

Federated Learning for Connected and Automated Vehicles: A Survey of Existing Approaches and Challenges

Vishnu Pandi Chellapandi, *Member, IEEE*, Liangqi Yuan, *Student Member, IEEE*, Christopher G. Brinton, *Senior Member, IEEE*, Stanislaw H. Źak, *Life Member, IEEE*, and Ziran Wang, *Member, IEEE*

Abstract—Machine learning (ML) is widely used for key tasks in Connected and Automated Vehicles (CAV), including perception, planning, and control. However, its reliance on vehicular data for model training presents significant challenges related to in-vehicle user privacy and communication overhead generated by massive data volumes. Federated learning (FL) is a decentralized ML approach that enables multiple vehicles to collaboratively develop models, broadening learning from various driving environments, enhancing overall performance, and simultaneously securing local vehicle data privacy and security. This survey paper presents a review of the advancements made in the application of FL for CAV (FL4CAV). First, centralized and decentralized frameworks of FL are analyzed, highlighting their key characteristics and methodologies. Second, diverse data sources, models, and data security techniques relevant to FL in CAVs are reviewed, emphasizing their significance in ensuring privacy and confidentiality. Third, specific applications of FL are explored, providing insight into the base models and datasets employed for each application. Finally, existing challenges for FL4CAV are listed and potential directions for future investigation to further enhance the effectiveness and efficiency of FL in the context of CAV are discussed.

Index Terms—Federated learning, connected and automated vehicles, distributed computing, privacy protection, data security.

I. INTRODUCTION

CONNECTED and automated vehicles (CAV) are the key to future intelligent transportation systems (ITS) that encompass both ground and air transportation [1]–[9]. With the advent of big data, the Internet of Things (IoT), edge computing, and intelligent systems, CAVs have the potential to improve the overall transportation system by reducing traffic accidents, congestion, and pollution [10]–[13]. CAVs integrate both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication capabilities, facilitating an enhanced perception of the environment beyond the direct line of sight [14]–[16]. This involves interaction with other vehicles, traffic signals, pedestrians, and other elements of the transportation ecosystem. Furthermore, CAVs are designed to assume control of driving tasks by the

V. P. Chellapandi, L. Yuan, C. G. Brinton, S. H. Źak, and Z. Wang are with the College of Engineering, Purdue University, West Lafayette, IN 47907, USA (e-mails: cvp@purdue.edu, liangqiy@purdue.edu, cgb@purdue.edu, zak@purdue.edu, ryanwang11@hotmail.com).

human operator under certain conditions, using a variety of sensors and sophisticated machine learning (ML) algorithms to achieve autonomous operation.

Currently, CAVs are generating a tremendous amount of raw data, between 20 and 40 TB per day, per vehicle [17]. The various sources of these data include engine components, electronic control units (ECU), perception sensors, and vehicle-to-everything (V2X) communications. This large amount of data is sent to other vehicles, roadside infrastructures, or the cloud, continuously or periodically for monitoring, prognostics, diagnostics, and connectivity features [18]. This flow of data has driven the flourishing deployment and application of ML in CAVs, including areas such as Advanced Driver-Assistance Systems (ADAS) [19], automated driving [20], ITS [21], and sustainable development [22].

A. Motivation

Due to the large amount of data required to train ML models, concerns have been raised about data security in terms of the legitimacy of data collection, data misuse, and privacy breaches. Data collected by various sensors in CAVs, are also considered private and are subject to stringent privacy protection regulations in different regions. One such example is the General Data Protection Regulation (GDPR) in the European Union [23], which imposes strict requirements and guidelines on the handling and processing of personal data to ensure individuals' privacy rights are protected. Even with the development of advanced ML techniques and vehicle connectivity, it has not been feasible to have a secure framework to collect data from every vehicle and train an ML model. These limitations led to the development of a new ML paradigm known as Federated Learning (FL) [24], [25]. The term Federated Learning (FL) has been coined by Google [26]. FL was initially used for mobile keyboard prediction in Gboard [27] to allow multiple mobile phones to cooperatively and securely train an ML model. FL has been extensively applied in various fields such as industry [28]–[30], energy [31], [32], healthcare [33], [34], and more.

In FL, edge devices/clients only send the gradients or the learnable parameters to cloud servers rather than sending massive local datasets in a centralized learning framework.

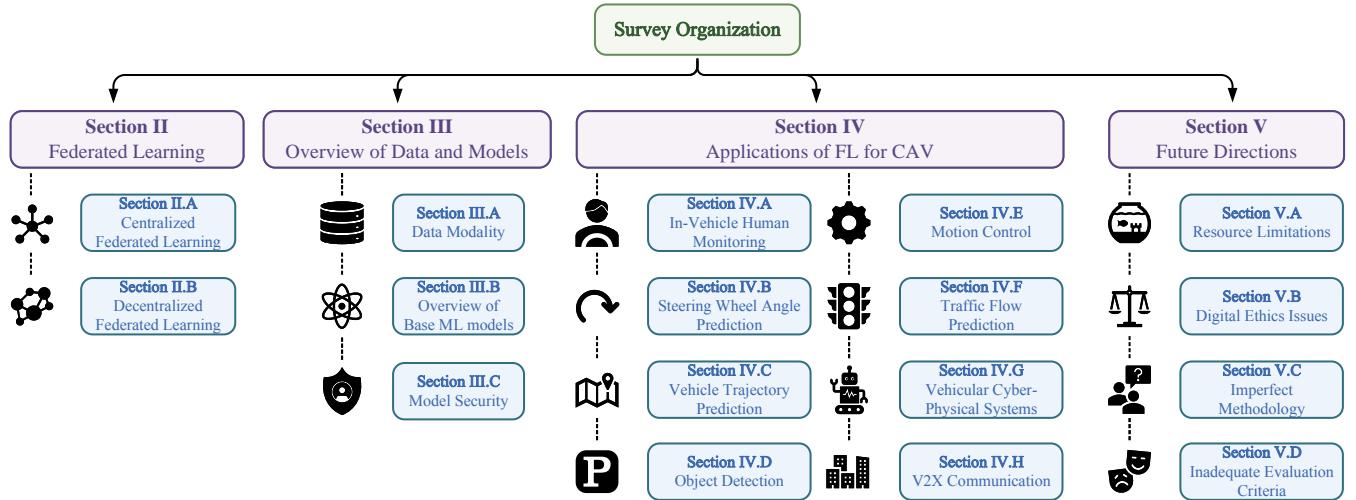


Fig. 1. Roadmap of this survey paper.

Cloud servers perform a secure aggregation of the received gradients/weights and update the global model parameters that are transmitted back to clients/edge devices [35]. This procedure, known as a communication round, continues iteratively until the convergence criteria are met in the global model optimization. The key advantage of FL is reducing the strain on the network while also preserving the privacy of the local data. FL is a potential candidate that can utilize the data available from each CAV and develop a robust ML model.

Despite the benefits of V2X communications among CAVs, the invasion of privacy, accuracy, effectiveness, and communication resources is an essential concern to be addressed. FL frameworks have received attention for their natural ability to preserve privacy by transmitting only model data between the server and its clients without including local vehicle data. In particular, the model data packets are smaller than the user data, thus saving the consumption of communication resources. Similarly, FL frameworks distribute training tasks to each client, and the server does not perform training but only aggregates, which can reduce the computational demand on the server and improves training efficiency. Recently, there have also been efforts to train a decentralized FL that allows multiple vehicles to collaboratively train a model without needing a central server [36], [37]. In our first survey of FL for CAV (FL4CAV) presented in [38], we emphasized applications and explored foundational challenges in the subject. Building upon that conference version, this extended journal paper further delves into the underlying methodologies, provides a more comprehensive review of recent developments, and introduces novel insights and evaluations, thereby presenting a more exhaustive and nuanced understanding of the field.

B. Paper Organization

In this paper, we provide a survey of FL4CAV, including deployment of various FL frameworks on CAVs, data modalities and security, diverse applications, and key challenges. The organization of this survey is shown in Fig. 1. The following topics are covered in this survey:

- A systematic review of FL algorithms is conducted, specifically focusing on their deployment in CAVs. Additionally, we examine the integration of ML models within the FL framework for CAV applications.
- Data modalities and data security considerations in CAVs are summarized, highlighting the diverse range of multi-modal data generated by various sensors.
- Critical applications of FL4CAV are explored, such as driver monitoring, steering wheel angle prediction, vehicle trajectory prediction, object detection, motion control application, traffic flow prediction, and V2X communications.
- Current challenges and future research directions of FL4CAV are highlighted, such as performance, safety, fairness, applicability, and scalability. A comparison of our survey with other related surveys can be found in Table I.

The remainder of this survey is organized as follows. In Section II, we describe the two main FL frameworks along with their algorithms. In Section III, we discuss various data modalities, ML methods used in FL4CAV applications, and FL data security in CAVs. Section IV reviews various applications of FL in CAVs. The multi-modal data, algorithms, and datasets used in the relevant literature are also summarized. Challenges and potential research areas are discussed in Section V. In Section VI, we present conclusions of this survey.

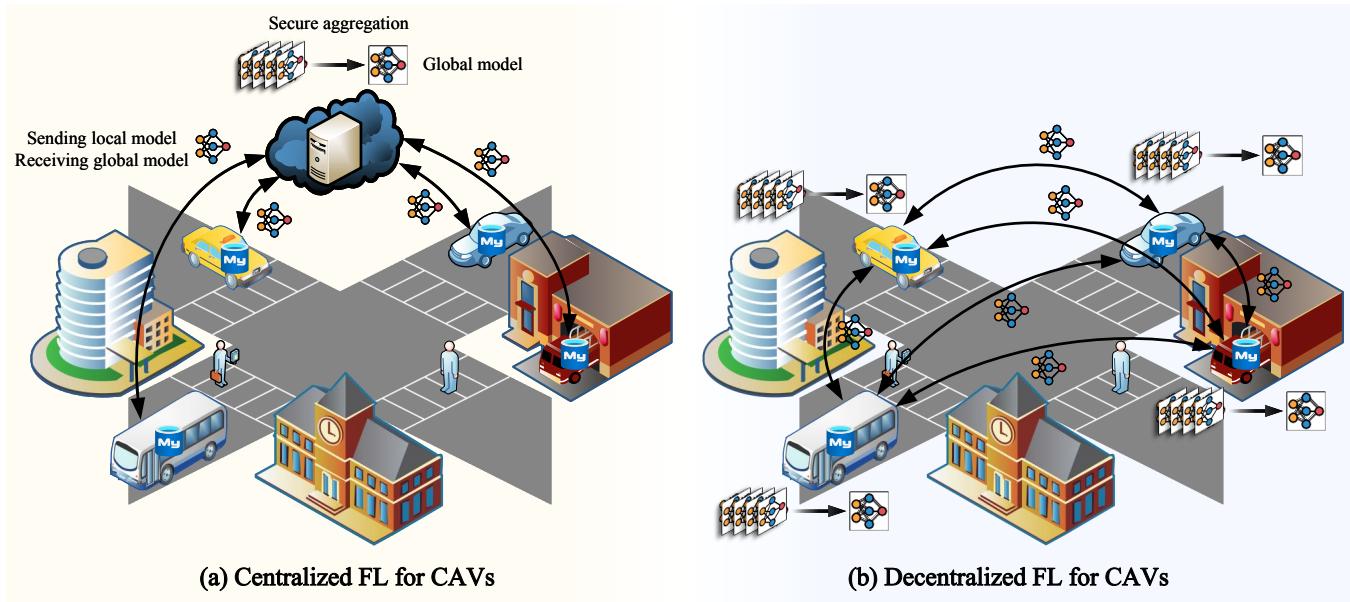


Fig. 2. Illustration of (a) centralized and (b) decentralized federated learning for connected and automated vehicles.

aggregation process on the server—see Table III. FedAvg applies SGD optimization to local vehicles and performs a weighted averaging of the weights of the vehicles on the central server. FedAvg performs multiple local gradient updates before sending the parameters to the server, reducing the number of communication rounds. For FL4CAV, data on each CAV are dynamically updated at each communication round.

A typical FL setup has K vehicles that have their own local data sets and the ability to perform simple local optimization. At the central server, the optimization problem can be represented as

$$\min_{x \in \mathbb{R}^d} \left[f(x) = \frac{1}{K} \sum_{i=1}^K f_i(x_i) \right], \quad (1)$$

where $f_i : \mathbb{R}^d \rightarrow \mathbb{R}$ for $i \in \{1, \dots, K\}$ is the local objective function of the i^{th} vehicle. The local objective function of the i^{th} vehicle can have the form,

$$f_i(x_i) = \mathbb{E}_{\xi_i \sim \mathcal{D}_i} [\ell(x_i, \xi_i)], \quad (2)$$

where ξ_i represents the data that have been sampled from the local vehicle data \mathcal{D}_i for the i^{th} vehicle. The expectation operator, \mathbb{E} , is acting on the local objective function, $\ell(x_i, \xi_i)$, with respect to a data sample, ξ_i , drawn from the vehicle data, \mathcal{D}_i . The function $\ell(x_i, \xi_i)$ is the loss function evaluated for each vehicle, x_i , and data sample, ξ_i . Here, $x_i \in \mathbb{R}^d$ represents the model parameters of vehicle i , and $X \in \mathbb{R}^{d \times K}$ is the matrix formed using these parameter vectors. The learning process is performed to find a minimizer of the objective function, $x_i = x^* = \arg \min_{x \in \mathbb{R}^d} f(x)$.

The data obtained from CAVs are typically non-independent and non-identically distributed (non-IID). Fe-

dAvg faces challenges in realistic heterogeneous data settings, as a single global model may not perform well for individual vehicles, and multiple local updates can cause the updates to deviate from the global objective [45]. Several variants of FedAvg have been proposed to address the challenges encountered by FL, such as data heterogeneity, client drift, local vehicle data imbalance, communication latency, and computation capabilities. FedProx algorithm, FedAvg with a proximal term, has been proposed to improve the convergence and reduce communication cost [46]. Dynamic Federated Proximal [47] algorithm (DFP) is an extension of FedProx that could effectively deal with non-IID data distribution by dynamically varying the learning rate and regularization coefficient during the learning process. FedAdam [48] has shown improved convergence and optimization performance by incorporating ADAM optimization in the FedAvg algorithm. Improving the performance of the FL model is an ongoing research activity [49]–[52].

2) *Knowledge Distillation*: In this subsection, we discuss the integration of knowledge distillation with FL. Federated Distillation (FD) [53] uses knowledge distillation to transfer knowledge in a decentralized manner, leading to a significant reduction in the communication size compared to a traditional FL. It also has the ability to handle non-IID data samples [54]. Wang *et al.* [55] proposed a conceptual framework called FD for CAV (FDCAV), where CAVs share their outputs (e.g., bounding boxes) with a central server, which computes the average output from the global model and sends it back to vehicles. The vehicles then update their local models based on the output of the global model [55].

Another approach is to deploy a teacher model on the server and student models on the clients. In this process,

However, DFL also encounters notable limitations, including hindered convergence (caused by the heterogeneity of data) and network latency, and the need to synchronize/arbitrate parameters and adapt to dynamic network topologies during vehicle communications. These challenges arise from the decentralized nature of the FL framework, which requires efficient mechanisms to address disparities in data distribution and network connectivity among the participating vehicles [61]–[65].

III. OVERVIEW OF DATA MODALITIES, BASE MACHINE LEARNING MODELS, AND SECURITIES

The concept of FL4CAV is illustrated in Fig. 2. Each CAV as a client, undertakes sensing data acquisition, signal processing, storage, communication, perception, and decision-making. For sensing data acquisition, a variety of sensors are integrated into CAVs, including Global Navigation Satellite Systems (GNSS), multi-modal cameras, Radio Detection And Ranging (Radar), Light Detection And Ranging (LiDAR), and Inertial Measurement Unit (IMU) to capture the vehicle, driver, passenger, and external information.

CAV tasks are diversified to include tracking the target speed, prediction of behavior, motion planning, motion control, object detection, and in-vehicle human monitoring. After training on ML models with local data, clients send the trained model to the server. Then, the server shares a generalized model with clients for perception, prediction, and decision-making purposes. The FL4CAV framework shows a trend towards multi-modal sensing data, massively parallel clients, and multi-class tasks.

An overview of the data modalities, the base ML models of CAVs, and data security is presented next.

A. Data Modality

CAVs collect multi-modal data from various sensors to perform tasks such as navigation and perception. The impact of different types of data modalities during the FL process on sensor fusion is dynamically diverse [66]. The data collected by sensors depend on the sensor type, the sensor's range, the accuracy/precision of the sensor, sensor placement, and the operating environment. The operating environment, such as snow, heavy rain, or fog, can reduce sensor visibility, thereby deteriorating data quality. These factors lead to variations that can significantly affect the sensor performance. The performance of the FL model is directly dependent on the quality of the data collected by the vehicles. The data resolution, size, and sampling rate obtained from CAVs are generally heterogeneous, and processing the data is also a challenging task. In the following, we review the various data modalities in FL4CAV applications that are illustrated in Fig. 4.

1) Image: Images, especially visible RGB images, are one of the most important data modalities for CAVs. Vision-related tasks, such as driver monitoring IV-A, steering wheel angle prediction IV-B, object detection IV-D, traffic sign recognition [67], and semantic segmentation [68] use images captured by the camera as the data source. In most applications, various ML models are trained to achieve the intended functionality. However, due to its intrusive design, privacy issues are always a concern for image-based systems, especially for in-cabin and driver-related applications [69]–[73]. Privacy concerns for visual image-based systems are addressed by FL since only the model parameters are transmitted while the user data are kept locally in the vehicle. Moreover, FL also solves the data transmission problem due to the large size of images and video data, thus leading to a more communication-efficient learning framework.

2) LiDAR: LiDAR data is vital for automated driving capabilities, which has been used for object detection tasks [74], [75] and cooperative perception scenarios [76], [77]. LiDAR generates 3D point clouds that can detect objects accurately even under adverse weather conditions, unlike camera data that are unreliable under similar conditions. However, the dense point cloud of LiDAR data makes transmission a demanding task. FL system for LiDAR data can improve learning efficiency and save communication resources while being able to handle large data sets.

3) Radar: Radar sensors are used for object detection and collision avoidance in applications such as automatic emergency braking, traffic alerts, and adaptive cruise control [78]–[81]. Radars have long operating ranges, good measurement accuracy, and are operational in varying weather conditions [82]. Radar data provides critical information about the vehicle's surroundings, including the position and the speed of other objects. Similarly to LiDAR, the FL system for Radar can also improve learning efficiency and save communication resources.

4) Vehicle Status and GNSS: Vehicle status data such as velocity, acceleration, throttle/brake command, vehicle global position through GNSS, and other vehicle parameters are also an important part of the CAV data modality. These parameters are relevant primarily to the vehicle rather than to the external environment. These data typically reveal sensitive information about driver locations, habits, and behaviors that could potentially compromise their privacy and security. FL addresses these privacy concerns well while utilizing these data to improve several applications such as collision avoidance [83], vehicle trajectory prediction IV-C, and motion control application IV-E.

B. Base Models in FL4CAV Applications

ML has been widely used to achieve superior performance in various complex tasks, given the availability of multi-modal data from in-vehicle sensors. Furthermore, the ML in FL4CAV shows the feasibility of implementation in real

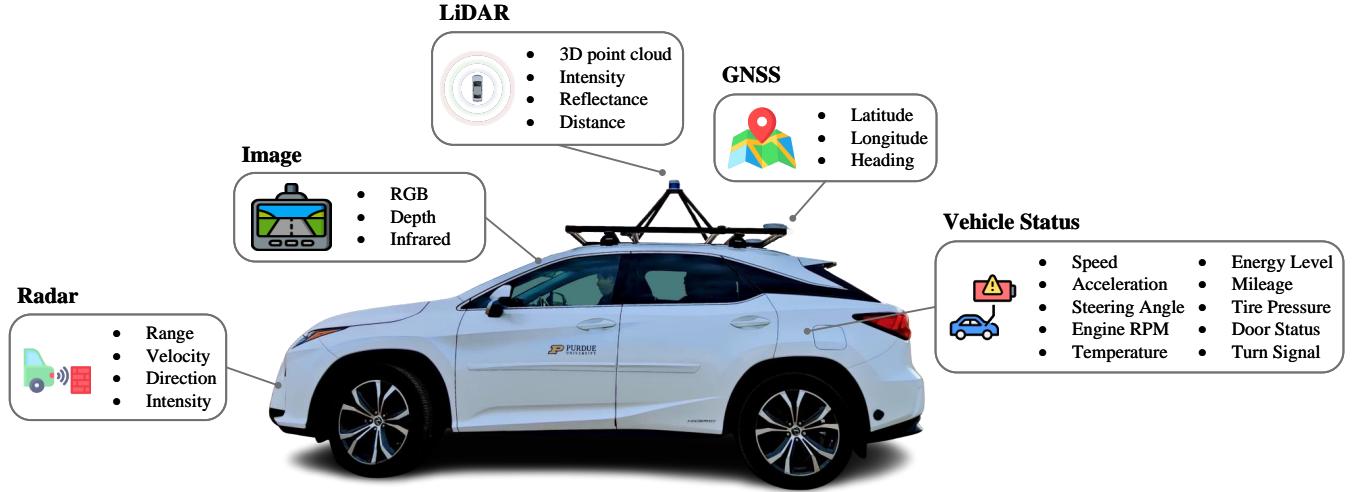


Fig. 4. Illustration of various data sources from a connected and automated vehicle.

time, which is required due to the limited computing and communication resources of vehicle equipment. We next discuss the various ML architectures that are used as base models in critical tasks of CAVs.

1) Multilayer Perceptron: A Multilayer Perceptron (MLP), as a classic ML architecture, consists of multiple layers of fully connected neurons. It can be applied to various vehicle-related tasks, including perception, decision-making, and control. MLP provides a flexible and versatile tool for modeling complex relationships in vehicle-related data. However, its performance in specific tasks may be limited due to the computational demand for large models. Due to their applicability, MLPs are widely employed in vehicle trajectory prediction (Sec. IV-C), motion control (Sec. IV-E), and traffic flow prediction (Sec. IV-F).

2) Convolutional Neural Network: Convolutional Neural Networks (CNNs) are presently one of the most popular architectures in ML. They are known for their excellent performance in handling image-related tasks. CNN uses convolutional layers to automatically extract features from images and learn to associate these features with corresponding labels. CNNs exhibit versatile performance in performing a wide range of tasks, including, but not limited to, classification (as exemplified by LeNet [84], ResNet [85]), object detection (such as the YOLO [86] framework), and mask generation for semantic segmentation (represented by models such as U-Net [87], BiSeNet [88]), among others. Due to its high efficiency in extracting features from image data, CNNs are widely applied in various vehicle-related applications, such as in-vehicle human monitoring (Sec. IV-A), steering wheel angle prediction (Sec. IV-B), object recognition (Sec. IV-D).

3) Recurrent Neural Network: Recurrent Neural Networks (RNNs) excel at extracting spatial relationships in features. They are specifically designed to capture temporal dependencies in sequences of data. Some popular RNN architectures

include Long Short-Term Memory (LSTM) [89] and Gated Recurrent Unit (GRU) [90]. In the context of vehicles, RNNs have found extensive applications in modeling the motion and behavior of vehicles, their surroundings, and targets. Using their sensitivity to time series data, RNNs can effectively capture the dynamics and temporal patterns in various vehicle-related scenarios, for example vehicle trajectory prediction (Sect. IV-C) and traffic flow prediction (Sec. IV-F).

4) Transformer: Transformer [91] architecture and its variant, Vision Transformer (ViT) [92], have emerged as powerful alternatives to traditional CNNs and RNNs. The Transformer architecture, initially introduced for natural language processing tasks, has shown exceptional performance in various domains, including computer vision. Transformers take advantage of self-attention mechanisms to capture global dependencies across the input sequence or image. This allows them to effectively model long-range dependencies and contextual relationships, leading to improved performance in tasks such as image classification, object detection, and semantic segmentation. Transformers' ability to capture global context and long-range dependencies makes them well-suited for various tasks in the automotive domain [93]. Transformers and ViTs have attracted substantial attention in the fields of FL [94] and CAV [95] due to their ability to effectively capture global information. Transformers and ViTs have a potential for a wide range of vehicular applications (Sec. IV).

5) Generative Network: Generative networks form images based on input data, such as mask labels and super-resolution. These networks, also known as Generative Adversarial Networks (GANs) [96] or Variational Auto-Encoders (VAEs) [97], exhibit a distinctive ability to generate high-quality and realistic images. Generative networks have attracted attention in both the FL [98] and CAV [99] domains. However, there is still no unified framework that incorporates all three technologies. With the extensive application of generative networks in CAV, combined with FL's enhancement

of privacy protection and learning efficiency, they have a potential for various applications. In vehicular applications, generative networks provide several use cases, such as vehicle trajectory prediction (Sec. IV-C). One application lies in super-resolution, where generative networks can enhance the resolution and details of low-resolution images, proving useful for tasks such as license plate recognition and surveillance systems. Furthermore, generative networks can also be utilized to augment and improve data sets in training data sets for vehicle-related tasks.

6) Reinforcement Learning: Reinforcement learning (RL) demonstrated superior capabilities in solving complex decision-making problems, surpassing human-level performance in various domains [100]. RL improves the abilities of the agent through interaction with the environment, enabling the agent to learn optimal policies through trial and error. RL has been extensively applied in CAV operations, such as motion control (Sec. IV-E), vehicle trajectory prediction (Sec. IV-C), vehicular CPS (Sec. IV-G), and resource allocation [101]–[103].

C. Model Security

Robust and secure privacy preservation techniques are essential to protect sensitive data during the FL training process for CAVs. It is demonstrated that the training can still be vulnerable to various malicious attacks, such as when one or more participants are compromised, and they could transmit false parameters to hinder the global model performance. The FL central server is also prone to attacks that may cause the entire learning process to collapse [104]. The type of data considered in this section refers to the model parameters, such as gradients or weights, that are transmitted to the server/neighboring vehicles. These are not the raw data used for the training of the local model, as they are inherently preserved in the FL process.

Homomorphic encryption, differential privacy, and blockchain-based techniques are notable methods to preserve privacy in FL4CAV. These approaches aim to minimize the trade-offs between model performance and data privacy, ensuring data security while enabling effective model performance. A review of various cyber-security threats can be found in [105]–[110]. We will next discuss some of the widely used privacy-preserving techniques.

1) Homomorphic encryption: Homomorphic Encryption (HE) is a powerful technique that allows the server to perform training on encrypted vehicle data without the need for decryption, thus ensuring data privacy and security. In particular, it allows direct computation on encrypted data with decrypted results [111].

2) Differential Privacy: Differential Privacy (DP) is an approach that safeguards data privacy by injecting random noise into the data before transmitting them to the server, preventing unauthorized extraction of sensitive information while also preserving data ownership and alignment with regulatory

compliance. However, there is a trade-off between privacy settings and accuracy that can impact the performance of the models. DP has been used in multiple applications of FL4CAV for incorporating data security [112]–[116].

3) Secure Multi-Party Computation: Secure Multi-Party Computation (SMPC) employs cryptographic techniques to encrypt and partition the data, enabling collaborative computation on these data with output results accessible to vehicles. While SMPC introduces considerable communication overheads, it excels in preserving data security and privacy. The SMPC integration framework with FL facilitates model training on data without exposing model parameters [117], [118]. In an FL setup, SMPC can substantially encrypt the communication of model updates. Furthermore, vehicles can apply SMPC for collaborative intermediate computations, ensuring that even if the central server is compromised, no meaningful information can be derived from these computations.

4) Physical Security: In model security enhancement, reinforcement at the physical layer emerges as a key approach. Beyond the security measures required for both the vehicle and the server, hardware-level security technologies, such as the Trusted Execution Environment (TEE), offer participants in FL an isolated, secure, and confidential execution environment [119]. With the support of TEE, vehicles can process and store data within a protected environment, iterating and refining their local models. Similarly, the server, using the support of TEE, can execute model aggregations in a secure context.

5) Blockchain: Another disruptive technology gaining traction in CAV applications is blockchain-based methods, leveraging the decentralized and tamper-resistant nature of blockchain to improve data integrity, transparency, and security [120]–[127]. Blockchain is a type of digital ledger technology that securely transfers data in a decentralized framework. CAVs share their data with the vehicular network and the information is stored on the blockchain. Blockchain provides a secure, credible, and decentralized approach to FL, enabling collaborative model training while safeguarding data privacy [128]. The system is designed to protect data privacy and security, as well as to provide greater security to the general vehicular networks involved in the learning process [129]. An analysis of various privacy preservation approaches is given in [106], [130].

In FL4CAV, the model parameters of individual vehicles can be stored as transactions on the blockchain, ensuring transparency and accountability. This creates trust among the vehicles, as the model updates can be verified. Additionally, blockchain enables incentive mechanisms through smart contracts, which reward CAVs that contribute high-quality model updates or share their computational resources for training. These incentives encourage active participation and foster collaboration among vehicles [111], [131]–[133].

IV. APPLICATIONS OF FL FOR CAV

In this section, we review some applications of FL in CAV. The FL4CAV literature, including FL configuration, data modalities, underlying models, applications, FL algorithm, and datasets, can be found in Tables III and IV. The strengths of FL, such as protecting privacy, improving learning efficiency, improving generalization ability, and reducing communication overhead, resulted in several FL4CAV applications.

A. In-Vehicle Human Monitoring

In-vehicle human monitoring is a critical issue for CAV and ITS. The in-vehicle human monitoring serves not just the driver but also extends to the other passenger monitoring in vehicles [174]. Beyond the application in commercial taxis, human monitoring becomes particularly critical in large public transportation modes such as buses, subways, ferries, and more, where adequate human personnel for service may be lacking. Consequently, computer-aided monitoring programs can effectively offer superior service quality and protect passenger safety by handling tasks such as passenger counting, passenger traffic, detecting elderly falls, and emergency situations such as fires.

FL significantly enhances privacy protection, enriches and diversifies knowledge, and improves learning efficiency, which makes it crucial for the application of human monitoring in the vehicle in the deployment of CAVs. Given the sensitivity of personal privacy and the rarity of traffic accidents, FL serves as a valuable tool in these contexts. FL has the potential to enhance the security of user data onboard while enabling knowledge transfer and ensuring the generalizability of the model. However, in human-related applications where data are highly heterogeneous and personalized, it can be challenging to balance the generalization ability of the model with the need for personalization to specific users [175].

Driver monitoring applications, such as distraction detection, are critical safety features that monitor driver stability and alertness and warn distracted drivers to apply safety-critical actions [149], [176]–[179]. The computational and communication efficiency issues in driver activity recognition are addressed in [71] and a novel framework (FedGKT) was proposed to reduce communication bandwidth and asynchronous training requirements. Driver privacy may be a greater concern than steering wheel angle prediction and object recognition, leading to FL's ability to be more highlighted in terms of privacy protection. However, the driver monitoring application is a highly personalized application where the driver's behavior is strongly associated with personal habits, emotions, cultural background, and even the interpretation of instructions. This user heterogeneity poses a challenge for FL systems. For human-related applications, such as driver monitoring, personalized FL is the dominant solution [72]. A DFL framework was proposed in [148] that incorporates a gossip protocol for knowledge dissemination.

This framework not only achieves personalized models without requiring any additional processing, but also incorporates a knowledge dissemination technique that significantly accelerates the training process.

Passenger monitoring applications are an emerging research area that involves detecting passengers' intents to board and leave and warning of dangerous behavior in public transportation [180]. However, this field has not yet received much attention due to the lack of available datasets and the difficulty of monitoring multiple users simultaneously. Nevertheless, the ability of FL to integrate knowledge about public transportation and the growing demand for passenger monitoring makes FL a promising application in this area.

B. Steering Wheel Angle Prediction

The prediction of the angle of the steering wheel has become a crucial feature of self-driving. The performance of ADAS features, such as lane keep assist and lane departure warning, is based on the prediction of the steering angle [181], [182]. The steering wheel angle prediction is used to estimate the steering wheel rotation angle based on the input of road images. The prediction of the steering wheel angle manages the lateral positioning of the vehicle, even under challenging circumstances, such as on unpaved and unmarked roads. The steering wheel angle prediction needs to adapt to different driving and environmental conditions, and thus requires continuous model updates for high accuracy.

FL achieves the above objectives by enabling several vehicles to collaborate in learning from new data and updating the model in a relatively short time. FL offers the benefit of continuous and collaborative learning, low communication overhead, and data security that is needed to develop a robust prediction model.

It was demonstrated that FL can collectively train the prediction model while, at the same time, significantly reducing communication costs. The study presented in [136] demonstrated a significant improvement in edge model quality through the use of FL in CAV. Specifically, the study involved predicting steering wheel angles using two modalities of data: images and optical flow. In [137], the performance of FL and centralized learning in steering angle prediction was assessed under different levels of noise and the results were comparable. Furthermore, this study considered the implications of communication load and disruptions, providing a comprehensive evaluation of the systems. This makes FL suitable for applications involving an increasing number of CAVs, specifically for tasks such as steering wheel angle prediction.

C. Vehicle Trajectory Prediction

An accurate vehicle trajectory prediction allows CAVs to perform proper motion planning, as well as anticipate potentially dangerous behaviors of other vehicles, such as sudden lane change, skidding, or hard braking, react proactively and

prevent accidents [183]–[187]. This is a challenging task and would require substantial amounts of sensitive vehicle data to train a model for trajectory prediction.

FL is a viable solution that provides a collaborative learning framework with multiple vehicles while keeping sensitive local data private and secure. FL models are trained on diverse data from various vehicles operating in different scenarios. This enhances the generalization of the model and enables vehicles to handle rare events such as traffic accidents, adverse weather, and risky behaviors. Additionally, the FL framework supports continuous learning and model updates, allowing quick adaptation to dynamic traffic, road conditions, and unfamiliar scenarios.

Trajectory prediction models commonly rely on time series data that encompass vehicle/passenger position, velocity, and acceleration. These models leverage the strength of deep neural networks, mainly RNNs, and Transformers, that have proven effective in predicting trajectories for various entities, including vehicles and pedestrians, while also capturing their behavioral patterns [188]. FL framework has been shown to be effective in learning spatio-temporal features with the Transformer model [147] (or the LSTM model [189]) while also protecting user privacy. FL coupled with One-Class Support Vector Machine (OC-SVM) has been used to detect anomalous trajectories at traffic intersections [190]. The reported findings indicate that the federated approach improves both the overall accuracy of anomaly detection and the benefit of individual data owners. FL has been reported to perform similarly to centralized learning [144], [191], [192]. Centralized learning requires that all data from the private vehicle be transferred to the central server for training, whereas the data are kept locally in the vehicle in the case of FL.

D. Object Recognition

Object recognition is one of the main functions of the visual perception system of CAVs intended to detect and localize objects using sensor data such as LiDAR and high-resolution image/video. These data are large in size and sensitive from a privacy point of view. As a result, there are limitations to deploying robust detection models in a traditional centralized learning approach due to privacy and communication overhead. These concerns can be mitigated by using an FL-based approach for CAVs. FL can effectively help CAVs detect various objects in different driving scenarios, road types, traffic conditions, and weather types. FL enables the CAV framework to learn efficiently with low communication overhead, which is particularly advantageous when the volume of data is much larger than the size of the ML model while also ensuring the privacy of the data.

FL has already been used in computer vision-related tasks, such as developing safety hazard warning solutions in smart city applications [193]. The accuracy of object detection models is generally poor under adverse weather conditions

such as snow and rain. FL frameworks have been shown to improve detection accuracy [194] and perform better than the centralized and gossip-decentralized models [138]. Recently, studies have been carried out to improve the performance of FL on complex tasks such as object detection [195]. In [55], it has been shown that with multistage resource allocation and appropriate vehicle selection, FL performance improved significantly compared to traditional centralized learning and baseline FL approaches. In [142], a decentralized FL method is used for object classification using LiDAR on CAVs. The parameters of the ML model (PointNet [196]) are communicated through V2V networks. It has been experimentally confirmed that FL is highly effective compared to self-learning approaches.

Another important application of FL is the recognition and detection of license plates. It is used in ITS for applications such as traffic safety and violations, traffic monitoring, illegal/overtime parking detection, and parking access authentication. ML techniques have been shown to be highly efficient in detecting objects and recognizing license plates [197]–[200]. However, due to the large size of the data from all vehicles, it is not feasible to train on a real-time edge device. FL techniques offer numerous advantages to license plate detection and recognition systems, namely: privacy protection, enabling collaborative learning, and reduced network bandwidth requirements. These benefits of using FL contribute to increased effectiveness and adaptability of such systems in real-world scenarios [201], [202].

E. Motion Control

The motion controller of the vehicle executes the desired trajectory by determining the optimal control of the acceleration pedal position (longitudinal acceleration motion), the steering of the vehicle (lateral motion) and the brake position (longitudinal deceleration motion) [203]–[205]. FL enables CAVs to train and optimize controller parameters collaboratively. Some potential benefits of using FL are enabling CAVs to adapt to unseen routes/traffic scenarios or operating conditions due to previous data from other CAVs, acceleration on the ramp, driving in congested conditions, or challenges associated with higher vehicle speed [206]. FL enables CAVs to adapt to different driving scenarios, including unfamiliar roads, cities, and countries. Furthermore, FL may allow CAVs to adjust driving styles based on different driving habits, climates, scenarios, and cultural norms.

FL has been used to dynamically update the controller parameters, resulting in improved achievement of the target speed with enhanced driver comfort and safety [47]. Additionally, FL finds application in collaborative optimization of control parameters between multiple vehicles at traffic intersections, resulting in the avoidance of collisions and improved driving comfort [207], [208]. In [209], FL is utilized to improve brake performance under different driving conditions and environments by accurately determining road

friction coefficients. This approach ensures the privacy of the driver while optimizing the braking action. In [47], an FL framework is proposed to optimize the controller design for CAVs with variable vehicle participation in the FL training process.

Reinforcement Learning (RL) approach has been widely applied for motion control in vehicles due to its ability to train in complex scenarios with dynamic environments. RL enables CAVs to learn control policies for the required objectives with user feedback and sensor measurements [101], [210]–[213]. There are open research problems in motion control of CAVs that could be addressed by FL such as platooning, lane change maneuvers, merging on-ramps, signalized, and unsignalized intersections. A review of existing CAV control methods is provided in [214]–[216], while applications of ML to CAV control are reported in [217]–[222].

F. Traffic Flow Prediction

Traffic flow prediction is one of the critical components of an ITS for efficient traffic control, safety, and management. Accurate predictions using historical data to forecast future traffic conditions can lead to reduced traffic congestion, such as optimal route recommendation and variable road signal timing. Predicting traffic flow can also allow timely notification to authorities of occurrences of events, such as accidents and congested road conditions. ML techniques, such as CNNs and RNNs, have shown promising results in predicting traffic flow [223]–[225].

FL has been used to predict traffic flow with improved accuracy while ensuring privacy and scalability. Sources for model training include data from CAV, RSUs, and traffic sensors. The predictions could be in real-time or for future time intervals, and the model can be trained to predict traffic patterns and improve the accuracy of traffic flow predictions. FL allows CAVs to collaboratively learn from their data while addressing privacy concerns.

In [135], a Gated Recurrent Unit (GRU) network is trained using FL to predict traffic flow. Experimental evaluations of a real-world data set show that the FL-based approach can achieve predictions comparable to those of traditional centralized approaches. In [226], an FL-based Spatial-Temporal Networks (FedSTN) algorithm was proposed to predict traffic flow. The algorithm employs various methods like Recurrent Longterm Capture Network, Attentive Mechanism Federated Network, and Semantic Capture Network (SCN) to learn spatial-temporal and semantic information. It is reported that the FedSTN algorithm outperforms in terms of higher prediction accuracy compared to existing baselines such as Auto-Regressive Integrated Moving Average (ARIMA), eXtreme Gradient Boosting (XGBoost), FedGRU, and ST-ResNet [227]. In [228], a Long-Short-Term Memory (LSTM) is trained in an FL framework for traffic flow prediction along with an RL that is used for resource optimization. In [145], an

FL framework employing LSTM algorithm has been trained on a real Vehicular Ad hoc NETwork (VANET) data set based on V2V and V2R communication for the prediction of network traffic. The above developments show the benefits of using FL for complex tasks such as traffic flow prediction.

G. Vehicular Cyber-Physical Systems

Vehicular Cyber-Physical Systems (VCPS) encompass the integration of physical systems, cyber systems, and vehicular communication networks [229]. Physical systems comprise vehicles, roads, and telematics/edge devices, while cyber systems include data centers, central servers (i.e., cloud), and traffic management systems. Vehicular networks, namely Cellular Vehicle-to-Everything (C-V2X) and V2X communication networks, play a key role in facilitating information sharing to improve driving comfort, safety, and traffic management. VCPS utilizes various technologies to enhance the vehicular network and enable seamless and robust communication between vehicles and systems.

FL plays a critical role in VCPS by enhancing data privacy and addressing resource constraints. FL uses a collaborative and distributed learning framework that captures data heterogeneity while eliminating the need to transfer local data from vehicles. This enables VCPS to benefit from FL's ability to preserve data privacy and facilitate efficient learning without compromising resource limitations.

In [230], an FL framework is proposed to detect and mitigate data leakage in VCPS while enhancing data privacy. The proposed scheme achieves good accuracy, efficiency, and high security based on simulations of a real-world data set. In [231], an FL framework (OES-Fed) is proposed for outlier detection and noise filtering in vehicular networks. In [232], extreme value theory (EVT) and personalized FL are proposed to model anomalous events caused by the non-heterogeneous data distribution among vehicles in vehicular networks. In [233], an efficient and secure FL framework is combined with the Deep Q-Network (DQN) to ensure an efficient and secure scheme to reduce the latency of vehicular data sharing in vehicular networks.

FL has gained significant acceptance for enhancing the resilience and robustness of VCPS networks against adversarial attacks. This is achieved through the integration of FL with techniques such as differential privacy [234] and blockchain-based approaches [133], [235]. These combinations have shown promising results in improving the security and reliability of the VCPS network.

H. Vehicle-to-Everything Communication

An efficient and robust V2X communication such as V2V and V2I is a crucial step towards achieving an ITS. V2X communication plays a pivotal role in improving traffic management and enhancing driving comfort. As ITS development progresses further, we expect a substantial increase in data transmission due to a large number of vehicles. This

surge in data poses challenges in terms of communication and energy consumption. Moreover, given the private and sensitive nature of the data, ensuring data security is essential. Therefore, it is crucial to address these issues by adopting energy-efficient approaches and establishing low-latency transmission in V2X communication [236].

FL offers a promising solution for learning parameters with minimal latency and data transmission due to its decentralized training framework. It ensures data security while enabling efficient client/server selection during the training process [237]–[239] and resource management [240], [241]. These approaches have demonstrated an effective reduction in communication overload, addressing a significant challenge in FL implementations.

In [242], [243], extreme value theory was used in conjunction with an FL framework to model anomalous events, specifically large queue lengths. Lyapunov optimization was also incorporated for power allocation, which contributed to improving system performance.

V. CHALLENGES AND FUTURE DIRECTIONS

In this section, we review various challenges in the use of FL4CAV as well as future research directions.

A. Resource Limitations and Utilization

1) Collaboration capabilities and management in massively parallel CAVs: Significant participation of CAVs in FL could increase the solve time and memory utilization, and therefore calls for an increase in computational demand for a global model update. In particular, vision- and LiDAR-related perception tasks are characterized by large data sets that lead to high communication costs. Decentralized FL and clustered FL [244]–[247] are being explored to reduce communication overhead.

The high communication demands and low reliability of 5G networks call for the development of 6G-V2X systems. Integrating 6G, V2X, and multi-access edge computing (MEC) powered by ML techniques creates the potential to achieve efficient and collaborative processing at the network edge. This approach aims to overcome the limitations of current 5G systems and pave the way for improved performance and reliability in future networks [248], [249].

2) Challenges due to lack of sufficient real-world datasets, simulators, and pre-trained base models: There is a need for more real-world datasets (different weather conditions and traffic scenarios), realistic high-fidelity FL4CAV simulators for seamless FL integration [55], [250]–[252], and good pre-trained models.

3) Low model accuracy: FL often struggles with a trade-off between the accuracy achieved through model personalization and imposing high computational requirements on edge devices during learning. Split learning is one potential solution that enables efficient inference in resource-constrained edge clients while capturing both generalization and personalization capabilities [253].

4) Inefficient resource utilization: Some of the issues of FL related to resource optimization include idle of powerful edge devices, underutilized network infrastructure, neglected edge devices without proper network connectivity, and discouraged sharing of parameters from edge devices with diverse privacy requirements [254]. Therefore, there is a need for a robust FL framework that jointly utilizes and optimizes the resources of the device, server, and network infrastructure.

Cooperative FL is a promising solution that overcomes these shortcomings and has been shown to be feasible and beneficial for learning processes leading to improved ML performance and resource efficiency [255]. In another related study [256], a cooperative architecture and an FL combined with an RL-based algorithm are proposed for the allocation of resources in CAV networks.

B. Digital Ethics Issues

1) Privacy and security issues: Massive data also leads to privacy and security concerns. This problem must be addressed to train the ML model efficiently without compromising the model's accuracy and redundancy.

2) Fairness and incentives: There is a need for appropriate rewarding policies and incentive mechanisms for CAVs to share the quality data needed for efficient model training performance [257].

C. Imperfect Methodology

1) Lack of methods for efficient vehicle selection and resource allocation: Currently, there are no efficient methods that can filter useful data from CAVs to minimize network loading. There are ongoing efforts to develop reliable methods to optimally select vehicles and resource allocation schemes for efficient model training and communication [258]–[261]. In [262], the overall training process was demonstrated to be efficient when incorporating a client selection model. The setup looks at the resource availability of the clients and then determines the clients eligible to be part of the FL global model learning process. In [191], it is demonstrated that the model performance was improved with CAVs that were selected by trust-based deep RL.

2) Catastrophic forgetting: CAVs cannot store all user data due to storage capacity limitations, and new data will always be generated during training iteration. Therefore, when the FL framework is updated on new data in iteration, the global model might forget the previous knowledge, which may lead to catastrophic forgetting. This is another open research problem in FL4CAV.

3) System heterogeneity in FL4CAV: Poor performance of the FL model (longer training time and a larger number of communication rounds) is generally caused by poor connectivity and slower devices (straggler devices). In traditional FL, a communication round is not complete until the data from all the chosen devices are available. Hence, various

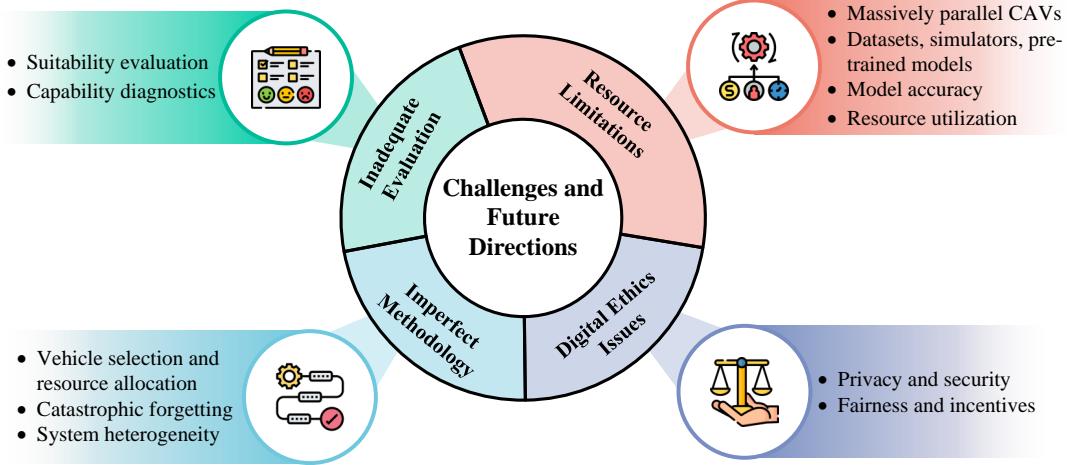


Fig. 5. Illustration of challenges and future directions of federated learning for connected and automated vehicles.

adaptive strategies have been proposed to minimize the impact of stragglers and also eliminate them, if possible [263], [264].

D. Inadequate Evaluation Criteria

1) *FL suitability evaluation for new users:* It is often difficult for the newcomer vehicle to make any informed decisions. In [191], a trust-aware Deep RL model is proposed to assist new vehicles in making better trajectory and motion planning decisions.

2) *Need for high capability diagnostics:* There are several noise factors that could influence the decision of the FL, such as faulty sensors in a visual perception case and incorrect imputation of missing data. The development of robust diagnostics that can identify and eliminate the updates from these vehicles is needed.

VI. CONCLUSIONS

This survey paper reviews FL algorithms, data modalities, model security, and provides a list of critical applications and challenges of FL4CAV. Currently, FL4CAV also presents unique challenges, such as ensuring data integrity, addressing communication latency, managing heterogeneous data sources, and maintaining model synchronization across different vehicles. However, with proper design and implementation, FL can offer significant advantages in terms of privacy preservation, network efficiency, and collaborative intelligence for CAVs.

Further promising applications of FL are in the areas, such as privacy-preserving driver behavior modeling, anomaly detection, and predictive maintenance. With the advent of cloud infrastructure, 6G, V2X technology, and flying cars, the use of FL models is expected to provide significant breakthroughs.

REFERENCES

- [1] G. Pan and M.-S. Alouini, "Flying car transportation system: Advances, techniques, and challenges," *IEEE Access*, vol. 9, pp. 24586–24603, 2021.
- [2] X. Zhang, J. Huang, Y. Huang, K. Huang, L. Yang, Y. Han, L. Wang, H. Liu, J. Luo, and J. Li, "Intelligent amphibious ground-aerial vehicles: State of the art technology for future transportation," *IEEE Transactions on Intelligent Vehicles*, 2022.
- [3] M. Biparva, D. Fernández-Llorca, R. I. Gonzalo, and J. K. Tsotsos, "Video action recognition for lane-change classification and prediction of surrounding vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 7, no. 3, pp. 569–578, 2022.
- [4] D. Cao, X. Wang, L. Li, C. Lv, X. Na, Y. Xing, X. Li, Y. Li, Y. Chen, and F.-Y. Wang, "Future directions of intelligent vehicles: Potentials, possibilities, and perspectives," *IEEE Transactions on Intelligent Vehicles*, vol. 7, no. 1, pp. 7–10, 2022.
- [5] A. Hadjigeorgiou and S. Timotheou, "Real-time optimization of fuel-consumption and travel-time of cavs for cooperative intersection crossing," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 1, pp. 313–329, 2022.
- [6] H. Pei, J. Zhang, Y. Zhang, X. Pei, S. Feng, and L. Li, "Fault-tolerant cooperative driving at signal-free intersections," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 1, pp. 121–134, 2022.
- [7] L. Guo, H. Chu, J. Ye, B. Gao, and H. Chen, "Hierarchical velocity control considering traffic signal timings for connected vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 1403–1414, 2022.
- [8] Z. Wang, C. Lv, and F.-Y. Wang, "A new era of intelligent vehicles and intelligent transportation systems: Digital twins and parallel intelligence," *IEEE Transactions on Intelligent Vehicles*, 2023.
- [9] H. Zhang, G. Luo, Y. Li, and F.-Y. Wang, "Parallel vision for intelligent transportation systems in metaverse: Challenges, solutions, and potential applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022.
- [10] Y. Liu, Z. Wang, K. Han, Z. Shou, P. Tiwari, and J. H. Hansen, "Vision-cloud data fusion foradas: A lane change prediction case study," *IEEE Transactions on Intelligent Vehicles*, vol. 7, no. 2, pp. 210–220, 2022.
- [11] L. Chen, Y. Li, C. Huang, B. Li, Y. Xing, D. Tian, L. Li, Z. Hu, X. Na, Z. Li, et al., "Milestones in autonomous driving and intelligent vehicles: Survey of surveys," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 1046–1056, 2022.
- [12] M. Hu, J. Li, Y. Bian, J. Wang, B. Xu, and Y. Zhu, "Distributed coordinated brake control for longitudinal collision avoidance of multiple connected automated vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 1, pp. 745–755, 2022.

