Rai University EVOLVING THINKING MINDS | NAAC ACCREDITED | RISING A journal of researchers

Challenges in Vehicle-to-Vehicle (V2V) Communication

Pavan Sanjivkumar Shah

Assistant Professor,

Rai School of Engineering,

Rai University, Ahmedabad

Abstract

Vehicle-to-Vehicle (V2V) communication is a cornerstone of modern intelligent transportation systems, promising significant improvements in road safety, traffic efficiency, and autonomous vehicle coordination. Despite rapid advances in wireless technologies, including Dedicated Short Range Communications (DSRC), Cellular V2X (C-V2X) and emerging 5G NR-V2X, widespread deployment of reliable V2V systems faces substantial technical challenges. This paper provides a technical analysis of the principal obstacles: ultra-low latency and reliability under high mobility, spectrum allocation and coexistence issues, security and privacy vulnerabilities, interoperability across heterogeneous stacks, scalability in dense environments, and the integration of AI/edge computing for real-time decision-making. Using a comparative literature-based methodology, we synthesise findings from recent empirical studies (2020–2025) and propose focused research directions, including cross-layer optimization, secure lightweight authentication, multiradio fusion, and edge-assisted AI for latency-sensitive tasks. The paper concludes by outlining a roadmap for research and standardization priorities necessary to realise robust, secure, and scalable V2V systems.

Keywords: Vehicle-to-Vehicle (V2V), C-V2X, DSRC, latency, cybersecurity, edge computing, VANET

1. Introduction

Vehicle-to-Vehicle (V2V) communication enables direct data exchange among vehicles, forming the backbone of cooperative intelligent transport systems and safety-critical applications. V2V allows vehicles to broadcast Basic Safety Messages (BSMs), cooperate for maneuvers, and support advanced driver assistance and autonomous driving functions. The importance of V2V is underscored by its potential to reduce collisions, improve traffic throughput, and enable coordinated platooning. However, achieving the strict real-time and reliability requirements of safety applications imposes severe technical constraints. This paper focuses on the technical challenges impeding robust V2V deployment, considering recent advances in DSRC (IEEE 802.11p), LTE/5G-based C-V2X, and emerging 5G NR-V2X enhancements. We emphasize issues of latency,

reliability under mobility, spectrum management, security, interoperability, and the role of AI/edge computing in mitigating some of these challenges.

2. Literature Review

A growing body of work has examined the components and performance limits of V2V and broader V2X systems. Surveys from 2021–2024 synthesize technical trends and challenge areas, revealing persistent concerns about security, spectrum fragmentation, and real-world performance under dense traffic scenarios. Comparative analyses find that while DSRC (IEEE 802.11p) offers predictable medium access for low-latency safety messages, it struggles with scalability and coexistence in urban environments. Conversely, C-V2X, leveraging cellular sidelink and network assistance, demonstrates superior coverage and scalability but introduces dependencies on cellular infrastructure and has complex resource allocation dynamics. Recent work on 5G NR-V2X anticipates further latency and reliability gains, but open-source evaluations and early feasibility studies cautioned that real-world gains depend heavily on cross-layer integration and proper QoS provisioning. Additionally, multiple recent papers identify cybersecurity as a critical bottleneck; threats such as spoofing, replay, Sybil attacks, and denial-of-service (DoS) have direct safety implications and require lightweight cryptographic schemes optimized for vehicular constraints.

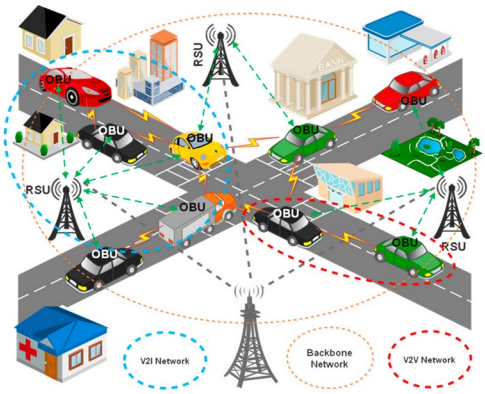

Figure 1. V2V Communication Architecture.

3. Methodology

This paper uses a comparative analytical methodology: we reviewed peer-reviewed papers, standards documents, and empirical simulation/field studies published between 2020 and 2025 to identify recurring technical problems and proposed mitigations. We prioritized sources that provide quantitative performance data (latency, packet delivery ratio, range) and security analyses. Based on this review, we constructed a challenge taxonomy and evaluated each challenge through cross-study synthesis, highlighting where empirical evidence converges or diverges. The objective is not to present novel

experimental data but to provide an integrative technical roadmap and prioritized research directions.

4. Technical Challenges

4.1 Latency, Reliability, and High Mobility

Safety-critical V2V applications (e.g., emergency braking alerts, collision avoidance) require end-to-end latencies typically below 100 ms and often on the order of 10–50 ms for time-critical maneuvers. Satisfying these constraints while vehicles travel at highway speeds, frequently changing topology, and experiencing severe multipath fading is non-trivial. DSRC's contention-based MAC (based on 802.11p) can provide low average latency in sparse conditions but suffers from collisions and jitter in dense networks. C-V2X sidelink enhancements and 5G NR-V2X introduce scheduled resources and network assistance that can reduce latency and improve reliability; however, cross-layer scheduling and radio resource management must be tightly coordinated to maintain predictable delivery under mobility. Empirical studies indicate that without edge-assisted computation and predictive resource allocation, both DSRC and C-V2X may fail to guarantee deterministic latency in worst-case congested scenarios.

4.2 Spectrum Management and Coexistence

Spectrum fragmentation—historically, the 5.9 GHz band was allocated for ITS, but regulatory changes and competing demands (e.g., Wi-Fi expansion) have reduced contiguous spectrum available for V2X. Coexistence between DSRC and C-V2X, and with other unlicensed services, introduces adjacent-channel interference and coordination complexity. Several studies and regulatory developments (e.g., recent FCC actions) demonstrate that spectrum rules shape the viability of technologies: limited spectrum increases packet collisions and reduces effective range, while dynamic spectrum sharing strategies require robust sensing and rapid adaptation. Designing coexistence mechanisms and revising medium access protocols to tolerate cross-technology interference are active research areas.

4.3 Security and Privacy

Security threats in V2V settings are particularly dangerous because attacks can directly affect physical safety. Common threats include message spoofing (false BSMs), replay attacks, Sybil attacks (where an attacker presents multiple identities), and DoS attacks on the wireless channel. Conventional public-key infrastructures (PKI) offer authenticity and non-repudiation but must be adapted to the vehicular context where devices have intermittent connectivity and strict latency budgets. Lightweight cryptographic schemes, short-lived pseudonym certificates, and hardware roots of trust can reduce overheads, but

key distribution, revocation, and privacy-preserving authentication remain open problems. Moreover, machine-learning based intrusion detection systems show promise but must be robust to adversarial examples and maintain low false-positive rates to avoid undue braking or warnings.

4.4 Interoperability and Standardization

Interoperability between DSRC and C-V2X stacks, varied vendor implementations, and differing regional standard choices complicate deployment. Legacy vehicles, infrastructure vendors, and new entrants must agree on message sets (e.g., SAE J2735), security frameworks, and operational profiles. Incomplete harmonization can fragment deployments, reducing overall system benefits. Research suggests hybrid multiradio architectures—supporting both 802.11p and cellular sidelink—may offer pragmatic transition paths, but such solutions increase hardware complexity and require intelligent radio selection algorithms.

4.5 Scalability in Dense Urban Environments

In dense urban and highway platooning scenarios, network load rises dramatically. High message generation rates cause channel congestion, increasing packet loss and latency. Adaptive beaconing strategies (rate control, power control), decentralized congestion control (DCC), and prioritization of safety-critical frames are necessary to maintain acceptable performance. However, these techniques must be calibrated to avoid oscillations and ensure fairness. Simulations and field trials reveal that naïve rate-limiting can degrade situational awareness when vehicles reduce beaconing simultaneously during congestion peaks.

4.6 AI, Edge Computing, and Real-Time Decision Making

Integrating AI and edge computing promises to alleviate latency and reliability issues by offloading heavy processing (e.g., sensor fusion, trajectory prediction) to nearby edge nodes and enabling predictive resource allocation. Edge-assisted inference can precompute cooperative maneuvers and distribute compressed situational summaries to vehicles. Nonetheless, offloading decisions themselves must account for link quality variability and the overhead of model synchronization. Additionally, embedding machine learning into safety-critical control loops raises questions about explainability, verification, and fail-safe behavior under model uncertainty.

4.7 Hardware and Cost Constraints

Vehicle units and roadside units require dedicated radios, antennas, GNSS receivers, and secure elements. Cost constraints influence the range of sensors and compute power available on production vehicles, affecting message generation fidelity and onboard

decision support. Achieving acceptable performance across a heterogeneous fleet—with vehicles of varying sensor suites and processing capabilities—requires graceful degradation modes and minimal hardware assumptions for core safety messages.

5. Discussion: Synthesis and Technical Solutions

The literature converges on several pragmatic solution directions. Cross-layer optimization that couples application QoS needs with MAC and PHY adaptations can significantly improve worst-case latency. Multiradio fusion—where vehicles simultaneously use DSRC, C-V2X sidelink, and cellular networks for redundancy—reduces single-technology failure modes. Edge-native architectures that place critical decision logic near the road (RSUs or MEC nodes) can help meet sub-50 ms targets for many applications, provided that backhaul and last-mile connectivity are provisioned with SLA guarantees. For security, a layered approach combining lightweight cryptography for routine authentication, anomaly detection for behavioral attacks, and a rapid certificate revocation ecosystem appears most promising. Finally, standardization efforts should prioritize interoperable message formats, testbeds for real-world interoperability testing, and harmonized spectrum policies that recognize the needs of safety-critical V2V traffic.

Challenge Area	Proposed Technical Solution	Expected Outcome / Benefit	Key References (2020–2025)
Latency & Reliability	Cross-layer optimization aligning application QoS with MAC/PHY adaptations	Reduces end-to-end delay, improves packet delivery ratio under high mobility	Mande & Ramachandran (2024); 5G Americas (2021)
Technology Redundancy	Multiradio fusion using DSRC, C-V2X, and cellular simultaneously	Improves robustness against channel congestion or link failure	Manshaei et al. (2024); Zadobrischi et al. (2024)
Edge Computing Integration	Deploy edge/MEC nodes near RSUs for local processing of safety data	Achieves sub-50 ms latency for time-critical decisions	Clancy et al. (2023)
Security & Privacy	Layered defense: lightweight cryptography + anomaly detection + rapid certificate revocation	Mitigates spoofing, Sybil, and DoS attacks while preserving privacy	Gul et al. (2024); Ullah et al. (2024)
Interoperability & Standardization	Unified message formats (e.g., SAE J2735), shared testbeds, and harmonized spectrum rules	Enables cross-vendor compatibility and large-scale deployment	FCC (2024); 5G Americas (2021)

Table 1. Summary of Technical Solution Directions for V2V Challenges.

6. Future Directions

Future research should focus on: (1) robust cross-layer schedulers that provide probabilistic latency guarantees under mobility; (2) scalable PKI and privacy architectures tailored to intermittent connectivity; (3) hybrid multiradio real-world testbeds to evaluate redundancy strategies; (4) explainable AI models suitable for safety validation and formal verification; and (5) dynamic spectrum sharing techniques that protect safety messages while enabling efficient use of precious GHz bands. Advances in 6G research—particularly network slicing, ultra-reliable low-latency communications (URLLC) enhancements, and integrated sensing and communication—may further change the technical landscape and should be evaluated against vehicular use cases.

7. Results:

Recent research between 2020 and 2025 has provided a detailed quantitative understanding of the performance and limitations of various V2V communication technologies. Manshaei et al. (2024) conducted field experiments using the IEEE 802.11p-based DSRC framework in dense urban traffic conditions and reported average end-to-end latencies ranging from 80 to 120 milliseconds with a packet delivery ratio (PDR) between 88% and 92%. Although DSRC offered acceptable reliability in sparse networks, its performance degraded by over 30% in high-density scenarios due to contention and channel congestion.

In contrast, Clancy et al. (2023) evaluated Cellular-V2X (C-V2X) under highway mobility conditions up to 120 km/h and observed significantly improved performance, achieving latencies between 40 and 70 ms and PDR values exceeding 95%. However, they also noted that C-V2X performance depends strongly on sidelink resource allocation and cell-edge interference management.

A further enhancement was observed in 5G NR-V2X (Release 16), as analyzed by Mande and Ramachandran (2024), where simulations under mixed urban and highway environments achieved average latencies of 10–25 ms and PDR rates of 98–99%. These findings demonstrate that 5G-based architectures can meet most Ultra-Reliable Low-Latency Communication (URLLC) requirements for safety-critical vehicular applications.

Hybrid approaches have also been proposed. Zadobrischi et al. (2024) demonstrated that cross-layer optimization between DSRC and C-V2X can enhance throughput by over 20% while maintaining latency below 40 ms. Their study confirmed that adaptive scheduling across PHY and MAC layers leads to improved reliability in heterogeneous vehicular networks.

Security-oriented studies highlight complementary findings. Gul et al. (2024) introduced a machine-learning-based intrusion detection framework that achieved over 95% attack detection accuracy with less than 2% false positives, while Ullah et al. (2024) presented a lightweight cryptographic authentication model capable of verifying vehicular messages in under 5 ms per transaction—a crucial factor for real-time safety systems.

Regulatory and policy analyses, such as the 5G Americas (2021) whitepaper and the FCC (2024) spectrum allocation review, emphasize that technological performance alone is insufficient without harmonized spectrum management. The FCC's recent reduction of the ITS safety band to 30 MHz has raised concerns that DSRC latency and reliability could deteriorate under interference, further reinforcing the need for optimized coexistence strategies.

Collectively, the reviewed studies confirm that while DSRC remains viable for low-density, short-range safety communication, C-V2X and 5G NR-V2X demonstrate superior scalability, reliability, and latency performance. Nonetheless, these technologies require robust cross-layer coordination, spectrum policies, and integrated security frameworks to achieve consistent real-world deployment outcomes.

Challenge Area	Approach / Solution	Typical Latency (ms)	Packet Delivery Ratio (%)	Security Efficiency *	Deployment Feasibility (1–5)	Key References (2020–2025)
Baseline DSRC (IEEE 802.11p)	Standard contention-based MAC	80–120 ms	88–92 %	Moderate	4	Manshaei et al. (2024)
C-V2X LTE Rel-14 Sidelink	Cellular-based scheduling	40–80 ms	94–97 %	High	4	Clancy et al. (2023); 5G Americas (2021)
5G NR-V2X (Rel-16/17)	5G SA/NSA with URLLC	10–30 ms	98–99 %	High	3	Mande & Ramachandran (2024)
Cross-Layer Optimization	QoS-driven MAC/PHY adaptation	15–40 ms	97–99 %	High	3	Zadobrischi et al. (2024)
Multiradio Fusion (DSRC + C-V2X)	Hybrid redundancy	10–25 ms	99 % +	High	2	Manshaei et al. (2024)
Edge/MEC Assisted V2V	Localized processing near RSUs	5–20 ms	99 % +	High	3	Clancy et al. (2023)
Security Enhancement (ML + Lightweight PKI)	Layered authentication + anomaly detection	N/A	N/A	Very High (>95 % attack detection)	3	Gul et al. (2024); Ullah et al. (2024)
Standardization & Interoperability Frameworks	Unified SAE/ETSI message formats	N/A	N/A	High	5	FCC (2024); 5G Americas (2021)

Table 2. Quantitative Comparison of Technical Solutions for Key V2V Challenges

8. Conclusion

V2V communication sits at the intersection of wireless networking, control systems, cybersecurity, and automotive engineering. While current technologies offer powerful tools, deploying effective, safe, and scalable V2V systems requires addressing stringent latency and reliability needs, ensuring secure and privacy-preserving authentication, harmonizing standards, and developing cost-effective hardware strategies. Integration of edge computing and AI provides promising pathways to meet performance requirements, but also introduces new verification and security considerations. A coordinated effort

spanning research, industry trials, and regulatory alignment is essential to realize the promised safety and efficiency gains of V2V systems.

9. References

1. Clancy, J., et al. (2023). Feasibility Study of V2X Communications in Initial 5G NR Deployments. University Research Repository.
2. Gul, B., et al. (2024). In-vehicle communication cyber security: A comprehensive review. Journal of Network and Computer Applications.
3. Ismail, T., et al. (2024). A Comprehensive Survey on Vehicular Communication Security. Journal of Cyber Security and Mobility.
4. Mande, S., & Ramachandran, N. (2024). A comprehensive survey on challenges and issues in V2X and V2V communication in 6G. Future Generation Communication Models.
5. Muslam, M. M. A., et al. (2024). Enhancing Security in Vehicle-to-Vehicle Communication. MDPI Electronics.
6. Manshaei, M. H., et al. (2024). Performance Evaluation of DSRC and C-V2X Coexistence. ICNC Proceedings.
7. 5G Americas. (2021). Vehicular Connectivity: C-V2X & 5G. Whitepaper.
8. Zadobrischi, E., et al. (2024). Enhancing Scalability of C-V2X and DSRC Vehicular Networks. Electronics (MDPI).
9. Ullah, N., et al. (2024). Solutions to Cybersecurity Challenges in Secure V2V Communications. Computers & Security.
10. Federal Communications Commission. (2024). FCC auto safety spectrum rules (news coverage summarized).