Theory and Practice of Science and Technology
2025, VOL. 6, NO. 11, 106-110
DOI: 10.47297/taposatWSP2633-456920.20250611

A Review of Research on Internet of Vehicles Communication Technologies and Information Security Mechanisms

Xingyan Liu

Glasgow College, University of Electronic Science and Technology of China, Chengdu, Sichuan, 611731, China

ABSTRACT
Internet of Vehicles (IoV) is a key enabling technology to improve the safety and efficiency of road traffic, which realises intelligent collaboration through the interconnection of Vehicle-to-Everything (V2X). However, IoV faces serious information security threats due to its open communication environment and dynamic network topology. This article aims to systematically review the current research status of core communication technologies and information security mechanisms in the Internet of Vehicles, and focuses on analyzing the collaborative relationship and existing challenges between the two. Through a systematic review of domestic and foreign literature in the past five years, This study clarifies the technological evolution path from Dedicated Short-Range Communication (DSRC) to Cellular Vehicle-to-Everything (C-V2X). And the development context from traditional Public Key Infrastructure (PKI) to security mechanisms such as lightweight authentication and hybrid trust models. Research findings reveal that there are core gaps in the current field, such as the absence of a quantitative model for "communication-security collaboration", performance disputes over lightweight solutions, and insufficient joint optimization for high-density scenarios. Based on this, this paper proposes future research directions such as cross-layer optimization of communication-security, cross-scenario adaptive security architecture, and the integration of new technologies like blockchain and artificial intelligence, with the aim of providing precise guidance for subsequent research.

KEYWORDS
Internet of vehicles; V2X; C-V2X; Information security; Research review

1 Introduction

With the deep integration of information and communication technology, artificial intelligence and the automotive industry, the Internet of Vehicles emerged and quickly became a research hotspot in the global intelligent transportation field. The Internet of Vehicles takes vehicles as intelligent nodes Through Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2V), An intelligent network system that realizes the all-element data interaction and collaborative control of "vehicle-road-cloud-human" through multiple communication modes such as V2P and Vehicle-to-Network (V2N) [1]. Its core objective is to significantly enhance the safety, efficiency and intelligence level of road traffic through efficient and reliable real-time communication.

The unique charm of the IoV lies in its dynamic and open nature, but this precisely constitutes the inherent vulnerability of its security defense. The high-speed movement of vehicles causes the network topology to change rapidly. The instantaneous access of a large number of nodes brings huge pressure to identity authentication and key management, while security-critical applications put forward almost strict requirements for the real-time performance and integrity of messages [2]. Against this backdrop, security threats such as Sybil attacks, Denial of Service (DoS) attacks, message tampering and privacy leaks have emerged one after another, seriously restricting the large-scale deployment of the Internet of Vehicles and the development of advanced autonomous driving applications [3].

Domestic and international scholars have conducted extensive research on the communication technology and security mechanism of the Internet of Vehicles. At the communication technology level, the technical route has undergone a significant evolution from DSRC to C-V2X [1, 4]. At the security mechanism level, the exploration has gradually shifted from the traditional centralized public key infrastructure to directions such as lightweight authentication, distributed trust management, and cross-layer in-depth defense [5-7]. However, existing research either focuses on the performance optimization of a single communication technology or the improvement of specific security protocols, lacking a systematic review and integration of the inherent trade-offs and synergy between "communication performance" and "security strength". At the same time, there are many contradictions and controversies between different studies in terms of technology route selection and performance evaluation conclusions, which need to be clarified urgently.

Therefore, this study aims to fill the above gap and conduct a review of the communication technology and information security mechanism of the Internet of Vehicles with ‘collaborative relationship’ as the core. This article will not only systematically sort out the development trajectory of technology, but also strive to identify the key contradictions and gaps in existing research, and based on this, propose forward-looking and feasible future research directions, providing theoretical references and practical guidance for building a safe, reliable and efficient Internet of Vehicles ecosystem.

2 Literature Review

2.1 The Current Research Status of Internet of Vehicles Communication Technology

Vehicle networking communication technology is the cornerstone for achieving 'vehicle-road-cloud-human' collaboration. Its evolution, from Dedicated Short Range communication (DSRC) to cellular vehicle-to-Everything (C-V2X), has always centered on enhancing key indicators such as latency and reliability. Domestic research shows the characteristics of 'application orientation', with a high focus on the performance of C-V2X in complex environments. Shen Yafei et al. verified the stability of the resource allocation mechanism in C-V2X mode 4 through simulation [8]. Liu Ruipeng et al. further pointed out that security mechanisms need to be integrated into scheduling to defend against malicious nodes [9]. Bo Tao et al. explored link recovery technology based on SDN to enhance robustness [10]. With the development of NR-V2X, Chen Shanzhi, Huang Chenheng and Li Ying all pointed out the necessity of the deep integration of communication and security, and called for the establishment of a cross-layer defense system [1,4,11].

In contrast, foreign research places more emphasis on infrastructure design and standardization, presenting a 'systematic' feature. The IEEE 1609.2 standard implements the binding of messages and security policies through PSID and uses algorithms such as ECDSA to ensure security [12]. Sharma et al. pointed out that traditional encryption is difficult to meet real-time demands and advocated a low-overhead solution based on the trust model [7]. Sun et al. explored the defense effect of secure routing protocols [13]. However, the discussions on the security differentiation design of C-V2X and DSRC abroad are still relatively limited.

2.2 Research Status of Information Security Mechanisms in the Internet of Vehicles

In terms of information security mechanisms, domestic research focuses on lightweight and hardware-level solutions. Wang Xuecong developed a V2X security chip integrating domestic cryptographic algorithms [5]. Zhou Jun et al. designed a hybrid trust model that combines the advantages of centralized and distributed systems [6]. Wu Qian proposed a certificateless public key system, which effectively reduces management overhead [14]. Although these schemes are innovative, large-scale empirical evidence is still insufficient.

Foreign research is dedicated to building a complete defense framework. Sri et al. divided the threat system into four layers and advocated integrating multiple technologies to build a defense system [2]. Kumar et al. proposed a defense-depth framework to achieve dynamic risk assessment through machine learning [3]. In terms of lightweighting and privacy protection, Loussaief et al. focused on the protection of weak nodes, Cheng et al. proposed a hierarchical encryption strategy, and Shahzad et al. developed a server-assisted public key distribution mechanism [15-17].

Most existing studies view communication and security in isolation, lacking quantitative modeling of interaction mechanisms. Moreover, there are disputes over the performance of lightweight solutions and the applicable scenarios of architectures, and there is no unified evaluation benchmark. In addition, there are also deficiencies in the exploration of joint optimization of communication and security in high-density dynamic topologies and high-level autonomous driving scenarios.

3 Method

This research takes the literature review method as its core and combines qualitative analysis, information research and experience summary methods to ensure the systematicness and accuracy of the research.

3.1 Literature research Method

As the core method, the literature research method follows a three-step process of 'keyword search - literature screening - intensive reading of core literature' to obtain data. Search key words including 'car networking communication technology' and 'C - V2X security' 'IoV privacy protection' and so on, a searchable database covering IEEE Xplore academic database, Web of Science and other international and domestic core academic database; The screening criteria are 'published in the last five years' and 'from core journals/conferences' to ensure the timeliness and authority of the literature. Ultimately, 17 key documents and 26 extended core documents were selected for intensive reading to extract key information such as communication technology performance indicators, security mechanism design logic, and research conclusions.

3.2 Qualitative Analysis Method

Qualitative analysis is used to sort out the research context and identify contradictions and gaps: on the one hand,

according to the timeline of 'communication technology evolution (DSRC→LTE-V2X→NR-V2X)' and 'security mechanism development (traditional PKI→ lightweight authentication → distributed trust)', the evolution laws of technologies and mechanisms are qualitatively summarized to clarify the development context; On the other hand, by comparing the differences between domestic and foreign research in terms of core architecture, technical route selection, performance optimization goals, security threats, solution design logic, and performance overhead, core contradictions such as performance disputes over lightweight solutions and conflicts in the adaptation scenarios of centralized and distributed security architectures can be identified, and the applicable boundaries of existing research can be clarified.

3.3 Information Research Method

The information research method is used to extract and integrate key data from literature: for communication technology, core performance indicators such as latency, bandwidth, and reliability are extracted; For security mechanisms, collect key parameters such as authentication time consumption, encryption overhead, and anti-attack capability. Through information sorting and integration, it provides data support for identifying research gaps and comparing the advantages and disadvantages of technologies.

3.4 Experience Summary Method

The experience summary method is used to summarize research characteristics and propose future directions: By extracting the domestic research experience of 'application-oriented and localization breakthroughs' and the foreign research experience of 'theorization and standardization', and in combination with the development trend of the intelligent transportation industry, we sort out future research directions such as 'communication-security collaboration', 'cross-scenario adaptation', and 'integration of new technologies' And in combination with the current technological development trends of 5G/6G, blockchain, artificial intelligence and so on, summarize and demonstrate the feasibility of future research directions.

4 Conclusion

4.1 Main Research Findings

This study takes 'communication-security collaboration' as its core logic, systematically reviews the research status of communication technology and information security mechanisms in the Internet of Vehicles over the past five years, and concludes the following key findings:

First, at the communication technology level, C-V2X has surpassed DSRC to become the mainstream technical route due to its superior scalability, coverage capability and integration advantages with cellular networks. NR-V2X and its integration with technologies such as SDN and edge computing are the key to future evolution. Domestic research focuses on performance optimization of C-V2X in complex scenarios. Foreign research focuses on the formulation of communication standards and theoretical analysis of technical performance, laying the foundation for the interconnection of communication technologies.

Second, at the level of security mechanisms, it has evolved from the traditional PKI system to lightweight authentication, hybrid trust models, and cross-layer defense systems. Domestic research has achieved remarkable results in areas such as the integration of domestic security chips and hybrid key management. Foreign research has formed a relatively complete security defense framework and leads in the panoramic analysis of threats and the exploration of innovative security paradigms.

Overall research shows a development trend from centralized to distributed, from high overhead to lightweight, and from single-point protection to cross-layer in-depth defense, in order to adapt to the resource-constrained and highly dynamic characteristics of the Internet of Vehicles.

Thirdly, 'communication-security collaboration' is the core difficulty and weak link in current research. There are three key gaps in the current research: First, quantitative models of the interaction between communication and security are generally lacking; Second, there are many contradictory conclusions regarding the performance of lightweight solutions and the selection of security architectures. Thirdly, there is a lack of empirical research on extreme scenarios such as high-density dynamic topology and the integration of new technologies.

Table 1 A summary table of Research Achievements on Internet of Vehicles Communication Technology and Security Mechanism

Technical Type	Core Solution	Performance Metrics	Applicable Scenarios
Traditional Communication Technology	DSRC	Latency: 100-200 ms Bandwidth: Up to 27 Mbps Reliability: Medium	Low-speed, low-density traffic scenarios
Mainstream Communication Technology	LTE-V2X	Latency: 50-100 ms Bandwidth: 10-100 Mbps Reliability: High	Urban roads, suburban roads scenarios
Mainstream Communication Technology	NR-V2X	Latency: <50 ms Bandwidth: >100 Mbps Reliability: Extremely High	High-level autonomous driving, platooning scenarios
Auxiliary Communication Technology	SDN	Link recovery time: <100 ms Robustness: High	Complex traffic environments with frequent node anomalies
Auxiliary Communication Technology	Edge Computing	Authentication latency reduced by 30-50% Cross-domain collaboration efficiency improved by 40%	Large-scale dynamic topology scenarios
Security Mechanism	Domestic Security Chip	Signature verification rate: Up to 1000 times/sec Resistance to attack types: Forgery, Replay attacks	Various V2X communication scearios
Security Mechanism	Hybrid Trust Model	Key distribution latency: <50 ms Privacy protection level: High	Wide-area and closed platoon scenarios
Security Mechanism	Certificate-less Public Key Cryptography	Signature verification efficiency improved by 50% Data integrity: 100%	High-density communication scenarios
Security Mechanism	Hierarchical Encryption Strategy	Encryption overhead reduced by 40% Confidentiality: High	Scenarios requiring differentiated protection for private vs. regular data

4.2 Future Research Directions

Based on the above research gaps and in combination with the development trends of technology, future research should focus on the cross-layer optimization design of communication-security, the construction of cross-scenario adaptive security architectures, as well as the innovative application of blockchain and artificial intelligence in trust management and threat detection. At the same time, strengthening standardization collaboration and large-scale empirical research are important ways to promote the application of technology. The specific and feasible future research directions are as follows:

First, cross-layer optimization of communication and security: Relying on 5G/6G technology, explore the joint scheduling mechanism of resources and security policies, establish a quantitative model of communication performance and security strength, and achieve a dynamic balance between communication efficiency and security.

Second, cross-scenario safety adaptation: In response to the differentiated demands of scenarios such as platooning and remote driving, customized safety solutions are designed to enhance the scenario adaptability and effectiveness of safety mechanisms.

Third, the integrated application of new technologies: Explore the implementation path of blockchain in the trust management of the Internet of Vehicles, and utilize its decentralized and immutable characteristics to solve the problem of cross-domain trust authentication. Apply machine learning and artificial intelligence technologies to real-time threat detection and abnormal behavior recognition to enhance the proactive defense capabilities of security systems.

Fourth, standardization and coordination: Enhance the connection and coordination between domestic Internet of Vehicles security standards and international frameworks. Draw on international advanced experience, combine domestic technical features and application demands, and promote the formation of a unified and standardized security standard system to support the large-scale development of the Internet of Vehicles industry.

4.3 Research Significance

This research can fill the gap in the systematic integration of fragmented research results, break through the limitation

of traditional reviews that 'emphasize sorting over analysis', identify research gaps from a structured perspective, clarify the collaborative relationship between communication technology and security mechanisms, provide a critical perspective and direction guidance for subsequent research, and contribute to the in-depth development of IoV research. Meanwhile, the research results sorted out can help solve the problem of insufficient connection between domestic standards and international frameworks, providing theoretical support for national transportation strategic security. The summarized lightweight authentication, distributed trust and other solutions can provide car manufacturers with 'low cost and high reliability' safety technology selection references, promoting the implementation of high-level scenarios such as platooning and remote driving.

References

[1] S. Chen, "Critical thinking and suggestions on C-V2X with the developments of intelligent connected vehicles," Telecommunications Science, vol. 38, no. 7, pp. 1-17, Jul. 2022.

[2] D. V. Sri and B. J. Lakshmi, "A review of security infrastructure, protocols, a taxonomy of security threats and intrusion detection in the Internet of Vehicles (IoV)," in 2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC), Guntur, India, 2024, pp. 1-8.

[3] R. Kumar, R. Gill, A. Singh, R. Kumar, D. Singh, and M. Al-Farouni, "A comprehensive analysis of Internet of Vehicle security vulnerabilities in smart cities," in Proc. Int. Conf. Data Sci. Netw. Secur. (ICDSNS), Tiptur, India, 2024, pp. 1-6.

[4] C. Huang, "Evolution of V2X wireless access technology and networking schemes," Designing Techniques of Posts and Telecommunications, no. 11, pp. 46-52, Nov. 2020.

[5] X. Wang, "5G Internet of Vehicles security based on V2X security chip," Journal of Information Security Research, vol. 6, no. 8, pp. 705-709, Aug. 2020.

[6] J. Zhou, Q. Li, Y. Wang, et al., "Identity authentication and V2X communication security assurance in vehicle-road collaboration scenarios," Communications Technology, vol. 54, no. 11, pp. 2538-2544, Nov. 2021.

[7] G. Sharma, "SecureV2X: Overview of secure cellular based vehicle-to-everything communication in intelligent transportation system," in Proc. 12th Int. Conf. Internet Everything, Microw., Embedded, Commun. Netw. (IEMECON), Jaipur, India, 2024, pp. 1-6.

[8] Y. Shen, Z. Qian, and X. Feng, "Key technologies and performance evaluation of C-V2X PC5 interface communication," Automobile and New Power, vol. 5, no. 1, pp. 35-39, Jan. 2022.

[9] R. Liu, "Research on distributed resource scheduling algorithm for Internet of Vehicles based on LTE-V2X," Ph.D. dissertation, Henan Polytech. Univ., Henan, China, 2024.

[10] T. Bo, X. Wang, K. Feng, et al., "Application of V2X technology in communication system architecture," Automobile Applied Technology, vol. 48, no. 6, pp. 64-68, Jun. 2023.

[11] Y. Li, "Research on the evolution and development of key technologies in vehicle-road cooperative C-V2X," Industrial Technology Innovation, vol. 6, no. 5, pp. 116-120, May 2024.

[12] IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1-240, Mar. 2016.

[13] Y. Sun et al., "Security and privacy in the Internet of Vehicles," in Proc. Int. Conf. Identif., Inf., Knowl. Internet Things (IIKI), Beijing, China, 2015, pp. 116-121.

[14] Q. Wu, "Research on secure and private vehicle-to-vehicle communication and cooperative downloading schemes in Internet of Vehicles," Ph. D. dissertation, East China Normal Univ., Shanghai, China, 2024.

[15] I. Loussaief, S. Ksibi, F. Jaidi, and K. Nouri, "A comprehensive multi-layered cybersecurity framework for Internet of Vehicles: Securing vulnerable nodes of V2X communication systems," in Proc. Int. Wirel. Commun. Mob. Comput. (IWCMC), Abu Dhabi, United Arab Emirates, 2025, pp. 1597-1603.

[16] W. Cheng, E. Luo, Y. Tang, L. Wan, and M. Wei, "A survey on privacy-security in Internet of Vehicles," in Proc. IEEE Intl Conf. Dependable, Auton. Secure Comput., Intl Conf. Pervasive Intell. Comput., Intl Conf. Cloud Big Data Comput., Intl Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech), Edmonton, AB, Canada, 2021, pp. 644-650.

[17] K. Shahzad, M. R. Raza, and A. Varol, "Security threats mitigation for Internet of Vehicles using cryptographic protocols," in Proc. 13th Int. Symp. Digit. Forensics Secur. (ISDFS), Boston, MA, USA, 2025, pp. 1-6.