Simulating Federated Learning for Smartphone based Indoor Localisation

Litian Li
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
l.li-4@student.utwente.nl

ABSTRACT

Satellite navigation such as Global Positioning System (GPS) cannot accurately and quickly locate indoors due to signal congestion and path complexity caused by the building structure. In indoor positioning technology based on wifi fingerprint is a general solution. As the demand for indoor positioning increases and people's awareness of privacy protection increases. It is essential to protect privacy in the crowdsourced method of collecting user location information. Compared to traditional centralized machine learning and distributed machine learning. In federated learning, user data is only trained locally without leaving the local device. Only model parameters and gradients are transmitting between the service and the client. Thus federated learning has become a solution as a machine learning method to protect user privacy. The author will select a suitable open-source indoor positioning data set based on wifi fingerprints, and choose a suitable framework by evaluating the existing mainstream federated learning frameworks. Conducting federated learning and non-federal learning based on the selected data and framework. Observing whether it can have good training results under the premise of protecting user privacy characteristics of federated learning and compare it with the performance under traditional machine learning.

Keywords

Federated learning, federated learning framework, federated learning simulation, federated learning simulator, indoor Localisation, Wifi fingerprint, indoor positioning

1. INTRODUCTION

Since the development of Global Positioning System (GPS), it has been possible to achieve high-precision, timely, and high-efficiency positioning in various outdoor fields. GPS is widely used in many different application scenarios, from daily entertainment to aviation, navigation, and military applications. However, GPS services cannot achieve the same ideal result in indoor positioning as outdoor positioning. The reason is that the precise positioning of GPS relies on strong enough satellite signals, but the GPS signal will be greatly weakened after penetrating the building. Moreover, the indoor building structure is generally complex, which in turn will cause a distance deviation due to the signal reflection path.

With the rapid development of the Internet of Things (IoT) and related applications in the last decades, the demand for high-precision indoor positioning is increasing. A variety of different technologies have been used for indoor Localisation. This research mainly focuses on Received Signal Strength Indication (RSSI) Wifi fingerprints in indoor Localisation.

Indoor Localisation based on wifi fingerprints includes two stages, training and testing. The on-site investigation is difficult in the training stage because collecting training data is time-consuming and labor-intensive. Meanwhile, because RSSI is easily affected by the indoor environment, the database often needs to be rebuilt over time, so the use of mobile devices to dynamically collect data has become a solution, avoiding on-site data collection.[11].

Due to the rapid development of computer processing capabilities and the explosive growth of available data, thus using crowdsourcing for indoor wifi fingerprint-based Localisation to collect training data for machine learning has naturally become a convenient and effective solution. However, the crowdsourcing method of collecting user data has the hidden danger of privacy leakage, since the sensitive data related to the user's location needs to be transmitted from the user device to the central server for model training in traditional machine learning.

As the awareness of personal data protection has increased, the crowdsourcing method of uploading sensitive user data has caused users' concerns. In this case, the concept of federated learning came into being[8].

Traditional centralized learning requires various terminal users to upload their data on smartphones to a central server in the cloud. The central server will use the collected data for model training, and then send the training results to each terminal. But the problem is that users are not necessarily willing to upload their privacy-related data to the cloud, especially when data involve their privacy.

Meanwhile, although traditional distributed learning can make data only perform machine learning locally on the terminal, it does not allow data to leave the terminal, ensuring data privacy, however, to improve the learning effect and efficiency, traditional distributed learning sometimes requires a certain degree of processing between different terminals data exchange, named shuffle[14], which can make the data independent and identical distribution (IID), that is more conducive to efficient algorithm design and implementation. Moreover, worker nodes of traditional distributed machine learning are all connected to high-speed wired bandwidth, each worker node has ideal computing power, and the computing power between them

28^{th} Twente Student Conference on IT Febr. 2^{nd}, 2018, Enschede, The Netherlands.

is almost the same. But in the actual smartphone applications of IoT, the network status of the worker nodes is unstable, the computing power is different and limited, and the data distribution is also every unbalanced that data distribution is not independent and identically distributed (Non-IID). Which also one of the problems that federated learning wants to solve.

This research will select a suitable open-source data set and a open-source federated learning framework for indoor positioning based on wifi fingerprints. To simulate a machine learning scenario in which the data in the federated learning is Non-IID in the clients. Observe whether the federated learning can have good performance in indoor positioning based on wifi fingerprint under the premise of protecting privacy, and compare the learning performance with non-federal learning.

The structure of this paper is as follow. In section 2, it will state the problem that this research is going to solve. In section 3, it will introduce the current research background of indoor positioning based on wifi fingerprint and privacy protection in indoor positioning. And the background of current federated learning mainstream simulation tools. In section 4, it will mention what approaches will be used at different stages for this research. In section 5, the results of federated learning and non-federal learning implementation will be described and discussed. In section 6, it will summarize the experimental results and the direction of future research.

2. PROBLEM STATEMENT

Although there has been a lot of research on deep learning of indoor Localisation based on wifi fingerprints. But there is still a lack of indoor Localisation based on wifi fingerprints using federated learning. Because the wifi fingerprint data collection is a very time-consuming and labor-consuming stage, and the database often needs to be updated due to changes in site factors. Therefore, crowdsourcing is a feasible method in the data collection stage. However, there is a hidden danger of privacy leakage in the process of users uploading location information. Therefore, federated learning has become a feasible solution. Whether the use of federated learning for indoor positioning based on wifi fingerprints can have ideal training performance and prediction results, and what is the difference compared with traditional machine learning methods.

2.1 Research Question

The problem statement brings the following research question.

Can the ideal training performance and prediction result be obtained by performing federated learning of indoor localisation based on wifi fingerprint?

This research question can be answered by the following sub-questions:

1. Can indoor localisation based on wifi fingerprints use federated learning to obtain ideal results?
2. What are the differences between indoor localisation based on wifi fingerprint in federated learning and non-federal learning?

3. RELATED WORK

Location Based Services(LBS) has played an important role in the development of GPS. However, the positioning accuracy of GPS indoors and outdoors is very different. It has a good performance in outdoor positioning applications, but its performance in indoor positioning applications is not satisfactory.

In order to solve the accuracy problem of indoor positioning, a variety of solutions based on different technology classifications have been proposed[16].

Among these technologies, the Received Signal Strength (RSS)-based Localisation technology is divided into two categories. One is to use the loss model of the RSS on the path to obtaining position information, however this method often has the problem of low Localisation accuracy due to the complexity of the indoor path. The other is based on wifi fingerprints. This method collects RSSI from multiple wireless access points as the fingerprint feature, to performs indoor Localisation[1].

In order to protect the privacy of data uploaded by users under the crowdsourcing method, several different approaches have been proposed[4][9][5][7], these methods are different methods of encrypting the transmitted sensitive data.

In addition to the above privacy protection methods, federated learning addresses users' concerns about privacy leakage from another perspective.

After the concept of federated learning emerged, there have been open source frameworks led by different companies and institutions to support simulation model training for federated learning. Currently, the mainstream open source frameworks that support federated learning simulation are Tensorflow federated(TFF), Pysyft, Fate.

These frameworks provide a variety of federated learning algorithms and traditional machine learning algorithms components. In terms of privacy protection, they also provide different privacy algorithms to ensure the data confidential during the model parameter transmission. This allow people and institutions with scientific research and industrial needs to conduct simulation model training through these frameworks to improve their models and algorithms.

The three mainstream frameworks are introduced as follow.

TFF[2] is an open source machine learning framework developed by Google, TFF has released 18 versions from its birth to the present. Users can not only simulate existing federated learning algorithms through TFF, but also implement their own algorithms.

Openmind open source pysyft deep learning framework[12], support federated learning, differential privacy, and encrypted computation. This framework also supports tensorflow and pytorch.

Fate[15] is an open source project initiated by the Webank AI department. It supports many federated learning algorithms, including vertical federated learning, horizontal federated learning, and federated transfer learning.

4. METHODS OF RESEARCH

This research focuses on Wifi, RSSI fingerprint technology in indoor Localisation technology. The federated learning framework will be used to simulate the deep learning process of indoor positioning based on Wifi fingerprints.

4.1 Define Smartphone-based indoor localisation with Federated Learning

The application will simulate a complete wifi fingerprint-based indoor positioning process from model training to

location prediction. The simulation process will be carried out under the federated learning framework. To evaluate, it will also be carried out under the non-federal learning version of the same framework with the same parameters. The data set used conforms to the characteristics of the N-IID distribution in the real situation. The data in the client that contains multiple RSSI of Wifi access points (WAP) information will be labeled as features, and the data contains the corresponding latitude and longitude will be labeled as the target, they will be used to train the model, and then until the model converges. Analysis and training results and evaluate the performance of the trained model on the test data set.

4.2 Dataset Selection

Because the selected indoor localisation technology is based on wifi fingerprint, therefore the selected data sample must contain the RSSI strength characteristics of the mobile device accessing different Wifi Access Points(WAP). And the corresponding location information, such as latitude and longitude.

The selection of the data set[13] focuses on the data with indoor Wifi fingerprint Localisation characteristics. Thus a indoor location data set was chosen from Kaggle. The data set has following features, WAP001-520, The Received Signal Strength Intensity (RSSI) of 520 different Wifi Access Points (WAP), Longitude, Latitude, Floor, UserId, PhoneId, BuildingId, and Timestamp.

In the simulation, only the RSSI of 520 WAP, Longitude, Latitude, and PhoneID will be used. The specific information of these features are as follows:

1. WAP520, The RSSI strength value ranges from -104 to 0, and the value +100, the + 100 is represented that the signal is not detected.
2. Longitude, Negative real values from -7695.9387549299299000 to -7299.786516730871000.
3. Latitude, Positive real values from 4864745.7450159714 to 4865017.3646842018.
4. PhoneID, Android device identifier (see below). Categorical integer values.

4.3 Federated Learning Framework Selection

The current mainstream federated learning frameworks are TFF, Pysyft, Fate.

Compared with traditional centralized learning and distributed learning, the application scenarios of federated learning[10] are closer to reality.

Federated learning has following characteristics.

1. In Federated learning, the worker nodes have greater autonomy while the server in traditional distributed learning has greater control over the worker nodes, for example, allowing worker nodes to exchange data to improve learning efficiency.
2. Worker node is very unstable, since most worker nodes are smartphones, laptops, and tablets, since these terminals sometimes have different conditions of network connection, some terminals may in the shutdown condition, and have different computational capabilities.
3. The communication cost of federated learning is expensive, since the network connection status is generally poor, most terminals are remotely connected to the server that it is difficult to ensure a good network connection status of the worker nodes. Under this condition, this leads to a high communication cost of sending a large number of model parameters and gradients at once.
4. The data in the worker nodes are N-IID, for example, different people have different smartphone habits in use, and the collected data may vary greatly. This makes it difficult to design some efficient algorithms.
5. The data sets of different terminals are very unbalanced, some worker nodes may collect a large amount of data while some worker nodes may only collect a very small amount of data. The result is that modeling is difficult.

Due to the characteristics of federated learning, simulation tools that can meet the various needs of federated learning are essential.

These requirements include:

1. Support different types of federated learning.
2. Support more different federated learning algorithms.
3. Support more different federated learning security protocols.
4. Support Non-independent and identically distributed data set training.
5. Can better test the performance of the algorithm.

Three mainstream three federal learning frameworks will be compared. They are TFF, Pysyft, Fate respectively.

The selected standard is based on the existing technical documents and network resources, simple and easy to use, and not cumbersome to configure. Meanwhile, it can perform simulation simulation of federated learning close to the real environment with the selected data set.

Specific comparison of the three frameworks could be found on Table 1[6][3]

Due to the TFF is the most easy for use and configuration among these three tables, and the features supported is sufficient with the selected data set for indoor Localisation. Thus TFF has been chosen.

4.4 Fingerprint Localisation With Federated Learning

Based on the selected federated learning framework and data set, the data training of indoor positioning based on wifi fingerprint is simulated, and the training scene simulates the characteristics of N-IID data distribution in the real scene. To test the difference between training performance of federated learning and non-federal learning under the condition that, with the increase of training clients and samples, and the number of training epoch, whether the training results can be close to the training results of non-federal learning under the premise of protecting privacy. Whether it can have good positioning performance.

Data will be allocated to different clients based on phoneid. The data distribution is very obvious N-IID. The amount of data and the characteristics of different features are very unbalanced among different clients. In the application, only the WAP001-WAP520, the latitude, and Longitude will be used, WAP001-WAP520 will be used for features, the Latitude and Longitude will be used as regression prediction target.

Table 1. Framework Comparison

Features	Tensorflow Federated	Fate	Pysyft
OS	Mac/Linux	Max/Linux	Mac/Linux/Win/iOS/Android
Data Partitioning	Horizontal	Horizontal/Vertical	Horizontal/Vertical
Security Protocal	DP	HE/SecertShared/RSA/DiffieHellman	HE/SecertShared
License	Apache-2.0 License	Apache-2.0 License	Apache-2.0 License
Language	Python	Python	Python
Ease of use	⋆⋆⋆⋆⋆	⋆⋆⋆	⋆⋆

Table 2. sample size for different client groups

number of clients	client ids	total amount of samples
5 clients	[23,13,16,18,3]	6783
10 clients	[23,13,16,18,3,19,6,1,14,8]	15401
16 clients	[23,13,16,18,3,19,6,1,14,8,24,17,7,11,22,10]	19937

Table 3. Client training sample distribution

Client ID	amount of sample
client 23	1091
client 13	4516
client 16	192
client 18	374
client 3	610
client 19	980
client 6	1383
client 1	507
client 14	4835
client 8	913
client 24	437
client 17	841
client 7	1596
client 11	498
client 22	724
client 10	440

The training data is distributed among 16 clients with a total of 19937 examples, while testing data is distributed among 11 clients with a total of 1111 examples. And the data sample amounts in the clients are different.

Data in each clients is represented by data matrix.

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_{520} \\ \cdots & \cdots & \cdots & \cdots \\ x_{j1} & x_{j2} & \cdots & x_{j520} \\ \cdots & \cdots & \cdots & \cdots \\ x_{k1} & x_{k2} & \cdots & x_{k520} \end{bmatrix}$$

$$\begin{bmatrix} y_1 & y_2 \\ \cdots & \cdots \\ y_{j1} & y_{j2} \\ \cdots & \cdots \\ y_{k1} & y_{k2} \end{bmatrix}$$

The distribution of samples in the total of 16 clients shows the characteristics of N-IID.

Sample size per client could be found in Table 3, clients are divided by phone id.

Federated learning training and non-federated learning will be conducted in three different situations, 5 clients, 10 clients, and 16 clients. The client id and total sample size of these three groups of clients could be found in Table 2.

The model uses three layers, the first layer flatten accepts 520 columns of RSSI vectors, the Flatten layer is used to "flatten" the multi-dimensional input into one dimension. The second hidden layer contains 100 neurons, and the activation function is tf.nn.relu, which will apply rectified linear unit function element-wise. The last layer of layer outputs two columns of vectors of longitude and latitude.

Layer(type)	Output Shape	Param
flatten (Flatten)	(None, 520)	0
dense (Dense)	(None, 100)	266752
$\text{dense}_1(Dense)$	(None, 2)	1026

5. EXPERIMENTAL RESULTS

5.1 Implementation

Colab is chosen as the runtime environment, the VM specific information as follow, two processes, both CPU: Intel(R) Xeon(R) CPU @ 2.30GHz, 2299.998 Mhz, cache size 46080 KB, 13GB RAM, 33GB HDD.

In federated learning and non-federal learning, the parameters used are as follows. The metrics select Mean Absolute Error (MAE), and the loss function is Mean Squared Error (MSE). The preprocessing of the data set uses a shuffle value of 100, the batch size is 50, the number of repeats time is 10. The optimizer for model training chose SGD. The training epoch is 10.

For power consumption comparison, the current CPU usage will be calculated at the end of each epoch for both federated learning and non-federated learning. This will be used to evaluate the power consumption information based on the wifi fingerprint indoor positioning on the smartphones.

The training of the model and the evaluation of the model using the test set will be carried out under different conditions where 5 clients participate in training, 10 clients participate in training, and 16 clients participate in training.

5.2 Fingerprint localisation with federated learning

Indoor localisation based on wifi fingerprint performed under federated learning, model training will be carried out with 5, 10 and 16 clients participating in the training respectively.

The training performance results can be observed In figure 1. As the number of clients participating in training increases, which means the increase in the number of samples. The value of MAE and RMSE in the training

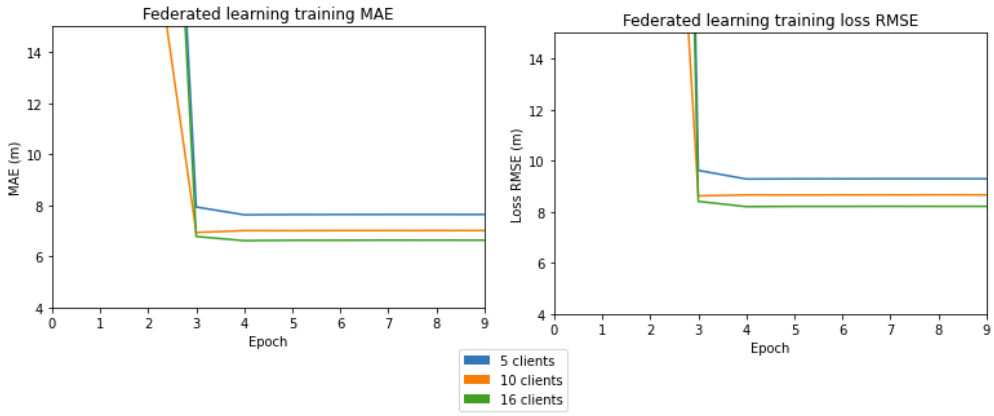

Figure 1. Federated learning metrics

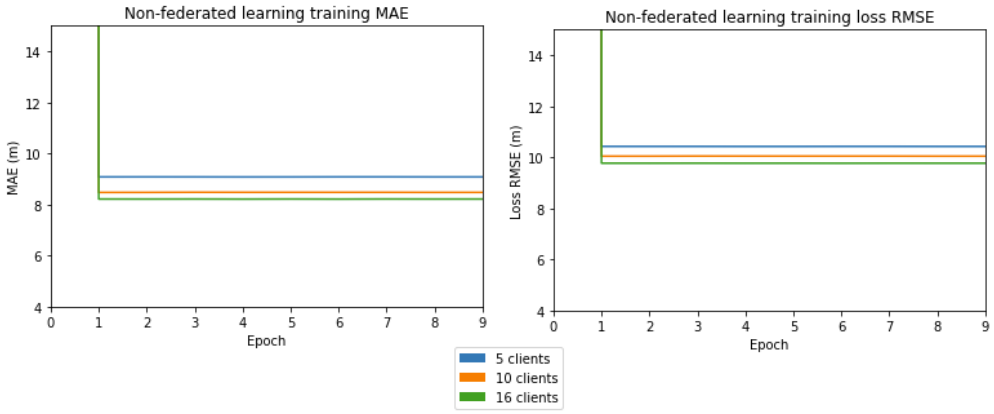

Figure 2. Non-federated learning metrics

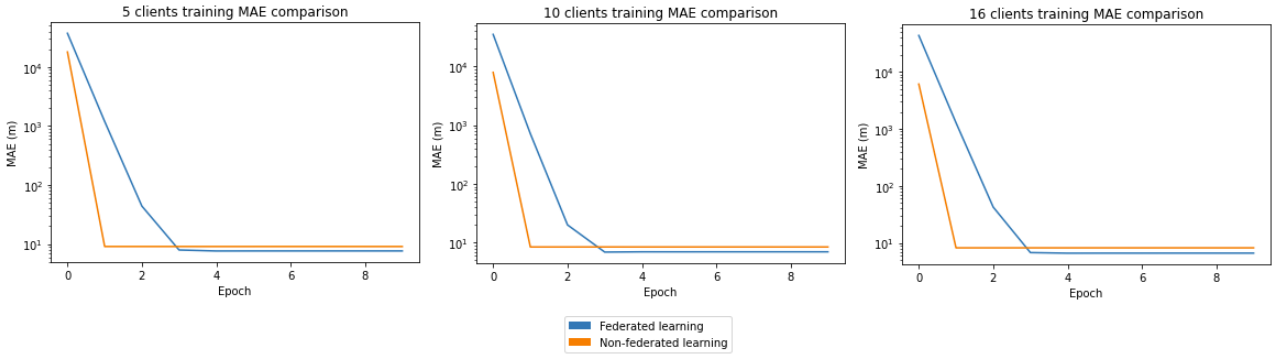

Figure 3. MAE comparison between Federated learning and Non-federated learning

Figure 4. Loss RMSE comparison between Federated learning and Non-federated learning

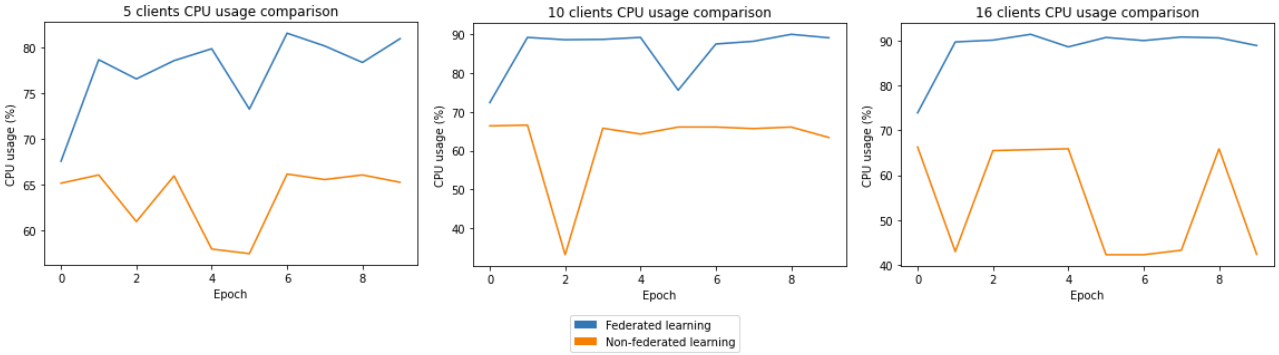

Figure 5. CPU usage comparison

results is getting smaller, and the training accuracy is getting higher. After the model converges, the value of MAE changes from about 8 to close to 6. The value of RMSE changes from about 9 to close to 8. The model tends to converge in the third round of the epoch. Furthermore, there is a slight improvement in training performance after the fourth round of the epoch.

5.3 Fingerprint localisation with non-federated learning

Indoor localisation based on wifi fingerprint performed under non-federated learning, model training will be carried out with 5, 10 and 16 clients participating in the training respectively.

The training performance results can be observed In figure 2. As the number of users participating in training increases, the MAE and RMSE in the training results are getting smaller, the training performance is getting better, and the accuracy is more accurate. After the model converges, the value of MAE changes from about 9 to close to 8. The value of RMSE changes from about 10.5 to close to 9.5. Model training tends to be stable after the first round of epoch, and there is no slight improvement in subsequent epoch training.

5.4 Federated learning and non-federated learning comparison

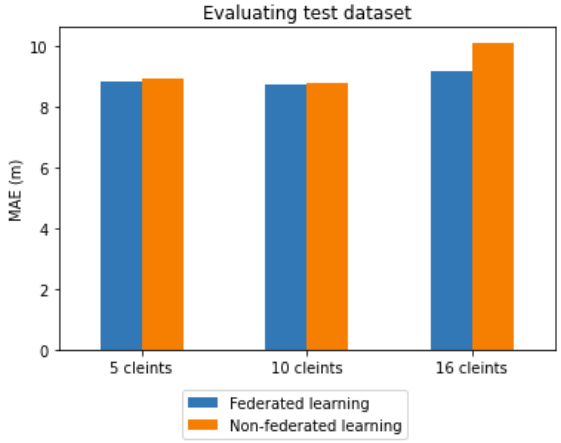

Figure 6. Evaluating comparison

According to Figure 3 and Figure 4, it can be observed that under the same number of clients participating in training, federated learning tends to converge later than non-federal learning, and the stable MAE and RMSE after convergence are lower, and the accuracy is higher.

For smartphone users, the power consumption factor will get more attention. In figure 5, the indoor positioning application based on wifi fingerprints respectively shows the different CPU usage of federated learning and non-federal learning under 3 different conditions of the number of clients participating in the training. It can be clearly observed that under the three conditions, the CPU usage of federated learning is much greater than that of non-federal learning. The fluctuating range of CPU usage for federated learning is about 70 to 90, while the fluctuating range of CPU usage for non-federal learning is about 40 to 65.

In Figure 6, Using the test set to evaluate the trained model, it can be seen that the performance of federated learning and non-federal learning is not much different. Under the condition that the same client participates in model training, federated learning has a very slight improvement over the evaluation results of non-federal learning. When the number of clients participating in the training increased from 5 to 10, the evaluation results all improved. However, when the number of clients participating in the training increases from 10 to 16, the evaluation accuracy decreases. This may be because the data distribution is N-IID, the data in the subsequent training client is quite different from the data in the training set.

6. CONCLUSION AND FUTURE WORK

The federated learning of indoor positioning based on Wifi fingerprints reflects a good learning curve and performance. The final MAE value of the training dataset is close to 6 meters. Use the test dataset to evaluate the trained model, the value of MAE is between 8 and 10 which answers research question 1 well. Compared with non-federal learning, the model training of federated learning converges later, the final learning result has a very slight improvement, and power consumption is much higher. which answers research question 2.

In this research, the features of federated learning are mainly used to protect data privacy. The data does not need to leave the client's local premises, and the model training is performed locally, only the gradient is sent to the server, and the server sends the latest model parameters to the client, and iterated until the model converges. However, there is still the risk of privacy leakage, since gradient and model parameters contain some relevant information of data, therefore there is a possibility that data can be derived from gradient and model parameters. Research on the application of privacy protection algorithms in federated learning will be very meaningful.

On the other hand, in federated learning, the communication cost is very high, so studying how to increase the number of calculations in the federated learning communication algorithm and reduce the number of communications is a very effective way to improve communication efficiency.

7. REFERENCES

[1] M. Elbes, E. Almaita, T. Alrawashdeh, T. Kanan, S. AlZu'bi, and B. Hawashin. An indoor localization approach based on deep learning for indoor location-based services. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pages 437–441, 2019.

[2] Google. Tensorflow federated. https://www.tensorflow.org/federated.

[3] C. He, S. Li, J. So, X. Zeng, M. Zhang, H. Wang, X. Wang, P. Vepakomma, A. Singh, H. Qiu, et al. Fedml: A research library and benchmark for federated machine learning. *arXiv preprint arXiv:2007.13518*, 2020.

[4] S. Holcer, J. Torres-Sospedra, M. Gould, and I. Remolar. Privacy in indoor positioning systems: A systematic review. In *2020 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–6, 2020.

[5] K. Järvinen, H. Leppäkoski, E.-S. Lohan, P. Richter, T. Schneider, O. Tkachenko, and Z. Yang. Pilot: Practical privacy-preserving indoor localization using outsourcing. In *2019 IEEE European Symposium on Security and Privacy (EuroS P)*, pages 448–463, 2019.

[6] I. Kholod, E. Yanaki, D. Fomichev, E. Shalugin, E. Novikova, E. Filippov, and M. Nordlund. Open-source federated learning frameworks for iot: A comparative review and analysis. *Sensors*, 21(1):167, 2021.

[7] J. W. Kim, D.-H. Kim, and B. Jang. Application of local differential privacy to collection of indoor positioning data. *IEEE Access*, 6:4276–4286, 2018.

[8] J. Konečnỳ, B. McMahan, and D. Ramage. Federated optimization: Distributed optimization beyond the datacenter. *arXiv preprint arXiv:1511.03575*, 2015.

[9] A. Konstantinidis, G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, and Y. Theodoridis. Privacy-preserving indoor localization on smartphones. *IEEE Transactions on Knowledge and Data Engineering*, 27(11):3042–3055, 2015.

[10] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas. Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 54:1273–1282, 2017.

[11] J. Niu, B. Wang, L. Cheng, and J. J. P. C. Rodrigues. Wicloc: An indoor localization system based on wifi fingerprints and crowdsourcing. In *2015 IEEE International Conference on Communications (ICC)*, pages 3008–3013, 2015.

[12] T. Ryffel, A. Trask, M. Dahl, B. Wagner, J. Mancuso, D. Rueckert, and J. Passerat-Palmbach. A generic framework for privacy preserving deep learning. *arXiv preprint arXiv:1811.04017*, 2018.

[13] J. Torres-Sospedra, R. Montoliu, A. Martínez-Usó, J. P. Avariento, T. J. Arnau, M. Benedito-Bordonau, and J. Huerta. Ujiindoorloc: A new multi-building and multi-floor database for wlan fingerprint-based indoor localization problems. In *2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pages 261–270, 2014.

[14] J. Verbraeken, M. Wolting, J. Katzy, J. Kloppenburg, T. Verbelen, and J. S. Rellermeyer. A survey on distributed machine learning. 53(2), Mar. 2020.

[15] Webank. Fate federated learning framework. https://fate.fedai.org.

[16] F. Zafari, A. Gkelias, and K. K. Leung. A survey of indoor localization systems and technologies. *IEEE Communications Surveys Tutorials*, 21(3):2568–2599, 2019.