

# Federated Learning for Spatiotemporal Traffic Prediction: Privacy, Efficiency, Security and Emerging Extensions

Yanzhao Zhu

Statistics, University of Minnesota, Minneapolis, United States

zhu01020@umn.edu

**Abstract.** Spatiotemporal traffic prediction is very important for improving traffic flow and reducing congestion. But standard centralized prediction methods often cause big worries about data privacy and security, because they need to collect and store lots of sensitive traffic data on central servers. To solve this problem, this survey looks at using distributed federated learning for spatiotemporal traffic prediction. This paper reviews and sorts recent studies in this area, grouping them into a few main directions. These include privacy-preserving Federated Learning (FL) frameworks, efficiency-oriented FL methods, security and trust-enhanced FL systems, emerging optimization and heterogeneity-aware extensions. The survey shows that distributed federated learning can reach good prediction results, and it protects raw traffic data by keeping it on local devices. It also shows that recent studies make better models using graph-based spatial modeling, time learning modules, adaptive aggregation, blockchain-assisted checking, and personal collaboration. But, the literature also points out some big limits. These are mainly high communication costs, non-independent and non-identically distributed data, and the hard work of building secure, scalable, and steady real-world systems. So, this survey finds that distributed federated learning is a good way for privacy-preserving traffic prediction. Even so, further study still needs more research on adaptive optimization, strong collaboration under mixed data, and combined privacy and security tools for real large-scale uses.

**Keywords:** Distributed federated learning, spatiotemporal traffic prediction, data privacy, security.

## 1. Introduction

With the rapid development of Intelligent Transportation Systems and the Internet of Vehicles, traffic spatiotemporal prediction has become an important task for improving traffic efficiency and reducing congestion. Traditional traffic prediction methods usually depend on centralized data collection and model training. But because they require the sharing and storage of large amounts of sensitive user data on central aggregation servers, these methods often raise serious concerns about data privacy and security.

To solve these problems, Federated Learning has become a promising distributed learning method. FL allows multiple participants to jointly train a global model without sharing their raw data, so it can greatly reduce the risk of privacy leakage [1]. Also, FL has been widely used in many fields, including healthcare, finance, and intelligent transportation, showing strong potential for privacy preserving data analysis [2].

In traffic prediction, several studies have explored the combination of FL and advanced deep learning models. For example, Wang et al., 2026 proposed a federated spatiotemporal prediction framework that combines Graph Attention Networks with Transformer modules [3]. This framework can capture complex traffic patterns and model long term temporal dependencies. The results show that, compared with centralized approaches, FL based models can achieve competitive prediction performance while also protecting data privacy. In the same way, recent studies have also shown that FL can effectively support real time traffic prediction tasks in smart city environments [4].

But even with these advantages, existing FL based traffic prediction methods still face many challenges. One main problem is the difficulty of maintaining model training efficiency in dynamic environments such as the IoV, where communication delay and data heterogeneity can seriously weaken model performance. To deal with this problem, He et al., 2023 proposed an Efficient Federated Learning algorithm, which introduces an agile aggregation mechanism to improve both training efficiency and model accuracy [1]. Another important challenge is system security and

trustworthiness, especially in decentralized operating environments. To deal with this issue, some studies have added blockchain technology to improve the robustness and reliability of federated learning systems by reducing interference from malicious nodes and protecting data integrity [5]. Although this work was done in an NFV network traffic environment rather than a road traffic prediction setting, it is still cited here mainly because of its methodological relevance to decentralized federated systems.

Although these studies have made important progress, the existing literature is still somewhat fragmented. Current research mainly focuses on improving prediction accuracy, increasing training efficiency, and strengthening system security. But there is still a lack of clear understanding of how these aspects work together in traffic spatiotemporal prediction tasks. So, a survey of distributed federated learning methods in this field is necessary.

This paper aims to provide a structured survey of distributed federated learning for spatiotemporal traffic prediction. More specifically, it summarizes existing methods, classifies different research directions, and discusses future research opportunities.

## **2. Distributed Federated Learning in Spatiotemporal Traffic Prediction**

### **2.1. Privacy-Preserving Federated Learning Frameworks**

#### **2.1.1. FL-based predictive traffic management systems**

Alqubaysi et al., proposed a Federated Learning-based Predictive Traffic Management (FLPTM) system designed for intelligent transportation environments [4]. The main idea of this method is combining the Contained Privacy-Preserving Scheme (CPPS) with Federated Learning, and this allows the decentralized training of models while also protecting sensitive vehicle data.

The workflow of this framework can be explained as follows: First, vehicles and infrastructure nodes collect traffic-related data, such as speed, location, and congestion status, via V2X communication. Rather than sending raw data to a central aggregation server, each node uses its own data to independently train a local model. Then, only the model parameters are transmitted to a central aggregation server, which is used for generating a global model and distributing it back to all participating entities. This process means that raw data remains resident on local devices at all times, and so greatly reduces the risk of privacy leakage.

Besides the basic Federated Learning architecture, the CPPS mechanism uses state modeling and access control capabilities. Vehicles must complete identity authentication and authorization verification before they can join and use the system. Also, the model integrates a classifier-based state learning mechanism that can quickly change traffic service response strategies, and improve the efficiency of real-time traffic management.

Results show that the FLPTM system, while still keeping high predictive accuracy, reduces communication overhead by 23.29%, reduces the impact of adversarial attacks by 16.1%, and shortens access response time by 18.95%. These results clearly show that, in real ITS use cases, a privacy-preserving Federated Learning framework can balance both efficiency and security well.

#### **2.1.2. FL with deep spatiotemporal models**

Another important research direction is combining federated learning with modern deep learning architectures to capture spatiotemporal dependencies. Wang et al., 2026 proposed a framework combining GATs and Transformer modules for traffic prediction [3]. The key idea of this method is that it can model two different types of relationships at the same time: first, the spatial relationships between road nodes (modeled by a GAT); and second, long-term temporal dependencies (modeled by a Transformer). In this framework, each client uses its local traffic data to train a local GAT-Transformer model. Then, the parameters of these local models are aggregated using a federated averaging strategy. Compared with traditional centralized deep learning models, this approach still keeps very strong performance while avoiding the need for data sharing.

Results show that the predictive accuracy achieved by this federated model is on par with that of centralized models, exhibiting particularly strong performance in capturing complex traffic patterns. This shows that FL can support high-dimensional spatiotemporal modeling tasks without compromising data privacy.

## **2.2. Efficiency-Oriented Federated Learning Methods**

One main challenge for distributed federated learning is training efficiency, mainly in dynamic settings such as the IoV, where communication latency, data heterogeneity, and device instability can strongly affect model convergence. Some studies in this area are cross-cutting, because they contribute not only to training efficiency through decentralized coordination and incentive design, but also to trust and security through blockchain-based verification and traceability [5].

He et al., 2023 proposed an EFL algorithm to solve these issues [1]. The main new part of this method is the use of an agile aggregation mechanism, which is able to flexibly change the aggregation frequency and the selection of participants. The EFL workflow includes task release, local vehicle training, identity authentication, quality assessment, and agile aggregation. This approach not only cuts unnecessary communication overhead but also speeds up convergence. Results show that, compared to the standard FedAvg algorithm, EFL achieves faster training speeds and higher accuracy in scenarios characterized by heterogeneous data distributions.

Also, Hu et al., 2025 proposed a decentralized federated learning framework that uses a node incentive and role-switching mechanism, made for traffic prediction tasks within NFV environments [5]. The main new point of this framework is removing a central aggregation server and the introduction of dynamic roles, such as Worker, Evaluator, and Aggregator types.

The workflow of this method is as follows: Worker nodes are responsible for training local models and uploading model parameters. Evaluator nodes are responsible for assessing model quality and detecting malicious behavior. Aggregator nodes are responsible for putting local models that meet quality requirements into a global model. A blockchain mechanism is used for recording the model update process, and so keeps the system transparent. A key feature of this framework is its contribution-based incentive mechanism, where the system gives rewards or penalties based on the actions of individual nodes. This mechanism not only improves the system's robustness but also encourages more high-quality participation overall.

Results confirm that the model maintains stable predictive accuracy, even when there are still a significant number of malicious nodes. Also, the framework greatly improves the system's adaptability within dynamic network environments.

## **2.3. Security and Trust-Enhanced Federated Learning**

In distributed federated learning systems, mainly in decentralized ITS settings, security and trust are critical. One main security risk is the presence of malicious nodes, which may upload and update poisoned models. To fix this problem, some studies have added blockchain technology.

Hu et al., 2025 proposed a blockchain-assisted federated learning framework that keeps data unchanged and keeps model aggregation secure [5]. Its main idea is the combination of FL with a decentralized ledger, which is used for safely recording all model updates. This mechanism not only stops data tampering but also makes model contributions traceable. The workflow of this framework mainly involves these steps: enabling individual nodes to perform local model training, uploading model parameters to the blockchain, validating updates via a consensus mechanism, and aggregating the validated models. This approach effectively reduces malicious interference and clearly enhances system trust. Experimental results show improved prediction stability and robustness in adversarial environments.

Also, other related studies have explored blockchain-based trust management and privacy-preserving authentication mechanisms within IoV systems. For example, Alqubaysi et al., 2025 integrated authentication protocols and access permission control into the FL framework, making sure there is secure communication between vehicles and infrastructure [4]. These security-enhanced

FL methods offer the following capabilities: protection against Man-in-the-Middle attacks, secure access control mechanisms, and robust model aggregation capabilities. But, they also introduce additional computational overhead and communication complexity, and these still remain challenges.

## **2.4. Cross-Domain Extensions and Emerging Optimization Strategies**

The following studies are not all direct road traffic spatiotemporal prediction papers, some are included for methodological inspiration on lightweight optimization, heterogeneity mitigation, and decentralized trust.

### **2.4.1. Lightweight and structure-aware federated prediction**

Another new path in distributed federated learning is boosting model efficiency while keeping the structural information of traffic data. Liu et al. proposed a PFL-GTCN framework that combines spectral graph partitioning, graph-temporal convolutional modeling, and dynamic client weighting in a personalized federated setting [6]. The main point of this method is to split the traffic network into many subgraphs using spectral clustering, and then use changing aggregation weights to boost prediction results in distributed environments. This method shows that structure-aware partitioning can cut the impact of weak spatial dependence across regions, and personalized aggregation can also drop communication cost and boost prediction accuracy. Also, Jin et al. made LFedSG, a lightweight federated learning framework for spatiotemporal cellular traffic prediction [7]. Their framework uses subgraph partitioning and adaptive transmission weight pruning to keep inter-client links while cutting communication overhead and training time. These papers show that lightweight design and structure-aware modeling are becoming key optimization steps in federated traffic prediction.

### **2.4.2. Heterogeneity-aware collaborative learning**

Another big step is boosting model robustness under heterogeneous data distributions. Lonare and Ravi built a FedGCN-based framework with differential privacy, proving that privacy protection and spatiotemporal modeling can work together in one federated system [8]. Jiang et al. also brought federated prediction to satellite-terrestrial integrated networks [9], where AGCN, LSTM, and weighted FedAvg were used to balance privacy and prediction accuracy under much harder communication conditions. Also, even though Xue et al. focused on network traffic classification and not traffic prediction [10], their FLDML framework still gives a helpful idea for this field, since it shows that deep mutual learning on a shared public dataset can cut the bad effect of non-IID data. So, heterogeneity-aware collaboration may become a key future path for federated spatiotemporal traffic prediction.

## **3. Discussion**

### **3.1. Challenges**

#### **3.1.1. Communication cost and training efficiency**

A major challenge in distributed federated learning for spatiotemporal traffic prediction is the high communication cost during repeated parameter exchange. Even though federated learning does not need raw data sharing, clients still have to upload model updates many times. This can become a bottleneck in dynamic traffic environments. This problem is especially serious in IoV and STIN settings, because unstable connections, node mobility, and limited computing resources may slow down aggregation and reduce training efficiency [1, 9]. Also, recent traffic prediction models have become more complex, since they often combine graph neural networks, temporal modules, and attention mechanisms. These models improve prediction performance, but they also increase the size of transmitted parameters and the burden on local devices. Liu et al. and Jin et al. both pointed out that communication overhead is still one of the main barriers to practical deployment, even when privacy can be kept [6, 7]. So the current challenge is not only how to train accurate models, but also how to make the whole distributed learning process efficient enough for real traffic systems.

### **3.1.2. Data heterogeneity and limited generalization**

Another central challenge is data heterogeneity. Traffic data collected from different vehicles, intersections, cities, or communication nodes usually follow different distributions. This means local data are often non-IID. This can make local models overfit to their own environments and weaken the quality of the aggregated global model [2]. The problem is even harder in traffic prediction because the task depends on complex spatial and temporal relationships. Uneven traffic density, different road structures, and changing demand patterns can all reduce model consistency across clients. Wang et al. showed that even strong spatiotemporal models still need better ways to handle hidden spatial dependencies and uneven task complexity [3]. Similarly, Lonare and Ravi and Jiang et al. both said that privacy-preserving prediction is possible, but keeping stable accuracy under heterogeneous settings remains hard [8, 9]. Even cross-domain work like Xue et al. confirms that heterogeneity can seriously hurt federated model performance when client data distributions differ a lot [10]. So model generalization across distributed traffic scenarios is still an open issue.

### **3.1.3. Security, trust, and deployment reliability**

The third challenge is the joint problem of security and trust. Even though federated learning improves privacy by keeping raw data local, it does not fully remove security risks. Bad nodes may upload poisoned updates, and distributed environments may have authentication problems, model tampering, or unreliable aggregation. Alqubaysi et al. emphasized the importance of authenticated access, state modeling, and adversary resistance in ITS communication [4]. Hu et al. further showed that decentralized settings need ways to trace model updates and resist bad provider behavior [5]. Also, mobile or satellite-terrestrial environments bring extra risks because communication links may be unstable and more exposed to interception [9]. Current methods often strengthen one part, like privacy, accuracy, or trust, but it is still hard to optimize all of them at the same time. So making distributed federated prediction both secure and practically reliable remains a major challenge for future real-world deployment.

## **3.2. Future Prospects**

### **3.2.1. Lightweight and adaptive federated optimization**

A possible solution to the efficiency problem is to design lighter and more adaptive federated optimization strategies. Instead of just using standard aggregation, future models can combine agile aggregation, personalized weights, subgraph partitioning, and adaptive pruning to cut down unnecessary communication while keeping useful traffic structure information. He et al. already proposed agile aggregation to shorten waiting time in IoV settings [1], and Liu et al. used dynamic parameter weights to improve distributed short-term traffic prediction [6]. Jin et al. further showed that subgraph partitioning and adaptive transmission pruning can greatly lower computation and communication costs [7]. These ideas suggest that future systems should focus more on client-aware aggregation, lightweight model design, and efficient structure-preserving transmission.

### **3.2.2. Heterogeneity-aware collaborative learning**

To deal with limited generalization, future research should focus more on heterogeneity-aware collaborative learning. One good direction is to combine federated learning with personalization, mutual learning, and adaptive weighting. For example, Liu et al. used personalized federated learning to better fit local node characteristics [6], and Jiang et al. introduced weighted FedAvg to give different importance to different clients [9]. Also, Xue et al. showed that deep mutual learning on a shared public dataset can improve robustness under non-IID settings, even though their task was network traffic classification [10]. Wang et al. also suggests that richer spatiotemporal representations can better capture hidden traffic dynamics [3]. So future federated traffic prediction models may benefit from combining stronger spatiotemporal feature extraction with personalized or collaborative mechanisms that are clearly designed for heterogeneous data.

### 3.2.3. Integrated privacy, security, and trustworthy deployment

For the security and trust challenge, future work should move toward integrated frameworks that combine privacy protection, trustworthy aggregation, and real deployment support. Alqubaysi et al. showed that authentication and controlled access can strengthen secure traffic management [4], and Hu et al. showed that blockchain-based decentralized verification can improve trust and stability [5]. Lonare and Ravi also highlighted the value of differential privacy for protecting local traffic data. More broadly [8], Wen et al. argued that privacy, communication efficiency, and heterogeneity should be studied together instead of separately [2]. This means future solutions should not only protect local data, but also give traceable updates, defense against bad nodes, and scalable deployment strategies across IoV, ITS, and STIN settings. In this way, federated spatiotemporal traffic prediction may become more reliable, practical, and suitable for large-scale intelligent transportation systems.

## 4. Conclusion

In the end, this survey goes back to the problem in the introduction of how to make spatiotemporal traffic prediction accurate without losing privacy, efficiency, or security. It shows that distributed federated learning is a promising solution because it lets parties train models together while keeping raw traffic data local. This review summarized three research directions, including privacy-preserving frameworks, efficiency-oriented methods, and designs that improve security and trust, and it also discussed progress in lightweight optimization and heterogeneity-aware collaboration. Overall, the reviewed studies show that federated learning can achieve competitive prediction performance and give privacy protection in intelligent transportation scenarios. But the field still has limits, especially communication overhead, non-IID data, and the difficulty of building secure and scalable real-world systems. In the future, more work is needed on adaptive aggregation, personalized collaboration, and privacy and security mechanisms to support reliable deployment in large-scale ITS environments.

## References

- [1] He X, Hu X, Wang G, Yu J, Zhao Z, Lu X. Towards efficient federated learning using agile aggregation in Internet of Vehicles. *Security and Communication Networks*, 2023, 2023: 2265852.
- [2] Wen J, Zhang Z, Lan Y, Cui Z, Cai J, Zhang W. A survey on federated learning: challenges and applications. *International Journal of Machine Learning and Cybernetics*, 2023, 14: 513-535.
- [3] Wang R, Yue J, Guo Q, Zhong P, Jia C. Traffic dynamics HD: a federated learning traffic flow prediction model inspired by high-definition image generation techniques. *Information Sciences*, 2026, 745: 123405.
- [4] Alqubaysi T, Al Asmari AF, Alanazi F, Almutairi A, Armghan A. Federated learning-based predictive traffic management using a contained privacy-preserving scheme for autonomous vehicles. *Sensors*, 2025, 25: 1116.
- [5] Hu Y, Liu B, Li J, Jia L. Decentralized federated learning with node incentive and role switching mechanism for network traffic prediction in NFV environment. *Symmetry*, 2025, 17: 970.
- [6] Liu T, Wang Y, Zhou H, Luo J, Deng F. Distributed short-term traffic flow prediction based on integrating federated learning and TCN. *IEEE Access*, 2024, 12: 148026-148036.
- [7] Jin Z, Zhang X, Su J, Zhang L, Shen J. Subgraph-driven lightweight federated learning for spatiotemporal cellular traffic prediction. *IEEE Transactions on Network and Service Management*, 2026, 23: 1435-1448.
- [8] Lonare S, Bhramaramba R. Federated approach for privacy-preserving traffic prediction using graph convolutional network. *Journal of Shanghai Jiao Tong University (Science)*, 2024, 29(3): 509-517.
- [9] Jiang W, Mu J, Han H, Zhang Y, Huang S. Federated learning-based mobile traffic prediction in satellite-terrestrial integrated networks. *Software: Practice and Experience*, 2025, 55: 613-628.
- [10] Xue H, Hu Y, Wang Y. Federated distributed network traffic classification based on deep mutual learning. *Electronics*, 2025, 14: 4928.