Proceedings of CONF-FMCE 2025 Symposium: Semantic Communication for Media Compression and Transmission
DOI: 10.54254/2755-2721/2025.GL28988

V2X Technology Transformation and Challenges for Autonomous Driving Safety

Enrui Liu

Dongguan Hanlin High School, Dongguan, China
eerrr_867@qq.com

Abstract. In recent years, the level of vehicle intelligence has significantly increased, driven by the rise of autonomous driving technology. This article, based on the rise of autonomous driving, explores the advantages and challenges of V2X technology compared to single-vehicle intelligent technologies, providing insights for future V2X development in areas such as cybersecurity, latency system improvements, and regulatory development. This study aims to uncover the limitations of single-vehicle intelligent technologies and explore future directions for V2X development. Using a literature review, case studies, and comparative analysis, this study systematically examines the progress and shortcomings of V2X in autonomous driving. By comparing autonomous driving safety architectures before and after V2X implementation, the relationship between V2X and single-vehicle intelligent technologies becomes clearer: V2X is an expansion and extension of single-vehicle intelligent technologies, not a replacement. This article highlights the advantages of V2X technology and identifies potential cybersecurity risks, communication latency, actuator-related risks, and ethical risks. This article aims to provide insights for the future development of autonomous driving.

Keywords: V2X technology, safety architecture, vehicle intelligence, autonomous driving

1. Introduction

In recent years, autonomous driving has become a hot topic in the automotive industry. The shift from single-vehicle intelligent technology to vehicle-to-everything (V2X) technology provides safer technical support for autonomous driving, but it also faces numerous challenges. Therefore, exploring the challenges of V2X technology is of great significance. This article first introduces V2X technology, compares and contrasts V2X technology before and after its deployment, and addresses three issues facing V2X technology: communication latency, network security, and ethical considerations. This article aims to analyze V2X before and after its deployment, identify its "double-edged sword" potential, and provide references for its future technological evolution and risk mitigation, thereby providing theoretical support for the further development of autonomous driving.

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2025.GL28988

2. Technical foundation of V2X perception

The technology that enables vehicles to exchange information with all external entities is called "V2X technology." It aims to break the perceptual barriers of single-vehicle skills and build a collaborative perception network with V2V, V2P, V2I, V2N and other technologies. In recent years, V2X technology has been used to provide safety technology for autonomous driving because it can effectively expand the perception range of vehicles and people. It can provide a "God's eye view" for autonomous driving technology and transmit a variety of information. Its functions are shown in the figure below. As shown in Table 1 [1].

Table 1. Applications of V2X

V2X (3)	Use case for V2X access when roaming
	Mixed Use Traffic Management
	V2X Minimum QoS

V2X technology also enables information sharing between vehicles, addressing the challenges caused by weather restrictions. This inter-vehicle perception provides a more accurate, safer, and more comprehensive environmental model for autonomous driving. V2X is not a new technology; its origins date back to the late 20th century, with a milestone in its development in 2004. Since then, the investment in V2X technology has revolutionized the automotive industry.

3. Autonomous driving safety architecture before V2X application

Before the introduction of V2X, the core safety architecture for autonomous driving relied on "single-vehicle intelligent technology." In terms of system architecture, the ego-only approach was proposed, emphasizing complete vehicle self-sufficiency in autonomous driving. While practical, this approach, relying solely on onboard sensing and computing, is insufficient for autonomous driving and has limited application scenarios [2]. Ego-Vehicle Intelligence (EVI) technology simply uses onboard sensors (such as cameras and ultrasonic radar) to acquire road information. High-precision maps and GPS are then used to determine positioning, which is then transmitted to the onboard platform for computation and ultimately vehicle control (This is a practical path: perception → positioning → computation → control). However, EVI technology has numerous limitations, significantly increasing the risks of autonomous driving. The sensitivity of onboard sensors can decrease in severe weather (heavy rain, typhoons, hail). This means that cities prone to inclement weather are difficult to deploy this technology. It also lacks the ability to quickly respond to dynamic objects (such as suddenly appearing pedestrians or a suddenly blocked windshield). Under such conditions, the sensor's reflex arc efficiency is reduced. Sometimes, even on sunny days, strong light can affect the sensor's judgment of the environment and may not be able to accurately identify road conditions. Furthermore, the limited range of information it acquires significantly reduces driving efficiency (making it difficult to accurately judge traffic flow, leading to traffic jams). This inability to accurately judge unexpected scenarios can easily lead to delays or even failures in the entire technology chain. While EVI technology undoubtedly has a theoretical ceiling for safety performance, its inability to provide a comprehensive and accurate environmental model makes it an unsuitable solution for supporting autonomous driving.

DOI: 10.54254/2755-2721/2025.GL28988

4. Enhanced autonomous driving safety after V2X application

The emergence and continuous optimization of V2X technology have broken the monopoly of single-vehicle intelligent technology, becoming the most suitable technology for supporting autonomous driving in today's society and ushering it into an unprecedented era. The introduction of V2X has evolved the safety architecture of autonomous driving into a "vehicle-road-rain" model. The technology's most notable capabilities are "beyond-line-of-sight perception" and "collaborative decision-making." Beyond-line-of-sight perception expands the range of perception (for example, by including information between vehicles and on road surfaces), effectively compensating for the incomplete information provided by single-vehicle sensors due to physical limitations. Collaborative decision-making frees vehicles from being isolated entities, enabling information sharing (for example, enabling faster response to accidents or sudden road collapses, and preventing accidents through inter-vehicle information exchange when vision is obstructed). This provides a better understanding of road conditions, improving driving efficiency (for example, allowing drivers to avoid rush hour traffic and save significant commuting time) and ensuring safer driving. Overall, V2X technology complements traditional sensors. Data transmission relies entirely on the application layer V5 interface, providing an additional layer of data security [3]. This expanded perception range allows autonomous driving to proactively prepare for the next step, a leap from just seeing danger emerging to anticipating it and reacting in advance. This reduces accidents caused by uncertainty and allows for better handling of extreme situations. LTE-V2X technology provides security for applications that are highly sensitive to latency, enabling complete information exchange within milliseconds [4].

5. Functional safety challenges, communication delays and actuator response

While the introduction of V2X technology has undoubtedly injected new life into autonomous driving, it also faces numerous unavoidable challenges. One of the most obvious is communication latency: end-to-end communication latency, combined with the inherent delay of the vehicle's drive-by-wire system, can result in a total delay exceeding the critical time window for specific safety scenarios, potentially degrading safety system performance and even introducing new safety risks. Current systems cannot fully guarantee that expected V2X technology instructions will be fully implemented before unexpected situations occur. This can lead to delays in the perception system (such as the preceding vehicle suddenly braking or the sudden appearance of a pedestrian), server computation time, and, most critically, the response time between the actual braking force generated and the delay between the decision-making system issuing the braking command and the brake-by-wire system. This problem is not unsolvable. In the paper "Causality-Sensitive Scheduling to Reduce Latency in Vehicle-to-Vehicle Interactions," researchers demonstrate that delay bursts can be addressed or even eliminated through causality-sensitive scheduling. To address this issue, engineers have combined 5G and V2X technologies. V2X leverages 5G for higher network bandwidth and faster information transmission. Combining 5G with edge computing also enables autonomous driving to respond even faster in complex traffic scenarios. However, due to the diverse range of driving scenarios and the susceptibility to unique circumstances, further advancements are needed [5].

DOI: 10.54254/2755-2721/2025.GL28988

6. Cybersecurity challenges

Besides latency issues, V2X's collaborative decision-making capabilities, while benefiting autonomous driving, also pose significant cybersecurity challenges. V2X technology shares information between vehicles, placing it in a relatively open network environment. Now, V2X uses public key infrastructure (PKI) to add a layer of technical protection for V2X4, making data less likely to be tampered with. However, with the popularization of V2X, the network security of vehicles is still in an imperfect state.V2X technology requires direct information exchange between vehicles, so the authenticity and integrity of the information will directly affect the vehicle's decision-making. For example, if one vehicle's system is compromised, the systems of multiple vehicles could also be compromised. User privacy could also be compromised, and the spread of false information could even lead to a series of accidents. In a review of Internet of Vehicles security, the authors categorize cybersecurity into network-level, component-level, and platform-level security. Typical cyber threats, such as eavesdropping, denial of service, and man-in-the-middle attacks, can all threaten the security of autonomous driving [6]. Cybersecurity is a prerequisite for the advancement of V2X technology. Without ensuring network security, collaborative decision-making is out of the question. Cybersecurity requires not only the efforts of users and automakers, but also the joint efforts of the nation and even the world.

7. Ethical issues in autonomous driving

Next, this paper will explore the ethical dilemmas raised by the rise of autonomous driving. The classic "trolley problem" illustrates the differences between autonomous driving and human decision-making. Human drivers rely on subconscious brain reactions, meaning that the responses of thousands of drivers are not necessarily identical. Autonomous driving relies on pre-programmed algorithms, meaning that autonomous vehicles may make the same choices in different situations and at different times. To transform uncertain choices into certain choices, we should discuss the utilitarian and deontological perspectives. This paper develops an ethical trajectory plan to better prepare for all possible scenarios on public roads. Their proposed solution transforms the philosophical question of ethical norms into a mathematical equation, using a more rational approach to treat everyone equally and ensure fairness [7]. Although society has put forward many suggestions on the ethical issues of autonomous driving, there is no real implementation plan so far. Amid the rapid development of autonomous driving, many countries' laws and regulations haven't kept pace. Furthermore, due to cultural diversity, each country has different responses to the question of whether to prioritize protecting vulnerable groups. Therefore, establishing a globally shared decision-making framework is a crucial issue for the future development of autonomous driving.

8. Conclusion

In summary, this article has systematically explored the potential for V2X technology's implementation and the accompanying challenges. While acknowledging the stable and secure technical support it provides for autonomous driving, it also highlights the challenges presented by the "double-edged sword" of V2X's unique capabilities. Communication system delays can paralyze the entire system, and the cybersecurity issues that arise in collaborative decision-making create a trust crisis and raise ethical questions to a new level. The future of autonomous driving requires multifaceted efforts. Regarding functional safety challenges, this article mainly relies on literature

DOI: 10.54254/2755-2721/2025.GL28988

references in its research methods, and has not yet explored in depth whether communication problems can truly be improved using 5G technology. Future autonomous driving research can advance along three key fronts. First, on the technical level, efforts should be made to minimize the potential harm caused by delays through technology, while leveraging the power of computing to minimize delays. Second, on the cybersecurity level, efforts should be made to improve cybersecurity inspection mechanisms and implement multiple layers of protection within the autonomous driving safety system. Third, on the ethical governance level, efforts should be made to ensure that ethical issues are addressed in a manner that facilitates technological solutions. Only through continuous progress on these three fronts can autonomous driving truly achieve large-scale implementation.

References

[1] LI F, FANG J Y, ZHAO L. 3GPP LTE-V2X standard progress and technology introduction [J]. Telecommunication Network Technology, 2016, (06): y.
[2] Yurtsever E, Lambert J, Carballo A, et al. A survey of autonomous driving: Common practices and emerging technologies [J]. IEEE Access, 2020, 8: 5845.
[3] CHEN S Z, HU J L, SHI Y, et al. LTE-V2X vehicular network technology, standards and applications [J]. Telecommunications Science, 2018, 34(4): 1-11.
[4] HUANG Y L, HUANG H P, ZHANG H P. Exploration on the application of Internet of Vehicles technology in automobile autonomous driving [J]. Automobile of the Times, 2025, (08): 16-18.
[5] Hanna J P, Törngren M. Causality-sensitive scheduling to reduce latency in vehicle-to-vehicle interactions [J]. Sensors, 2024, 24(22): 7142. DOI: 10.3390/s24227142.
[6] LI X H, ZHONG C, CHEN Y, et al. A survey on Internet of Vehicles security [J]. Journal of Information Security Research, 2019, 4(3): 17-33. DOI: 10.19363/J.cnki.cn10-1380/tn.2019.05.02.
[7] Geisslinger M, Poszler F, Betz J, et al. Autonomous driving ethics: From trolley problem to ethics of risk [J]. Philosophy & Technology, 2021, 34: 1033-1055.