Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/46/20241098

Federated learning in autonomous driving: Progress, challenges, and outlook in perception, prediction, and communication

Zelong Xiang

School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, United Kingdom

zx3u22@soton.ac.uk

Abstract. In the ever-evolving field of autonomous driving, vehicles have evolved into mobile computing centres, accumulating and processing vast amounts of data, including environmental variables, driver behaviours, and preferences. Conventional centralized data processing methods face privacy and security vulnerabilities. To address these challenges, federated learning technology has emerged as a promising alternative, with its decentralized, privacy-preserving architecture. This review explores the application of federated learning in autonomous driving, focusing on perception, prediction, and communication scenarios, including research such as using federated learning to enhance the vehicle's ability to predict steering angle, object detection, and multimodal sensor data fusion. In addition, this review investigates the improvement of communication efficiency through techniques such as Distributed Federated Learning (DFL), Selective Federated Reinforcement Learning (SFRL), and Vehicle-to-everything (V2X) communication. The analysis indicated that federated learning holds great promise in autonomous driving, significantly enhancing vehicle performance in perception, prediction, and communication. However, challenges like data heterogeneity and communication costs persist. Future research should prioritize refining aggregation algorithms, minimizing communication overhead, and adapting federated learning to evolving autonomous driving technologies.

Keywords: Federated Learning, Autonomous Driving, Perception, Communication.

1. Introduction

Autonomous driving represents the convergence of cutting-edge technology and human-centered transportation aspirations [1]. As vehicles become smarter, they always accumulate and process large amounts of data, thus evolving into mobile computing centres. This data is the basis for advanced operations, including environmental factors while the vehicle is traveling and information about driver habits and preferences. The proper handling of these data helps to improve the driving experience and safety protocols, but they also raise societal concerns about user data privacy leakage. Traditional data collection and processing methods are essentially centralized and have vulnerabilities in terms of privacy and security [2]. However, as federated learning techniques have evolved, user privacy and security issues in the autonomous driving field seem to be well addressed.

DOI: 10.54254/2755-2721/46/20241098

As an alternative, the rise of federated learning has seen significant traction in recent research. With vehicles transitioning into mobile computing hubs, the demand for innovative methods that prioritize both efficiency and privacy is paramount. In this context, FL, with its decentralized and privacy-preserving architecture, is being extensively studied to reshape the landscape of autonomous driving in two primary realms: perception and recognition, as well as communication.

In the field of perception and recognition for autonomous driving, the focus has been on steering the autonomous vehicles with precision. Traditional steering algorithms that predominantly relied on centralized data are now being replaced or supplemented by federated learning approaches. For instance, FL shows promise in steering angle prediction, aiming to capture the nuances of real-world driving without compromising data privacy [3].

In the arena of perception and recognition, the focus has been on steering the autonomous vehicles with precision. Traditional steering algorithms that predominantly relied on centralized data are now being replaced or supplemented by federated learning approaches. For instance, FL shows promise in steering angle prediction [4] and image processing [5], aiming to capture the nuances of real-world driving without compromising data privacy. Delving deeper, the challenge of crafting human-like vehicle perception in dynamic driving conditions has also been addressed through FL, integrating data from various sources like vehicular sensors and road-based inputs [6]. Such advancements hint at vehicles soon being able to make decisions with a perceptual clarity mirroring that of an experienced human driver, but within a decentralized data framework.

In the field of autonomous driving communication, the focus is mainly on facilitating collaboration between vehicles without violating privacy protocols. Communication, especially real-time communication, is crucial for vehicles to safely navigate through complex terrain and traffic scenarios. It has been shown that a Dispersed Federated Learning approach (DFL) can address challenges such as packet errors and transmission delays in autonomous driving scenarios in the 6G context to make vehicle communication more seamless [7]. Another interesting development is a new structured approach for vehicle-tailored Transformers proposed by fusing Transformer, collaborative computing and federated learning, which can efficiently represent and fuse different data inputs to enable private collaborative computing in autonomous driving [8]. Motivated by these significant advances in the application of joint learning to autonomous driving, the aim of this paper is to conduct a comprehensive literature review, which focuses on the evolving landscape, emerging challenges, and promising directions in the dynamic intersection of autonomous driving and federated learning.

The rest of this chapter is organized as follows. Firstly, this paper will provide an overview of the theoretical knowledge underpinning federated learning and the research methodology of federated learning in the context of perception and communication scenarios in autonomous driving in chapter 2. Then, in chapter 3, the progress, limitations and future challenges of federated learning in both of these scenarios in the field of autonomous driving will be discussed. Finally, chapter 4 summarizes the section and presents conclusions drawn from the applications discussed here.

2. Method

2.1. Preliminaries of the federated learning

Federated learning enables collaborative training among dispersed users, emphasizing data privacy and integrity. It keeps user data on the original device, addressing the privacy concerns of centralized learning. Users benefit from trained machine learning models while ensuring data privacy. This method also alleviates data pressure on central servers, enhancing model training efficiency. Federated learning includes categories such as horizontal, vertical, and federated transfer learning.

2.1.1. Horizontal federated learning. Horizontal Federated Learning, also known as Homogenous Federated Learning, has two characteristics of the data form for its applicable scenarios: the first is that each participant's data has the same feature or schema. The second is that the datasets of different

DOI: 10.54254/2755-2721/46/20241098

participants contain different instances and samples. The steps of its algorithmic principle are shown as follows:

(1) Each client obtains the latest model from the aggregator and performs the decryption operation.

(2) Clients train the model based on their local data and encrypt the obtained gradients and upload them to the server. The server gathers these gradients and fine-tunes the model parameters accordingly. Subsequently, through the utilization of sophisticated aggregation algorithms, the server further enhances the model to guarantee superior performance.

(3) Subsequently, the server encrypts the updated model and releases it for download by various authorized clients. In this way, these clients can enjoy the up-to-date and optimized models, thus improving the processing and analysis of their data.

2.1.2. Vertical federated learning. Vertical federated learning has two characteristics of the data form of its applicable scenarios: the first is that the data of each participant has at least the same ID, and the second is that the feature of the datasets of different participants is different. The steps of its algorithmic principle are:

(1) Using the oblivious transfer encryption algorithm [9] and introducing a trustworthy outside C for producing key pairs. C sends public keys to A and B, while retaining the private decryption key.

(2) A and B encrypt their data, swap it, and compute gradients and loss values, ensuring data privacy.

(3) With encrypted samples, A and B calculate the gradient and apply masks. B, having a label, computes encrypted loss. Both send these to C.

(4) C decrypts the gradient and loss, returns them to A and B, who update their models, ensuring collaborative training with data privacy.

2.1.3. Federated transfer learning. Federated Transfer Learning proves its worth when there is minimal overlap between the data held by participants. It aims to create a unified feature representation by finding common ground between two datasets. Essentially, it maps the source and target domain features into a shared space. In this space, a classifier is trained using labels from the source domain [10].

2.2. Perception and recognition

2.2.1. Object detection. Object detection in autonomous driving is the technique of identifying and locating objects and obstacles on the road. It ensures that the vehicle can navigate safely and avoid collisions with other objects. Shah et al. [11] proposes a blockchain-based federated learning target detection scheme, which addresses the privacy, and single-point vulnerability issues present in traditional centralized models. In this system, all nodes train their models locally and exchange only model parameters instead of raw data, thus enhancing the privacy protection of data. The scheme further enhances the system's resilience to potential threats by introducing the Interplanetary File System (IPFS), a distributed system that enables nodes to access the global model, thereby eliminating the need for a Central Authority (CA). In addition, the blockchain-based FL system includes an automated code for on-time local model training and updating, which regulates the data flow in the blockchain network and handles network requests, ensuring stable and efficient operation of the network. The results show that using this scheme for vehicles outperforms traditional algorithms in terms of accuracy, latency, and precision. Jallepalli et al [12] introduced a unique federated learning prototype. It is designed to ensure that the data characteristics of all self-driving vehicles remain uniform by employing a horizontal federated learning strategy, but each sample is distinctive. A central server first distributes the model parameters to all vehicles. Each vehicle then employs deep learning methods to process its local data. After completing training, these model parameters are encrypted and returned for aggregation to the central server. Compared to traditional detection algorithms, this method demonstrates higher efficacy.

DOI: 10.54254/2755-2721/46/20241098

2.2.2. Fusion and location of multimodal sensors. The fusion and localization of multimodal sensors is a core component in autonomous driving technology, and they can enhance the vehicle's environment perception by integrating data from different sensors. The heterogeneity between data generated by different sensors poses a challenge to federated learning, and to address this problem, Zheng et al. [13] introduces AutoFed, a federated learning framework tailored for self-driving vehicles. It processes heterogeneous data from in-vehicle sensors using loss tuning of the Regional Proposal Network (RPN) and autoencoder technology for missing data recovery. AutoFed employs a k-d tree strategy for client model selection, considering environmental and data differences. Tests reveal AutoFed surpasses commercial methods in precision and recall, excelling in variable weather, underscoring its utility in vehicle perception. Another study [14] designs a novel multi-vehicle SLAM approach using a RHS-assisted radar system, where RHS stands for Reconfigurable Holographic Surface. By integrating federated learning and utilizing RHS metasets, AutoFed is capable of providing high quality detection results. Learning and utilizing RHS metasurface antennas, it offers a cost-effective solution. The proposed system includes algorithms for RHS radiation The proposed system includes RHS radiation optimization algorithms as well as federated learning enhanced localization and mapping algorithms. Simulations demonstrate its superiority over traditional phased arrays and non-cooperative methods. Simulations demonstrate its superiority over traditional phased arrays and non-cooperative methods.

2.3. Communication

In autonomous driving systems, it is crucial to achieve continuous, efficient communication with low latency. Federated learning provides multiple solution strategies to this challenge, and certain of these techniques have made significant progress in communication optimization.

Khan et al. [7] introduces a Distributed Federated Learning (DFL) framework. This method is designed for autonomous vehicles, aiming to provide stable learning that efficiently utilizes communication resources while prioritizing privacy. By dispersing data processing and learning across individual vehicles, it reduces reliance on a central server, thereby minimizing communication load and latency. Importantly, DFL enhances communication stability and efficiency by mitigating the accuracy loss of federated learning models due to packet errors and transmission delays.

The next is the Selective Federated Reinforcement Learning (SFRL) strategy [15]. This strategy allows the selection of specific vehicles before uploading the local model, thus reducing unnecessary communication overheads. Considering the efficiency of federated learning and the additional communication overhead it imposes, selective uploading can significantly reduce the network load and thus improve the overall communication efficiency. Simulation results show that SFRL can significantly reduce the communication overhead compared to the traditional federated learning strategy.

Alternatively, the use of vehicle-to-everything (V2X) communication [4] is also a method with significant optimization results. This technique allows each vehicle to share the collected data with a central server, providing a large amount of heterogeneous data for training machine learning models. The federated learning approach combined with this, especially in the presence of noisy images, provides higher communication efficiency and less bandwidth consumption, making V2X communication more valuable in practical applications.

3. Application and discussion

3.1. Perception and prediction

3.1.1. Applications and challenges of federated learning in perception and prediction for autonomous driving. Prediction and perception are a core part of the Autonomous driving technology. Traditional prediction and perception techniques mainly rely on centralized data processing and model training, but as the amount of equipment and data grows, the centralized approach becomes overwhelming.

DOI: 10.54254/2755-2721/46/20241098

Federated learning is gradually gaining attention as a distributed learning method, especially in the field of prediction and perception for autonomous driving. For instance, recent research has explored the application of federated learning in autonomous driving, focusing on tasks such as route planning and perception enhancement for connected autonomous vehicles [6].

However, while federated learning shows great potential in the area of prediction and perception for autonomous driving, it also faces several challenges:

Challenge 1: Data and System Diversity

In federated networks, particularly in autonomous driving, data from devices is highly diverse due to various sensors and external conditions like weather and driving scenarios. Additionally, each node's capabilities and conditions differ, meaning only some devices might be active, while others face disruptions due to network or power issues.

Challenge 2: Model Variability and Complexity

Models in federated learning vary based on data and external factors like weather and road conditions. Maintaining consistency in annotations, model architecture, and weight aggregation further complicates the process.

3.1.2. Future Directions for Federated Learning in Prediction and Perception for Automated Driving. The application of federated learning in autonomous driving must face a series of data heterogeneity, such as annotation heterogeneity, perceptual model heterogeneity, and environment heterogeneity. To address these heterogeneities, future research needs to further improve the efficiency of handling data diversity and to conduct in-depth studies on the problem of model divergence, especially due to various environmental factors such as weather and road conditions.

3.2. Communication

3.2.1. Applications and Challenges of Federated Learning in the Communication Domain of Autonomous Driving. In the communication realm of automated driving, federated learning provides a decentralized framework for inter-vehicle data sharing and model training, allowing multiple vehicles to learn and refine models together without directly exchanging raw data. Federated learning has now demonstrated superior performance in this area, for example by effectively improving steering angle prediction and reducing communication overhead [3]. In addition, it has been shown that federated learning outperforms centralized training, especially in the presence of high BER, while also saving bandwidth [4].

Challenge 1: Communication Overhead and Interference

The increasing number of CAVs participating in FL, coupled with iterative rounds, amplifies the communication burden, further intensified by the interference from reusing orthogonal resource blocks and uncertainties in wireless channels.

Challenge 2: Variability in Model Quality and Resource Constraints

Diverse local model performances and inadequate consideration of their impact can compromise the global model's accuracy. This challenge is exacerbated by varying computing capacities among CAVs and inconsistent communication link qualities, leading to prolonged model update times and strained communication resources.

3.2.2. Future Directions for Federated Learning in Communication for Autonomous Driving. Communication delays, resource consumption, storage capacity limitations, and differences in training capabilities are challenges in federated learning-based communication scenarios.

Future research should prioritize strategies for minimizing communication costs, such as reducing the frequency of communication rounds. Additionally, it should explore methods to balance data consumption rates and training capabilities among diverse nodes. In addition, the research on the independence of edge-based devices and the decentralization of the central server have also become important directions for research.

DOI: 10.54254/2755-2721/46/20241098

4. Conclusion

This systematic review aims to comprehensively survey and analyze the application of federated learning in the areas of vehicle perception, prediction and communication in autonomous driving. This review shows the potential of federated learning in improving the performance of perception and communication in self-driving vehicles. Federated learning-based approaches demonstrate excellent precision and recall in multimodal sensor fusion and localization, especially in challenging weather conditions. In addition, federated learning enhances vehicle communication by reducing packet errors and transmission delays, thus simplifying the communication process and ensuring optimal data integrity and transmission fidelity.

However, this review also highlights the challenges in integrating federated learning with autonomous driving technologies. A prominent issue is data heterogeneity, which stems from the diversity of data sources and environmental variables, which complicates the development of universally applicable models. In addition, the communication costs incurred between vehicles require the use of more efficient algorithms and communication protocols. These challenges emphasize the need for further innovations and improvements in federated learning applications.

In addition, the limitations of this review include a primary focus on existing literature, which may overlook ongoing, unpublished research and advances in the field. Future trends should focus on addressing the highlighted challenges, and research may delve into improving aggregation algorithms, increasing communication efficiency, and developing adaptive federated learning models for seamless integration with evolving autonomous driving technologies. These advances are critical to realizing the full potential of federated learning in autonomous driving, paving the way for safer, more efficient, and smarter transportation systems.

References

[1] Naranjo J E González C García R et al 2005 Power-steering control architecture for autonomous driving IEEE Transactions on Intelligent Transportation Systems 6(4) 406-415

[2] Xiong Z Cai Z Han Q et al 2020 ADGAN: Protect your location privacy in camera data of auto-driving vehicles IEEE Transactions on Industrial Informatics 17(9) pp 6200-6210

[3] H Zhang J Bosch H H Olsson 2021 End-to-End Federated Learning for Autonomous Driving Vehicles 2021 International Joint Conference on Neural Networks (IJCNN) pp 1-8

[4] Panda A M P G R M 2021 Steering Angle Prediction for Autonomous Driving using Federated Learning: The Impact of Vehicle-To-Everything Communication 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) Kharagpur India pp 1-7

[5] Sohan M F Basalamah A 2023 A Systematic Review on Federated Learning in Medical Image Analysis IEEE Access 11 pp 28628-28644

[6] Wang S et al 2023 Federated Deep Learning Meets Autonomous Vehicle Perception: Design and Verification IEEE Network 37(3) pp 16-25

[7] Khan L U Tun Y K Alsenwi M Imran M Han Z Hong C S 2022 A Dispersed Federated Learning Framework for 6G-Enabled Autonomous Driving Cars IEEE Transactions on Network Science and Engineering

[8] Tian Y Wang J Wang Y Zhao C Yao F Wang X 2022 Federated Vehicular Transformers and Their Federations: Privacy-Preserving Computing and Cooperation for Autonomous Driving IEEE Transactions on Intelligent Vehicles 7(3) pp 456-465

[9] Ishai Y Kilian J Nissim K Petrank E 2003 Extending Oblivious Transfers Efficiently Advances in Cryptology - CRYPTO 2003 CRYPTO 2003 Lecture Notes in Computer Science vol 2729 Springer Berlin Heidelberg

[10] Saha S Ahmad T 2021 Federated Transfer Learning: Concept and Applications 1 Jan 2021: 35-44

[11] Shah K Kanani S Patel S 2023 Blockchain-based object detection scheme using federated learning Security and Privacy 6(1) pp e276

DOI: 10.54254/2755-2721/46/20241098

[12] Jallepalli D et al 2021 Federated Learning for Object Detection in Autonomous Vehicles IEEE Seventh International Conference on Big Data Computing Service and Applications (BigDataService) Oxford United Kingdom 107-114
[13] Zheng T Li A Chen Z Wang H Luo J 2023 AutoFed: Heterogeneity-Aware Federated Multimodal Learning for Robust Autonomous Driving arXiv 2302.08646
[14] Zhang H Yang Z Tian Y Zhang H Di B Song L 2023 Reconfigurable Holographic Surface Aided Collaborative Wireless SLAM Using Federated Learning for Autonomous Driving IEEE Transactions on Intelligent Vehicles
[15] Fu Y Li C Yu F R Luan T H Zhang Y 2023 A Selective Federated Reinforcement Learning Strategy for Autonomous Driving IEEE Transactions on Intelligent Transportation Systems 24(2) pp 1655-166