Edge Intelligence for V2X Communications: Advances in Collaborative Perception and Privacy Preservation

Siyi Wang
Bell Honors School, Nanjing University of Posts and Telecommunications, Nanjing, China

Abstract: With the latest developments in AI, the proliferation of Internet of Things (IoT) devices, and the rise of edge computing, the potential of edge AI has already been released. Edge AI also plays a significant role in autonomous driving technology. It refers to running AI on devices or edge servers close to users, which can be applied to improve IoT services in autonomous driving. This article systematically reviews the technological evolution and application challenges of Edge Intelligence in V2X communications. Firstly, it analyzes how Edge Intelligence functions in information exchange within V2X, V2V, and V2I scenarios and its effectiveness in enhancing performance. Subsequently, it explores the privacy protection mechanism integrating federated learning and blockchain to address the risks of identity tracing and data leakage. Finally, it discusses the implementation challenges, lessons learned, and future research directions of Edge AI. The study demonstrates that EI is a key enabler for achieving a balance between "real-time" and "security" in V2X communications.

Keywords: AI; Edge AI; Automobile Driving; Vehicle-to-Everything Communication(V2X)

1. Introduction

In the booming development of intelligent transportation systems, Vehicle-to-Everything (V2X) technology has become a focal point of joint attention in academia and industry, regarded as a vital force driving transformation in the transportation sector. V2X technology is dedicated to enabling comprehensive information interaction between vehicles (V2V), vehicles and infrastructure (V2I), and vehicles and networks (V2N), thereby constructing a vast and complex traffic information network.

Edge computing plays a crucial supporting role in the V2X architecture, whose core value lies in addressing the bottleneck constraints of real-time performance and security in the Internet of Vehicles through localized processing capabilities. Edge nodes can parse real-time information generated by vehicles and roadside devices in proximity, compressing decision-making response delays to the millisecond level and avoiding lag risks caused by cloud transmission. Meanwhile, they support closed-loop processing of sensitive data locally, reducing cross-domain transmission links and mitigating the risk of data leakage.

Although edge computing has realized localized data processing and low-latency transmission, Edge AI endows edge nodes with capabilities of autonomous analysis, reasoning, and dynamic adaptation. It can predict potential risks and generate collaborative avoidance strategies without relying on the cloud, upgrading response speed from "millisecond-level transmission" to "microsecond-level decision-making". In terms of resource utilization, Edge AI dynamically allocates computing power and storage of edge nodes through intelligent scheduling algorithms, prioritizing resource allocation for critical tasks and addressing the bottleneck of limited computing power in edge devices.

V2X is a key technology for Intelligent Transportation Systems (ITS). It promotes the evolution of driving modes from "human-dominated" to "intelligent collaboration". Vehicles can automatically receive real-time traffic conditions, parking space availability, charging station locations, and other information, thereby reducing the decision-making burden on drivers. In the future, combined with autonomous driving technologies, V2X will enable "hands-free and feet- free" full autonomous driving, making travel more convenient and comfortable.

In addition, V2X also serves as a crucial link in smart cities. The massive traffic data generated by V2X can be integrated with urban management systems to optimize public transportation scheduling, energy allocation, and emergency responses. This facilitates a deep integration between the transportation system and the urban ecosystem.

The contributions of this work are as follows:

1) We conduct a detailed analysis of the role of artificial intelligence (AI) and edge artificial intelligence (Edge AI) in addressing technical challenges within V2X systems.

2) We analyze the potential implementation challenges associated with the application of Edge AI in V2X, and delineate feasible solutions to mitigate these challenges.

3) We summarize the lessons learned, key research issues, and future directions concerning the utilization of Edge AI in V2X.

2. Related Works

2.1 Edge Computing

Edge computing is a computing paradigm that migrates data processing capabilities from remote centralized data centers to network edge nodes close to users or data sources. Its core goal is to address the limitations of cloud computing in terms of high latency, bandwidth constraints, and privacy protection. By deploying computing, storage, and network resources at edge nodes, edge computing enables low-latency data processing, improves bandwidth utilization, and enhances location awareness and context understanding. It is suitable for scenarios requiring real-time responses, such as intelligent transportation, industrial automation, and smart homes. It encompasses various paradigms including cloudlets, Fog Computing, Mobile Edge Computing (MEC), and micro data centers (mDCs)[19]. Although these paradigms focus on different scenarios, they all reduce reliance on the cloud through distributed architectures and provide efficient and reliable computing support for IoT devices and mobile terminals.

2.2 Edge AI

Edge AI refers to the practice of deploying artificial intelligence algorithms on edge devices of a network to realize local processing and analysis of data, rather than relying on the computing mode of cloud data centers[19]. Building on the advantages of edge computing in low latency and high bandwidth, it integrates the perception and decision-making capabilities of artificial intelligence, and can quickly respond to real-time data needs on the device side, such as local face recognition of smart cameras and real-time environmental perception of self-driving vehicles. Through technologies like model compression and federated learning, Edge AI can be adapted to resource-constrained edge devices, reducing the amount of data transmission, protecting privacy, and at the same time improving the response speed and reliability of intelligent applications. It is widely used in fields such as smart homes, industrial automation, and intelligent transportation, and has become a key technical bridge connecting terminal devices and cloud intelligence.

2.3 Automobile Driving

Autonomous Vehicles (AVs), as a core component of intelligent transportation systems, are reshaping future mobility patterns through the integration of advanced sensors, artificial intelligence, and vehicle networking technologies. Their primary objective is to enable vehicles to realize autonomous navigation, environmental perception, and decision-making control with minimal or no human intervention. This approach aims to address traffic accidents arising from human driving errors, alleviate traffic congestion, and reduce carbon emissions[20].

From a technical architecture perspective, autonomous driving systems rely on multi-level collaboration to realize their functions. The perception layer captures real-time environmental data around the vehicle through devices such as LiDAR, cameras, and millimeter-wave radars. The decision layer parses the perceived data using machine learning, such as deep learning neural networks, to generate control commands for path planning, acceleration, and deceleration. The execution layer implements physical operations through Electronic Control Units (ECUs) and actuator systems. Meanwhile, the integration of V2X communication technologies, including V2V and V2I, further expands the vehicles' environmental perception range, supporting cooperative driving and dynamic traffic management.

According to Society of Automotive Engineers (SAE) International standards, autonomous driving is classified into levels 0 to 5[5], ranging from full reliance on human driving (level 0) to full-scenario autonomous driving without intervention (level 5). Currently, level 4 autonomous driving has been implemented in specific scenarios like closed parks and ports, while level 5 technology still faces challenges in adapting to complex road conditions and ethical

decision- making.
With the evolution of technology, autonomous driving is not only an innovation in transportation tools but also involves multi-dimensional issues such as data security, privacy protection, and regulatory standards. For example, the massive amount of sensitive data generated by vehicles needs to be protected from leakage, and V2X communications must resist malicious attacks to avoid misleading decisions. These challenges have promoted the integration of blockchain, edge computing, federated learning, and other technologies with autonomous driving. It provides new pathways for building a secure and trustworthy intelligent mobility ecosystem.

3. V2X Cooperative Perception Optimization VIA
EDGE AI

Vehicle-edge-cloud collaboration is a synergistic paradigm integrating vehicles, edge nodes, and cloud platforms, as shown in Figure 1. It enables task processing locally in vehicles, vertical offloading to edge nodes for low latency, and horizontal collaboration among edges for load balancing, with the cloud supporting non-real-time operations. This framework meets the requirements of ultra-low latency and high reliability.

3.1 Vehicle-to-Vehicle communication
V2V is an important part of V2X. On the road, a multitude of vehicles are categorized into several groups according to specific criteria. Given their potential similarities, mutual information transmission among these groups facilitates the formulation of more efficient driving paths. V2V focuses on direct connections between vehicles and enables functions like cooperative driving through information exchange, such as cooperative adaptive cruise control.

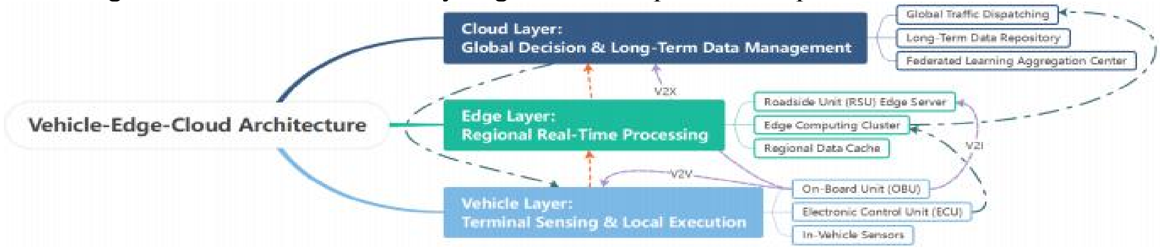

Figure 1. System Framework Diagram

Illustration: Purple arrows represent V2V, V2I, and V2N communication paths; Green arrows represent data flows; Orange arrows represent task offloading directions.

An autonomous vehicle group refers to a set of autonomous vehicles with similar positions, movement trends, and close communication. However, the construction of a stable and interconnected vehicle group, coupled with the mastery of its dynamic evolution, remains a challenging endeavor. Cheng proposed a dynamic evolution method for autonomous vehicle groups in highway scenarios, AVGF, with the aim of solving this problem[3]. It forms groups by defining vehicle states and transition rules, constructs models to evaluate performance, and detects and predicts dynamic evolution events. However, in view of the deficiencies of AVGF, Cheng proposed a side chain consensus-based decentralized autonomous vehicle group formation and maintenance method (SCCAVGF)[12]. It addresses the issues of unbalanced computing tasks, information asymmetry, weak stability, and limited scenario adaptability. Also, it improves the stability and node participation of vehicle groups while maintaining continuous information exchange under high-speed conditions.

Moreover, in practical scenarios, due to the inherent limitations of on-board computing resources, individual vehicles often struggle to handle a multitude of computation- intensive or delay-sensitive tasks independently. Consequently, offloading a portion of these tasks to external devices with superior computing capabilities becomes a necessary strategy. With Edge AI integrating, the model not only boosts reliability, cooperativeness, and punctuality but also acts as the "brain" that solves the problem of computing capabilities allocation. Mao proposed an edge computing-based cooperative model, hierarchical multi-role autonomous vehicle group formation method (HMAF), for autonomous vehicle groups in highway scenarios[2]. It significantly improves the group's reliability, cooperativeness, punctuality, and dynamic adaptability, and serves as the core support for achieving high-performance vehicle group cooperation. Edge AI plays a role in enabling distributed cooperation through V2V computation offloading, supporting vehicles to dynamically adjust their computing capacity and flexibly offload tasks.

After the formation of a stable autonomous vehicle group, to further optimize the collaborative efficiency among nodes within the group, the focus shifts to the rational allocation of computing resources within the group, so as to match the task loads and computing power constraints of different nodes.

V2V communications suffer from severe wireless resource conflicts and limited system capacity due to high frequency, group transmission/reception, and periodicity. Additionally, rapid channel changes in high-mobility environments make it difficult for base stations to centrally manage resources. To solve the problem, Ji proposed a D3QN-LS multi-agent reinforcement learning resource allocation method. It integrates low-dimensional fingerprints and a soft-update architecture, which treats V2V links as agents to reuse V2I spectrum resources[14]. Experimental results show that this method performs excellently in terms of the total capacity of V2I links and the success rate of periodic secure message transmission in V2V links, especially in high-data-volume and spectrum-scarce scenarios. It improves the success rate by approximately 40% in high-data-volume transmission compared with related methods, while the training time does not increase significantly.

In cities, there are often times when the traffic density is very high, which may lead to complex interference problems caused by overlapping communication areas of vehicles in densely deployed Internet of Vehicles (IoV). Zhang constructed an interference hypergraph model to analyze the independent and cumulative interference relationships among multiple vehicles, and transforms the resource allocation problem into a hypergraph vertex coloring problem[13]. They proposed a Federated Double Dueling Deep Q-Network (FD3QN) algorithm, which combines federated learning with multi-agent reinforcement learning. Experimental results demonstrate that the proposed algorithm exhibits significant advantages as the number of vehicles increases, showing excellent performance in densely deployed IoV scenarios.

3.2 Vehicle-to-Infrastructure Communication

V2I also falls under the scope of V2X and mainly realizes the interaction between vehicles and fixed infrastructure such as Road Side Units (RSUs). V2V is restricted by vehicle mobility and communication range, whereas V2I, relying on fixed infrastructure, can provide long-term and stable computing and communication support as well as continuous energy supply. It facilitates cross-regional global collaboration and resource scheduling, thereby laying a solid foundation for optimal decision-making in the overall transportation system. Fabio Busacca in 2023 defined VMEC-in-a-Box which can dynamically adjust its computing capacity to strike the optimal balance between performance and power consumption, while also collaborating through mutual task offloading to enhance the system's performance and reliability[1].

In Vehicle-to-Infrastructure (V2I) communication, due to vehicles being extended targets (non-point targets), it is difficult to align the beam, which affects communication performance. Zhang proposed a dynamic predictive beamforming scheme based on integrated sensing and communication (ISAC), which breaks through the traditional point target assumption and can still maintain stable and reliable communication in high-mobility scenarios[6].

After addressing the alignment issue, there are also challenges in the information transmission process. Similar to V2V communication, V2I also suffers from the inadequacy of traditional channel estimation algorithms in high-speed mobile scenarios, where their performance is suboptimal. The MEC server, with its storage and computing capabilities, trained the deep learning-based CNN-CRU channel estimation model to leverage edge AI advantages[11]. The model is deployed on on-board units (OBUs) and roadside units (RSUs) to achieve localized real-time channel estimation. It improves the accuracy of channel estimation, reduces the bit error rate, and enhances robustness.

3.3 Vehicle-to-Everything Communication

V2X offers notable advantages: leveraging 5G/6G for ultra-low latency and high reliability to meet real-time safety and autonomous driving needs. It enables global collaboration through multi-entity data fusion, adapts to complex environments via robust designs, and integrates with smart cities to drive transportation toward active intelligence. Such capabilities allow it to outperform traditional communication technologies.

In the scenario of vehicular edge computing within the Internet of Vehicles, several critical issues arise: excessive total task processing delay stemming from task and vehicle diversity, inadequate collaboration between V2I and V2V modes, the coupling of resource allocation and task scheduling, and constraints imposed by vehicle mobility. To address these challenges, Fan proposed two algorithms, specifically OJTR and HJTR[4]. OJTR solves for the optimal solution based on Generalized Benders Decomposition and Reformulation Linearization, while HJTR obtains a suboptimal solution with low complexity by decomposing the problem. The advantages lie in a lower total delay compared to other schemes. Additionally, they can adapt to scenarios with changes in the number of different items and the algorithm efficiency meets real-time requirements.

With the help of artificial intelligence, Zhang introduced a deep learning model to address the issues of insufficient real-time performance and poor adaptability of traditional multi-intersection traffic flow prediction and control methods in complex traffic environments[8]. He proposed a multi- intersection traffic flow prediction and control method based on vehicle-road collaboration (V2X) and improved LSTM. One innovation lies in enabling real-time information interaction between vehicles and roadside devices via V2X, thereby enhancing dynamic perception capabilities. The other involves integrating a sliding time window update mechanism and an incremental learning strategy into the improved LSTM model, which reduces computational complexity while preserving prediction accuracy. In terms of effectiveness, the improved LSTM significantly shortens the computation time in high traffic flow scenarios. Under high traffic conditions, the average vehicle delay is reduced, and the road network throughput is improved, with comprehensive performance superior to fixed-time control and independent adaptive control.

Edge AI technology also plays a vital role in the V2X misbehavior detection system within 5G edge networks. Dario Sabella proposed applying federated reinforcement learning (FRL) to cooperative edge intelligence in C-V2X communication[9]. They utilize in-vehicle edge servers (ES) as edge nodes, which generate local models by processing sensor data through locally trained deep Q-networks (DQN) and duelling DQNs. The central parameter server (PS) aggregates the edge node models, broadcasts updates, and optimizes the global model in combination with federated averaging (FedAvg) to realize collaborative intelligent decision-making between edge nodes and the center. From a performance perspective, the number of communication rounds is decreased with this scheme. It demonstrates superior throughput and end-to-end latency in processing 8 video streams. Moreover, under varying numbers of vehicles and discount factors, it outperforms traditional methods in terms of model convergence speed and stability, thereby effectively enhancing the efficiency and reliability of C-V2X networks.

4. V2X Privacy Protection

The United States is committed to reducing road fatalities and serious injuries[15]. V2X technology enables vehicles to communicate with other road users and roadside infrastructure, sharing critical information to enhance road safety, mobility, and efficiency. This initiative aims to achieve a safer, more reliable, and efficient transportation system through the widespread deployment of V2X technology, while safeguarding privacy and consumer rights.

In V2V and V2I communications, when vehicles exchange data with random and untrusted entities like other vehicles (for V2V) and smart traffic lights (for V2I), there are risks including location privacy leakage and malicious messages. propagation. Maanak Gupta introduced a trusted cloudlet architecture and managed communication permissions through vehicle attributes and dynamic policies, supporting the implementation of fine-grained security policies[16]. Cloudlets can immediately intercept messages sent by malicious vehicles by dynamically updating the list of such vehicles, thereby reducing bandwidth consumption. Attribute-based policies can precisely control the range of message recipients, mitigating the impact of fake messages.

4.1 Federated Learning-Edge Cloud Architecture

Federated learning distributes the model training process to the local end of each data holder, transmitting only the trained parameters instead of raw data. It achieves cross-node collaborative modeling while ensuring data security, with its core principle being "models move, data stays". The workflow of this technology is illustrated in Figure 2.

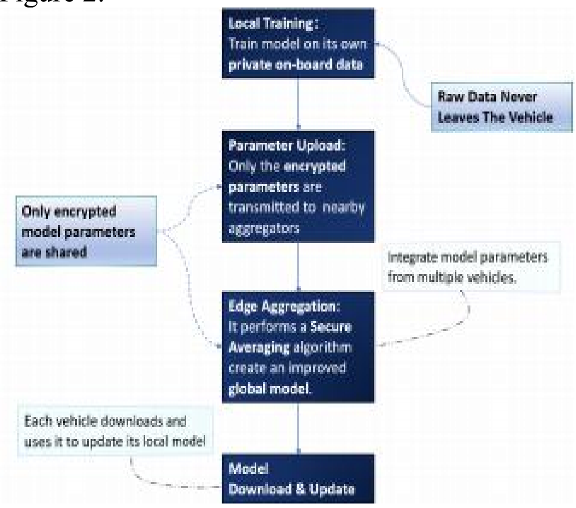

Figure 2. Federated Learning Workflow with Privacy Preservation in V2X

Traditional LSTM models struggle to effectively identify complex attacks that mimic legitimate behaviors, such as position falsification, eventual stop, and delayed messages. These attacks mimic normal vehicle movement patterns. For LSTM models, which rely on temporal dependencies, such mimicry renders attack detection challenging. This often results in misjudgments or missed detections, thereby posing a threat to road safety. Meanwhile, challenges such as the concealment of internal threats in V2N communications, alongside the balance between data privacy protection and model scalability, remain to be addressed. The ultimate objective is to achieve accurate and efficient detection of diverse malicious behaviors.

Missura deployed Misbehavior Detection Functions (MDFs) as edge nodes within edge networks, where Transformer- based AI models were executed. Leveraging the self-attention mechanism, these models capture temporal and spatial dependencies in vehicle movement data, thereby enabling localized real-time detection. Meanwhile, with the help of a federated learning framework, MDFs train models locally and only share parameters with the central server, which not only ensures data privacy but also improves system scalability[10].

This study focuses on a hierarchical federated learning system based on edge-cloud collaboration. Its objective is to tackle challenges in traditional federated learning, including low communication efficiency, irrational resource allocation, and constrained model performance, within scenarios involving heterogeneous devices and non-independent and identically distributed (Non-IID) data. Su proposed an Adaptive Hierarchical Federated Learning Process (AHFLP), which divides the learning process into multiple cloud intervals[7]. Within each interval, parameter estimation is performed, and the aggregation frequencies of edge and cloud are adaptively adjusted. Convex optimization methods are integrated to conduct distributed optimization of device CPU frequencies and wireless channel bandwidth allocation, thus realizing the joint optimization of aggregation frequencies and resource allocation. In V2X, vehicles, as edge devices, exhibit high mobility and heterogeneity, and the data presents significant Non-IID characteristics. The hierarchical architecture of AHFLP can utilize Roadside Units (RSUs) as edge nodes to implement local aggregation, reducing direct communication between vehicles and the cloud, lowering latency, and saving bandwidth. The adaptive aggregation frequencies can adapt to the dynamically changing network environment of vehicles, while the optimization of resource allocation can balance the computing resources and energy consumption of vehicles.

4.2 Decentralized Identity Authentication

Focusing on the limitations of traditional Public Key Infrastructure (PKI) in the IoT environment, such as poor scalability, centralization, and single points of failure, Akli proposed the ISIF (IOTA-Assisted Self-Sovereign Identity Framework) based on the principles of Self-Sovereign Identity (SSI)[17]. This framework employs Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to achieve mutual authentication between devices. It further leverages the IOTA Tangle distributed ledger for the management and verification of DIDs and VCs, thereby ensuring the decentralization and immutability of identity management. Such a design effectively guarantees authentication performance in large- scale IoT scenarios. The application of this framework in V2X is highly feasible. The DIDs and VCs in ISIF can enable autonomous identity management and privacy protection for vehicles, infrastructure, and other entities. The advantage lies in reducing reliance on centralized authorities, enhancing the security of identity authentication and privacy protection.

Table 1. Comparison Table of Privacy Protection Mechanisms

Solution	Privacy Protection	Scalability	Latency	Application Scenarios
Traditional PKI	1. Relies on central certificate authorities (CAs).2. Users have no control over identities and real identities are exposed during authentication.	Faces significant central- ized bottlenecks, struggles with massive nodes due to high CA load.	Latency ranges from hun- dreds of milliseconds to seconds in cross-CA scenarios.	Only applicable to traditional centralized scenarios.
Blockchain + DID	1. Only proves "legitimacy" to verifiers without exposing real identities or redun- dant information.2. Sensitive information is stored locally by users rather than centrally managed.	Supports efficient expansion of over 250 nodes with some architecture, and new nodes can join by writing DIDs to the blockchain without centralized approval.	DID verification latency of tens to hundreds of milliseconds, with no need for centralized interaction and support for basic offline verification.	Suitable for decentralized identity management of IoT devices.
Federated Learning	1. Raw data stays local; only model parameters are transmitted.2. Enhances privacy with differential privacy encryption.	Supports parallel operation of tens of thou- sands of nodes, with new nodes only participating in local training and the central node merely aggregating parameters, adapting to dynamic nodes.	Requires multiple iterations for training, but has inference latency 20ms after deployment, and low parameter transmission latency due to small parameter volume.	Suitable for extended scenarios like V2X collision warning model training and IoT device fault prediction.

The issue of user privacy leakage and security risks is also involved during electric vehicle charging. Parameswarath proposed a user-centric authentication protocol based on Decentralized Identifiers (DIDs) and blockchain technology, which combines Verifiable Credentials (VCs) and Zero- Knowledge Proofs (ZKPs) to realize autonomous control of user identities and privacy protection[18]. This protocol achieves security attributes such as user privacy protection, unlinkability, and mutual authentication. In V2X, interactions between vehicles and roadside units require protection of identity and location privacy. The user-centric authentication mode of this protocol enables vehicles to manage their identities autonomously; ZKPs can complete authentication without revealing sensitive information; and the immutability of blockchain ensures the validity of credentials. This not only enhances users' control over their identities and reduces the risk of privacy leakage but also guarantees communication security, making it adaptable to multi-entity interaction scenarios in V2X.

5. Lessons Learned and Future Directions

5.1 Summary of Industrial-Grade Experience

Edge AI performs brilliantly in V2X scenarios, with its core value reflected in in-depth optimization of real- time performance, privacy, and scenario adaptability. By deploying AI models on in-vehicle terminals or roadside units, Edge AI achieves localized inference, avoiding the long-distance transmission delay caused by uploading data to the cloud. It provides millisecond-level response support for critical scenarios such as collision warning and emergency braking, enabling vehicles to quickly respond to sudden road conditions. Regarding privacy protection, distributed training models like federated learning support vehicles in updating models locally, ensuring that only parameters are uploaded. This not only prevents the leakage of sensitive information such as location and speed but also improves model performance through multi-vehicle collaboration, achieving a balance between safety and privacy protection.

At the same time, Edge AI can flexibly adapt to the resource constraints of in-vehicle devices. Through model lightweight technology[21], it reduces energy consumption while ensuring inference accuracy, ensuring the stable operation of devices during long-time driving. Facing different scenarios such as urban congestion and smooth highways, it combines multi-source data fusion and transfer learning technologies to enhance the cross-scenario generalization ability of the model, enabling vehicles to accurately identify traffic participants and abnormal behaviors even in complex road conditions.

5.2 Future Directions

To address the challenges of data privacy, security, and cross-scenario adaptability in V2X Edge AI, a multi-layered technical framework can be constructed as follows.

First, a V2X federated learning framework should be established. Within this framework, vehicles and RSUs conduct local model training and only upload parameter updates to edge servers for aggregation. This approach prevents the leakage of raw data that contains sensitive information such as vehicle positions and trajectories.

Moreover, federated distillation technology can be leveraged to distill the knowledge of multiple local vehicle models into a global model, effectively integrating heterogeneous data features from different regions and enhancing the model's generalization ability across scenarios, such as enabling accurate recognition of abnormal behaviors in both urban and highway environments. Meanwhile, blockchain technology should be integrated. The model aggregation process of edge servers needs to be recorded on the blockchain to ensure that the aggregated parameters cannot be tampered with by malicious nodes, while vehicle identities are authenticated through decentralized identifiers (DIDs) to prevent unauthorized access and forged data injection.

For communication needs, 5G slicing provides dedicated resources for V2X Edge AI tasks, ensuring low-latency delivery of high-priority services like emergency braking commands, key to avoiding collisions. Exploring 6G air interface intelligence will further enable dynamic adjustment of communication frequency bands and transmission rates through collaboration between edge nodes and base stations, adapting to the real-time data needs of Edge AI models. For instance, in high-density vehicle scenarios, it can increase uplink bandwidth to support multi-vehicle collaborative inference, thereby improving the efficiency of collective decision-making.

Finally, building a V2X Edge AI test dataset that includes diverse scenarios such as extreme weather and special traffic participants will drive the standardization of model evaluation. It provides a reliable benchmark for technology iteration and accelerating the practical application of Edge AI in V2X.

6. Conclusion

Edge Intelligence (EI), as an emerging paradigm integrating edge computing and AI, not only enhances real-time responsiveness and privacy preservation in V2X but also lays the foundation for a trustworthy and scalable intelligent transportation ecosystem. In Vehicle-to-Vehicle communication, EI enhances the response speed and accuracy of dynamic information interaction between vehicles through localized data processing and real-time decision support. In Vehicle-to-Infrastructure communication, it empowers Roadside Units to conduct real-time analysis on data such as traffic flow and abnormal road conditions, providing intelligent support for signal timing optimization and regional traffic management, thus significantly improving road network operational efficiency. Aiming at the increasingly prominent issues of privacy security and data credibility in V2X communication, this paper further analyzes the applicable scenarios and potential bottlenecks of the integration of the two technologies, offering theoretical references for constructing a trusted V2X communication environment. This paper systematically sorts out the implementation challenges of edge intelligence in the deployment of V2X and prospects future research directions.

References

[1] Fabio Busacca and Christian Grasso and Sergio Palazzo and Giovanni Schembra, “A Smart Road Side Unit in a Microeolic Box to Provide Edge Computing for Vehicular Applications,” IEEE Transactions on Green Communications and Networking, 7(1), 194-210. 2023.

[2] Qichao Mao and Jiujun Cheng and MengChu Zhou and Shangce Gao and Shoufei Han, “An Edge Computing-Based Autonomous Vehicle Group Cooperation Model in a Highway Scene,” IEEE Transactions on Vehicular Technology,73(7), 9682-9695. 2024.

[3] Cheng, J., Ju, M., Zhou, M., Liu, C., Gao, S., Abusorrah, A. and Jiang, C. “A Dynamic Evolution Method for Autonomous Vehicle Groups in a Highway Scene. IEEE Internet of Things Journal”, 9(2), 1445-1457. 2022.

[4] Fan, W., Su, Y., Liu, J., Li, S., Huang, W., Wu, F. and Liu, Y. “Joint Task Offloading and Resource Allocation for Vehicular Edge Computing Based on V2I and V2V Modes”.

IEEE Transactions on Intelligent Transportation Systems, 24(4), 4277-4292. 2023.

[5] SAE International. (2021). Standard Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (SAE J3016).

[6] Zhen Du et al., “Integrated Sensing and Communications for V2I Net- works: Dynamic Predictive Beamforming for Extended Vehicle Targets,” in IEEE Transactions on Wireless Communications, vol. 22, no. 6, pp. 3612-3627, June 2023, doi: 10.1109/TWC.2022.3219890.

[7] Yi, S., Wenhao, F., Qingcheng, M., Penghui, C., and Yuan’an, L. Joint Adaptive Aggregation and Resource Allocation for Hierarchical Federated Learning Systems Based on Edge-Cloud Collaboration, IEEE Trans Cloud Comput, 13.1: 369-382.2025

[8] Renyong, Z., Shibiao, H., and Peng, L. “Multi-intersection Traffic Flow Prediction Control Based on Vehicle-Road Collaboration V2X and Improved LSTM”, Int J Inf Commun Technol, 25.11: 52-68. 2024.

[9] Sabella, D. and Lei, M. “AI and Sensor Fusion on Roadside MEC: Stan- dards and Implementations for V2X”. IEEE Communications Standards Magazine, 9(2), 80-87. 2025.

[10] R. Missara, H. Yakan, H. Kchok, I. Fajjari and N. Aitsaadi, “Misbehavior Detection System in V2X 5G Edge Networks based on Transformer,” 2025 Global Information Infrastructure and Networking Symposium (GIIS), Dubai, United Arab Emirates, 2025, pp. 1-6.

[11] Y. Liao, Z. Cai, G. Sun, X. Tian, Y. Hua and X. Tan, ”Deep Learning Channel Estimation Based on Edge Intelligence for NR-V2I,” in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 13306-13315, Aug. 2022.

[12] Cheng, J., Xu, G., Yuan, G., Yang, L., Huang, Z., Huang, C. and Hugo, V. ”A Side Chain Consensus-Based Decentralized Autonomous Vehicle Group Formation and Maintenance Method in a Highway Scene. IEEE Transactions on Industrial Informatics, 18(12), 9250-9258. 2022.

[13] Zhang, S., Yang, C., Yu, T., Liu, T., Chen, J., Yu, K. and Guizani, M. Resource Allocation in V2V Communication via Federated Multi- Agent Reinforcement Learning. 1-6. 2025.

[14] Yuxin, J., Yu, W., Haitao, Z., Guan, G., Haris, G., Hikmet, S., and Fumiyuki, A. Multi-Agent Reinforcement Learning Resources Allo- cation Method Using Dueling Double Deep Q-Network in Vehicular Networks, IEEE Transactions on Vehicular Technology, 72.10: 13447- 13460. 2023.

[15] U.S. Department of Transportation. (2024).” Saving Lives with Connectivity: A Plan to Accelerate V2X Deployment”. https://www.transportation.gov/briefing-room/usdot-releases-national-deployment-plan-vehicle-everything-v2x-technologies-reduce

[16] M. Gupta, J. Benson, F. Patwa and R. Sandhu, Secure V2V and V2I Communication in Intelligent Transportation Using Cloudlets, in IEEE Transactions on Services Computing, vol. 15, no. 4, pp. 1912-1925, 1 July-Aug. 2022.

[17] A. Akli and K. Chougdali, IOTA-Assisted Self-Sovereign Identity Framework for Decentralized Authentication and Secure Data Sharing, in IEEE Access, vol. 13, pp. 80191-80205, 2025.

[18] R. P. Parameswarath, P. Gope and B. Sikdar, “Privacy-Preserving User- Centric Authentication Protocol for IoT-Enabled Vehicular Charging System Using Decentralized Identity,” in IEEE Internet of Things Magazine, vol. 6, no. 1, pp. 70-75, March 2023.

[19] Raghubir Singh, Sukhpal Singh Gill, ”Edge AI: A survey”, Internet of Things and Cyber-Physical Systems, Volume 3, Pages 71-92, ISSN 2667-3452, 2023.

[20] Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N. and Shiaeles, S. “Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence”. IEEE Transactions on Intelligent Transportation Systems, 24(4), 3614-3637. 2023.

[21] Wael Aljabri, Md. Abdul Hamid, Rayan Mosli. ”Enhancing real-time intrusion detection system for in-vehicle networks by employing novel feature engineering techniques and lightweight modeling”. Ad Hoc Networks, Volume 169, 103737, ISSN 1570-8705. 2025.