FLoc: Fingerprint-based Indoor Localization System under a Federated Learning Updating Framework

Yuxiang Liu, Huichuwu Li, Jiang Xiao, and Hai Jin
National Engineering Research Center for Big Data Technology and System
Services Computing Technology and System Lab, Cluster and Grid Computing Lab
School of Computer Science and Technology, Huazhong University of Science and Technology
Wuhan, 430074, China
Email: jiangxiao@hust.edu.cn

***Abstract*—Fingerprinting-based indoor localization via WiFi has achieved a great breakthrough in the past decade. However, it suffers from an inherent problem that the localization accuracy declines sharply over time due to the dynamic environment and unstable WiFi devices. Researchers have designed many methods to update the localization model, e.g., crowdsourcing-based model updating, in order to maintain the localization accuracy. Unfortunately, they have not taken the privacy into consideration during the updating process. This will lead to a threat that the eavesdroppers could guess the location providers' private information according to the updating model.**

For the goal of maintaining the localization accuracy without the risk of privacy breaching, we proposed FLoc, a fingerprinting-based indoor localization system which updates the localization model via a federated learning framework. In FLoc, every provider maintains a local localization model in their own device. They will regularly encrypt the updating parameters and share them to a common model server. At the model server, it aggregates the encrypted information of the local models to maintain a general model, which will be sent back to the local devices for next updating iteration. We evaluate FLoc in an APs unknown laboratory corridor. The experiment results show that FLoc has a comparable localization performance. Moreover, it can successfully protect the providers' privacy, since the information transferred is all encrypted.

***Index Terms*—Indoor Localization, Fingerprinting, Federated Learning**

I. Introduction

Industry and academia have been devoting massive efforts for indoor localization due to its promising future [1]. Thanks to the ubiquitous deployment of WiFi instruments, WiFi-based indoor localization systems have obtained a lot of attention. Current systems can be classified into two-folds: *Propagation Model-based* and *Location Fingerprinting-based* [2]–[5]. *Propagation Model-based* methods estimate the distance between transmitter and receiver according to some propagation models such as the *Free Space Model*. Then, by computing the relative locations of the receiver to some specific defined transmitters, *Propagation Model-based* methods can estimate the user's coordinates in the indoor environment. Hence, these methods need the prior knowledge of the *Access Point* (AP) locations [6].

Location Fingerprinting-based methods extract the representative and distinguishable characters, named as fingerprint, from the received WiFi signals of different places to estimate mobile devices' locations. Typically, *Location Fingerprinting-based* localization systems are composed of offline phase and online phase. During the offline phase, WiFi signals of the predefined reference locations are collected to build the fingerprinting database. In the online phase, the systems extract the fingerprints from the real-time signals in the same way, and match the real-time fingerprints to those saved in the database. According to the most similar reference fingerprints' locations, *Location Fingerprinting-based* systems can estimate the users' locations.

However, a key drawback of location fingerprints is the unstable localization accuracy caused by the inconsistency between pre-collected fingerprints and real-time measurements. Therefore, many systems were proposed to solve the inconsistency problem of fingerprints. Some of them requires specific people to conduct site surveys regularly to maintain localization accuracy, which increases the burden of data collection in exchange. Some other systems utilize intelligent machine to collect location fingerprints automatically [2]. These systems need special devices which are required to traverse the entire indoor area. Crowdsourcing is another widely used method that can use *Commercial Off-The-Shelf* (COTS) WiFi devices (e.g., cellphone and smartwatch) to update the fingerprinting model in real-time without special devices [3], [4]. Unfortunately, the current crowdsourcing-based systems have not taken the privacy into consideration, these systems require users to provide their location information. As a result, the location providers are exposed to the risk of privacy breaches.

In this paper, we present FLoc, a federated learning-based indoor localization system that can update fingerprints without privacy leakage or special devices. FLoc utilizes *Deep Neural Networks* (DNN) model to estimate targets' locations and location fingerprints are model inputs. In order to realize FLoc, there are three challenging issues. The first challenge is how to generate the fingerprints of the locations. We extract the representative fingerprints from the noisy signals via a modified version of *Deep Autoencoder* (DAE) owing to its good performance on noise reduction and feature extraction. The second challenge is how to update the fingerprints dataset for the purpose of maintaining the localization accuracy. Due to the impacts of jobs, living habits, physiological state, and other factors, people's activity areas have a pattern similar to

978-1-7281-5212-7/19/$31.00 ©2019 IEEE
DOI 10.1109/MSN48538.2019.00033

the principle of locality. Therefore, the personal localization models may have location bias, that is, the models have high localization accuracy in the areas where their own users occur frequently, and the localization accuracy in other areas is low. In order to design a general localization model without such bias, we aggregate the personal models of all the users together like a jigsaw puzzle. Hence, FLoc requires users to share their local models to the public, and it will cause a threaten that the eavesdropper may reversely use the models to guess our privacy information. Thus, the third challenge is how to avoid privacy breaching when sharing the personal models. Inspired by the researches about Federated Learning [7], FLoc combines the distributed fingerprints updating method with a homomorphic encryption-based federated learning framework to achieve the safe updating goal. We evaluate FLoc in a laboratory corridor located at our university, where the locations of APs are unknown. The results show that FLoc is able to be adapted to the dynamic environment without the risk of location privacy breaching and keep stable localization performance all the time.

The major contributions of this paper are summarized as follows:

- To our best knowledge, FLoc is the first work to apply the federated learning to fingerprinting-based indoor localization scenario in order to solve the security problem in fingerprint database updating.
- We design a DNN model for indoor localization. The model consists of an autoencoder and a classification-based DNN of which the output layer has been modified for location estimation.
- We implement the system in a laboratory corridor. The experiment results show the robustness and stable performance of FLoc in dynamic environment and unstable signals.

The remainder of this paper is organized as follows: Section II introduces the related work. Section III presents the system architecture and mathematical model. The methodology is described in Section III-B, and the evaluation is in Section IV. At last, we conclude this work in Section V.

II. Related Work

In this section, we introduce the related work from two aspects: fingerprinting-based indoor localization methods and federated learning work.

Fingerprinting-based Methods. As a commonly used indoor localization method, the fingerprinting-based method does not need extra hardware or firmware modification. Fu et al. [8] use the feature-scaling-based k-nearest neighbor algorithm to distinguish RSSI fingerprints of different positions for indoor localization. Li et al. [9] leverage probabilistic techniques to infer the location represented by the fingerprints. Furthermore, machine-learning methods are also used to classify location fingerprints, such as random forest [10], [11], neural networks [12], [13]. For these methods, a key defect, causing unstable localization accuracy, is the inconsistency between the pre-collecting database and real-time measurements. Thus, the key problem is how to guarantee the timeliness and effectiveness of fingerprinting database. Site survey, collecting new fingerprints, is an inefficient and expensive method. Therefore, Piao et al. [2] use an Unmanned Aerial Vehicle to collect location fingerprints instead of manual collecting. Additionally, crowdsourcing is often used to update the fingerprinting database by wireless mobile devices [3], [4], but crowdsourcing has the risk of location privacy breaching when sharing the fingerprinting information. FLoc utilizes federated learning to make mobile devices collaboratively train model, and improve localization model without extra devices or privacy leaking risk.

Federated Learning. For breaking isolated islands of data and strengthening data privacy and security, Google first proposes federated learning framework [14] in 2016. According to the feature space and sample space of dataset, Yang et al. [7] proposed three federated learning frameworks, including horizontal federated learning [15], vertical federated learning, and federated transfer learning [16]. Hard et al. [15] train a neural network model using a distributed, on-device learning framework to predict next-word in a virtual keyboard of smartphones. Moreover, federated learning is also used in the medical field to protect health records of patients while using health records from different hospitals to serve patients. Brisimi et al. [17] propose a new federated learning framework that can train predictive models to predict patient hospitalization through hospital-to-hospital collaboration without raw data exchanges. FLoc introduces federated learning into a fingerprinting-based localization model and achieves real-time update of the model and protection of user location information.

III. System Design

A. System Overview

As shown in Fig. 1, FLoc consists of two modules: *Fingerprinting-based Localization* and *Model Updating*. In the Fingerprinting-based Localization module, FLoc uses *Reading Alignment* to process the raw RSSI readings from location unknown APs in the interest indoor area. Then, in the *Location Estimation* phase, FLoc extracts features by using AutoEncoder to decrease the dimension of RSSI vectors and uses DNN model to estimate the location. In the Model Updating module, mobile devices, in different locations, use the localization model to local position and update local model in real-time. Moreover, while mobile devices obtain a model from the model server, the model server gets updating gradients from mobile devices for updating model in the server.

In the initialization phase, to get the initial localization model, FLoc uses WiFi terminals to scan the indoor APs and get their RSSI at the different fingerprinting locations in the localization area. The reading alignment module is used to transform the WiFi measurements to a fixed format that is required in the location estimation phase. The preprocessed data is fed into the localization model, which includes autoencoder for dimension decreasing and DNN model for localization. The

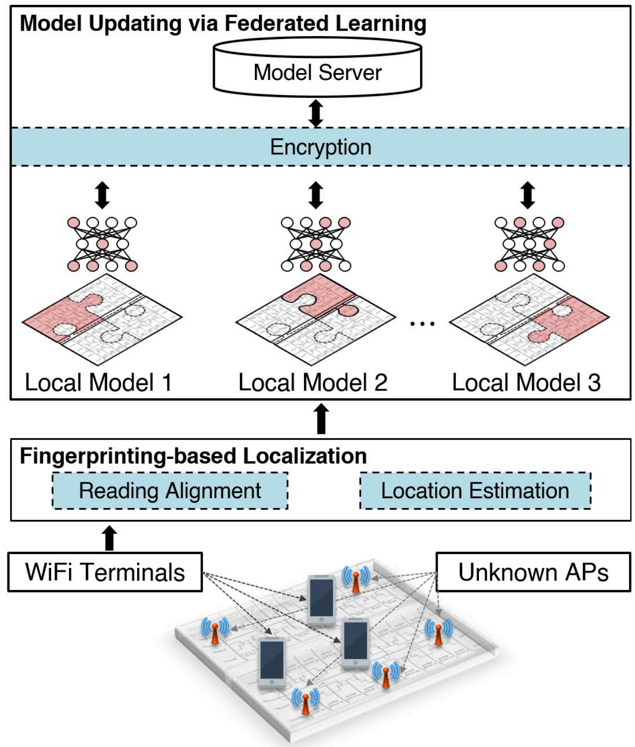

Fig. 1. The Architectural Design of FLoc

initial model is saved into model server for serving various mobile devices.

Obviously, with the environment changing and signal fluctuation, the mobile devices, having the initial localization model, lose the localization accuracy. Therefore, in the model updating module, each mobile device collects the new RSSI readings, which experience reading alignment and feature extraction, for updating the local localization model. At the same time, mobile devices help model server updating its model. For protecting the location privacy of users, mobile devices use federated learning framework and only share the updating gradients to model server, instead of location fingerprints. Thus, the localization model in model server always keeps the good localization performance.

B. *Fingerprinting-based Localization*

This section presents the details of the offline model training phase and the online localization and model updating phase.

Reading Alignment. *Reading Alignment* is responsible for transferring the scanning results, X, into a structured format of length-fixed vectors. In this 2-D localization problem, we assume that there are M reference locations distributed over the indoor area, where exists N unknown fixed APs. During the localization phase, a mobile device, hold by a user at an unknown location l, scans the RSSIs from the nearby APs, and a single scanning result is saved as a vector $\boldsymbol{X} = [x_1, x_2, ..., x_N]$. Element x_i records the RSSI reading

Access Points	MAC_1	MAC_2	MAC_3	MAC_4	MAC_5	MAC_6	MAC_7	···	MAC_n
X	x_1	x_2	x_3	x_4	x_5	x_6	x_7	···	x_n
Raw RSSI (dB)	-83	-92	null	-67	-54	null	null	···	-33
Structured RSSI (dB)	-83	-92	-100	-67	-54	-100	-100	···	-33

Fig. 2. The Preprocessing of RSSI Readings

from the i-th access point. Since the APs are unknown in this problem, the heard APs in each scan processing are different. If directly using the RSSI signals transmitted by the random occurring APs to construct the RSSI recording vectors, the localization result will be confused by the random element orders. For the purpose of generating order fixed RSSI recording vectors in the AP unknown environment, FLoc maintains a mac address list in increments during the initial site survey process. When FLoc detects a new AP, it adds the AP's mac address to the tail of the mac list saved in the model server. After the initial site survey process, the mac address list includes all of the potential APs. Thus, according to the mac address list, we could record the RSSI signals in a stable order. Note that not all APs in the target area can be heard in any location at any time. Due to the absence signals of some APs, the unstable structure of input data could result in a complex algorithm design. According to our observation, the received RSSI values are no smaller than $-100dB$. Therefore, as shown in Fig. 2, we assign the weakest RSSI value $-100dB$ to the APs which are not heard.

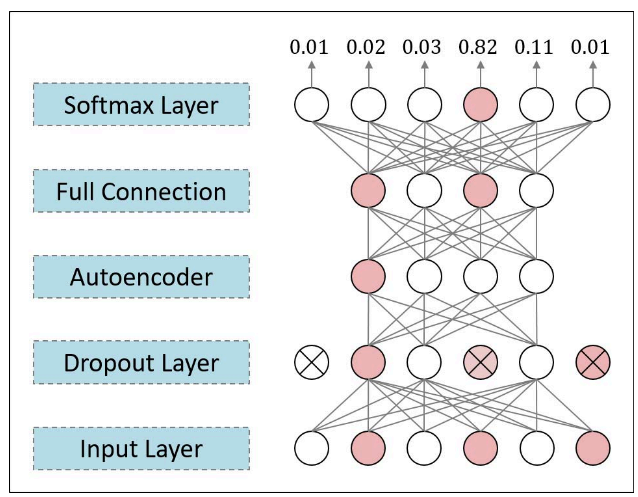

Fig. 3. The Localization Model Structure

Location Estimation. Due to the long distances and obstacles between the receiver and some hidden APs, the recording vector is often sparse. Since FLoc assigns the weakest RSSI value to the APs that are not heard in a fingerprint location, the length of RSSI vectors is more than 200, including the repeated -100. For DNN model training, the RSSI values are bad to improve the training efficiency and convergence. Therefore, we train an autoencoder to extract the most representative fingerprints, $\boldsymbol{Y} = [y_1, y_2, ..., y_T], T < N$, from the raw recording vectors X. In the real scenarios, WiFi AP absence and noise cannot be predicted in advance. In order to imitate the AP absence in real life, FLoc adds a dropout layer before sending the vector to the autoencoder, as shown in Fig. 3. Without loss of general, we insert Gaussian noise to Y to improve the robustness of autoencoder. This process makes the localization model more robust and more suitable for the complex real environment.

After autoencoder, FLoc adds traditional DNN, including full connection layer and softmax layer, in the localization model structure in Fig. 3. In the softmax layer, the output is the probabilities that the current location corresponds to each reference locations. Intuitively, the larger probability values represent the closer distance between current location and reference locations. If we only rely on the reference location with the highest probability, the location estimation result is not accurate enough unless the current location coincides with the reference location, totally. Therefore, FLoc modifies the output of the softmax layer and makes full use of all probabilities. We aggregate all probabilities to a vector $\boldsymbol{P} = [p_1, p_2, ..., p_T]$ and coordinates of all reference locations to a vector $\boldsymbol{L} = [l_1, l_2, ..., l_T], l_i = (x_i, y_i)$, whose order corresponds to the order of the vector $\boldsymbol{P}$. Thus, the location estimation formula is

$$l_{cur} = L * P^{\mathrm{T}} = l_1 * p_1 + l_2 * p_2 + ... + l_T * p_T \qquad (1)$$

which has considered all reference locations and is able to get more accurate result.

C. Model Updating via Federated Learning

Definition of Federated Learning. First of all, we briefly introduce the definition of federal learning [7]. Defining N data owners as $\{F_1, ...F_N\}$, all data owners wish to get a good performance model by using own data set $\{D_1, ...D_N\}$, respectively. Obviously, a conventional deep learning is to collect all data set together and utilize $D = D_1 \cup ... \cup D_N$ to train a model M_{SUM}. Conversely, a federated learning framework makes the data owners collaboratively train a model M_{FED}, and guarantee that any data owner F_i needs not provide its data set D_i to others. Furthermore, the performance of M_{FED}, recorded as V_{FED} would better be close to the M_{SUM} performance, V_{SUM}. As shown in equation. 2, let δ be a non-negative real number, we evaluate the federated learning framework has δ-accuracy loss. For an effective federated learning method, δ should be as small as possible.

$$|V_{FED} - V_{SUM}| < \delta \qquad (2)$$

Model Updating. According to the taxonomy concluded by Yang et al. [7], federal learning can be divided into three categories. Among three categories, horizontal federated learning is used to the scenarios that data sets enjoy the same feature space but different in samples. Since FLoc focuses on utilizing location fingerprinting to achieve indoor localization and update model with mobile devices, FLoc belongs to horizontal federated learning.

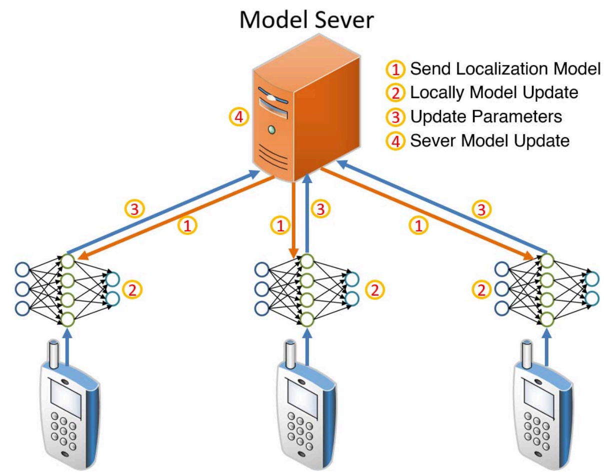

Fig. 4. The Federated Learning Framework of FLoc

The federated learning framework of FLoc is shown in Fig. 4. In the initialization phase, FLoc relies on the manual to obtain the initial localization model that is saved in the model server. The federated learning framework can update the model of the server in real-time, ensuring that the model always adapts to the environment and guarantees high localization accuracy. When entering the indoor area, a new mobile device obtains a localization model from the model server. The mobile device receives WiFi signals from different APs, and then process the signals into fixed fingerprinting features, that are as input to Localization model for getting location output. When the environment has been changed, the location fingerprinting features are also different. Therefore, the model of mobile device can not offer accurate location information. In this time, mobile devices collect RSSI, processed into fingerprinting features, and re-train the model in mobile devices by using new fingerprinting samples. At the same time, the re-trained mobile device sends update parameters of local model to model server for helping model server update localization model. After that, the server model is adapted to the changed environment and can provide the newest localization model to the new entering mobile devices.

IV. Evaluation

In this section, we evaluate the performance of FLoc in a laboratory corridor. We first display the basic situation of data collection. Then, we compare federated learning with conventional deep learning in fingerprinting localization model. Finally, we analyze the adaptability of FLoc to dynamic environment and unstable signals.

A. Data Collection

We have invited three volunteers responsible for data collection. Two of them utilize cellphone to collect RSSI signals in

Laboratory, while the other one uses LapTop. Fig. 5 shows the floor plan of the testing place where the corridor is $2.4m$ width and $138m$ length. The number of RSSI readings, that can be heard in the laboratory corridor, is about 225 from different MAC addresses. We use laptop and mobile phones to collect RSSI of different APs in each reference fingerprinting location. In order to evaluate the robustness to the changed RSSI, we collect RSSI at different time periods including daytime and night, because different time periods have different personnel activities and signal status. During the period of data collection, we use mobile devices to scan APs at different reference locations and set the distance between adjacent reference locations to 1.8m. We leverage a software, WiFi Collector, to collect data. The software is able to collect the MAC address and corresponding RSSI from heard WiFi APs. Referring to other fingerprinting localization systems, we set the scanning interval to one second. We implemented our localization model training and testing, using the PyTorch package and PySyft package on the PyCharm IDE.

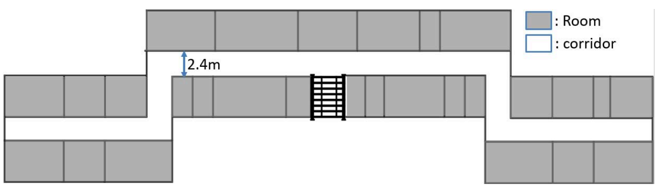

Fig. 5. The Indoor Area of Experiment

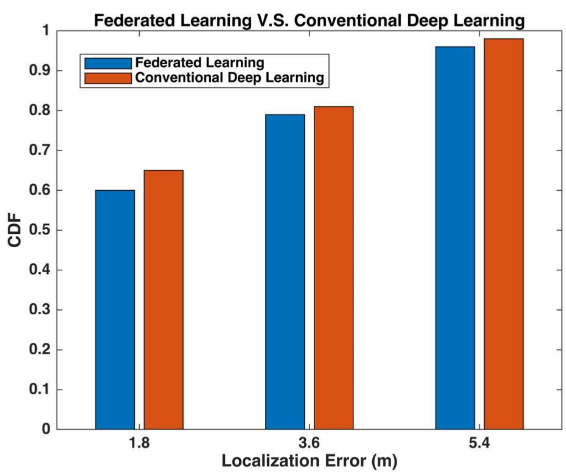

Fig. 6. The Federated Learning Comparing with Conventional Deep Learning

B. Federated Learning V.S. Conventional Deep Learning

In this section, we compare the performance of localization models that are trained by conventional deep learning and federated learning, respectively. We artificially set some test locations, and the deviation between the predicted locations and their related test locations are the localization errors. First, we gathered data of all the volunteers to train a general localization model, and then record its location estimation results for comparison. Next, we leverage the PyTorch federate learning framework to assign the training tasks to two clients. The two clients use their own data to train models locally and send only encrypted model parameters to the server. Then, the server aggregates parameters and re-sends back to two clients for helping them updating local models. The performance is shown in Fig. 6, and the confidence of both cases is 80% within the allowable error range of 3.6m. Intuitively, by increasing the reference point density, the accuracy of FLoc will increase accordingly. The experimental results confirm that federal learning can be compared with traditional deep learning, and the difference between them is within acceptable limits.

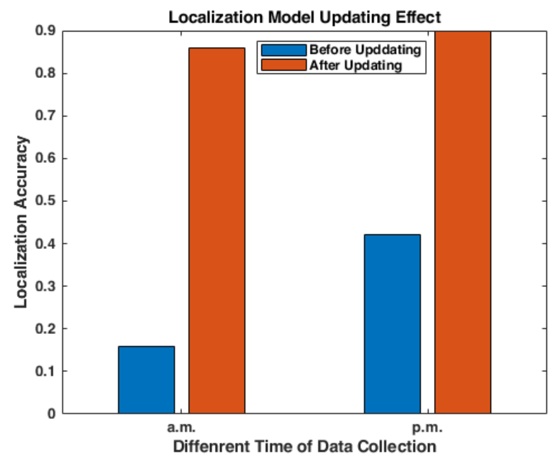

Fig. 7. The Federated Learning-based Localization Model Updating Effect

C. Effect of Localization Model Updating

In this part, we evaluate the updating effect by federated learning framework. Due to the active members at night are less than daytime, the laboratory environment is more stable. Therefore, we collect RSSI fingerprints at night to training the initial localization model. Then, we collect RSSI fingerprints in the morning and afternoon, respectively. Obviously, due to the different time has different dynamic environment and signal status, the collect RSSI fingerprints is inconsistent in the same reference location. Thus, before updating the model, from Fig. 7 we can learn that the initial model performance, directly applying to the daytime data, is lower than 50%. Then, we update the initial model in federated learning framework. Such updating process can significantly improve the model performance to be up to 90%. As shown in Fig. 7, federated learning updating makes the localization model be adapted to the dynamic environment and unstable signals and solves the inconsistency problem. At the same time, the users' location information is not leaving the local devices all the time without location privacy breaches.

V. Conclusion

We proposed FLoc, a robust WiFi indoor location fingerprinting localization system based federated learning. The system focuses on reducing the risk of privacy breaching when updating the fingerprinting-based localization model. To avoid the private location information from leaking, FLoc uses a federated learning framework to update the localization model and only needs model update parameters instead of location fingerprints from mobile devices.

We evaluated FLoc in a laboratory corridor. The experimental results show that federated learning is comparable to conventional deep learning. Furthermore, the FLoc is able to solve the inconsistency problem by updating the localization model, which is adapted to the dynamic environment and unstable signals. Additionally, the FLoc protects the location privacy of mobile devices users relying on federated learning. Finally, we intend to consider the difference of different mobile devices in future work.

Acknowledgment

This work is supported by National Science Foundation of China under Grant No. 61702203, Hubei Provincial Natural Science Foundation No. 2018CFB133. Jiang Xiao is the corresponding author.

References

[1] D. Lymberopoulos and J. Liu, "The microsoft indoor localization competition: Experiences and lessons learned," *IEEE Signal Processing Magazine*, vol. 34, no. 5, pp. 125–140, 2017.

[2] S. Piao, Z. Ba, L. Su, D. Koutsonikolas, S. Li, and K. Ren, "Automating csi measurement with uavs: from problem formulation to energy-optimal solution," in *Proceedings of the 2019 IEEE International Conference on Computer Communications (INFOCOM)*. IEEE, 2019, pp. 2404–2412.

[3] Y. Li, Z. He, Z. Gao, Y. Zhuang, C. Shi, and N. El-Sheimy, "Toward robust crowdsourcing-based localization: A fingerprinting accuracy indicator enhanced wireless/magnetic/inertial integration approach," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3585–3600, 2018.

[4] P. Zhang, Q. Zhao, Y. Li, X. Niu, Y. Zhuang, and J. Liu, "Collaborative wifi fingerprinting using sensor-based navigation on smartphones," *Sensors*, vol. 15, no. 7, pp. 17 534–17 557, 2015.

[5] J. Xiao, Y. Yi, L. Wang, H. Li, Z. Zhou, K. Wu, and L. M. Ni, "Nomloc: Calibration-free indoor localization with nomadic access points," in *Proceedings of the 34th IEEE International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2014, pp. 587–596.

[6] A. Bose and C. H. Foh, "A practical path loss model for indoor wifi positioning enhancement," in *Proceedings of the 6th International Conference on Information, Communications & Signal Processing (ICICS)*. IEEE, 2007, pp. 1–5.

[7] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, p. 12, 2019.

[8] Y. Fu, P. Chen, S. Yang, and J. Tang, "An indoor localization algorithm based on continuous feature scaling and outlier deleting," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1108–1115, 2018.

[9] Y. Li, Z. He, Y. Li, H. Xu, L. Pei, and Y. Zhang, "Towards location enhanced iot: Characterization of lora signal for wide area localization," in *Proceedings of the 2018 International Conference on Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS)*. IEEE, 2018, pp. 1–7.

[10] Y. Wang, C. Xiu, X. Zhang, and D. Yang, "Wifi indoor localization with csi fingerprinting-based random forest," *Sensors*, vol. 18, no. 9, pp. 2869–2891, 2018.

[11] X. Guo, N. Ansari, L. Li, and H. Li, "Indoor localization by fusing a group of fingerprints based on random forests," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4686–4698, 2018.

[12] H. Chen, Y. Zhang, W. Li, X. Tao, and P. Zhang, "Confi: Convolutional neural networks based indoor wi-fi localization using channel state information," *IEEE Access*, vol. 5, pp. 18 066–18 074, 2017.

[13] M. Abbas, M. Elhamshary, H. Rizk, M. Torki, and M. Youssef, "Wideep: Wifi-based accurate and robust indoor localization system using deep learning," in *Proceedings of the International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 2019.

[14] J. Konečnỳ, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated optimization: Distributed machine learning for on-device intelligence," *arXiv preprint arXiv:1610.02527*, 2016.

[15] A. Hard, K. Rao, R. Mathews, F. Beaufays, S. Augenstein, H. Eichner, C. Kiddon, and D. Ramage, "Federated learning for mobile keyboard prediction," *arXiv preprint arXiv:1811.03604*, 2018.

[16] Y. Liu, T. Chen, and Q. Yang, "Secure federated transfer learning," *arXiv preprint arXiv:1812.03337*, 2018.

[17] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. C. Paschalidis, and W. Shi, "Federated learning of predictive models from federated electronic health records," *International journal of medical informatics*, vol. 112, pp. 59–67, 2018.