FedRFID: Federated Learning for Radio Frequency Fingerprint Identification of WiFi Signals

†Jibo Shi, †Han Zhang, †Sen Wang, ‡Bin Ge, §Shiwen Mao, †Yun Lin*
†,*College of Information and Communication Engineering, Harbin Engineering University, Harbin, China
‡College of Mathematical Sciences, Harbin Engineering University, Harbin, China
§Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849-5201, USA
E-mail:{JiboShi,hldzhh1997,wangsen,gebin791025,linyun}@hrbeu.edu.cn,smao@ieee.org

***Abstract*—With the rapid development of the cognitive radio networks, the number of terminal devices has exploded. Massive devices generate a large amount of privacy-sensitive data, typically WiFi signals. This paper proposes a method for Radio frequency (RF) fingerprinting identification of WiFi signals based on federated learning, which trains a cooperative model to complete RF fingerprinting identification without transmitting privacy-sensitive data. The experimental findings on a real-world dataset validate that the strategy described in this study increases the RF fingerprinting identification accuracy in a variety of size circumstances, and ensures that data privacy will not be compromised.**

***Index Terms*—Privacy Security, RF Fingerprint Identification, Federated Learning, Cognitive Radio**

I. Introduction

With the rapid development of cognitive radio driven by the artificial intelligence (AI) technology, a large number of terminal devices have been deployed. The massive devices generate large amounts of data, most of which are transmitted over wireless networks. The wireless network's communication environment is open, which means that any user on the network can receive information sent over the air. This trait constantly exposes wireless network information transfer to prospective attacks. As more investigation are being made, it has been shown that the RF fingerprinting technology may greatly enhance wireless network security.

Deep learning has recently been applied in the field of signal detection as motivated by its exceptional performance in picture classification, signal recognition, and other domains[1–5]. The deep learning-based RF fingerprint recognition approach has attracted a lot of interest. The RF fingerprint identification method based on deep learning has also received extensive attention. Although deep learning has shown its powerful capabilities, it still faces a very critical problem: a large-scale high-quality dataset is a necessary condition for training a high-performance deep model. An important issue is that most of the data generated by devices is privacy-sensitive, and the large-scale transmission of data undoubtedly increases the risk of privacy leakage.

Faced with this challenge, Google proposed Federated Learning as a solution. Federated learning is a decentralized computing paradigm that allows neural networks to be collaboratively trained on local devices. Federated learning may offer strong anonymity and privacy guarantees to the neural network training process when used in conjunction with techniques such as differential privacy and secure aggregation. Federated learning enables each participant to jointly train data among multiple nodes without directly exchanging data, so as to achieve the goal of establishing a shared and globally effective artificial intelligence learning model.

In order to solve the privacy problem in RF signal fingerprint identification, this paper proposes a RF fingerprint identification method based on Federated learning, namely FedRFID. The rest of this paper is organized as follows. In Section II, we describe previous work in RF fingerprinting and federated learning. The simulation results are presented in Section IV, after our federated learning-based RF fingerprinting method presented in Section III. Finally, the paper concludes in Section V.

II. Related Work

Deep learning has made excellent achievements in various fields, and it is no exception in the field of RF fingerprint identification. With deep learning, can directly use the transmitted signal of RF equipment to train the neural network model for equipment identification and classification. Reference [6] developed a hybrid adaptive classification technique that adapts to changing environmental conditions by combining four modulation features from constellation. The feature weights are determined during the training phase for various channel conditions. The classification error rate is as low as 4.8% in the LOS scenario, and 11.05% when a different receiver is used for classification 18 months after training. The genuine device authentication success rate (ASR) and malicious device detection success rate (RSR) are both 90% when the SNR is 15dB. Reference [7] proposed a novel multi-channel convolutional neural network (MCCNN) for LTE terminal identification. The experimental findings demonstrate that when the SNR is 30dB, the classification accuracy for the line-of-sight (LOS) case may reaches 98.96%. Reference [8] used convolutional neural network (CNN) to classify wireless signals to identify devices. The identification accuracy on 7 Zigbbe devices is 92.29%, and the channel robustness is high. The multi-stage training deep neural network model proposed in [9] can achieve 100% identification accuracy of 12 devices.

GLOBECOM 2022 - 2022 IEEE Global Communications Conference | 978-1-6654-3540-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/GLOBECOM48099.2022.10001439

Although deep learning can achieve high identification accuracy of signal RF fingerprints, when privacy constraints lead to the lack of original training data, using deep learning becomes a challenging problem. Federated learning provides a solution where data owners can collaboratively train a machine learning model without exposing their private data. Federated learning has been widely used in many fields[10–13]. In the field of signal recognition, the technique proposed in [14] uses a distributed recognition architecture to provide federated learning-based global optimization of numerous sub-networks. Simulation results show that the method achieves an excellent recognition performance in the case of small datasets. A method of differential privacy-based federated learning for signal modulation recognition was proposed in [15], and the results showed that it achieves recognition rates comparable to centralized neural networks while satisfying privacy protection and data security requirements.Reference [16] studied the unique identification of RF received signal strength fingerprints based on feature extraction and spectral clustering methods. The proposed algorithm can perfectly detect RF fingerprints with shorter running time.

As mentioned above, in the field of RF fingerprinting, both traditional RF fingerprinting methods and deep learning-based RF fingerprinting methods have made great progress. However, both of them lack in the consideration of data privacy. This paper proposes a WiFi signal RF fingerprinting method based on federated learning, which leverages the privacy-preserving benefit of federated learning to develope an effective deep learning model while protecting the privacy of WiFi signals.

III. Proposed Methods

A. Federated Learning

The federated learning training process is shown in Fig. 1. In the federated learning framework, there is a trusted central server, which can be a third-party government agency or some other organization with integrity. Clients participating in federated learning do not exchange local user data with other clients, nor can they expose user data to the central server. Before each round of FL training starts, the server will first filter out a valid subset from all devices as participants in this round of federated training.

After the participants are selected, all devices in the participant subset will receive the global model from the server, and then the relevant client will train the model on its local node. After obtaining the intermediate parameters of the model, it sends the parameters to the central server. The central server cannot reversely deduce the data of the client through the received parameters, thereby ensuring the privacy of the data. With the received parameters, the central server conducts security aggregation, and then returns the results after security aggregation to each client. After receiving the updated model returned by the central server, each client performs training to update the model parameters again.

Federated learning aims to solve the problem of interactive training of global functions between multiple devices and a central server. Specifically, the optimization problems solved by federated learning are as follows:

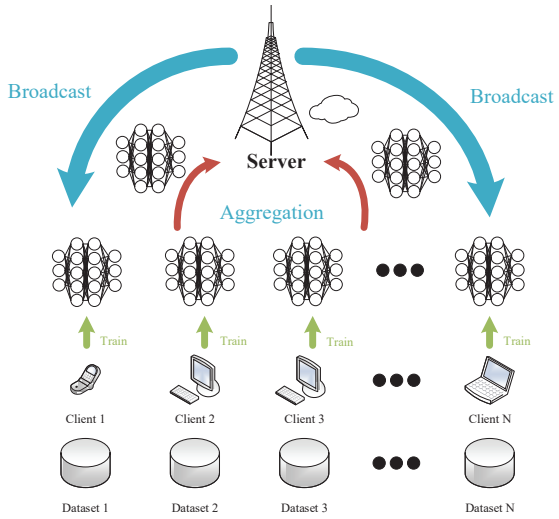


Fig. 1. The federated training process

$$\min_{\omega \in \mathcal{R}^d} \left\{ f(\omega) := \frac{1}{m} \sum_{j=1}^{m} f_j(\omega) \right\} \tag{1}$$

where m represents the number of devices and w represents the model parameters, $f_j(\cdot)$ is the local loss function of the jth device with the following expression:

$$f_j(\omega) = \frac{1}{n} \sum_{j=1}^{n} f_{j,i}(\omega, (x_i, y_i)) \tag{2}$$

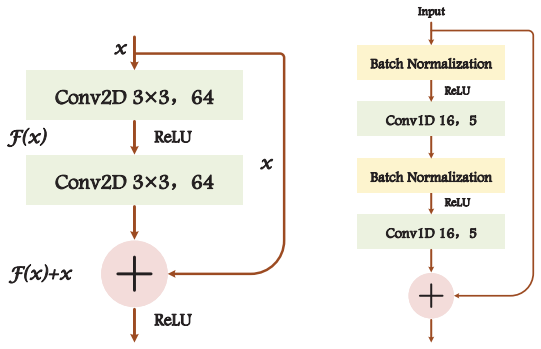
where n is the local sample size of each device, and x_i and y_i are the local training data and corresponding labels. For the problem of RF fingerprint identification of WiFi signal, the softmax cross entropy loss function is used in the training process. For the $i-th$ sample, the loss function is:

$$\begin{aligned} f_i(\omega; y_i, \hat{y}_i) &= -\sum_{c=1}^{C} y_i^c \log p_i^c \\ p_i^c &= \frac{e^{\hat{y_i}^c}}{\sum_{l=1}^{C} e^{\hat{y_i}^l}} \end{aligned} \tag{3}$$

where C is the number of prediction categories, $\hat{y}_i^c$ is the true distribution of the input data, p_i^c is the probability that the sample belongs to category c, and $\hat{y_i}^c$ represents the predicted value of category c. The predicted value $\hat{y_i}^c$ is obtained from the training sample x_i by the local neural network model, which is related to the input value of the model and the model parameters. The loss function first converts the output of the convolution network into a probability form through an exponential transformation, and then measures the difference between the two distributions through cross entropy.

The steps of federated aggregation are as follows:

- Step 1 (SEVER):
  1. Initialize the global model and model weight ω.



(a) Classical residual unit (b) 1D residual unit

Fig. 2. The residual unit structure used in this paper

2. Perform k rounds of training until the model converges. In each round of training, the server first selects a set of devices S_k. T is the total number of devices. For each device i in the device set S_k, use the weight W_k^i of the kth round to perform step 2 to update the model parameters W_{k+1}^i of the next round. Finally, the federated average algorithm $W_{k+1} = \sum_{i=1}^{T} \frac{n_i}{n} * W_{k+1}^i$is used to obtain the new global model weight W_{k+1}.

- Step 2 (CLIENT):
  1. Perform E rounds of epoch training, where E is the given number of training times for each user equipment in each round. The batch of each round is B, which is also the local minibatch size on each device. After each round of training, an update will be uploaded to the server.

Algorithm 1 summaries the training process in Federated learning.

Algorithm 1 Federated Training Process

Initialize global model W;
for each round $k = 1, 2, ...$ **do**
  $S_k \leftarrow Select\ a\ subset\ of\ T\ devices$;
  $Send\ global\ model\ W^{k-1}\ to\ each\ device\ in\ S_t$;
  for each device $i \in S_k$ paralled **do**
    Local training neural network;
    Minimize cross entropy loss:
    $\underset{\omega}{min} f_i(\omega; y_i, \hat{y_i}) = -\sum_{c=1}^{C} y_i^c \log p_i^c$;
    $W_i^k \leftarrow LocalUpdate(i, W^{k-1})$;
  end for
  Modle aggregation;
end for

B. Local Model

Convolutional neural network has been widely used in various fields. Convolutional neural network mainly uses the convolution layer and pooling layer as its core layer, which has a stronger ability in feature extraction and generalization, as well as achieving a better identification and prediction performance. In theory, as the network depth increases, the learning ability of the network should also increase, and the training results will be improved. However, the actual result is not so. The simple stacking of layers not only does not improve the model training ability, but also caused model degradation, causes the gradient to explode or disappear.

Resnet solves this problem well. Resnet not only greatly improves the number of model layers, but also improves the accuracy of the model. It mainly improves the accuracy of the model by adding an identity mapping with equal input and output behind a shallow network with high accuracy. At the same time, it can transform the model into a shallow network again. If the identity mapping function $H(x) = x$ can be completely fitted, the degradation caused by network superposition will be mitigate. If the network can be designed as $H(x) = F(x) + X$, and the identity mapping is a part of the network, the problem needs to be transformed from obtaining the identity mapping to learning the residual function $F(x) = H(x) - X$. It is easy to see from this equation that when $f(x) = 0$, the identity mapping $H(x) = x$ holds, resulting in a residual unit structure. The classical residual unit structure is shown in Fig. 2(a). The curve on the right in Fig. 2(a) is the "Shortcut Connection," which means skipping one or more layers of connections and sending information to a deeper layer of the neural network. Through the "Shortcut Connection," the residual unit can be trained as a deeper neural network. A Resnet network can be created by stacking many residual unit together.

In the task of RF fingerprinting of WiFi signals, the input to the neural network is in a one-dimensional I/Q signal format, so the residual unit needs to be modified accordingly. There is a serious over-fitting phenomenon obserbed in fingerprint identification, so the batch-normalization layer is added to the residual unit used in this paper, that is, the combination of the BN layer and the Conv1D layer (16, 5) as shown in Fig. 2(b).

The local network used in this paper is shown in Fig. 3. In order to reduce the complexity of the network and suppress the over-fitting caused by federated learning, only four residual blocks are superimposed. In each residual block, the first layer is Conv1D (16,1), which is connected with two 1D residual units. The finally output is through the Maxpool layer. After four residual blocks, the extracted features pass through two Dense layers, and the prediction probability is output by the last Softmax layer. The number of neurons in the Softmax layer is consistent with the number of device categories to be predicted.

IV. Simulation Results

A. Dataset

The 2.4 GHz WiFi model used in this article is ESP8266, which is set to the 802.11b WiFi standard and the signal bandwidth is 20MHz. ESP8266 is a high-performance UART WiFi (serial-wireless) module, which uses serial port (LVTTL) to communicate with an MCU (or other serial port devices), and has a built-in TCP/IP protocol stack, which can realize the conversion between the serial port and WiFi. The spectrum analyzer is the FSW26 spectrum analyzer from Rohde&Schwarz. After setting the access channel, the WiFi module sends the

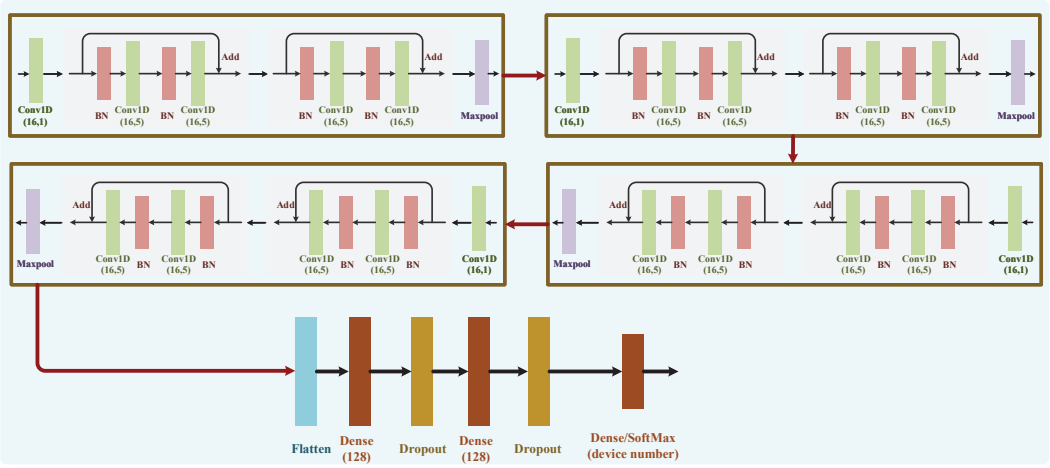


Fig. 3. The Local training network structure.

Beacon management frame cyclically, the spectrum analyzer receives wireless signals through the antenna, the PC and the spectrum analyzer are connected with a network cable, and the acquisition parameters of the spectrum analyzer are controlled by the host computer to carry out data collection and recording. This paper uses an 80M sampling rate to collect baseband I/Q signals from 100 target devices in channel 6 in a laboratory LOS environment.

B. Simulation Results

In the simulation experiment part, we conducted several groups of control experiments to test the performance of the centralized method, FedRFID (4 clients), FedRFID (5 clients) and FedRFID (10clients) in classifying 10, 25, 50 and 100 targets.

1) Classification performance of centralized Resnet for 100 targets: We first carried out the classification experiment of WiFi devices on the centralized Resnet, which is used as the baseline model in this paper. The centralized Resnet uses the network architecture introduced in Section III and the dataset mentioned above to classify 10, 25, 50, and 100 targets, respectively. Each category contains 100 samples, and each sample signal is preprocessed into 1000×2 signal length. The residual block structure is used to extract the RF fingerprint features of each target device, and then the target device is identified through the classifier layer. Fig. 4 shows the classification accuracy of the centralized Resnet on identifying 10, 25, 50, and 100 targets. As can be seen from Fig. 4, the centralized Resnet has oscillations in the early stage of training in four cases, but the accuracy tends to stabilize after 25 rounds. When identifying 10 target devices, an accuracy rate of 100% can be achieved because there are fewer targets; when identifying 25 and 50 targets, the accuracy rate are both higher than 98%, which are 98.199% and 98.774%, respectively; When identifying 100 targets, the recognition accuracy rate of 95.962% is achieved despite the large number of target devices. When classifying 25 and 50 targets, our local training network can well extract the RF fingerprint features of different WiFi devices because the number of target categories is not very large, so as to achieve similar high accuracy in classifying a medium number of target categories. When classifying 100 targets, because of the large number of target categories, our deep neural network cannot extract the best RF fingerprint features, resulting in a slight decline in classification accuracy.

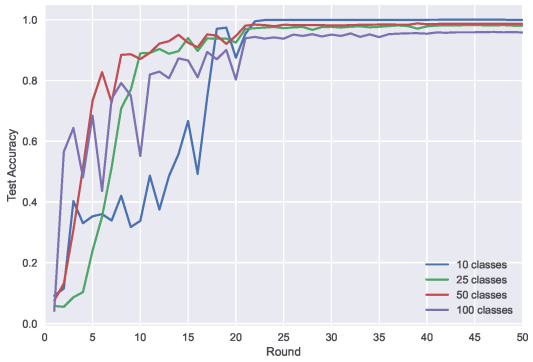


Fig. 4. Classification performance of centralized Resnet for 100 targets

2) Classification performance of FedRFID for 100 targets under different numbers of clients: In this experiment, FedRFID uses the local network architecture introduced in Section III, and uses the real-world dataset mentioned above to classify 100 targets. We consider the impact of different numbers of clients on FedRFID, which are 4, 5, and 10 clients respectively. The data category of each client is the same. In the federated scenario, each client is trained locally 3 times in each round of interactions. Similar to the centralized RESNET, the neural network of each client independently extracts the RF fingerprint features of their local WiFi device data, and uses their own classifiers to identify WiFi devices. The client then sends the local neural network parameters to the server for aggregation. We tested the classification performance of

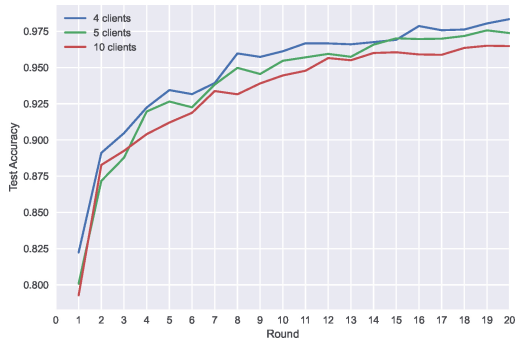


Fig. 5. Classification performance of FedRFID for 100 targets under different number of clients

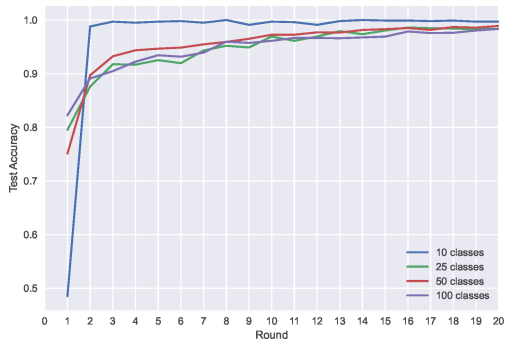


Fig. 6. Classification performance of FedRFID with 4 clients

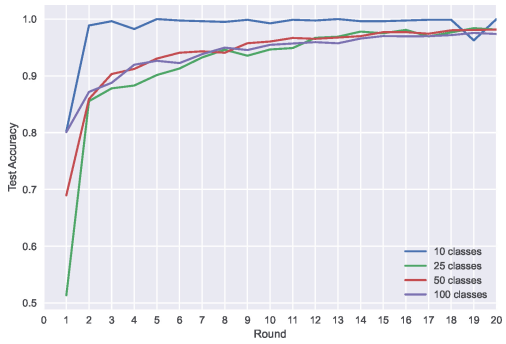


Fig. 7. Classification performance of FedRFID with 5 clients

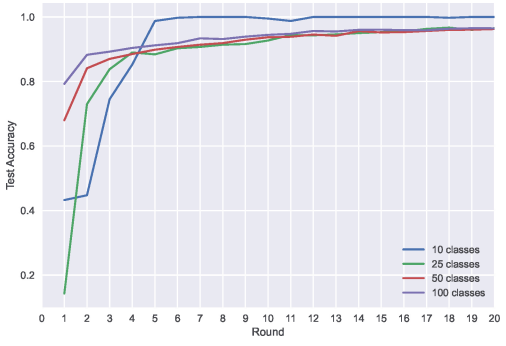


Fig. 8. Classification performance of FedRFID with 10 clients

Federated Resnet on 100 target devices under 4, 5 and 10 client conditions, as shown in Fig. 5. It can be seen from Fig. 5 that Federated Resnet achieves a high classification performance when identifying 100 WiFi devices. The classification accuracy under the condition of 4 clients is the highest, which reaches 98.339%. At the same time, the accuracy of 5 clients and 10 clients reaches 97.562% and 96.499% respectively. Fewer clients achieve higher accuracy. This may be due to the fact that in the federated learning process, the network parameter aggregation and average operation is performed. For WiFi RF fingerprint data, more clients mean more sub-weight iterations, which increases the risk of overfitting. Although the BN layer and the Dropout layer are added to the local network, 10 clients still have the problem of overfitting. Other application scenarios also have the problem of finding the optimal number of clients, but the optimal number of clients in this paper does not apply to other scenarios or other datasets, which is related to the characteristics and size of the dataset.

3) Classification performance of FedRFID for different numbers of targets: In the final simulation experiment, the local network and dataset of FedRFID are the same as the above. We consider the classification performance of different clients for different number of targets, and the data category of each client is the same. We conducted experiments to identify 10, 25, 50, and 100 target devices under 4, 5, and 10 clients, and the experimental results are shown in Fig. 6, Fig. 7, and Fig. 8, respectively. The accuracy rate of identifying 10 target devices is still the highest when the number of clients is different, but the accuracy rate of identifying 25, 50, and 100 target devices is almost the same. When using 4 clients for federated training, the classification accuracy is more than 98%. Compared with centralized Resnet, the improvement is most obvious when classifying 100 targets. This is because FedRFID carries out similar local training between clients during federated training, which is equivalent to increasing the batch size of local training in a sense, which alleviates the over fitting problem of centralized resnet, and it can more accurately extract the RF fingerprint features of WiFi devices, so as to classify WiFi devices. The specific values of the above experimental results are shown in Table I. From Table I, we find that compared with the localized neural network, FedRFID has improved classification performance when identifying 25, 50, and 100 target devices. When classifying 10 targets, both centralized Resnet and FedRFID can achieve 100% classification accuracy. The federated training of 4 clients has the best effect, which shows that the method proposed in this paper has good performance for both small-

TABLE I
COMPARISON OF CLASSIFICATION PERFORMANCE BETWEEN CENTRALIZED RESNET AND FEDRFID

Methods / Targets number	Centralized	FedRFID (4 clients)	FedRFID(5 clients)	FedRFID(10 clients)
10	100%	100%	100%	100%
25	98.199%	98.6%	98.4%	96.7%
50	98.774%	98.9%	98.15%	96.249%
100	95.962%	98.339%	97.562%	96.499%

scale scenarios and large-scale industrial IoT scenarios, and ensures the security of privacy-sensitive data.

V. CONCLUSIONS

In this paper, we proposed a method for RF fingerprinting of WiFi signals based on federated learning (FedRFID), and performed experimental verification on WiFi data actually collected in the real world scenario. The experimental results showed that FedRFID can not only effectively protect the privacy of sensitive data, but also improve the performance of RF fingerprinting. When identifying 10, 25, 50, and 100 targets, FedRFID achieves the highest accuracy of 100%, 98.6%, 98.9%, and 98.339% respectively, which outperforms the traditional centralized Resnet. FedRFID has great application potential in different scenarios such as small smart home systems and large-scale industrial IoT. In addition, in this paper, the sample category of each client were the same, but in the real IoT scenario, this maybe unrealistic. Therefore, our future work is to apply federated personalized learning to complete the identification of RF fingerprint signals in heterogeneous scenarios, and make full use of the heterogeneous devices scattered on each client to build a global model with good performance and high efficiency.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (61771154) and the Fundamental Research Funds for the Central Universities (3072021CF0801). This work is also supported by the Key Laboratory of Advanced Marine Communication and Information Technology, Ministry of Industry and Information Technology, Harbin Engineering University, Harbin, China.

REFERENCES

[1] T. J. O'Shea, T. Roy and T. C. Clancy, "*Over-the-Air Deep Learning Based Radio Signal Classification*," in IEEE Journal of Selected Topics in Signal Processing, vol. 12, no. 1, pp. 168-179, Feb. 2018.

[2] Y. Wang, M. Liu, J. Yang and G. Gui, "*Data-Driven Deep Learning for Automatic Modulation Recognition in Cognitive Radios*," in IEEE Transactions on Vehicular Technology, vol. 68, no. 4, pp. 4074-4077, Apr. 2019.

[3] Y. Lin, Y. Tu, Z. Dou, L. Chen and S. Mao, "*Contour Stella Image and Deep Learning for Signal Recognition in the Physical Layer*," in IEEE Transactions on Cognitive Communications and Networking, vol. 7, no. 1, pp. 34-46, Mar. 2021.

[4] Y. Lin, Y. Tu and Z. Dou, "*An Improved Neural Network Pruning Technology for Automatic Modulation Classification in Edge Devices*," in IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5703-5706, May. 2020

[5] Y. Tu, Y. Lin, C. Hou and S. Mao, "*Complex-Valued Networks for Automatic Modulation Classification*," in IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 10085-10089, Sept. 2020.

[6] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu and Y. Yan, "*Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme," in IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 349-360, Feb. 2019.

[7] P. Yin, L. Peng, J. Zhang, M. Liu, H. Fu and A. Hu, "*LTE Device Identification Based on RF Fingerprint with Multi-Channel Convolutional Neural Network*," in Proc.IEEE GLOBECOM'21 Virtual Conference, Dec. 2021.

[8] K. Merchant, S. Revay, G. Stantchev and B. Nousain, "*Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks*," in IEEE Journal of Selected Topics in Signal Processing, vol. 12, no. 1, pp. 160-167, Feb. 2018.

[9] K. Youssef, L. Bouchard, K. Haigh, J. Silovsky, B. Thapa and C. V. Valk, "*Machine Learning Approach to RF Transmitter Identification*," in IEEE Journal of Radio Frequency Identification, vol. 2, no. 4, pp. 197-205, Dec. 2018.

[10] T. Zhang and S. Mao, "*An introduction to the federated learning standard*," in ACM GetMobile, vol.25, no.3, pp.18-22, Sept. 2021.

[11] W. Zhang et al., "*Dynamic-Fusion-Based Federated Learning for COVID-19 Detection*," in IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15884-15891, Nov., 2021.

[12] P. Zhou, K. Wang, L. Guo, S. Gong and B. Zheng, "*A Privacy-Preserving Distributed Contextual Federated Online Learning Framework with Big Data Support in Social Recommender Systems*," in IEEE Transactions on Knowledge and Data Engineering, vol. 33, no. 3, pp. 824-838, Mar. 2021.

[13] J. Shi, B. Ge, Y. Liu, Y. Yan and S. Li, "*Data Privacy Security Guaranteed Network Intrusion Detection System Based on Federated Learning*," IEEE INFOCOM 2021 Virtual Conference, May. 2021.

[14] M. Liu, Z. Liu, W. Lu, Y. Chen, X. Gao and N. Zhao, "*Distributed Few-Shot Learning for Intelligent Recognition of Communication Jamming*," in IEEE Journal of Selected Topics in Signal Processing, vol. 16, no. 3, pp. 395-405, Apr. 2022.

[15] J. Shi, L. Qi, K. Li, Y. Lin, "*Signal Modulation Recognition Method Based on Differential Privacy Federated Learning*," in Wireless Communications and Mobile Computing, vol. 2021, Oct. 2021.

[16] Q. Li, H. Fan, W. Sun, J. Li, L. Chen and Z. Liu, "*Fingerprints in the Air: Unique Identification of Wireless Devices Using RF RSS Fingerprints*," in IEEE Sensors Journal, vol. 17, no. 11, pp. 3568-3579, 1 Jun, 2017