Computers and Artificial Intelligence；Vol.2, No.2; 2025
E-ISSN: 3006 -3728 P-ISSN：3006-371X
DOI: https://doi.org/10.70267/cai.25v2n2.0915
Published by: Zeus Press

Privacy Protection in Vehicle Platooning: Challenges, Technologies, and Future Directions

Tianxi Wang*, Yadong Peng, and Lilong Sima

Guizhou University of Finance and Economics, Guiyang, Guizhou, China

**Corresponding author: Tianxi Wang.*

Abstract

Vehicle platooning technology significantly enhances traffic efficiency and safety but introduces substantial privacy challenges. These include traditional threats like information leakage, data correlation, and sophisticated forgery attacks, which can mislead vehicle decisions and behaviors. To mitigate these, current research explores core protection strategies such as anonymization, differential privacy, various encryption techniques, trust management, and fine-grained access control. This paper also highlights the burgeoning role of blockchain in providing decentralized management and facilitating privacy-preserving machine learning within platooning systems. Despite advancements, significant hurdles persist concerning performance optimization, balancing security with privacy, ensuring real-time processing, guaranteeing robustness against evolving threats, and achieving standardization. This study systematically analyzes existing privacy protection technologies tailored for vehicle platooning, providing a comprehensive overview and identifying critical future research directions to foster secure and widespread adoption of this transformative technology.

Keywords

key word, vehicle platooning, privacy protection, internet of vehicles

1. Introduction

Vehicle platooning technology, a cornerstone of intelligent transportation, autonomous driving, and connected vehicle systems, leverages wireless communication and cooperative control to significantly enhance traffic efficiency, energy consumption, and driving safety (Khan et al., 2025). This innovative paradigm involves multiple vehicles traveling in close proximity, forming a tightly coupled convoy that optimizes aerodynamic drag, improves fuel efficiency, and increases road throughput. The technology is progressively transitioning from theoretical research to practical applications, demonstrating substantial potential in diverse scenarios such as freight transport, urban traffic management, and highway operations, thereby yielding notable economic and social benefits (Adas et al., 2025) .

However, the widespread deployment and sustained development of vehicle platooning heavily rely on Vehicle-to-Everything (V2X) communication and complex systems for large-scale data sharing. This dependence shifts security and privacy threat models from conventional mechanical failures to sophisticated cybersecurity domains. Platooning tasks necessitate the frequent exchange of sensitive information, including precise location data, real-time speed, dynamic path planning, and vehicle identity (Islam &

Zulkernine, 2025). This pervasive data exchange introduces significant privacy risks, suchalling trajectory tracking, enabling the reconstruction of individual behavior patterns, facilitating identity spoofing, and even leading to financial fraud. Furthermore, this data faces novel and evolving threats such as eavesdropping, tampering, forgery, advanced inference attacks, denial-of-service (DoS) attacks, side-channel attacks, and supply chain fraud (Avcı & Koca, 2024). Consequently, robust privacy protection has emerged as a critical foundational requirement for the widespread adoption and sustainable advancement of vehicle platooning technology. Ensuring efficient communication and seamless collaboration while fully safeguarding the privacy of vehicles and their users demands that privacy-preserving solutions encompass the entire data lifecycle, from collection and transmission to processing and storage (Zhang et al., 2017). This paper aims to systematically analyze these privacy challenges and review the state-of-the-art protection technologies, paving the way for future research.

2. Privacy Threats in Vehicle Platooning

This paper summarizes the primary privacy threats in vehicle platooning, as detailed in Table 1.

Table 1: Classification of privacy threats in vehicle platooning

Threat Categories	Description	Representative attack types	Document serial number
Personal Information Leakage	Unauthorized access, collection, or inference of sensitive data (location, behavior, identity) has occurred.	Trajectory tracing, identity re-identification, driver portrait reconstruction, and member inference attacks	Bensaoud and Kalita (2025); Islam and Zulkernine (2025)
Information Forgery and Tampering	Maliciously modifying or injecting false information to mislead vehicle decisions and behaviors.	Data poisoning, GNSS spoofing, LiDAR spoofing/replay, digital evidence manipulation	Aledhari et al. (2025); Avcı and Koca (2024); Li et al. (2025); Sato et al. (2025)
Denial of Service	Impeding the flow of critical information, resulting in system unavailability or degraded functionality.	Network flooding, resource exhaustion, communication interference	Aledhari et al. (2025)
Side-Channel Attack	Leverage information leakage in the system's physical implementation to infer sensitive data, such as keys.	Power consumption analysis, time analysis, electromagnetic radiation analysis, error injection attacks	Zhang et al. (2025)
Supply Chain Attacks	Injecting malicious components or vulnerabilities into hardware or software production/distribution.	Fake hardware injections, malicious firmware/software updates, backdoor implants	Avcı and Koca (2024)
Identity Authentication and Privacy Trade-offs	The inherent contradiction between authentication requirements and privacy protection can introduce new security risks.	Frequent pseudonym replacements lead to “ghost vehicles”, complex certificate chain management, and pseudonymous association under low-density traffic	Wang et al. (2016)

2.1 Personal Information Leakage

In Vehicular Ad-hoc Networks (VANETs) and vehicle platooning systems, the frequent exchange of sensitive information between vehicles (e.g., location, driving behavior, and even biometric data) poses significant risks of personal privacy leakage. The reliance on open communication channels exposes data to threats such as eavesdropping, tampering, or malicious exploitation (Islam & Zulkernine, 2025). In vehicle platooning, the high-frequency data exchange and data aggregation effects enable attackers to combine fragmented “quasi-identifiers” (e.g., age, gender, timestamps) with external information to reconstruct detailed driver profiles and life trajectories, achieving deep re-identification far beyond simple tracking. This can lead to severe privacy violations, potentially resulting in identity theft or fraud.

2.2 Data Correlation Attack

Data correlation attacks pose a severe threat to user privacy, as attackers can infer vehicle trajectories, driver identities, and behavioral patterns by integrating multi-source data, even when the data has undergone "de-identification" processes. This is because achieving true, irreversible anonymization is extremely challenging (Macena et al., 2023), and there exists an inherent trade-off between privacy protection and data utility. Traditional anonymization techniques struggle to address the high-dimensional and dynamic nature of Internet of Vehicle (IoV) data, rendering them ineffective against various attacks. Consequently, more sophisticated and dynamic privacy protection strategies are required to counter complex re-identification threats.

2.3 Information Forgery and Tampering Attacks

Attackers of information forgery attacks mislead other vehicles by falsifying vehicle communication data (e.g., emergency braking, speed, position), leading to traffic accidents and formation instability (Khan et al., 2025). These attacks have evolved into more sophisticated forms, such as "data poisoning," "digital evidence tampering," and "supply chain fraud," which not only threaten immediate safety but also undermine the trust foundation of transportation systems and the capabilities of AI-driven automation (Avcı & Koca, 2024). Specific attack methods include GNSS spoofing, LiDAR sensor replay attacks, malicious tampering with shared data, and attacks on deep learning vision systems (Aledhari et al., 2025). Furthermore, supply chain fraud introduces counterfeit hardware, while denial-of-service (DoS) attacks obstruct critical information flow, severely impacting system availability. To effectively counter these threats, establishing robust authentication and message signing mechanisms is crucial. However, ensuring security while maintaining real-time performance in high-frequency communication settings remains an urgent challenge.

2.4 Identity Authentication

In V2X communication, identity authentication and privacy protection are two core challenges for vehicle platooning systems. Existing Public Key Infrastructure (PKI)-based authentication schemes struggle to balance computational overhead and privacy. Although pseudonym mechanisms can enhance privacy through dynamic identity updates, in low-density traffic and highly dynamic environments, vehicle information remains susceptible to correlation, and real-time authentication faces challenges in certificate chain management (Wang et al., 2016). The trade-off between identity authentication and privacy protection is a central conflict: pursuing strong privacy (e.g., frequent pseudonym changes) often comes at the cost of degraded system performance, increased overhead, and even security risks such as "ghost vehicles." This trade-off is not static but depends on traffic density and contextual characteristics, necessitating dynamic and adaptive solutions for optimization. While high-frequency pseudonym changes can improve privacy, they also increase management burdens. In certain scenarios, even significant performance costs may yield suboptimal privacy protection outcomes, highlighting the need for more intelligent, adaptive strategies to dynamically adjust the intensity of privacy protection.

3. Vehicle Formation Privacy Protection Technology

3.1 Anonymization Technology

3.1.1 Location Anonymization

Location anonymization is a critical technique for protecting privacy in the Internet of Vehicles, employing methods such as location perturbation, location obfuscation, and virtual location generation to prevent vehicle tracking (Macena et al., 2023). Traditional statistical approaches, such as K-anonymity, L-diversity, and T-closeness, can effectively quantify and mitigate data re-identification risks. However, in the highly dynamic, large-scale data flow environment of vehicle platooning, these methods face the "utility-privacy" trade-off: excessive anonymization compromises data accuracy, impacting collaborative control and driving safety, while insufficient anonymization leaves systems vulnerable to advanced re-identification attacks.

3.1.2 Dynamic Identity Anonymization and Pseudonymization Management

Dynamic identity anonymization is a critical technology in the IoV for preventing long-term tracking, primarily achieved through pseudonym mechanisms to ensure anonymity, unlinkability, and traceability. Common pseudonym change strategies include time-based and location-based updates, as well as leveraging mix zones, cooperative changes, and silent periods to enhance anonymity. However, effective pseudonym management is a complex optimization problem, requiring a trade-off among pseudonym change frequency, coordination mechanisms, network performance, and the utility of secure data. High-frequency changes can improve privacy but may incur high overhead and the “ghost vehicle” issue. In low-traffic or uniform traffic scenarios, frequent changes may still allow tracking by attackers. Therefore, optimal pseudonym management should not rely on static configurations but adopt a dynamic strategy that adaptively adjusts based on real-time traffic conditions, computational resources, and security requirements (Wang et al., 2016).

3.1.3 Mixed Zone Mechanism

Mix Zones are a critical location privacy protection mechanism in vehicular networks, enabling vehicles to synchronously change pseudonyms in designated high-density areas (e.g., intersections), leveraging vehicle mobility to “mix” identifiers and prevent tracking by attackers (Macena et al., 2023). While Mix Zones effectively disrupt pseudonym linkage, their efficacy heavily depends on traffic density and is vulnerable to sophisticated threats such as timing attacks and transition attacks. To enhance robustness, researchers are exploring mitigation strategies, including non-rectangular or time-window-constrained Mix Zones, delay-tolerant Mix Zones, and potential integration of cryptographic techniques. The design of Mix Zones must comprehensively consider traffic impacts and safety applications, with evaluation through simulation tools to ensure robust privacy protection without disrupting traffic flow.

3.2 Differential Privacy

Differential Privacy (DP), as a rigorous mathematical framework, protects privacy in vehicle platooning by adding noise to shared data (e.g., sensitive information such as vehicle location and speed) (Islam & Zulkernine, 2025). Its core principle ensures that the algorithm’s output remains “almost identical” regardless of whether a specific individual’s data is included in the dataset, effectively preventing attackers from inferring individual behaviors or conducting long-term tracking. This is quantified through privacy parameters ò and δ, where a smaller ò indicates stronger privacy protection. Common mechanisms for implementing DP include the Laplace mechanism and the Gaussian mechanism, which add random noise following the respective distributions based on the function’s sensitivity and privacy parameters.

Local Differential Privacy (LDP), a variant of DP, is particularly suitable for distributed architectures like the Internet of Vehicles, as it does not rely on a trusted central aggregator. Instead, each user perturbs their data locally before transmission (Bensaoud & Kalita, 2025). While DP provides robust privacy guarantees, it faces the challenge of balancing accuracy and privacy protection: excessive perturbation may lead to inaccurate data, impacting vehicle control performance and increasing accident risks. Additionally, high-frequency, low-latency communication environments impose higher computational overheads on complex data processing (Khan et al., 2025).

3.3 Encryption

3.3.1 Homomorphic Encryption

Homomorphic Encryption (HE) enables data computation in the ciphertext state without decryption, offering significant privacy protection for handling sensitive position and velocity data in vehicle platooning (Islam & Zulkernine, 2025). HE is categorized into Partially Homomorphic Encryption (PHE) and Fully Homomorphic Encryption (FHE), with FHE supporting arbitrarily complex computations. HE demonstrates substantial potential in vehicle platooning, for instance, allowing service providers to perform computations on encrypted data to privately match vehicles with nearby platoons without revealing plaintext location or destination information (Quero et al., 2023). Despite progress in HE performance, achieving acceptable latency under practical platooning database scales, challenges persist due to high computational complexity and real-time requirements. Particularly for FHE, high-level encryption introduces significant computational overhead, impacting real-time decision-making.

3.3.2 Attribute Base Encryption and Searchable Encryption

Attribute-Based Encryption (ABE) and Searchable Encryption (SE) are critical cryptographic technologies for achieving advanced privacy protection and data management in V2X communications. ABE enables data owners to define access policies based on attributes, allowing decryption only when a user's attributes satisfy the policy, thereby facilitating fine-grained access control and policy privacy in decentralized environments while reducing computational and energy consumption (Wan et al., 2025). SE supports keyword searches without decrypting data, enhancing data usability, with techniques such as Keyword-Aggregate Searchable Encryption (KSE) and Dual-Policy Attribute-Based Searchable Encryption (DP-ABSE) further improving multi-category search and dynamic keyword update capabilities. Despite their significant advantages in data confidentiality and retrieval efficiency, the complexity of these technologies and potential vulnerabilities, such as key leakage and manipulation of search results, cannot be overlooked.

3.3.3 Secure Aggregation

Secure aggregation enhances information dissemination efficiency by aggregating multi-source data, applied in scenarios such as traffic density estimation and hazard detection, but it also faces privacy and security risks including false data injection, eavesdropping, and vehicle tracking (Adas et al., 2025). Secure Multi-Party Computation (SMC) is a critical cryptographic primitive for privacy-preserving data aggregation, enabling multiple parties to collaboratively compute without revealing their private inputs, which is particularly vital for aggregating vehicle data without exposing individual sensitive information (Islam & Zulkernine, 2025). Research focuses on developing lightweight, scalable, and attack-resistant privacy-preserving aggregation schemes, integrating cryptographic and anonymization techniques to balance data utility with strong privacy guarantees in real-time vehicular environments, and even leveraging Quantum Secure Multi-Party Computation (QSMC) to enhance resistance against quantum attacks (Sulimany et al., 2024).

3.4 Trust Management and Access control

Trust management and access control are core mechanisms for ensuring the security and privacy of vehicular networks. Trust models identify malicious nodes and filter unreliable data by evaluating the historical behavior and data authenticity of nodes. They increasingly integrate AI/ML technologies and decentralized blockchain architectures to address challenges of high dynamism and scalability, enabling robust real-time trust evaluation. AI-driven algorithms can efficiently detect malicious traffic and support vehicle identity verification.

Meanwhile, access control mechanisms protect privacy by restricting access to sensitive data and integrate with trust models to enable dynamic permission management, supporting Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) (Li et al., 2025). Fine-grained access control allows highly granular data management, ensuring sensitive information is accessible only to authorized users and for intended purposes. Attribute-Based Encryption (ABE) further ensures policy privacy. Blockchain technology provides decentralized solutions for trust management and privacy protection through tamper-proof ledgers, enabling decentralized pseudonym management, timely pseudonym revocation, enhanced authentication, and transparency, while strengthening secure credential management systems. However, blockchain deployment still faces challenges such as throughput, latency, and computational overhead of consensus mechanisms (Kang et al., 2025).

4. Challenges and Future Research Directions

While significant progress has been made in addressing privacy concerns in vehicle platooning, several formidable challenges remain, necessitating concerted future research efforts. Firstly, the inherent contradictions among performance, security, and privacy present a complex optimization problem. Privacy protection measures, such as advanced encryption and frequent anonymization, often introduce substantial computational overhead and communication delays. These delays can critically impact real-time decision-making within a platoon, potentially leading to reduced data accuracy and even critical security risks like "ghost vehicles" or platoon instability. Secondly, the highly dynamic and resource-constrained environment of vehicular networks poses severe challenges to the real-time performance and robustness of existing privacy solutions. Intrusion detection systems, trust management models, anonymization mechanisms, and AI models must operate under strict latency requirements and limited computational resources, making them vulnerable to sophisticated attacks such as inference delays, data poisoning, and denial-of-service. Thirdly, ensuring the interoperability and standardization of privacy-preserving solutions across diverse vehicle manufacturers and communication protocols is crucial for widespread adoption.

To effectively address these multifaceted challenges, future privacy protection schemes must move beyond isolated, single-technology solutions. Instead, a synergistic integration of multiple cutting-edge technologies is imperative. This includes advanced privacy-preserving machine learning techniques (e.g., federated learning), lightweight and efficient encryption techniques, secure multi-party computation for collaborative privacy, and blockchain technology for decentralized trust and data integrity. Emphasis should be placed on developing lightweight cryptographic protocols specifically designed for the vehicular environment to minimize overhead. Ultimately, the goal is to construct a multi-layered, adaptive defense system capable of ensuring real-time, robust privacy protection in dynamic platooning environments while maintaining optimal system performance and safety. Furthermore, addressing regulatory compliance and user acceptance will also be vital for real-world deployment.

5. Conclusion

Vehicle platooning technology, while enhancing efficiency and safety, also introduces significant privacy challenges, ranging from data breaches to sophisticated inference attacks. To address these, existing research has proposed diverse techniques, including anonymization, differential privacy, encryption, trust management, and blockchain. Future trends will focus on balancing performance and privacy security, deeply integrating cutting-edge technologies such as federated learning, blockchain, and lightweight encryption to construct efficient, privacy-protected intelligent transportation systems, while promoting the standardization and interoperability of V2X communication.

References

Adas, A., Arrigoni, S., Brambilla, M., Nicoli, M. B., & Sabbioni, E. (2025). Joint travel route optimization framework for platooning. *arXiv preprint*, arXiv:2504.07623.

Aledhari, M., Razzak, R., Rahouti, M., Yazdinejad, A., Parizi, R. M., Qolomany, B., Guizani, M., Qadir, J., & Al-Fuqaha, A. (2025). Safeguarding connected autonomous vehicle communication: Protocols, intra- and inter-vehicular attacks and defenses. *Computers and Security, 151*, Article 104352. https://doi.org/10.1016/J.COSE.2025.104352

Avcı, İ., & Koca, M. (2024). Intelligent transportation system technologies, challenges and security. *Applied Sciences (Switzerland), 14*(11), Article 4646. https://doi.org/10.3390/APP14114646

Bensaoud, A., & Kalita, J. (2025). Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models. *Ad Hoc Networks, 170*, Article 103770. https://doi.org/10.1016/J.ADHOC.2025.103770

Islam, N., & Zulkernine, M. (2025). Privacy-preserving machine learning in internet of vehicle applications: Fundamentals, recent advances, and future direction. *arXiv preprint*, arXiv:2503.01089.

Kang, J., Liao, J., Gao, R., Wen, J., Huang, H., Zhang, M., Yi, C., Zhang, T., Niyato, D., & Zheng, Z. (2025). Efficient and trustworthy block propagation for blockchain-enabled mobile embodied AI networks: A graph resfusion approach. *arXiv preprint*, arXiv:2502.09624.

Khan, R., Mehmood, A., Song, H., & Maple, C. (2025). A decentralized, secure, and reliable vehicle platoon formation with privacy protection for autonomous vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *26*(5), 6441-6450. https://doi.org/10.1109/TITS.2025.3537765

Li, K., Li, C., Yuan, X., Li, S., Zou, S., Ahmed, S. S., Ni, W., Niyato, D., Jamalipour, A., & Dressler, F. (2025). Zero-trust foundation models: A new paradigm for secure and collaborative artificial intelligence for internet of things. *arXiv preprint*, arXiv:2505.23792.

Macena, B., Albuquerque, C., & Machado, R. (2023). Cybersecurity and privacy protection in vehicular networks (VANETs). *Advances in Internet of Things, 13*(4), 109-118. https://doi.org/10.4236/AIT.2023.134006

Quero, N., Boudguiga, A., Sirdey, R., & Karam, N. (2023). *Towards privacy-preserving platooning services by means of homomorphic encryption* [Paper presentation]. VehicleSec 2023 - Inaugural Symposium on Vehicle Security and Privacy, San Diego, CA, USA.

Sato, T., Suzuki, R., Hayakawa, Y., Ikeda, K., Sako, O., Nagata, R., Yoshida, R., Chen, Q. A., & Yoshioka, K. (2025). *On the realism of lidar spoofing attacks against autonomous driving vehicle at high speed and long distance* [Paper presentation]. Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA.

Sulimany, K., Vadlamani, S. K., Hamerly, R., Iyengar, P., & Englund, D. (2024). Quantum-secure multiparty deep learning. *arXiv preprint*, arXiv:2408.05629.

Wan, Q., Liu, M., Wang, L., Wang, F., & Zhang, M. (2025). Dual-policy attribute-based searchable encryption with secure keyword update for vehicular social networks. *Electronics (Switzerland), 14*(2), Article 266. https://doi.org/10.3390/ELECTRONICS14020266

Wang, F., Xu, Y., Zhang, H., Zhang, Y., & Zhu, L. (2016). 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. *IEEE Transactions on Vehicular Technology*, *65*(2), 896-911. https://doi.org/10.1109/TVT.2015.2402166

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, *55*(1), 122-129. https://doi.org/10.1109/MCOM.2017.1600267CM

Zhang, K., Salek, M. S., Wang, A., Rahman, M., Chowdhury, M., & Lao, Y. (2025). Preparing for kyber in securing intelligent transportation systems communications: A case study on fault-enabled chosen-ciphertext attack. *arXiv preprint*, arXiv:2502.01848.

Funding

This work was sponsored by the Key Laboratory Building Program of Blockchain and Fintech of Department of Education of Guizhou Province under Grant QIAN JIAO JI[2023]014.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Copyrights