Unmanned Aerial Vehicles and Federated Learning

Subjects: Computer Science, Artificial Intelligence

Contributor: Sofiane Dahmane , Mohamed Bachir Yagoubi , Bouziane Brik , Chaker Abdelaziz Kerrache , Carlos Tavares Calafate , Pascal Lorenz

Unmanned aerial vehicles (UAVs) have gained increasing attention in boosting the performance of conventional networks due to their small size, high efficiency, low cost, and autonomously nature. The amalgamation of UAVs with both distributed/collaborative Deep Learning (DL) algorithms, such as Federated Learning (FL), and Blockchain technology have ushered in a new paradigm of Secure Multi-Access Edge Computing (S-MEC). Indeed, FL enables UAV devices to leverage their sensed data to build local DL models. The latter are then sent to a central node, e.g., S-MEC node, for aggregation, in order to generate a global DL model. Therefore, FL enables UAV devices to collaborate during several FL rounds in generating a learning model, while avoiding to share their local data, and thus ensuring UAVs' privacy.

UAV networks | Federated Deep Learning | UAVs selection | blockchain | edge computing

1. Introduction

The unmanned aerial vehicles (UAVs) paradigm is a revolutionary innovation with a strong potential for civic and industrial applications. Internet of Drones (IoD) or Internet of Flying Things (IoFT) is an actual result of UAVs connections to other smart devices by means of a powerful multi-sensor platform, communication technologies, computation units, and IP-based Internet connectivity. Many service providers are investigating to leverage UAV devices for products transportation and shipping, home package delivery, crop monitoring and agricultural surveillance, road traffic monitoring, and lastly, as a search and rescue assistance technology [1].

Recently, tech giants such as Amazon and Google expressed interest in implementing new drone-based parcel delivery systems, igniting a trend that has spawned a slew of commercial UAV-based services and applications. The Federal Aviation Authority (FAA) and civil aviation authorities in other governments; however, they steadfastly refuse to open up the national airspace (NAS) to such services and applications, until they fully meet specific safety and security standards [1][2].

As depicted in **Figure 1**, the high level of heterogeneity, pervasiveness, and large scale of UAV systems, are expected to increase security risks to modern aerospace, which is becoming increasingly reliant on humans, drones, and robots in multiple combinations. Furthermore, existing security countermeasures and privacy enforcement policies cannot be directly applied to UAV technology, due to its low computational power and payload

capacity. As a result, in order to attain UAVs full potential and obtain widespread adoption, appropriate confidentiality, privacy, and trust models must be designed for the heterogeneous UAV environment [2].

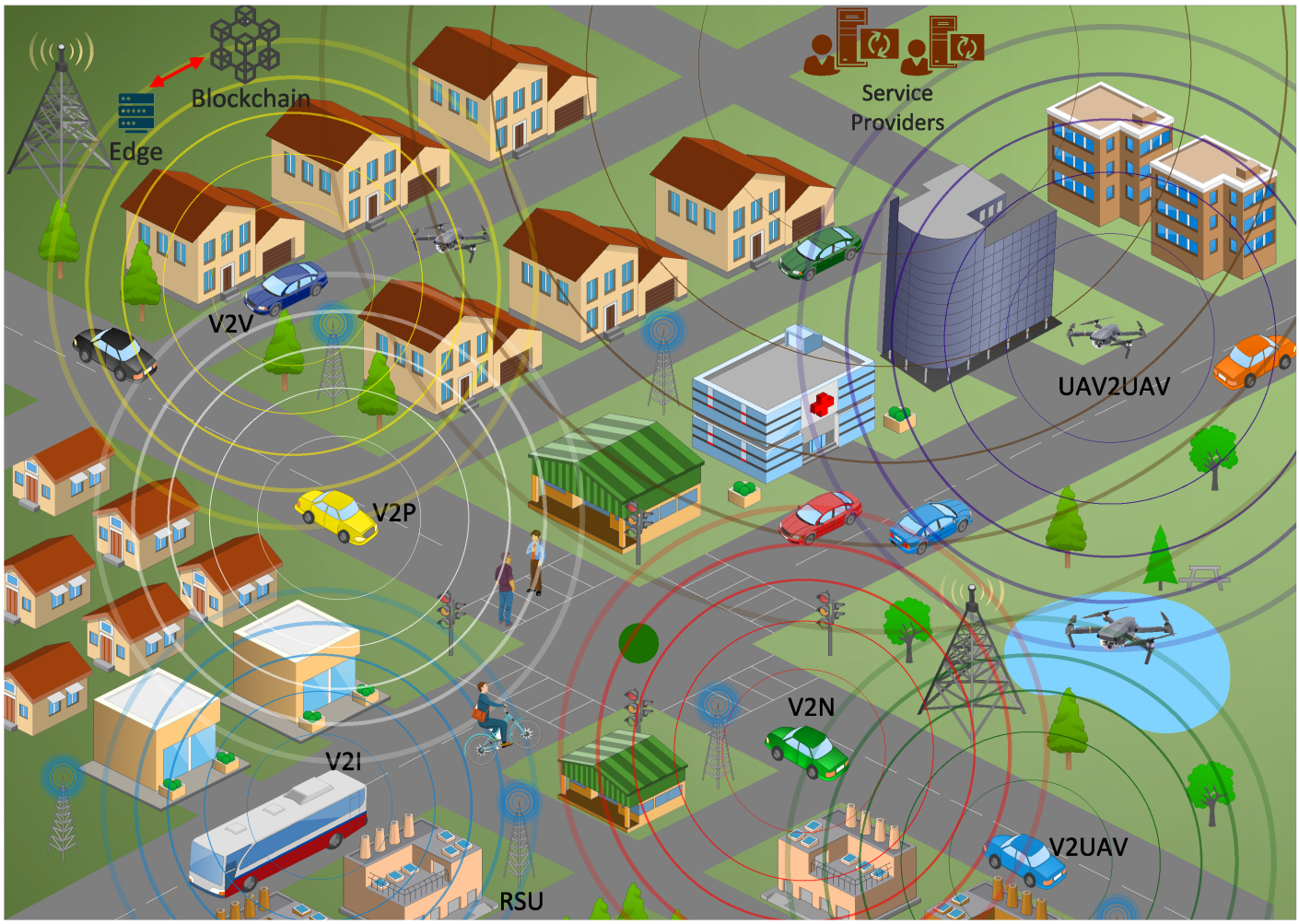

Figure 1. MEC-enabled Internet of Flying Things for Smart Cities.

Indeed, security could well be assessed from three main perspectives: (*i*) foremost, confidentiality and integrity of data ought to be assured for both stationary and transferred data, as well as controlling the access and authorisation to the system by other drones and users; (*ii*) users' personal information and data should be well preserved, since UAVs acquire and handle sensitive data; (*iii*) trust aspect since UAV environment is composed of several and heterogeneous devices/users, that handle data of various sorts [1][2][3].

In this context, on one hand, blockchain is emerging as a promising technology to provide the confidentiality and integrity of exchanged data between UAV devices, and generate trust between the involved UAVs, without the need for a trusted third entity [4][5]. On the other hand, collaborative/distributed Deep Learning (DL), such as Federated Learning (FL), emerges also to not only optimize UAV network management and thus meeting the requirement of their emerged applications, but also to ensure the UAVs' privacy by keeping the needed data (i.e., sensed data) on UAV devices [6][7][8][9][10]. Specifically, FL enables UAV devices to leverage their sensed data to build local DL models. The latter are then sent to a central node for aggregation, in order to generate a global DL

model. Therefore, FL enables UAV devices to collaborate during several FL rounds in generating a learning model, while avoiding to share their local data, and thus ensuring UAVs' privacy. Hence, the deployment of blockchain technology as a ledger to provide distributed FL training is a viable option to address the aforementioned security issues [11][12].

In addition, the amalgamation of UAVs with both collaborative FL and Blockchain technology have ushered in a new paradigm of Secure Multi-Access Edge Computing (S-MEC), where the objective is to bring computation very close to UAV devices and in a secure way. Indeed, a S-MEC node may act as a central node in the federated learning in order to aggregate the UAVs' local models and build a global DL model.

However, UAV devices are usually limited in terms of resources such as battery, memory, and CPU. Thus, some of the UAV devices may not be able to build a local learning models due to their resources capacity. Hence, there is a great need to select the adequate UAVs at each FL round, that are able to build a local DL model based on their resource capacities [5][13].

2. Client/Participant Selection in FL Process

In general context, a wide range of solutions have been designed, that investigate client/participant selection in FL. The authors in [14], suggested Oort as a strategy to enhance federated training and testing performance, by guided participant selection. Intending to increase model training time-to-accuracy performance, the proposal focuses on the use of customers who have both data, that can help improve model accuracy as well as time training complexity. Based on its present loss and estimated delay, each client is assigned a utility. Each epoch, they recalculate the utility of each client accessible for training and choose the top k clients. In their work, they consider captured statistical heterogeneity, but only to a low level of the loss function, used in model training.

The authors in [15] introduced a tier-based FL system (Tifl), which divides clients into tiers depending on training results. By optimizing both accuracy and training time, the algorithm dynamically selects participating clients from the same tier for each training session. As a result, the performance challenges caused by data and resource heterogeneity are reduced. It is a resource-demanding hardware-based solution. The overall training duration for each client is unknown initially, so they assess all of the clients at the beginning.

FedSAE is a self-adaptive FL system introduced in [16], which adaptively selects clients with higher local training losses, in each training cycle to accelerate global model convergence. To increase device dependability, a prediction technique for each client's affordable workload is also suggested. This would allow for dynamic modification of the number of local training epochs for each client. The authors measure their model convergence by training loss.

The authors in [17] introduced FAVOR, which selects a subset of participating clients for each training round to offset the bias generated by non-IID data. To maximize accuracy while reducing the number of communication

rounds, a deep Q-learning formulation for client selection is employed. However, the proposed algorithm requires a significant amount of offline training, and the data on each device should remain consistent during the process.

Similarly, in [18], a novel client selection method is designed, which is based on the Multi-Armed Bandit formulation to choose the subset of clients, with the least amount of class imbalance. They measure local class distributions, by comparing the similarity of FL server local gradient updates with gradients inferred from a balanced proxy data set on the server. It is necessary to understand the global data distribution, in order to generate such a proxy data set, which is difficult to do in FL contexts due to privacy-preservation issues.

3. Resource-Constrained Client/Participant Selection in FL Process

Implementing FL in resource-constrained networks has gained a lot of study attention in the past few years. Various studies investigated the use FL to increase learning efficiency and enhance network performance. Nonetheless, research targeting UAV selection in distributed learning is still in its infancy.

In [19], the authors intended to extend the FL process to interact with heterogeneous clients in a cellular network. To enhance the training process, they present a client selection scheme for FL at the mobile edge. They aim to solve the problem of longer update/upload times, due to insufficient computational capabilities or bad wireless channel conditions. To improve future selections and help design efficient service pricing schemes, it is necessary to evaluate the contribution of every single client in the training process. Proposing trust and reputation models to evaluate the reliability of the participating clients is also essential.

Another new resource allocation algorithm for UAV networks based on multi-agent collaborative environment learning is proposed in [20]. It aims to overcome the communication delay and enhance the network efficiency, caused by the centralized architecture. In a distributed architecture, they model each UAV as a self-contained agent, that enhances the utility of UAV networks, through dynamic selection decisions considering the UAV's deployment position, transmission power, and occupied sub-channels.

In [9], the authors introduced Federated Deep Learning concept as a potential solution for many resource-constrained UAV-enabled wireless applications. In the meantime, several issues need to be more investigated such as the optimal number of UAVs (clients), as well as the frequency of local and global model updates. UAVs are not always connected to the FDL due to energy and connectivity constraints. In this context, FDL algorithms should be robust to client loss by predicting such scenarios.

In [21], to handle dynamicity, the authors proposed, using a multi-armed bandit (MAB)-based strategy, to achieve learning convergence effectively in a short period. In permissioned blockchain context such as Hyper-ledger Fabric (HF), the authors addressed the trade-off in peers' number, caused by HF unique execute-order procedure. Meanwhile, advanced technologies such as federated learning have recently been a better solution for wireless system self-adaptation problems.

The authors in [22] introduced a combination of algorithms to maximize UAV data collection from ground sensors, while remaining within time constraints in both offline and online settings. They use an K-means method to group sensor nodes and deploy selected cluster heads, then, a UAV-based data collection is used. Tabu-search, simulated annealing (SA), and guided local search (GLS) were among the offline solutions, while reinforcement learning (RL) techniques were used online.

References

1. Billah, M.; Mehedi, S.; Anwar, A.; Rahman, Z.; Islam, R. A Systematic Literature Review on Blockchain Enabled Federated Learning Framework for Internet of Vehicles. arXiv 2022, arXiv:2203.05192.
2. Syed, F.; Gupta, S.K.; Hamood Alsamhi, S.; Rashid, M.; Liu, X. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. Trans. Emerg. Telecommun. Technol. 2021, 32, e4133.
3. Zhang, X.; Chen, X. UAV task allocation based on clone selection algorithm. Wirel. Commun. Mob. Comput. 2021, 2021, 5518927.
4. Kayalvizhi, M.; Ramamoorthy, S. Review of Security Gaps in Optimal Path Selection in Unmanned Aerial Vehicles Communication. In Sustainable Advanced Computing; Springer: Singapore, 2022; pp. 439–451.
5. Nguyen, D.C.; Hosseinalipour, S.; Love, D.J.; Pathirana, P.N.; Brinton, C.G. Latency Optimization for Blockchain-Empowered Federated Learning in Multi-Server Edge Computing. arXiv 2022, arXiv:2203.09670.
6. Liu, X.; Deng, Y.; Mahmoodi, T. A Novel Hybrid Split and Federated Learning Architecture in Wireless UAV Networks. In Proceedings of the IEEE ICC, Seoul, Korea, 16–20 May 2022; IEEE: Manhattan, NY, USA, 2022.
7. Brik, B.; Messaadia, M.; Sahnoun, M.; Bettayeb, B.; Benatia, M.A. Fog-Supported Low-Latency Monitoring of System Disruptions in Industry 4.0: A Federated Learning Approach. ACM Trans. Cyber-Phys. Syst. 2022, 6, 14.
8. Yang, H.; Zhao, J.; Xiong, Z.; Lam, K.Y.; Sun, S.; Xiao, L. Privacy-preserving federated learning for UAV-enabled networks: Learning-based joint scheduling and resource management. IEEE J. Sel. Areas Commun. 2021, 39, 3144–3159.
9. Brik, B.; Ksentini, A.; Bouaziz, M. Federated learning for UAVs-enabled wireless networks: Use cases, challenges, and open problems. IEEE Access 2020, 8, 53841–53849.

10. Brik, B.; Ksentini, A. On Predicting Service-oriented Network Slices Performances in 5G: A Federated Learning Approach. In Proceedings of the 2020 IEEE 45th Conference on Local Computer Networks (LCN), Sydney, Australia, 16–19 November 2020; pp. 164–171.
11. Saraswat, D.; Verma, A.; Bhattacharya, P.; Tanwar, S.; Sharma, G.; Bokoro, P.N.; Sharma, R. Blockchain-Based Federated Learning in UAVs Beyond 5G Networks: A Solution Taxonomy and Future Directions. IEEE Access 2022, 10, 33154–33182.
12. Abou El Houda, Z.; Brik, B.; Ksentini, A.; Khoukhi, L.; Guizani, M. When Federated Learning Meets Game Theory: A Cooperative Framework to secure IIoT Applications on Edge Computing. IEEE Trans. Ind. Inform. 2022, 1.
13. Otoum, S.; Al Ridhawi, I.; Mouftah, H. A Federated Learning and Blockchain-enabled Sustainable Energy-Trade at the Edge: A Framework for Industry 4.0. IEEE Internet Things J. 2022.
14. Lai, F.; Zhu, X.; Madhyastha, H.V.; Chowdhury, M. Oort: Efficient federated learning via guided participant selection. In Proceedings of the 15th USENIX Symposium on Operating Systems Design and Implementation (OSDI 21), Santa Clara, CA, USA, 14–16 July 2021; pp. 19–35.
15. Chai, Z.; Ali, A.; Zawad, S.; Truex, S.; Anwar, A.; Baracaldo, N.; Zhou, Y.; Ludwig, H.; Yan, F.; Cheng, Y. Tifl: A tier-based federated learning system. In Proceedings of the 29th International Symposium on High-Performance Parallel and Distributed Computing, Stockholm, Sweden, 23–26 June 2020; pp. 125–136.
16. Li, L.; Duan, M.; Liu, D.; Zhang, Y.; Ren, A.; Chen, X.; Tan, Y.; Wang, C. FedSAE: A novel self-adaptive federated learning framework in heterogeneous systems. In Proceedings of the 2021 International Joint Conference on Neural Networks (IJCNN), Shenzhen, China, 18–22 July 2021; pp. 1–10.
17. Wang, H.; Kaplan, Z.; Niu, D.; Li, B. Optimizing federated learning on non-iid data with reinforcement learning. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications, Toronto, ON, Canada, 6–9 July 2020; pp. 1698–1707.
18. Yang, M.; Wang, X.; Zhu, H.; Wang, H.; Qian, H. Federated learning with class imbalance reduction. In Proceedings of the 2021 29th European Signal Processing Conference (EUSIPCO), Dublin, Ireland, 23–27 August 2021; pp. 2174–2178.
19. Nishio, T.; Yonetani, R. Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–7.
20. Dai, Z.; Zhang, Y.; Zhang, W.; Luo, X.; He, Z. A Multi-Agent Collaborative Environment Learning Method for UAV Deployment and Resource Allocation. IEEE Trans. Signal Inf. Process. Over Netw. 2022, 8, 120–130.

21. Kim, S.; Ibrahim, A.S. Byzantine-Fault-Tolerant Consensus via Reinforcement Learning for Permissioned Blockchain-Empowered V2X Network. IEEE Trans. Intell. Veh. 2022.
22. Ghdiri, O.; Jaafar, W.; Alfattani, S.; Abderrazak, J.B.; Yanikomeroglu, H. Offline and Online UAV-Enabled Data Collection in Time-Constrained IoT Networks. IEEE Trans. Green Commun. Netw. 2021, 5, 1918–1933.