International Journal of Web of Multidisciplinary Studies

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

website: *http://ijwos.com*
Vol.02 No.12.

OPEN ACCESS

E-ISSN : 3049-2424

DOI: https://doi.org/10.71366/ijwos

Revolutionizing Intelligent Transportation: Emerging Trends in Vehicle-to-Vehicle (V2V) Communication and Security

Dr S. V. Viraktamath[1], Praveenakumar Budihal[2], Shriraksha Channalli[3], Preethi .S. Awate [4]

[1,2,3,4] *Department of Electronics and Communication, SDM college of Engineering and Technology, Dharwad, Karnataka, India.*

Article Info

Article History:

Published:31 Dec 2025

Publication Issue:
Volume 2, Issue 12
December-2025

Page Number:
944-953

Corresponding Author:
Praveenakumar Budihal

Abstract:

The emergence of Vehicle-to-Vehicle (V2V) communication marks a paradigm shift in modern transportation systems, transforming vehicles into intelligent, cooperative nodes capable of exchanging real-time information. By integrating technologies such as Dedicated Short-Range Communication (DSRC), 5G-V2X, Li-Fi, and Reconfigurable Intelligent Surfaces (RIS), vehicles can make autonomous, data-driven decisions with minimal latency and maximum reliability. This communication facilitates advanced safety mechanisms, traffic efficiency, and energy optimization. However, challenges such as scalability, interoperability, security vulnerabilities, and privacy concerns persist. This paper presents a comprehensive review of V2V communication, its architecture, enabling technologies, security mechanisms, and future research directions, emphasizing the convergence of Artificial Intelligence (AI), edge computing, and 6G in shaping the future of intelligent transportation networks.

Keywords: Vehicle-to-Vehicle (V2V), Dedicated Short-Range Communication (DSRC), Artificial Intelligence (AI), Reconfigurable Intelligent Surfaces (RIS), Intelligent Transportation Systems (ITS).

1. Introduction

Intelligent Transportation Systems (ITS) aim to revolutionize how vehicles, infrastructure, and drivers interact. The exponential increase in road vehicles, urban congestion, and accident rates has accelerated the need for cooperative vehicular communication [1]. V2V communication serves as a vital enabler for autonomous driving, ensuring vehicles can share situational data in milliseconds.V2V communication allows vehicles to transmit and receive critical information such as speed, direction, brake status, and environmental hazards. This capability forms the foundation of Vehicular Ad Hoc Networks (VANETs), where vehicles act as nodes that dynamically organize to maintain network connectivity [2].

The integration of AI-based decision systems, 5G/6G connectivity, and Block chain security is transforming V2V networks into self-learning, adaptive ecosystems. Major global initiatives, including the 5G Automotive Association (5GAA) and Europe's 5G-CARMEN project, are pioneering large-scale V2V deployments. Despite significant progress, challenges such as interoperability, latency control, and security standardization remain central to ongoing research [3]. Figure 1. Vehicle-Based Components and Architecture as shown below.

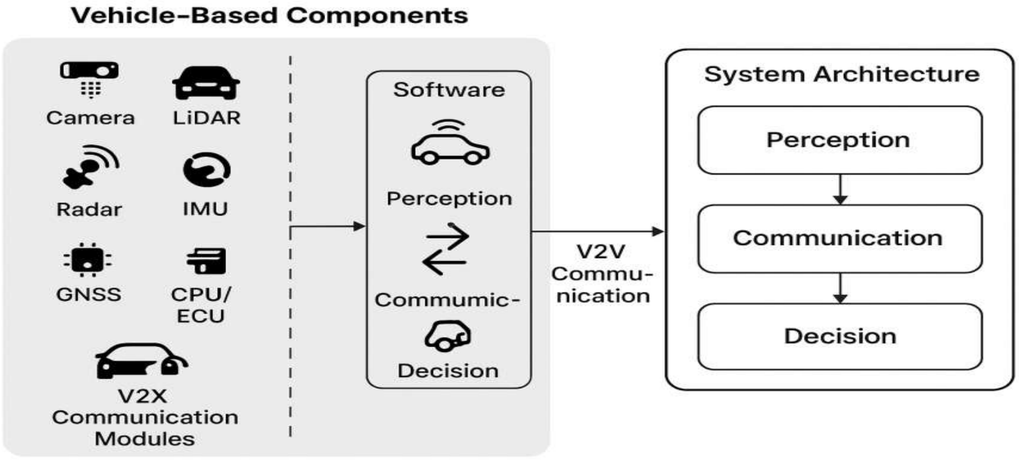

Figure 1 Vehicle-Based Components and Architecture adapted based on concepts [5]

2. Evolution of Intelligent Transportation Systems

ITS have evolved from basic vehicle tracking to complex, AI-driven autonomous ecosystems [4]. Evolution of ITS have undergone a remarkable transformation over the past three decades, evolving from basic sensor-based monitoring to intelligent, AI-driven autonomous ecosystems. The earliest phase of ITS (1990–2005) focused on centralized and infrastructure-dependent systems that relied on satellite navigation, fixed roadside sensors, and human-controlled decision-making. Technologies such as Electronic Toll Collection (ETC) and Traffic Light Synchronization represented initial automation efforts; however, they lacked real-time inter-vehicle coordination and adaptive learning capabilities. The subsequent phase (2005–2020) marked the introduction of DSRC and GPS-enabled networking, enabling vehicles to communicate directly with one another and with Roadside Units (RSUs). This era witnessed the emergence of cooperative awareness systems, including adaptive cruise control, lane-keeping assist, and collision avoidance mechanisms, which laid the foundation for connected and partially autonomous vehicles. Despite these advancements, cloud-based data analytics during this period suffered from limitations related to bandwidth constraints and latency, hindering large-scale scalability [5]. The integration of AI and Machine Learning (ML) technologies after 2020 brought a paradigm shift by introducing predictive decision-making, real-time congestion forecasting, and autonomous risk assessment capabilities. Major automotive innovators such as Waymo, Tesla, and Baidu Apollo have incorporated V2V-like communication modules and edge-AI processors into their platforms, allowing vehicles to share sensor data dynamically and improve route intelligence through continuous learning. Moving forward, next-generation ITS frameworks are expected to leverage 6G connectivity, edge AI processing, and quantum-secure communication protocols to establish hyper-connected transportation ecosystems that integrate vehicles, infrastructure, and pedestrians into a seamless digital fabric. Furthermore, the adoption of digital twin technology where virtual models of cities and vehicles mirror real-world dynamics will enable predictive traffic management, infrastructure optimization, and proactive safety measures, thereby realizing the vision of an adaptive, autonomous, and sustainable transportation ecosystem [6].

3. Vehicle-to-Vehicle (V2V) Communication Overview

V2V communication enables automobiles, trucks, public transport vehicles, and autonomous systems to exchange real time information using short range wireless technologies. Through continuous broadcasting of Basic Safety Messages (BSMs) or Cooperative Awareness Messages (CAMs), vehicles share critical data such as speed, acceleration, braking intent, lane position, heading, and environmental conditions. This direct, infrastructure less communication forms a cooperative vehicular network, allowing vehicles to perceive beyond their sensor range and react intelligently to dynamic road conditions. The core purpose of V2V technology is to enhance situational awareness, reduce collision risks, and support cooperative driving functionalities that are essential for autonomous mobility [7].

V2V communication typically operates through DSRC based on IEEE 802.11p, or C-V2X defined by 3GPP standards. DSRC provides low latency, high reliability communication ideal for safety messages, while C-V2X offers extended range, superior coverage, and integration with 5G for advanced applications. These technologies enable vehicles to implement critical safety applications such as Forward Collision Warning, Blind Spot Detection, Emergency Brake Light Notification, Cooperative Adaptive Cruise Control (CACC), and Platooning. Research has shown that cooperative maneuvers facilitated through V2V can reduce multi vehicle collision probability by over 80% and improve traffic throughput in congested areas [8].To support reliable communication, V2V networks employ standardized message formats, including SAE J2735, which defines message sets like MAP, SPaT, and BSM. These messages ensure interoperability among different manufacturers and allow seamless integration with V2I (Vehicle-to-Infrastructure) and V2X (Vehicle-to-Everything) systems. Furthermore, modern V2V systems integrate sensor fusion technologies, combining LiDAR, RADAR, ultrasonic sensors, cameras, and GNSS data to enhance the accuracy of shared information. Vehicles also rely on cooperative perception, where sensor data is combined across vehicles to eliminate blind spots and extend visibility in complex environments such as dense urban traffic or obstructed intersections [9].

Another essential component of V2V communication is the distributed decision making mechanism, where vehicles autonomously analyze exchanged data to make informed actions. For example, in lane merging or intersection crossing scenarios, vehicles negotiate priority and coordinate speed adjustments using predefined algorithms. Advanced implementations use ML to predict vehicle behavior, classify potential threats, and plan optimal maneuvers in cooperative environments. These ML driven approaches significantly improve system response time and decision quality compared to isolated, sensor only autonomous systems [10].

4. Communication Technologies in V2V

V2V systems enable real-time, reliable data exchange between vehicles to support safety and cooperative driving. The primary technology historically used is DSRC, based on IEEE 802.11p, which provides low latency communication ideal for safety alerts and cooperative maneuvers. However, DSRC's range limitations and congestion issues led to the emergence of C-V2X, introduced in 3GPP Release 14. C-V2X supports both device to device (PC5) and network assisted communication (Uu interface), offering significantly higher reliability and coverage. With 5G NR-V2X, vehicles gain ultra-low latency, high data rates, network slicing, and support for dense traffic environments. Additional technologies include Li-Fi, which uses visible light for secure short range communication, and Reconfigurable Intelligent Surfaces (RIS) that enhance signal propagation in urban areas. Together, these technologies form a robust communication ecosystem enabling cooperative perception, autonomous driving, and efficient traffic management. [9].

Dedicated Short Range Communication (DSRC):

Based on IEEE 802.11p, DSRC operates in the 5.9 GHz spectrum with a 300 meter range and latency under 10 milliseconds. It supports decentralized communication ideal for safety applications like intersection alerts and crash avoidance. However, DSRC faces spectrum congestion and limited scalability. Recent research integrates AI based congestion control algorithms to dynamically adjust transmission power and channel allocation [10].

Wi-Fi-Based Communication:

Wi-Fi standards (IEEE 802.11n/ac/ax) are used for urban mobility experiments and low cost testbeds. Wi Fi ensures high throughput but lacks the handover efficiency required for high speed vehicles [11]. It remains relevant in smart campus, parking automation, and urban shuttle prototypes.

5G and Cellular V2X (C V2X):

C-V2X technologies represent the most advanced communication framework for supporting next generation vehicular networks, providing high reliability, ultra-low latency, and massive connectivity essential for autonomous and cooperative driving systems. Unlike DSRC, which relies on IEEE 802.11p, C V2X is defined by 3GPP Releases 14, 15, and 16, enabling vehicles to communicate directly with one another (V2V), with infrastructure (V2I), with pedestrians (V2P), and with the network (V2N). C V2X operates through two communication modes: Device to Device (PC5 interface) for direct short range V2V messages, and Uu interface through the cellular base station for broader area V2N services. With the introduction of 5G NR V2X, latency is reduced to 1 ms, supporting highly time critical safety applications such as autonomous lane merging, cooperative collision avoidance, intersection movement assist, and platooning [13].

Li- Fi Communication:

Li-Fi utilizes visible light from LED sources to transmit data at multi gigabit speeds. It is immune to electromagnetic interference and offers enhanced security since light cannot penetrate walls or vehicles. Hybrid RF-Li-Fi systems allow adaptive switching between media based on environmental conditions [13].

Reconfigurable Intelligent Surfaces (RIS):

RIS deploys programmable met surfaces to dynamically reflect and amplify wireless signals, addressing non line of sight (NLOS) limitations in urban environments. This technology will play a central role in 6G V2V systems, optimizing mmWave communication and beamforming [14].

Hybrid Multi Access Integration:

Modern vehicles are equipped with multiple communication modules 5G, Wi-Fi, and DSRC that cooperate under a network orchestrator powered by AI. This system performs cross layer optimization, ensuring stable links and seamless switching [15].

Emerging 6G and Quantum V2V:

6G will introduce Terahertz (THz) frequencies, quantum key distribution (QKD), and AI native networks. Quantum V2V aims to create tamper proof communication using photon entanglement, preventing eavesdropping and data tampering [16].

5. Vehicle Based Components and System Architecture

A fully functional V2V communication system relies on a tightly integrated combination of advanced hardware components, intelligent software modules, and a layered system architecture that enables seamless sensing, communication, and cooperative decision making across vehicles. At the hardware level, modern connected vehicles incorporate a diverse set of sensing instruments such as LiDAR, RADAR, stereo and monocular cameras, ultrasonic sensors, infrared sensors, Global Navigation Satellite System (GNSS) modules (GPS, GLONASS, Galileo), and Inertial Measurement Units (IMUs). These sensors collectively generate high resolution spatial and temporal data necessary for environment perception, object detection, lane determination, and localization accuracy within a few centimeters. These sensing units feed data into the vehicle’s Electronic Control Units (ECUs) and Onboard Units (OBUs), which are responsible for executing communication protocols, managing vehicular networking stacks, performing sensor fusion, running AI models, and generating control commands for braking, acceleration, or steering.

6. Routing and Data Management Protocols

Routing determines how messages are disseminated efficiently in high mobility networks. Routing and Data Management Protocols play a pivotal role in ensuring efficient, reliable, and low latency information dissemination across V2V communication networks. The highly dynamic nature of vehicular networks characterized by rapid mobility, frequent topology changes, and varying node densities demands adaptive routing mechanisms capable of maintaining connectivity and data integrity in real time. Conventional routing algorithms designed for static or low mobility networks are inadequate in these fast changing environments, leading to packet loss and increased communication delay. To overcome these challenges, specialized vehicular routing protocols have been developed to accommodate mobility patterns and ensure timely data delivery. The Greedy Perimeter Stateless Routing (GPSR) protocol is one of the most efficient solutions, leveraging geographical positioning to forward packets to the nearest node based on destination coordinates rather than maintaining full routing tables. This stateless nature reduces network overhead and improves scalability, making GPSR particularly suitable for dense vehicular environments. The Ad hoc On Demand Distance Vector (AODV) protocol, in contrast, creates routes only when necessary, conserving bandwidth in sparse or highly mobile scenarios. Despite its adaptability, AODV can incur route discovery delays during frequent topology shifts. To address this, more advanced hybrid models have been introduced most notably, the Heuristic Reliable Low Latency Intelligent Geographic Routing (HRLLIGR) protocol, which incorporates AI and heuristic decision making to predict optimal routes, enhance reliability, and reduce end to end communication latency [18].

Beyond routing, data management in V2V networks has evolved through the integration of edge computing and distributed ledger technologies, significantly improving both efficiency and transparency. Edge driven data management frameworks process and analyze vehicular sensor data locally at edge nodes or RSUs, minimizing reliance on cloud servers and substantially reducing transmission latency. This local processing also ensures faster decision making, which is critical for applications like collision avoidance and CACC. Furthermore, block chain based distributed ledgers are being adopted to provide secure, tamper proof, and transparent data storage, enabling accurate fault diagnosis and auditability of vehicular transactions [19]. Complementing these developments, AI enhanced routing algorithms utilize ML models to forecast congestion, predict link stability, and perform intelligent load balancing across multiple communication channels. By dynamically adapting to environmental and network changes, these algorithms maintain optimal Quality of Service (QoS) while reducing packet loss and jitter. Collectively, the convergence of AI assisted routing, edge computing, and block chain based data integrity mechanisms is revolutionizing V2V communication, paving the way for autonomous, self optimizing, and resilient vehicular networks capable of meeting the stringent requirements of future intelligent transportation systems.

7. Energy Efficiency and Optimization

Energy optimization is a growing priority in sustainable vehicular systems. AI based power control dynamically adjusts transmission rates based on network load [20]. Green computing principles, solar powered RSUs, and energy harvesting sensors reduce carbon footprints.V2V systems also use sleep scheduling to deactivate idle transmitters, reducing energy waste without compromising safety critical communication.

8. Security in V2V Communication

Security in V2V Communication is a critical concern as vehicles continuously exchange safety critical data that influence driving behavior, navigation decisions, and accident prevention measures. Given the open, decentralized, and mobile nature of VANETs, ensuring the confidentiality, integrity, and authenticity of transmitted information is paramount. Vulnerabilities in this communication model expose systems to diverse attack vectors such as spoofing, Sybil, eavesdropping, and denial of service (DoS) attacks, which can cause severe disruptions to traffic operations or even compromise passenger safety [21]. In a spoofing attack, an adversary impersonates a legitimate vehicle to send falsified location or velocity information, potentially triggering unnecessary evasive actions. Similarly, Sybil attacks enable a single malicious entity to create multiple fake identities, thereby distorting routing tables or congesting the network. DoS attacks, on the other hand, overwhelm communication channels, preventing legitimate vehicles from exchanging vital data in real time. To counter these risks, modern vehicular systems employ a multi layered security framework combining cryptographic encryption, trust management, and AI based anomaly detection. Cryptographic mechanisms such as Elliptic Curve Cryptography (ECC) and Public Key Infrastructure (PKI) ensure secure message authentication and integrity, while pseudonym based certificates help maintain user privacy without compromising traceability. Trust management models dynamically assess node behavior, assigning reputation scores to detect and isolate malicious participants. Meanwhile, ML driven Intrusion Detection Systems (IDS) analyze communication patterns to identify deviations indicative of cyber-attacks. Furthermore, emerging block chain based decentralized architectures provide tamper proof transaction records, enhancing transparency and eliminating single points of failure. Collectively, these measures establish a resilient security framework that safeguards vehicular networks from internal and external threats, ensuring the reliable and secure functioning of V2V communication within intelligent transportation ecosystems.

9. V2V Security Options and Mechanisms

V2V Security Options and Mechanisms are essential to maintaining the integrity, confidentiality, and trustworthiness of vehicular communications in increasingly complex and interconnected ITS. The foundation of secure V2V communication lies in cryptographic and authentication techniques, which ensure that transmitted messages originate from legitimate sources and remain unaltered during transit. Elliptic Curve Cryptography (ECC) and Public Key Infrastructure (PKI) are two of the most widely used methods for securing vehicular data exchange due to their balance of efficiency and robustness. ECC provides high levels of encryption strength with shorter key lengths, making it ideal for computationally constrained vehicular systems, while PKI offers a hierarchical trust model enabling mutual authentication between nodes, digital signatures, and secure key distribution [22]. Together, these systems prevent unauthorized access, man in the middle attacks, and message tampering. However, as vehicular systems evolve toward real time decision making, static cryptographic schemes alone are insufficient to address emerging zero day threats and dynamic intrusion attempts. To address this, Tiny Machine Learning (TinyML) based IDS have been developed to perform on device anomaly detection. These lightweight AI models continuously monitor network traffic and vehicular behavior to identify deviations that indicate possible cyber intrusions, enabling rapid, autonomous responses without the need for extensive cloud infrastructure. This fusion of lightweight cryptography and edge based AI intrusion detection enhances the adaptive resilience of vehicular networks against complex attacks.

In addition to cryptographic and AI driven approaches, new security paradigms such as block chain, privacy preservation mechanisms, and adaptive safe state systems are revolutionizing the reliability and transparency of V2V communication. Block chain frameworks offer decentralized trust management by recording vehicular transactions and communication events in immutable distributed ledgers, ensuring that all data exchanges are transparent, verifiable, and resistant to tampering [23]. This distributed consensus model effectively eliminates single points of failure common in traditional centralized security systems. Furthermore, to maintain user confidentiality, privacy preserving technologies like Zero Knowledge Proofs (ZKPs) and dynamic pseudonymization are integrated into V2V architectures, allowing data verification without exposing sensitive personal or vehicular identity details. Complementing these, adaptive safe state systems driven by AI act as a final line of defense by autonomously overriding malicious or unsafe control instructions, thereby maintaining operational stability even under attack conditions. These systems utilize continuous environmental awareness and contextual reasoning to ensure that vehicle control mechanisms revert to a secure, fail safe mode when irregular activities are detected. Collectively, the combination of cryptographic assurance, AI enhanced anomaly detection, decentralized block chain trust, and privacy preservation forms a holistic, multi layered defense strategy. This integrated security architecture not only fortifies vehicular networks against present cyber threats but also provides a scalable and future ready foundation for secure V2V communication within emerging autonomous and intelligent transportation ecosystems.

10. Performance Evaluation Metrics

Performance metrics include:

- **Packet Delivery Ratio (PDR)**
- **Latency**
- **Throughput**
- **Energy Consumption**
- **Security Overhead** [25]

AI-assisted auto optimization helps maintain consistent quality across networks.

V2V communication has emerged as a critical enabler of modern ITS, providing the foundation for cooperative, connected, and automated mobility. By allowing vehicles to exchange real time data such as speed, braking intention, and hazard alerts V2V dramatically enhances situational awareness and supports applications like collision avoidance, adaptive platooning, and cooperative lane merging [7]. Communication technologies such as DSRC and C V2X/5G offer the low latency and high reliability needed for these safety critical interactions, while the integration of multi sensor perception and onboard AI further improves decision making accuracy and responsiveness [8], [9].

The evolution of vehicle architecture, incorporating powerful onboard units (OBUs), edge computing systems, and standardized communication stacks, has accelerated the deployment of scalable and resilient V2V frameworks. Edge assisted processing reduces dependency on remote servers and minimizes communication delays, enabling vehicles to respond quickly to dynamic traffic conditions [10], [11]. Furthermore, advanced capabilities in 5G NR V2X such as network slicing, beamforming, and multi hop communication support dense traffic environments and real time cooperative perception across diverse road scenarios [13], [14].

However, several challenges continue to hinder widespread V2V adoption. Security remains one of the most pressing concerns due to vulnerabilities such as spoofing, Sybil attacks, and jamming, which can compromise safety critical messaging [21]. To mitigate these threats, modern systems integrate ECC based encryption, PKI driven authentication, blockchain supported trust management, and TinyML intrusion detection frameworks that ensure message integrity and vehicle privacy [22], [23]. Interoperability across DSRC, C V2X, and emerging 6G platforms also requires coordinated standardization efforts, while regulatory issues related to spectrum allocation and liability must be addressed to support global deployment [18], [19], [20].

11. Conclusion

Communication technologies in V2V systems enable real-time, reliable data exchange between vehicles to support safety and cooperative driving. The primary technology historically used is DSRC, based on IEEE 802.11p, which provides low-latency communication ideal for safety alerts and cooperative maneuvers. However, DSRC’s range limitations and congestion issues led to the emergence of C-V2X, introduced in 3GPP Release 14. C-V2X supports both device-to-device (PC5) and network-assisted communication (Uu interface), offering significantly higher reliability and coverage. With 5G NR-V2X, vehicles gain ultra-low latency, high data rates, network slicing, and support for dense traffic environments. Additional technologies include Li-Fi, which uses visible light for secure short-range communication, and Reconfigurable Intelligent Surfaces (RIS) that enhance signal propagation in urban areas. Together, these technologies form a robust communication ecosystem enabling cooperative perception, autonomous driving, and efficient traffic management.

References

1. J. B. Kenney, “Dedicated short-range communications (DSRC) standards in the United States,” Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

2. H. Hartenstein and K. P. Laberteaux, “A tutorial survey on vehicular ad hoc networks,” *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, Jun. 2008.
3. 5G Automotive Association, “C-V2X use cases, technical requirements, and service level expectations,” *5GAA White Paper*, 2022.
4. M. Gerla, E. K. Lee, G. Pau, and U. Lee, “Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds,” *IEEE World Forum on Internet of Things (WF-IoT)*, pp. 241–246, Mar. 2014.
5. K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, “Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2377–2396, 2015.
6. X. Ge, Z. Li, S. Li, and L. Wang, “5G and beyond for intelligent transportation systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2714–2728, May 2021.
7. A. Vinel, “3GPP LTE versus IEEE 802.11p/WAVE: Which technology is able to support cooperative vehicular safety applications?,” *IEEE Wireless Communications Letters*, vol. 1, no. 2, pp. 125–128, Apr. 2012.
8. M. Sepulcre, J. Gozalvez, and J. Harri, “Congestion and awareness control in cooperative vehicular systems,” *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1260–1279, Jul. 2011.
9. A. Bazzi, B. M. Masini, A. Zanella, and M. Zorzi, “On the performance of IEEE 802.11p and LTE-V2V for the cooperative awareness of connected vehicles,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10419–10432, Nov. 2017.
10. F. Qu, F. Y. Wang, and L. Yang, “Intelligent transportation spaces: Vehicles, traffic, communications, and beyond,” *IEEE Communications Magazine*, vol. 48, no. 11, pp. 136–142, Nov. 2010.
11. H. Peng and Q. Chen, “Performance evaluation of 5G-V2X for vehicular communications,” *IEEE Access*, vol. 9, pp. 13430–13442, Jan. 2021.
12. M. Boban, J. Barros, and O. K. Tonguz, “Geometry-based vehicle-to-vehicle channel modeling for large-scale simulation,” *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4146–4164, Nov. 2014.
13. S. Rajagopal, R. D. Roberts, and S. K. Lim, “IEEE 802.15.7 visible light communication: Modulation schemes and dimming support,” *IEEE Communications Magazine*, vol. 50, no. 3, pp. 72–82, Mar. 2012.
14. Q. Wu and R. Zhang, “Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network,” *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, Jan. 2020.
15. A. Al-Dulaimi, X. Zhang, and H. Chien, “6G communications: Challenges and opportunities,” *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 22–31, Dec. 2020.
16. J. Qiu, Z. Feng, and M. Liu, “Quantum secure vehicular communications: A survey,” *IEEE Access*, vol. 10, pp. 14532–14549, Feb. 2022.
17. M. Al-Qutayri and J. Gomez, “Architectures and key technologies for connected and autonomous vehicles: A survey,” *IEEE Access*, vol. 8, pp. 185064–185083, Oct. 2020.
18. C. Campolo, A. Molinaro, and R. Scopigno, “From today’s VANETs to tomorrow’s planning and the advent of 5G,” *Vehicular Communications*, vol. 2, no. 3, pp. 134–144, 2015.
19. J. Contreras and S. Zeadally, “Intelligent transportation system security and privacy: Threats and countermeasures,” *IEEE Wireless Communications*, vol. 27, no. 3, pp. 102–108, Jun. 2020.
20. S. Sharma, S. A. Hossain, and P. K. Mahanti, “Energy-efficient communication protocols in vehicular networks: A survey,” *IEEE Access*, vol. 9, pp. 122532–122549, Sep. 2021.
21. M. Raya and J. P. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

22. A. B. R. Shinde, “Lightweight authentication and encryption in vehicular ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 11234–11245, Aug. 2022.
23. Y. Zhang, J. Kang, and D. Lin, “Block chain-based secure data sharing for vehicular edge networks,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110–9121, Sep. 2019.
24. S. Sommer, R. German, and F. Dressler, “Simulation of vehicular networks using OMNeT++,” *Proceedings of the 1st International Conference on Simulation Tools and Techniques (Simutools)*, pp. 1–8, 2008.
25. T. Osafune, L. Lin, and M. Lenardi, “Performance evaluation of vehicular ad hoc networks,” *IEEE Vehicular Technology Conference*, vol. 2, pp. 2110–2114, 2006.
26. European Commission, “5G-CARMEN: Piloting cross-border 5G V2X connectivity for connected and automated mobility,” *Horizon 2020 Project Report*, 2024.