Tan, K., Bremner, D., Le Kernec, J. and Imran, M. (2020) Federated Machine Learning in Vehicular Networks: a Summary of Recent Applications. In: 5th International Conference on the UK-China Emerging Technologies (UCET 2020), Glasgow, UK, 20-21 Aug 2020, ISBN 9781728194882 (doi:10.1109/UCET51115.2020.9205482).

Federated Machine Learning in Vehicular Networks: A summary of Recent Applications

Kang Tan
James Watt School of Engineering
University of Glasgow
Glasgow, UK
k.tan.3@research.gla.ac.uk

Duncan Bremner
James Watt School of Engineering
University of Glasgow
Glasgow, UK
Duncan.Bremner@glasgow.ac.uk

Julien Le Kernec
James Watt School of Engineering
University of Glasgow
Glasgow, UK
Julien.LeKernec@glasgow.ac.uk

Muhammad Imran
James Watt School of Engineering
University of Glasgow
Glasgow, UK
Muhammad.Imran@glasgow.ac.uk

***Abstract*—Future Intelligent Transportation Systems (ITS) can improve on-road safety and transportation efficiency and vehicular networks (VNs) are essential to enable ITS applications via information sharing. The development of 5G introduces new technologies providing improved support for connected vehicles through highly dynamic heterogeneous networks. Machine Learning (ML) can capture the high dynamics of VNs but the distributed data cause new challenges for ML and requires distributed solutions. Federated learning (FL), a distributed ML framework, gives a distributed ML framework while ensuring information privacy protection and is an exciting area to explore in VNs. This article provides a detailed summary of recent FL applications in VNs and gives insights on current research challenges. The included research topics are resource management, performance optimization and applications based on VNs.**

***Index Terms*—Vehicular Networks, Machine Learning, Federated Learning, 5G, Mobile Edge Computing**

I. Introduction

As vehicles have gained increasing communication, computing, and sensing capabilities, new opportunities have been revealed for both research and industrial applications to realize future intelligent transportation system (ITS) applications [1]. However, a major challenge in vehicular networks (VNs) is the rapid and continuous changes of network (Net) nodes, combined with their short connection time, requiring a dynamic Net topology. Traditional wireless Net solutions are based on parameterized mathematical models and an *a priori* knowledge of the environment making them highly sensitive to the highly dynamic nature of VNs resulting in non-optimal performance.

Another methodology utilizing Machine Learning (ML) can cope with the uncertainty in the dynamically changing environment by learning the patterns from collected data, or directly interacting with the environment to develop an optimal policy. Because of the adaptivity and flexibility provided by ML, it has gained traction in wireless communications research [2] and VNs [3]. Similarly, the growth of Deep Learning (DL) technique can further exploit the vast amount of data for improved task-specific performances.

Another major challenge raised by vehicular-to-everything (V2X) communication [4] and VNs is heterogeneity. VNs have various communication types with multiple radio access technologies of choice (Figure. 1). Due to the heterogeneity, VN data is collected and stored in different Net nodes such as vehicles, roadside units (RSUs), pedestrians, leading to incomplete local datasets for these nodes. Moreover, since data-driven learning methods require a rich dataset to fully extract the underlying patterns; the partially observed data stored locally will cause individual learners to underperform in VNs. Reinforcement learning (RL) algorithms for VNs also face a similar challenge that individual agents may only interact with a part of the whole environment, leading to suboptimal policies. To solve such problems, distributed learning methods integrating different learners in the same environment for an enhanced dataset or environment observation thus become a promising approach; presently, federated learning (FL) [5] is a major methodology in this category.

With the development of 5G, VNs have started to embrace a series of new communication standards and related enabling technologies [6]. Mobile edge computing (MEC), a key technology for 5G, provides edge caching and computation offloading functions [7], thus reducing latency and computation load by moving less computation-intensive tasks to Net edge and end devices instead of centralized cloud servers; thus opening up the possibility of implementing distributed FL deployment in VNs. Adoption of this architecture permits a decentralized FL setup to collectively learn while simultaneously reducing latency and increasing bandwidth efficiency.

For the sake of brevity, this paper is restricted to the most recent applications of FL in VNs and identifies current research challenges in networking and methodology optimization.

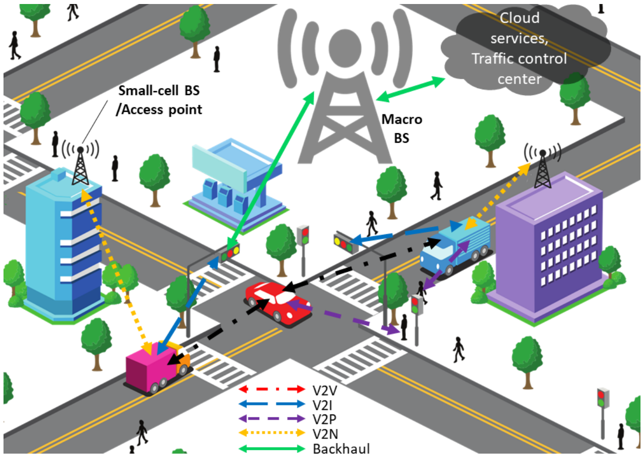

Fig. 1. An example scenario of the heterougenous vehicular network

II. FL in Vehicular Networks

Initially, FL was developed to exploit the values of distributed data among learners while protecting each learner's data privacy [5]. FL structures can be classified into two major types; vertical and horizontal and readers are referred to the excellent treatise on FL frameworks for further reading [8]. Normally, FL training (Figure. 2) includes 3 steps: Initialization, Local training, and Global aggregation. During Initialization, the FL server determines the training setup, data requirements, and the participants. Once step 1 is complete FL enters the Local training process where each participant receives the initialization information and uses this to train a local model using its local data. Step 3 is the Global aggregation process, where each participant uploads the parameters of its local model to the FL server. The server then performs model averaging and distributes the resulting global model among participants.

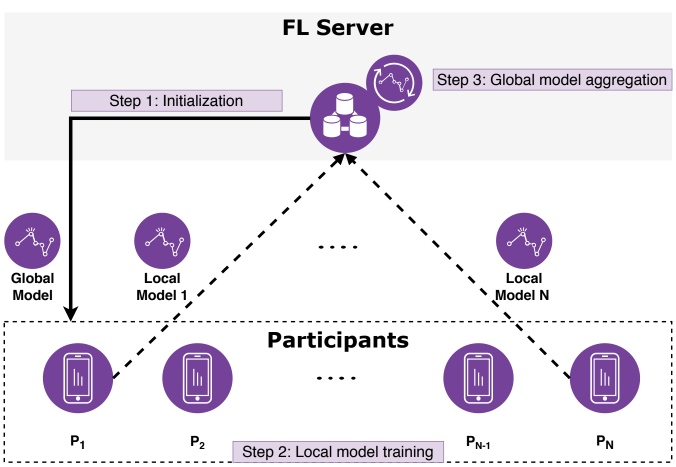

Fig. 2. General FL training process with N participants

When applied to VNs, FL frameworks can improve Net optimization problems including communication cost and resource allocation [9]. For example, an FL-based method [10] has been developed to deal with vehicular communications joint power and resource allocation problem to define an ultra-reliable and low-latency communication (URLLC) application specification. By utilizing extreme value theory [11] for modelling extreme queue lengths with Lyapunov optimization applied [12], this method is used to determine the optimal resource allocation policy per vehicle when considering resource sharing. The FL framework design allows vehicles to participate in the training process, train their local models, and upload the model parameters to the RSU in the specified region. The RSU will then average out all model parameters and send the updated global model back to participating vehicles. Also, this work developed both synchronous (SY) and asynchronous (ASY) algorithms. In the SY case, all vehicles upload their training parameters to the server periodically at the end of a predefined interval. However, the SY mode will experience communication delay when multiple vehicles upload simultaneously. Therefore, in the ASY case, each vehicle will complete its training and upload the parameters when sufficient information is collected locally; and the FL server will update the global model upon receipt of a set of parameter upload. Simulation results show the number of vehicles experiencing extreme queue length is lessened and data exchange is also reduced via the proposed centralized FL approach. However, the researcher presumes that the training data come from an independent and identical distribution (IID) which cannot be guaranteed in for the general case; centralized FL training may also cause more significant communication delay in real-world applications.

For MEC applications in mobile Nets, the optimization of edge storage and computational power management has become another topic in resource allocation research. In [13], an FL-based deep RL (DRL) algorithm has been developed for caching and computation offloading decision optimization in a MEC system. A double deep Q-learning Net [14] is designed for user equipment (UE) covered by a base station to decide whether to cache a file and offload tasks to an edge node. A further FL approach utilizes distributed computational power for faster training while keeping training data on individual UE only to protect privacy. To deal with the non-IID issue of distributed data, the FedAvg algorithm [15] is used to keep training results robust and balanced. Similarly, the authors of [16] have also utilized an FL-based double deep Q-learning algorithm for computation offloading in an internet of things (IoT) system. In their framework, randomly selected IoT devices download a copy of the global model from an edge node and train it with their local data, after which the trained parameters will be sent back to the edge node for aggregation.

Through the adoption of FL-based structures, relatively large-scale deployments for caching and computation offload is possible when compared to a centralized structure while continuing to protect the participants' data privacy. Training results from the above two examples approach the best performance achieved by the centralized structures used as baselines. While these examples are focused on a more general IoT use case, the highly dynamic mobility of nodes must be considered when adapting to VN applications. Conversely, both schemes may suffer long training delays when dealing with a Net consisting of numerous heterogenous UE with the proposed DRL methods.

With the increase in sensing and computational power, on-road vehicles are becoming rich data sources and images taken by on-board cameras can provide valuable information for intelligent applications. FL becomes a valuable framework to exploit such image data while protecting the underlying sensitive information. However, as the photographic and computational power of vehicles can vary, this affects global model accuracy causing communication latency. To address this asymmetric information challenge for FL, a multi-dimensional selective model aggregation approach for SY FL is proposed [17] relying on an image classifier within a vehicular edge computing structure. The FL server first proposes a DL model with a contract bundle containing the requirement of data quality levels, computation resources, and payoffs. Vehicles can self-evaluate and predict whether their images satisfy the contract requirements via instantaneous velocity observations. Competent vehicular participants will then download the global model after contract confirmation and upload their local models to the FL server for model aggregation while meeting the synchronization requirements. Simulation results show that this selective aggregation model effectively simplifies the information asymmetry problem to be solvable via a naïve greedy optimization algorithm . This work provides an innovative contract-theory based approach to tackling a data quality problem. This yielded the largest utility compared to economic models applied to mobile Nets such as the linear pricing and the Stackelberg competition model [18]. however the authors have not considered the high mobility aspects of on-road vehicles and only propose an SY FL model.

FL can also support utility applications using VNs such as the prediction of electric vehicles' energy demand, thus reducing energy transfer congestion at charging stations [19], resulting in improved on-road traffic efficiency. The charging data of vehicles at each station is essential for future energy demand prediction to pre-order and reserve electricity from the power grid suppliers. To ensure data privacy, the implemented DL algorithm with an SY FL structure only requires each station to upload result gradient data via local training and the FL server will aggregate and produce the final prediction model. Improvements to the model's accuracy can be achieved by implementing the constrained K-means clustering algorithm [20] to cluster charging stations based on geographic information. To evaluate the efficiency of these methods, simulations are conducted on real-world charging station data obtained from the UK city of Dundee. When the FL based method with clustering was applied, it outperformed all other methods as measured by the lowest root mean square error and control overhead. Pattern recognition of traffic flows and charging station recommendations for load balancing among available stations can be a promising further application.

This section introduced five distinct FL applications in VNs in detail with different types of applications included. DL and DRL methods can capture the highly dynamic VNs well when sufficient data are collected. FL enabling utilization of distributed data and privacy protection can improve DL applications. The works covered in this section is summarized in Table. I with their application types and central ideas.

III. Current Research Challenges

FL is a relatively new ML training framework and applications in VNs are still in their infancy presenting significant challenges requiring further research investment. The challenges include communication issues, deployment with data quality and method scalability, and security issues. In wireless mobile Nets, a significant challenge is interferences among devices as a function of the distance between participants following existing participant selection schemes [21], [22] with the number of mobile devices taken into account. The radio interference influences the communication quality during local result uploading causing possible data loss or false data and will decrease the reliability of the global aggregation model. To date, this challenge has received some attention in FL resource allocation research [10], [23], but the scalability of existing methods still needs investigation.

Data quality is another challenge in distributed systems. To improve training performance and deal with heterogeneous data issues in FL, some research have focused on participant selection algorithms [21], [24]. However, the assumption is that a permanently robust link exists between a potential participant and the FL server. In VNs, this assumption cannot be guaranteed as rapidly moving vehicles will result in unstable links, which causes a participant drop-out problem during FL training process and greatly affects the joint training performance. Future research for FL applications in VN needs to anticipate the drop-out situation and focus on robustness.

The identified FL applications use the SY training schemes as they guarantee convergence [25], but these also limit the system progression to that of the slowest participant, thereby restricting the scalability and training efficiency. To address the "straggler" effect the ASY scheme used in [10] is proposed which may also solve the participant dropping issue by allowing new participants to join an ongoing training session. However, this approach may introduce potentially more heterogeneous data and thus jeopardize training convergence. Future ASY FL research must address this while exploring the scalability and adaptability benefits.

As wireless communication is essential for data transmission in FL training in VNs and other MEC systems, communication and information security become major concerns as FL implementations in such systems are vulnerable to communication attacks such as distributed denial-of-service [26] and jamming attacks [27], impacting the FL systems' overall performance. Conversely, although an FL framework guarantees data privacy through keeping individual data locally, it is still exposed to information leaking risks [28]. According to Lim [9], countermeasures have been developed for both types of issues for FL implementation, but trade-offs between system safety and efficiency require further attention.

TABLE I
FL APPLICATIONS IN VEHICULAR NETWORKS (VNS) COVERED.

Application Type	**Ref.**	**Central Idea**
Resource Management	[10]	Joint power and radio resource allocation for VNs with extreme value theory to predict extreme queue lengths.
	[13], [16]	FL-based deep Q-learning networks to deal with edge caching and/or computation offloading in small scale MEC (IoT) systems.
Performance Optimization	[17]	A contract theoretic approach to cope with data asymmetry issues with the FL-based image recognition tasks in VNs.
V2X-based Application	[19]	An FL-based energy demand algorithm developed to tackle energy transfer congestion issues of electric vehicles at charging stations.

IV. CONCLUSION

This summarizes recent federated machine learning applications in VNs while aiming to address the distributed data and information privacy issues in such systems and providing some insights into the existing research challenges. A significant benefit of FL is that it can utilize the distributed data stored among vehicles and RSUs through joint training schemes while retaining data privacy by keeping individual participant data local. Real-world deployment and security issues are major challenges for FL applications that demand attention by future research ers. Outstanding real-world deployment challenges contain communication link interference, training data quality, and algorithm scalability while maintaining communication and information security.

REFERENCES

[1] L. Figueiredo, I. Jesus, J. A. T. Machado, J. R. Ferreira, and J. L. Martins de Carvalho, "Towards the development of intelligent transportation systems," in *ITSC 2001. 2001 IEEE Intelligent Transportation Systems. Proceedings (Cat. No.01TH8585)*, pp. 1206–1211, 2001.

[2] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, "Application of machine learning in wireless networks: Key techniques and open issues," *IEEE Communications Surveys Tutorials*, vol. 21, no. 4, pp. 3072–3108, 2019.

[3] L. Liang, H. Ye, and G. Y. Li, "Toward intelligent vehicular networks: A machine learning framework," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 124–135, 2019.

[4] 3GPP, "Study on LTE-Based V2X Services," Technical report (TR) 36.885, 3rd Generation Partnership Project (3GPP), 06 2016. Version 14.0.0.

[5] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," 2016.

[6] M. A. Imran, Y. A. Sambo, and Q. H. Abbasi, *Evolution of Vehicular Communications within the Context of 5G Systems*, pp. 103–126. IEEE, 2019.

[7] Z. Ning, X. Wang, and J. Huang, "Mobile edge computing-enabled 5g vehicular networks: Toward the integration of communication and computing," *IEEE Vehicular Technology Magazine*, vol. 14, no. 1, pp. 54–61, 2019.

[8] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, Jan. 2019.

[9] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020.

[10] S. Samarakoon, M. Bennis, W. Saad, and M. Debbah, "Distributed federated learning for ultra-reliable low-latency vehicular communications," *IEEE Transactions on Communications*, vol. 68, no. 2, pp. 1146–1159, 2020.

[11] L. De Haan and A. Ferreira, *Extreme value theory: an introduction*. Springer Science & Business Media, 2007.

[12] M. J. Neely, "Stochastic network optimization with application to communication and queueing systems," *Synthesis Lectures on Communication Networks*, vol. 3, no. 1, pp. 1–211, 2010.

[13] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Network*, vol. 33, no. 5, pp. 156–165, 2019.

[14] H. Van Hasselt, A. Guez, and D. Silver, "Deep reinforcement learning with double q-learning," in *Thirtieth AAAI conference on artificial intelligence*, 2016.

[15] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, *et al.*, "Communication-efficient learning of deep networks from decentralized data," *arXiv preprint arXiv:1602.05629*, 2016.

[16] J. Ren, H. Wang, T. Hou, S. Zheng, and C. Tang, "Federated learning-based computation offloading optimization in edge computing-supported internet of things," *IEEE Access*, vol. 7, pp. 69194–69201, 2019.

[17] D. Ye, R. Yu, M. Pan, and Z. Han, "Federated learning in vehicular edge computing: A selective model aggregation approach," *IEEE Access*, vol. 8, pp. 23920–23935, 2020.

[18] J. Kang, Z. Xiong, D. Niyato, H. Yu, Y.-C. Liang, and D. I. Kim, "Incentive design for efficient federated learning in mobile networks: A contract theory approach," in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, pp. 1–5, IEEE, 2019.

[19] Y. M. Saputra, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz, M. D. Mueck, and S. Srikanteswara, "Energy demand prediction with federated learning for electric vehicle networks," *arXiv preprint arXiv:1909.00907*, 2019.

[20] P. S. Bradley, K. P. Bennett, and A. Demiriz, "Constrained k-means clustering," *Microsoft Research, Redmond*, vol. 20, no. 0, p. 0, 2000.

[21] T. Nishio and R. Yonetani, "Client selection for federated learning with heterogeneous resources in mobile edge," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–7, 2019.

[22] T. T. Anh, N. C. Luong, D. Niyato, D. I. Kim, and L. Wang, "Efficient training management for mobile crowd-machine learning: A deep reinforcement learning approach," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1345–1348, 2019.

[23] M. M. Amiri and D. Gündüz, "Federated learning over wireless fading channels," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3546–3557, 2020.

[24] N. Yoshida, T. Nishio, M. Morikura, K. Yamamoto, and R. Yonetani, "Hybrid-fl: Cooperative learning mechanism using non-iid data in wireless networks," *CoRR*, vol. abs/1905.07210, 2019.

[25] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konecný, S. Mazzocchi, H. B. McMahan, T. V. Overveldt, D. Petrou, D. Ramage, and J. Roselander, "Towards federated learning at scale: System design," *CoRR*, vol. abs/1902.01046, 2019.

[26] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics. 'cybernetics evolving to systems, humans, organizations, and their complex interactions' (cat. no.0*, vol. 3, pp. 2275–2280 vol.3, 2000.

[27] Wenyuan Xu, Ke Ma, W. Trappe, and Yanyong Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.

[28] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction apis," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, pp. 601–618, 2016.