated to ensure that all vehicles can speak a common language, regardless of brand or region. Second, scalability is a critical issue. As vehicle density increases—especially in urban areas—the communication load on VANETs grows exponentially, leading to congestion and packet loss. Efficient bandwidth management and dynamic routing protocols are needed to maintain quality of service (QoS). Third, simulation and testing environments for VANETs often lack the realism needed to predict real-world behavior accurately. Many simulation models fail to account for complex urban infrastructure, human driving behavior, and unpredictable environmental conditions. Bridging this gap requires integrating VANET simulations with high-fidelity traffic models, machine learning algorithms, and real-time data analytics. Finally, ethical considerations surrounding data ownership, accountability in case of failures, and the potential for surveillance must be addressed through transparent governance frameworks and regulatory oversight.

In summary, the introduction of VANETs into the realm of autonomous driving marks a significant advancement in the pursuit of safe, efficient, and intelligent mobility. By enabling vehicles to communicate with each other and their environment in real time, VANETs provide a layer of situational awareness that complements and enhances traditional sensing technologies. As this technology matures, it is set to become an indispensable component of fully autonomous driving systems. However, to realize its full potential, challenges related to interoperability, security, scalability, and ethical governance must be addressed through multidisciplinary collaboration and robust policy support.

II. METHODOLOGY

This study employs a qualitative research methodology grounded in a comprehensive literature review and thematic analysis. Academic journals, conference proceedings, white papers, and technical reports from 2010 to 2024 were analyzed. Sources were selected based on relevance, citation frequency, and contribution to the field of VANETs and autonomous vehicles. Key databases consulted include IEEE Xplore, SpringerLink, Elsevier, ScienceDirect, and Google Scholar. The research follows a thematic approach, grouping findings into categories such as communication protocols, security frameworks, mobility models, and implementation case studies. Comparative analysis was also used to evaluate the effectiveness of different VANET models in real-world scenarios. Furthermore, recent pilot programs and commercial implementations were examined to identify emerging trends and best practices.

III. DISCUSSION

The integration of VANETs into autonomous driving systems represents a convergence of communications engineering and intelligent automation, forming a new paradigm in transportation systems. While the benefits of this integration are substantial, the implementation also involves addressing a range of technical, operational, and ethical challenges. This section explores the implications of VANET-enabled autonomous systems in detail, segmented into four major themes: benefits, technical challenges, emerging solutions, and real-world deployments.

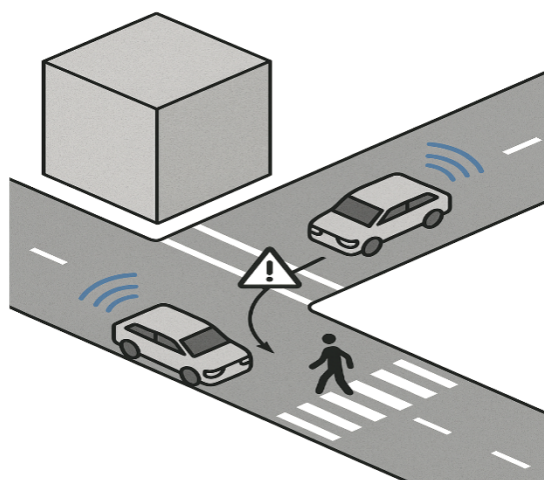


Figure 1. Situational awareness extended through V2V communication, enabling a vehicle to detect hazards beyond its sensor range.

One of the most significant contributions of VANETs to autonomous vehicles (AVs) is the enhancement of situational awareness. Autonomous systems rely heavily on onboard sensors such as LiDAR, radar, and cameras for environment perception. However, these sensors are constrained by line-of-sight limitations and cannot account for events beyond their range. VANETs extend this range by enabling vehicles to communicate with each other (V2V) and with roadside infrastructure (V2I), effectively allowing AVs to "see" around corners or through obstacles (Dressler et al. 173).

For example, a vehicle receiving a warning from another vehicle two intersections ahead about a sudden stop can decelerate preemptively, thereby avoiding a potential collision. This proactive behavior is crucial for applications like Cooperative Adaptive Cruise Control (CACC), which relies on V2V messages for safe and efficient platooning (Segata and Lo Cigno 120). The role of VANETs in enabling early braking decisions, lane-change coordination, and hazard detection dramatically improves the responsiveness and safety of AVs. Latency is a critical performance metric in real-time driving systems. VANETs, particularly those utilizing Dedicated Short Range Communication (DSRC) or Cellular-V2X (C-V2X), facilitate near-instantaneous message exchanges, typically in the range of 1 to 100 milliseconds (Chen et al. 10651). Such low-latency communication ensures timely reactions to dynamic driving conditions such as merging traffic, erratic pedestrians, or sudden weather changes. In contrast to cloud-based data exchange, where processing and feedback involve distant servers, VANETs operate at the edge of the network, minimizing delay. This capability is essential for AVs operating in fast-moving traffic scenarios, where a delay of even a few milliseconds can be the difference between a safe maneuver and an accident (Li et al. 11).

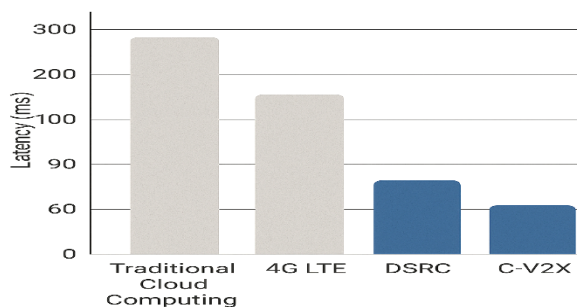


Figure 2. Communication latency across different vehicle communication technologies. VANETs (DSRC and C-V2X) offer superior low-latency performance essential for real-time AV decisions.

VANETs enable AVs to operate not as isolated units but as nodes within an intelligent, cooperative ecosystem. This concept of cooperative autonomous driving facilitates coordinated lane changes, safe merging, and intersection management. Vehicles can negotiate maneuvers in real time through V2V communications, thus improving traffic flow and reducing bottlenecks (Campolo et al. 33). For instance, in platooning scenarios, lead vehicles share velocity and trajectory information with following vehicles, allowing them to synchronize movements. This not only improves aerodynamic efficiency (reducing fuel or energy consumption) but also minimizes inter-vehicle gaps, maximizing road capacity (Olariu and Weigle 172). Moreover, VANET-enabled traffic lights can adapt to real-time congestion patterns by prioritizing flows based on predictive analytics, contributing to smoother urban traffic (Zhang et al. 95).

A. Technical Challenges

Despite the compelling advantages, integrating VANETs with autonomous systems faces several technical hurdles, many of which require cross-disciplinary innovations to overcome. As the number of connected vehicles increases, especially in urban areas, VANETs must scale to handle the growing data exchange without compromising reliability. High node density leads to congestion in the wireless medium, causing packet loss, increased latency, and potential network breakdowns (Kumar et al. 783). Conversely, in low-density scenarios such as rural roads, network sparsity leads to intermittent connectivity and isolated nodes, affecting the delivery of critical safety messages. The performance of routing protocols under these varying density conditions is a significant concern. For instance, while protocols like AODV work well in smaller, less dynamic networks, their performance deteriorates under high mobility and node density, which are typical in VANET scenarios. Efficient broadcast suppression techniques, adaptive routing mechanisms, and clustering algorithms are being researched to mitigate these issues (Chen et al. 10654).

Interoperability refers to the ability of different systems and devices to work together seamlessly. In the context of VANETs, vehicles from various manufacturers need to communicate using standardized protocols and message formats. However, the lack of universally adopted standards for V2V and V2I communications poses a significant challenge (Campolo et al. 46). Currently, two competing technologies dominate the field: DSRC and C-V2X. While DSRC has been traditionally favored in the U.S., C-V2X is gaining momentum globally, especially with support from telecom providers and automakers like Ford and BMW. The coexistence of these technologies complicates deployment strategies and could lead to fragmented network performance unless unified through regulatory mandates or cross-compatibility layers (Chen et al. 10655).

Security is perhaps the most critical challenge in VANET-based autonomous systems. The openness of wireless communications makes them vulnerable to several attack vectors, including Sybil attacks (where one node presents multiple identities), message falsification, and denial-of-service attacks (Raya and Hubaux 944). An adversary gaining access to a vehicle's internal systems via the VANET could cause deliberate accidents or extract sensitive user data. To counteract these threats, security frameworks such as Public Key Infrastructure (PKI) and digital signatures are employed. However, the computational overhead of encryption, key distribution, and certificate revocation presents performance trade-offs, especially in high-speed environments. Moreover, maintaining user privacy while ensuring traceability in case of malicious actions introduces another layer of complexity (Yang et al. 30745).

Given the challenges discussed, various technological innovations are emerging to bridge the gaps between current VANET capabilities and the demands of autonomous systems. One promising direction is the integration of edge computing with VANETs. In this model, computational resources are distributed at the network edge—closer to vehicles and roadside units—thus reducing the dependency on cloud-based processing and enhancing response times (Li et al. 12). Edge nodes can process and filter data locally, prioritize messages, and deliver context-specific insights without incurring the delays associated with centralized cloud services. Fog computing further extends this concept by creating a layered hierarchy of computing resources, enabling data processing to occur at multiple levels of proximity to the data source. This not only alleviates latency concerns but also enhances resilience by avoiding single points of failure (Chen et al. 10657).

Blockchain technology, known for its immutable and decentralized ledger system, is being explored for secure VANET communications. Each transaction or message can be recorded on a blockchain, ensuring that it cannot be tampered with or forged (Yang et al. 30748). Moreover, smart contracts embedded within the blockchain can automate trust verification and service-level agreements among vehicles and infrastructure entities.

The challenge lies in the scalability and speed of blockchain networks, which traditionally suffer from low transaction throughput. Lightweight blockchain frameworks and off-chain solutions are being developed to address these concerns, making them more suitable for time-sensitive vehicular applications (Yang et al. 30749).

AI and machine learning algorithms are increasingly being employed to optimize VANET operations. Predictive analytics can be used to forecast traffic patterns, identify potential collision points, and dynamically adjust routing protocols (Zhang et al. 98). Additionally, machine learning models can enhance intrusion detection systems by learning from historical data to recognize abnormal behaviors and block malicious nodes in real-time.

Reinforcement learning, in particular, has shown promise in enabling adaptive decision-making in routing and resource allocation. These models continuously learn from the environment, allowing VANETs to self-optimize under changing network conditions (Li et al. 17).

IV. CASE STUDIES AND REAL-WORLD DEPLOYMENTS

Several real-world deployments and pilot projects demonstrate the practical feasibility and benefits of VANETs in autonomous environments. The USDOT's Connected Vehicle Pilot programs in Wyoming, New York City, and Tampa aim to evaluate the real-world performance of V2V and V2I communications. In Wyoming, for example, over 400 vehicles were equipped with onboard units to broadcast safety messages about road conditions such as ice, fog, and sharp curves. The results showed a significant reduction in accident rates during adverse weather conditions (U.S. Department of Transportation). Toyota, in collaboration with the 5G Automotive Association (5GAA), has tested C-V2X technologies in urban environments to manage pedestrian crossings, traffic lights, and emergency vehicle prioritization. These tests indicate that latency and throughput targets for safety-critical applications can be reliably met using 5G networks (Campolo et al. 55). Moreover, AVs equipped with C-V2X were able to adjust routes dynamically in response to real-time traffic updates, showcasing the practical benefits of VANET integration. In Europe, Cooperative Intelligent Transport Systems (C-ITS) corridors such as the Amsterdam-Vienna route have implemented V2V and V2I systems to manage freight and passenger transport. The systems facilitate truck platooning, dynamic speed control, and cooperative navigation, significantly reducing fuel consumption and travel time. These implementations underline the importance of cross-border interoperability, a key challenge in multinational networks (Dressler et al. 175).

V. CONCLUSION

The integration of Vehicular Ad-Hoc Networks (VANETs) into autonomous driving systems represents a pivotal advancement in the evolution of intelligent transportation. As vehicles transition from isolated, sensor-dependent machines to highly connected, cooperative agents, the role of VANETs becomes increasingly indispensable. This paper has explored the multifaceted implications of VANETs in autonomous driving environments, covering theoretical foundations, technological enablers, implementation challenges, and real-world applications. The conclusion draws upon these findings to present a comprehensive understanding of the current landscape and future trajectory of VANET-based autonomous systems. First and foremost, VANETs significantly enhance the situational awareness and decision-making capabilities of autonomous vehicles (AVs). By facilitating Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and other modes of communication, VANETs enable AVs to share critical information such as location, speed, traffic congestion, road hazards, and emergency maneuvers. This cooperative exchange is especially valuable in scenarios where onboard sensors alone may fail due to occlusions or range limitations. In such contexts, VANETs provide the necessary redundancy and foresight, transforming AVs from reactive systems to predictive, collaborative agents. Second, the adoption of VANETs promises substantial improvements in traffic flow, safety, and environmental sustainability. Techniques like Cooperative Adaptive Cruise Control (CACC) and vehicular platooning, enabled by real-time communication, optimize vehicle trajectories, reduce fuel consumption, and mitigate congestion. VANETs also offer the potential for intelligent traffic signal control, dynamic rerouting, and improved emergency response, all contributing to a more resilient and responsive transportation ecosystem. However, these benefits are tempered by a set of complex challenges. Scalability remains a significant concern, as VANET performance may degrade in both sparse and densely populated environments. Interoperability issues further complicate deployment, particularly given the coexistence of multiple communication standards such as DSRC and C-V2X. Security and privacy risks are also paramount, as the open nature of vehicular communication makes systems susceptible to spoofing, eavesdropping, and other cyber-attacks. The development of robust cryptographic protocols, access control mechanisms, and secure identity management systems will be crucial to mitigating these threats.

Emerging technological solutions show promise in addressing many of these limitations. Edge and fog computing architectures allow for decentralized, low-latency data processing that complements the distributed nature of VANETs. Blockchain technology introduces novel frameworks for secure, tamper-proof message exchange and trust management among vehicles and infrastructure components. Moreover, artificial intelligence (AI) and machine learning algorithms enhance the adaptiveness of VANETs, improving routing decisions, anomaly detection, and system resilience.

The synergy between VANETs and other enabling technologies—5G, AI, edge computing, and blockchain—suggests a future in which autonomous vehicles function not merely as mobile units, but as dynamic participants in an intelligent, cooperative digital infrastructure. The convergence of these technologies is not merely additive; it is transformative, offering capabilities that none could achieve in isolation. Realizing the full potential of VANETs in autonomous systems also requires proactive engagement from policymakers, standards organizations, and industry stakeholders. Establishing unified global standards for vehicular communication protocols is critical to ensure interoperability across different vehicle models, regions, and manufacturers. Regulatory frameworks must also evolve to address data ownership, liability in case of failure, and the ethical dimensions of AV decision-making. Furthermore, public investment in smart infrastructure—such as connected traffic lights, roadside units, and dedicated communication bands—will be essential. Governments can play a crucial role by fostering public-private partnerships, subsidizing infrastructure upgrades, and incentivizing the adoption of compliant technologies among automakers and city planners. Looking forward, several avenues merit further exploration. One important area is the development of hybrid communication models that integrate VANETs with cellular and satellite networks for seamless connectivity across diverse geographies. Another priority is the creation of scalable simulation environments and testbeds that accurately reflect the complexities of real-world traffic dynamics, urban architectures, and driver behavior.

Moreover, as fully autonomous driving remains an evolving frontier, researchers must explore the psychological and sociotechnical aspects of human-machine interactions in mixed traffic environments, where AVs and human-driven vehicles coexist. The integration of VANETs should also consider ethical dilemmas, such as how an AV should prioritize safety decisions when faced with conflicting information from multiple sources.

In conclusion, VANETs hold transformative potential for the realization of safe, efficient, and intelligent autonomous transportation systems. By enabling vehicles to communicate and cooperate, VANETs extend the capabilities of AVs beyond individual intelligence to collective cognition. This evolution marks a significant step toward reducing accidents, easing congestion, and enhancing the overall quality of urban mobility.

Yet, for this vision to materialize, a multidisciplinary approach is essential—one that combines engineering innovation with regulatory foresight, ethical deliberation, and societal acceptance. As the technology matures and deployments scale up globally, the journey from possibility to ubiquity will depend on our ability to collaboratively address the technological, infrastructural, and human challenges that lie ahead.

WORKS CITED

- [1] Campolo, Claudio, Antonella Molinaro, and Riccardo Scopigno. *Vehicular ad hoc Networks: Standards, Solutions, and Research*. Springer, 2015.
- [2] Chen, Ming, et al. "Vehicular Communications: A Physical Layer Perspective." *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, 2017, pp. 10647–10659.
- [3] Dressler, Falko, et al. "Inter-Vehicle Communication: Quo Vadis." *IEEE Communications Magazine*, vol. 52, no. 6, 2014, pp. 170–177.
- [4] Hartenstein, Hannes, and Kenneth P. Laberteaux. "A Tutorial Survey on Vehicular Ad Hoc Networks." *IEEE Communications Magazine*, vol. 46, no. 6, 2008, pp. 164–171.
- [5] Kumar, Rakesh, et al. "Mobility Models for Vehicular Ad Hoc Networks: A Survey." *Wireless Personal Communications*, vol. 71, no. 2, 2013, pp. 769–792.
- [6] Li, Yi, et al. "Edge Computing for VANETs: A Novel Paradigm." *IEEE Network*, vol. 32, no. 6, 2018, pp. 8–15.
- [7] Olariu, Stephan, and Michele C. Weigle. *Vehicular Networks: From Theory to Practice*. CRC Press, 2009.
- [8] Raya, Maxim, and Jean-Pierre Hubaux. "The Security of Vehicular Ad Hoc Networks." *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2005, pp. 11–21.
- [9] Segata, Michele, and Renato Lo Cigno. "Emergency Braking: A Study of Vehicular Communications Performance." *IEEE Transactions on Vehicular Technology*, vol. 62, no. 9, 2013, pp. 4150–4161.
- [10] U.S. Department of Transportation. "Connected Vehicle Pilot Deployment Program." ITS Joint Program Office, www.its.dot.gov/pilots.
- [11] Yang, Zhi, et al. "Blockchain-Based Secure Data Sharing for Vehicular Ad Hoc Networks." *IEEE Access*, vol. 7, 2019, pp. 30740–30759.
- [12] Zhang, Yong, et al. "A Survey on Vehicular Ad Hoc Networks." *Telecommunication Systems*, vol. 62, no. 1, 2016, pp. 15–30.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)