Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 2537546, 13 pages
https://doi.org/10.1155/2021/2537546

Research Article

Signal Modulation Recognition Method Based on Differential Privacy Federated Learning

Jibo Shi, Lin Qi, Kuixian Li, and Yun Lin

College of Information and Communication Engineering, Harbin Engineering University, Harbin, China

Correspondence should be addressed to Yun Lin; linyun@hrbeu.edu.cn

Received 19 July 2021; Revised 5 September 2021; Accepted 11 September 2021; Published 4 October 2021

Academic Editor: Jinbo Xiong

Signal modulation recognition is widely utilized in the field of spectrum detection, channel estimation, and interference recognition. With the development of artificial intelligence, substantial advances in signal recognition utilizing deep learning approaches have been achieved. However, a huge amount of data is required for deep learning. With increasing focus on privacy and security, barriers between data sources are sometimes difficult to break. This limits the data and renders them weak, so that deep learning is not sufficient. Federated learning can be a viable way of solving this challenge. In this article, we will examine the recognition of signal modulation based on federated learning with differential privacy, and the results show that the recognition rate is acceptable while data protection and security are being met.

1. Introduction

At a time when the volume of information is rapidly increasing, various modulation methods are commonly employed to fully utilize the channel's ability to carry data swiftly and effectively. The modulation method has therefore become one of the essential features to differentiate different sorts of communications. In the military sector, the identification of signal modulation offers an essential basis for information interception and for selecting the best possible interference in electronic warfare systems. It is mostly apparent in the detection of hostile radar types, in the interception of the intelligence of the adversary, and in the recognition of enemy radio sources. In civil matters, modulation recognition is mostly utilized for radio station monitoring and radio platform usage monitoring, and also information provided by nonpartner signals is utilized for monitoring communication spectrum effectively. Wireless communication settings are diverse nowadays, as are modulation schemes. An essential research subject for military and civic usage is how to accurately detect the modular type of a signal in diverse wireless communications settings. Investigations into effective modulation-type recognition algorithms are very important in both the civil and military domains. The modulation recognition is considered to be an issue with the test of modulation, as long as the density of probability function of the signal is known and classified by comparing the probability function with a set threshold. In recent decades, similar approaches, such as mixed probability ratio tests and mean probability ratio tests, have emerged. Although they are straightforward to implement and function well for clear and well-known signals, the practice of this approach is continually constrained by updated communications technologies and complicated communication settings. Data-driven Chinese learning in the field of signal modulation has recently been actively utilized, and considerable progress has been made. For example, Reference [1] uses GNU radio to create a dataset containing 11 modulation radio signals with [−20,+18] dB SNR (each dataset sample has two raw data channels (I/Q) in size 2×128), and different profounder neural networks including CNN, SVM, and deep neural networks (DNN) are being tested in this set. Reference [2] combines the generation countermeasure network (GAN) with the semisupervised learning network in order to get a more efficient modulation recognition classification. [3] applies robust RPCA to a random forest and obtains the maximum recognition rate of 90%. RPCA is applied to random forests. A deep learning approach which trains and merges two CNN

on distinct training sets has been suggested in [4]. Reference [5] is classified by CV-SVM and achieved by a rate of recognition of 90%. [6] used the RadioML2016.10a dataset to compare and study three different neural network models and their complex-valued counterparts. Their results verified the excellent performance of complex-valued networks in AMC. Reference [7] has developed a framework to convert complex-valued signal waveforms into statistically significant images, called Contour Star Images (CSI), which can convey deep statistical information from the original wireless signal waveforms and represent them in an image data format. Reference [8] proposes a new filter-level pruning technique based on activation maximization (AM) that omits the less important convolutional filter. Semisupervised AMC (TL-AMC) based on transfer learning (TL) is proposed in zero forcing-assisted multiple input multiple output (zf-mimo) systems in [9]. Compared with CNN-based AMC trained on a large number of labeled samples, tl-amc also achieves similar classification accuracy under relatively high signal-to-noise ratio. Reference [10] presents a signal classification method of industrial Internet of things based on feature fusion.

Wireless communication has permeated every part of the work and life of people, and its safety problems cannot be disregarded. Reference [11] and Reference [12] discuss the opportunities and challenges of wireless communication in the 6G era. Because the physiothermal channel of wireless communications is open, the modulation signal containing important information is fully exposed and an attacker can retrieve important signal information by utilizing a blind signal processing technology, which poses a serious threat to legal communication that makes signal data available. For this issue, Reference [13] discusses the performance of a modulation recognition attack method, measures the effectiveness of adversarial attack on signal, and empirically evaluates the reliability of CNN. In particular, privacy and safety are crucial. In parallel, the world is starting to pay more and more attention to data privacy and security through the continuous development of machine learning. In many nations, the security of the data protection has been unparalleled, making it harder to collect data and presenting machine learning with unprecedented problems. No good answers to these issues are available now. Google suggested a distributed learning-federated learning in order to tackle these challenges.

A central server stores and starts sharing global data in a federated learning architecture. The local information is secured, and the local study model is trained based on local data by each client (participant, edge devise). Clicking on a specific communication mechanism, the client transfers data like model settings to the central server (the original data of the entire client are not sent). In order to create a global model, the central server collects the data each client uploads. In the whole federated learning process, each client has the same status.

Federated learning has many advantages. First, model training is spread among customers inside the federated learning framework, and each client group updates the gradient autonomously according to their local training data to reflect the learning model. Based on the fact that the original data is not sent but only the model parameters are changed throughout the training process, federated learning provides data privacy and security, which is also an excellent factor. Secondly, federated learning with the aid of edge computing devices may be deployed with the constant growth of big data and edge computing, which allows the full use of numerous data at the edge without the need for a centralized and efficient data center. And because the model is trained on the user terminal, local data does not leave the "house," reducing communication delay and communication costs due to original data transfer.

These reasons are hot subject federated learning, and several studies about federated learning have been written by various researchers. Reference [14] outlined the notion and application in many sectors of federated learning, defined the forms of federated learning, and forecasted federated learning prospects. Federated learning is influenced by wireless channel uncertainty, and an optimisation approach is provided in [15]. Reference [16] explores the way to improve the effectiveness of federated learning communication and to reduce communications costs. In [17], a new model aggregation approach is presented based on the superpositional features of wireless multiple access channels. This demonstrates the enormous potential and development area for federated learning. However, current privacy protection technologies can provide the privacy protection of federated learning. Common technologies such as anonymity, anonymity, 1-diversity, and t-closeness cannot withstand background know-how assaults and offer security. Differential privacy is a common and efficient data security technology, which can quantify the degree of data privacy protection. The establishment of an adequate budget for privacy helps create a fair balance between data access and privacy protection. In the privacy protection of training AI model data that can offer significant protection of privacy for federal education, differential privacy is commonly employed.

In 2006, Dwork et al. first suggested differential privacy [18]. This approach of privacy security can prevent leaking of private. This technique is used primarily to tackle two privacy protection concerns. The first difficulty is how data sharing should be carefully configured for confidentiality, and the second is how to guarantee the availability of data protection. A mathematical model for the preservation of privacy is constructed on the basis of the two concerns. Benefiting from the prior knowledge of attackers, the concept of differential privacy is regarded as an efficient privacy security method and is widely utilized in data mining, machine learning, and other disciplines. Many literatures employ differing privacy techniques to secure and enhance the security of model training data.

Differential network privacy (DP-GAN) was proposed by Xie et al. [19] and others in 2018, which might safeguard GAN's privacy by introducing a gradient in the training process and could produce high-quality "fake" ages. The authors offer strict mathematical evidence that DP-GAN meets the confidential privacy criteria. During the same year, Lee and Kifer [20] presented a method for adaptive downward

gradient descent that could change the noise in line with the gradient. Yan et al. [21] suggested a multiposition data publication adaptive sampling mechanism and privacy protection technique and constructed a proportional integral differential (PID) controller-based adaptive sample mechanism. They also developed a quadtree distribution method and the corresponding approach for the allocation of the privacy budget to secure the privacy of the released data. In 2020, they also provided a forecast for centralized posting of large-scale location data on the basis of the potential profound learning paradigm [22].

The RML2016.10a dataset is used in our study to recognize signal modulation based on federal learning and examines training performance. This article is based on our previous work [23], and the contribution is summarized as follows:

(1) In order to solve the problem of data privacy security in modulation recognition, we apply federated learning to modulation recognition. Different situations are considered to verify the performance of signal modulation recognition based on federated learning

(2) In view of the lack of defense methods against data attacks on clients in a federated learning framework, this paper introduces differential privacy technology, proposes a differential privacy-driven federated learning method, which is applied to the field of signal modulation recognition, and verifies the performance of signal modulation recognition under different privacy budgets

The rest of this paper is organized as follows. In Section 2, we introduced in detail the principles of federated learning, differential privacy, and convolutional neural networks. After we describe the proposed system model and its implementation process in Section 3, the simulation results are presented in Section 4. This paper is summarized in Section 5, and finally we pointed out the shortcomings of this article and future work.

2. Preliminary

We will explain the federated learning framework, differential privacy, and locally trained models in this part.

2.1. Federated Learning Framework. As shown in Figure 1, the federated learning system consists of a central server and a large number of remote devices. The central server picks first of all a set of devices $S_t \subseteq \{1, 2, \cdots T\}$ that fulfills the demands of all devices as training devices. We suppose that there are T devices in the federated learning system. For example, these criteria include connectivity capabilities of the device, computational power, and whether or not federated learning may take advantage of local data acquired by the device. A global model is then sent to each training device from the central server. Every trainers train a local network using the raw data gathered. After the local model has been trained by each device, updated model parameters are delivered encrypted to the central server and raw data

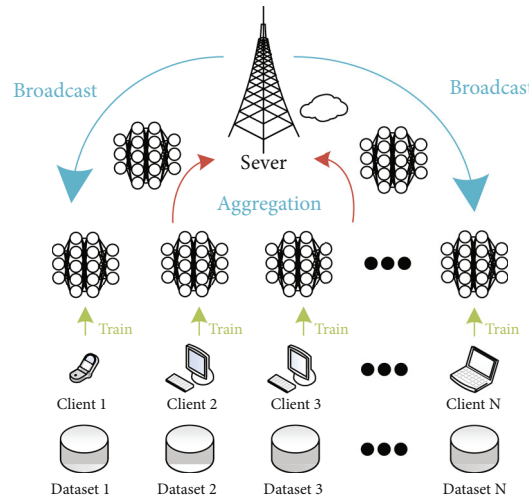

Figure 1: Federated learning system.

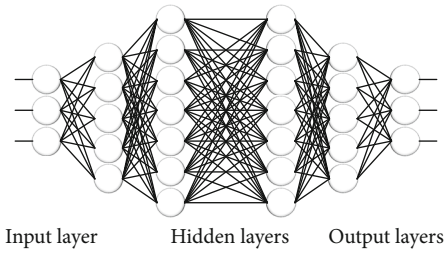

Figure 2: Typical convolutional neural network.

from the trainer does not fluctuate. We take the loss function of the local model, and the updated parameters sent by device i are

$$f_i = l_i(m; a_i, b_i), \tag{1}$$

where l_i is the input and output data loss function which refers to (a_i, b_i) the local models and m is the global model.

Once all the devices are updated on the central server, the aggregation operation is performed. In [24], which is termed secure aggregation, an aggregation approach is proposed. This aggregation procedure ensures the privacy and security of original data, and the attacker is not going to reverse the original data via the training device model update, preventing private data from leaking.

Next, the central server updates a global model by computing the average of local model updates and then sends the global updated model for the next training cycle to each device. The following may be stated in this connected learning model:

$$\min_{m \in \mathbb{R}^d} f(m) = \frac{1}{N} \sum_{i=1}^{N} f_i(m), \tag{2}$$

where N is the number of trainers.

Although the most important advantage of federated learning is the privacy protection of raw data, the size of the transmitted update parameters is significantly smaller

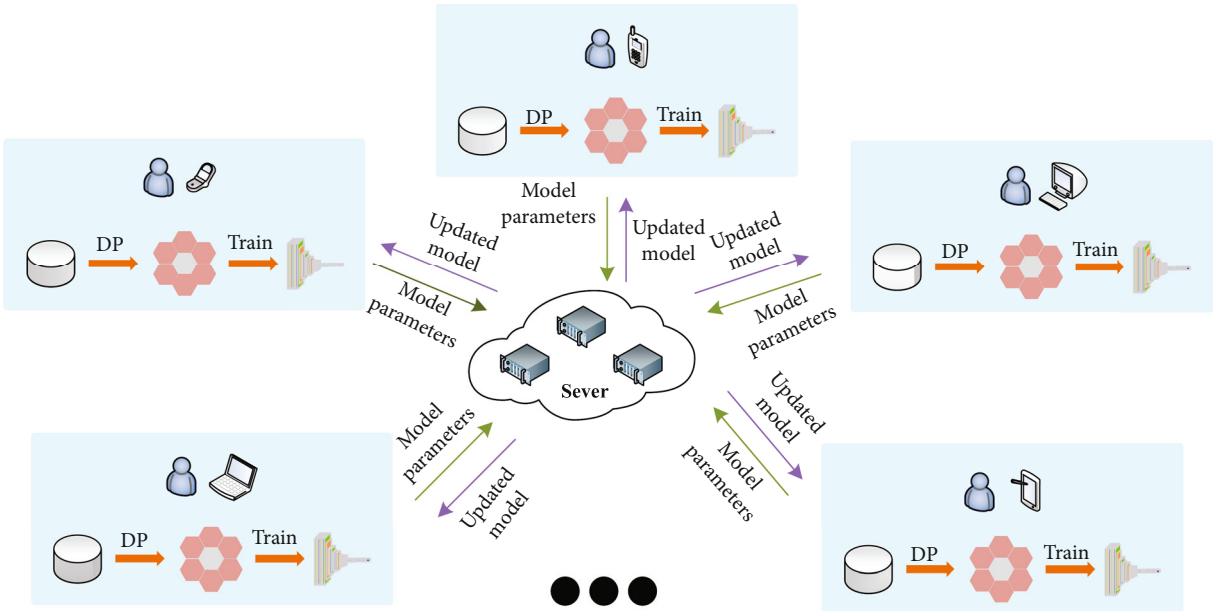

Figure 3: System model based on federated learning with differential privacy.

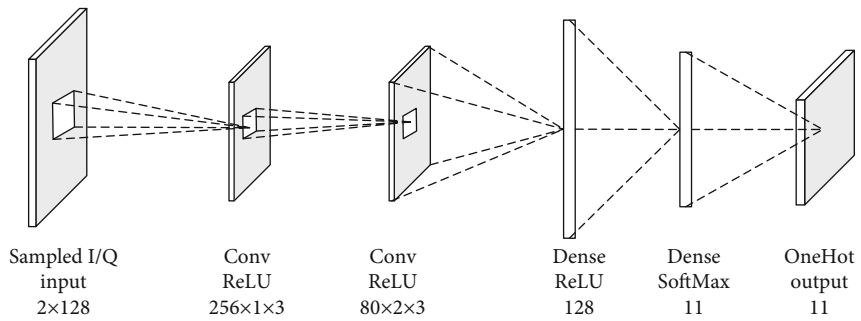

Figure 4: Local convolutional neural network.

1: initialization.
2: **for** each round $t = 1, 2, \cdots$ **do**
3: $S_t \longleftarrow$ *Select a subset* of N *devices*
4: *Broadcast global model* m^{t-1} to *each device* in S_t
5: Do differential privacy processing to get $\{D_{1'}, D_{2'}, \cdots D_{K'}\}$.
6: **for** each device $k \in S_t$ in paralled
7: $M_k^t \longleftarrow LocalUpdate(k, M^{t-1})$
8: **end for**
9: Transmit $\{P_t^1, P_t^2, \cdots, P_t^K\}$
10: Aggregation $P_{t+1}^{Global} = 1/K(\sum_{k=1}^{K} P_t^k)$
11: **end for**

Algorithm 1: Federated averaging algorithm.

than that of the original data during the process of federated learning and training, so communication costs and delays between devices and central servers are greatly reduced.

The convergence of the algorithm is an important characteristic of federated learning like virtually all algorithms which are distributed. However, federated learning's loss function does not ensure that it converges always. Reference [25] studies the convergence of the loss function in the federated learning model on a theoretical basis. We discover that the loss function may be reduced and the precise accuracy can be greater if the local model is CNN with random gradient descent (SGD). We thus pick the locale training model CNN (SGD) and present the local training model in the next section.

2.2. Differential Privacy. In 2006, Dwork et al. first proposed the concept of differential privacy (DP). Differential privacy mainly protects personal information [26]. In other words, after differential privacy processing, if a personal record is not in a dataset, the attacker can obtain almost the same information. The concept of differential privacy proposed by Dwork et al. is powerful enough to protect data privacy. Moreover, differential privacy is in line with people's understanding of the protection of personal privacy information. No matter whether a record exists in a dataset, the attacker cannot get more information about the record, even if the attacker has other external information. Differential privacy can resist background knowledge attack. After differential privacy processing, each personal information of the dataset is independent of the output of the dataset query. What can be guaranteed is that personal privacy information will not be infringed.

The implementation process of differential privacy is to add noise and introduce randomness into the data. The purpose of introducing randomness is to reduce the risk of privacy leakage to the greatest extent when querying data, while ensuring certain query accuracy. This can bring a benefit, which can add noise quantitatively and achieve a good balance between data availability and privacy protection.

If the two probability output results of a given random function K on an adjacent dataset D_1 and D_2 satisfy the following inequality, then the random function K satisfies the differential privacy:

$$\Pr[K(D_1) \in S] \leq \exp(\varepsilon) \Pr[K(D_2) \in S] + \delta. \quad (3)$$

Adjacent datasets refer to two datasets with one record difference at most; that is, one dataset is generated by adding or deleting one record from another dataset. In equation (3), $\Pr[K(D_1) \in S]$ represents the probability of the output of function K on D_1 in the range S, and the ratio of the two probability values is less than or equal to e^{ε}. ε is called privacy budget or privacy parameter, which is used to balance the degree of privacy protection and data utility. It can be seen from equation (3) that the smaller ε, the more consistent the two probability values tend to be; that is, the existence of a single record does not affect the output result; the higher the degree of privacy protection; and correspondingly, the lower the data utility. Similarly, the larger ε, the lower the degree of privacy protection and the higher the data utility. When $\varepsilon = 0$, the adjacent datasets are output with the same probability distribution, which, of course, completely loses the data availability.

2.3. Convolution Neural Network. The CNN is a classic and frequently used deep learning structure that tackles some of the issues that were difficult to overcome in prior artificial intelligence [27]. Great breakthroughs were made in image processing, video recognition, and other domains, which might contribute to the present deep learning boom exactly because of these successes. Figure 2 illustrates the CNN structure.

CNN has a convolution structure and a deep neural network. In order to ease the model problem, convolution structure can reduce the number of network parameters. Hidden layers are an important element of convolution neural networks. Normally, common CNN architectures contain input, convolution, fully connected, pooling, and output layers. CNN generally consists of many layers of convolution and pooling.

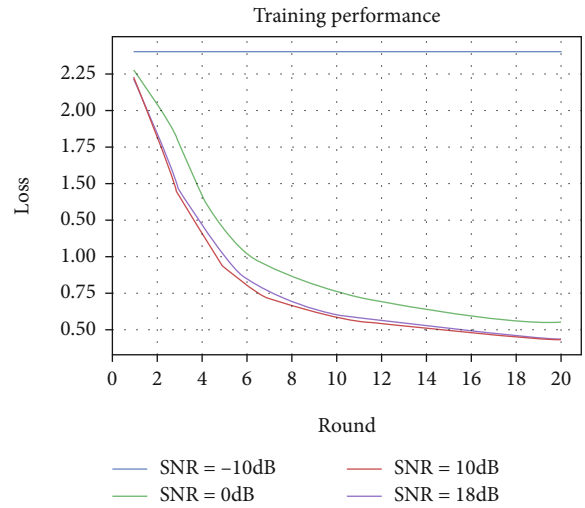

Figure 5: Training performance (different training signal SNRs).

The preceding layer's feature mapping employs the learning convolution kernel to finish the convolution process. It is highly necessary to convert the kernel to a convolution layer. Functional extractor is the heart of the convolution kernel. Its major task is to automatically extract the deep data from the input signal. With the activation function, the output of the convolution result produces the neurons of this layer and therefore generates the functional map of this layer known as the functional extraction layer. In order to extract the local area properties, the local receptive zone of the former layer is linked to the input of every neuron.

The fully connected layer is the last layer of the network. The preceding layer-by-layer transformation and map extraction features conduct redynamic categorization and other processing. Usually, the ReLU function is the activation function of each neuron in the all linked layers. In order to achieve the classification function, the final output layer might employ SoftMax activation.

Current networks can learn a great deal of input-output mapping, understanding the exact mathematical connection between input and output. There are far more unlabeled data than labeled data in real applications. Simultaneously, manual data labelling also needs considerable effort. However, a number of labeled training data are necessary, which restrict the practical use of CNN to a certain degree in order to completely train the supervised CNN and to have higher generalizing capacities.

3. System Model

Considering the privacy security problems in the field of modulation recognition, we propose a modulation

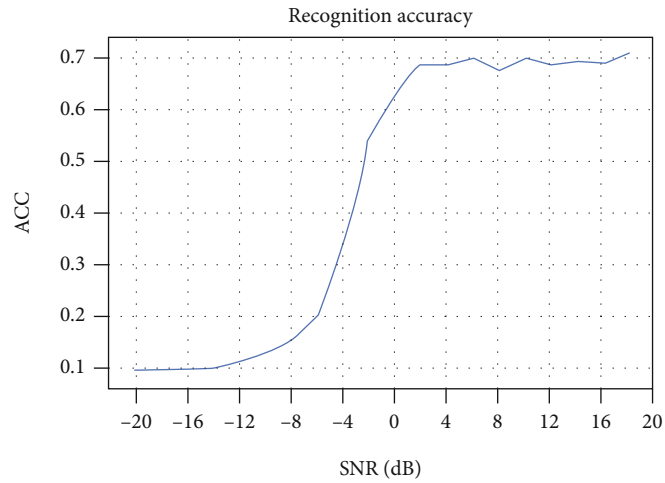

Figure 6: Recognition accuracy (different test signal SNRs).

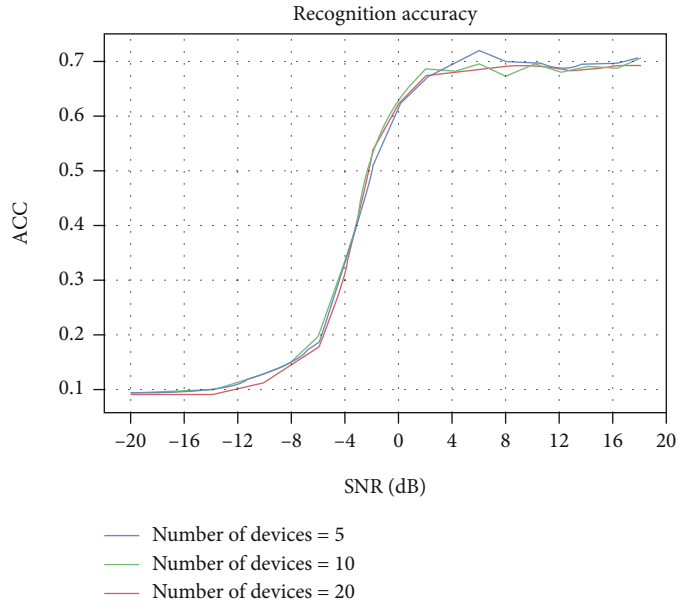

Figure 7: Recognition accuracy (different numbers of training devices).

recognition method based on federated learning under differential privacy protection.

Our differential privacy federated learning framework is shown in Figure 3. Each user has its own dataset; after differential privacy processing, each user updates the model locally. The cloud platform server collects the model parameters of users, updates and integrates the global model, and then sends the updated global model to users. Due to the equal amount of data for each user, the local model training process is basically consistent. The specific process is as follows:

(1) Suppose there are K users, and each user has its own collected dataset $\{D_1, D_2, \cdots, D_K\}$. Then, each user performs differential privacy processing on their own dataset to get $\{D_{1'}, D_{2'}, \cdots D_{K'}\}$. Finally, each user conducts the training of the deep learning model locally. The trained deep learning models are denoted as $\{M_1, M_2, \cdots, M_k\}$

(2) After each user trains locally, they can upload the model parameter $\{P_t^1, P_t^2, \cdots, P_t^K\}$ to the cloud platform server, where t represents the t round of interaction between the user and the cloud platform server and K represents the K-th user

(3) The cloud platform server aggregates and integrates the parameter updates from each user to obtain

$$P_{t+1}^{\text{Global}} = \frac{1}{K}\left(\sum_{k=1}^{K} P_t^k\right). \tag{4}$$

The significance of aggregation is to integrate the

parameters of each user, which is more helpful for model optimization.

(4) The cloud platform server transmits the aggregated and integrated global model parameters P_{t+1}^{Global} back to each user, and each user loads the updated model parameters into the deep learning model for the next round of training.

3.1. Differential Privacy Implementation. The implementation of differential privacy requires the introduction of a noise disturbance dataset. How much noise is added is related to the antinoise ability of the dataset. This antinoise ability is called global sensitivity (GS).

For any given query function, the sensitivity of function f is

$$\Delta f = \max \|f(D_1) - f(D_2)\|_1, \tag{5}$$

where $f : D \longrightarrow R^d$ represents mapping D to the d -dimensional real number domain space and D is the dataset. In equation (5), D_1 and D_2 are the adjacent datasets mentioned above or called sibling datasets, and $\|\|_1$ is the 1 -norm. To put it vividly, the global sensitivity represents the biggest difference obtained after adding or deleting a certain dataset; that is, it measures the sensitivity of the dataset to its modification. At present, the common mechanisms to realize differential privacy include the Laplace mechanism, Gaussian mechanism, and exponential mechanism. The Gaussian mechanism and Laplace mechanism are mainly aimed at numerical data, and the latter is mainly aimed at protecting labelled classified data. This paper uses the Laplace mechanism to make differential privacy dataset. The specific principles are as follows:

Laplace mechanism: for any given query function $f : D \longrightarrow R^d$, if $M(d)$ satisfies the output result of the following equation, the Laplace mechanism meets differential privacy:

$$M(D) = f(D) + \left(\text{Laplace}\left(\frac{\Delta f}{\varepsilon}\right)\right)^d, \tag{6}$$

where $\text{Laplace}(\cdot)^d$ is the d-dimensional Laplace distribution. It can be seen that the added noise level is proportional to Δf and inversely proportional to the privacy budget.

3.2. Local Deep Learning Model. The federated learning system's local training model structure is illustrated in Figure 4. The CNN network we employ is a four-layer network with two convolution layers. Other layers also employ the ReLU activation algorithm in addition to the final output layer with SoftMax. The data dimensions of the network are 2×128, as illustrated in Figure 4. The size of the kernel utilized in the first convolution layer is 1×13 with 256 kernels. The second layer of the convolution layer utilizes a bigger 2×13 kernel with 80 kernels.

After two layers of convolution, the complete connection layer, which includes 256 neurons, extracts additional global characteristics. Finally, for categorization, the final completely linked layer is employed. Since we utilize 11 modulation types in our dataset, we have 11 classification neurons in the output layer. The last neuron output is the probability in the current category of this input. The output with the highest probability is the outcome of categorization of current data after calculation of SoftMax activation function.

Algorithm 1 shows the above-mentioned federated training framework.

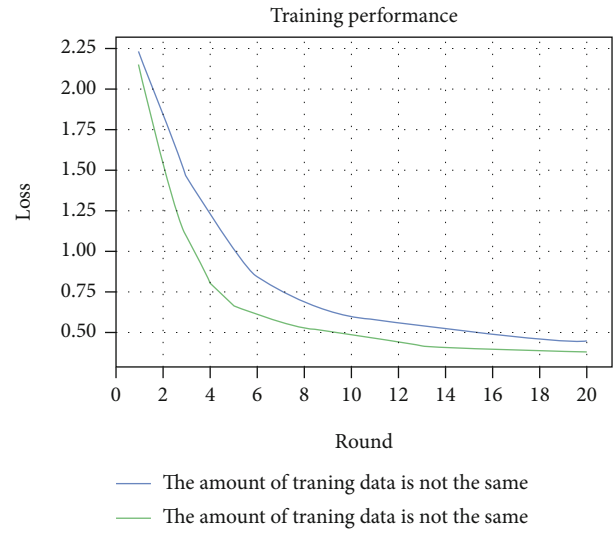

Figure 8: Training performance (different amounts of training data).

4. Simulation Results

We conducted several simulated tests in this section utilizing Google's federal learning framework (TFF) to assess the availability of signal modulation recognition based on federated learning. TensorFlow Federated (TFF) is an open-source framework for machine learning and other computations on decentralized data. In terms of hardware support, the CPU we use is Intel (R) core (TM) i7-9700 CPU @ 3.00 GHz, the memory is 32.0 GB, and the graphics card is NVIDIA geforce RTX 2080. We utilize the dataset suggested in [1] including 11 modulated [−20,+18] DB radio signals (each data sample has two raw I/Q channels data with a size 2×128). Under the federated learning framework, 20 local trainings are conducted in each round, and such a round takes about 100 s. In numerous situations, simulations have been evaluated for signal modulation identification.

4.1. Performance of Training Signals with Different SNRs. We initially evaluated when there are 10 training equipment and all modulation kinds are contained in the data taught by each device. There are 900 signals in the same number of training data for each device. After 20 training rounds, federated learning loss curves on data with the SNRs -10 dB, 0 dB, +10 dB, and +18 dB are obtained, as illustrated in Figure 5.

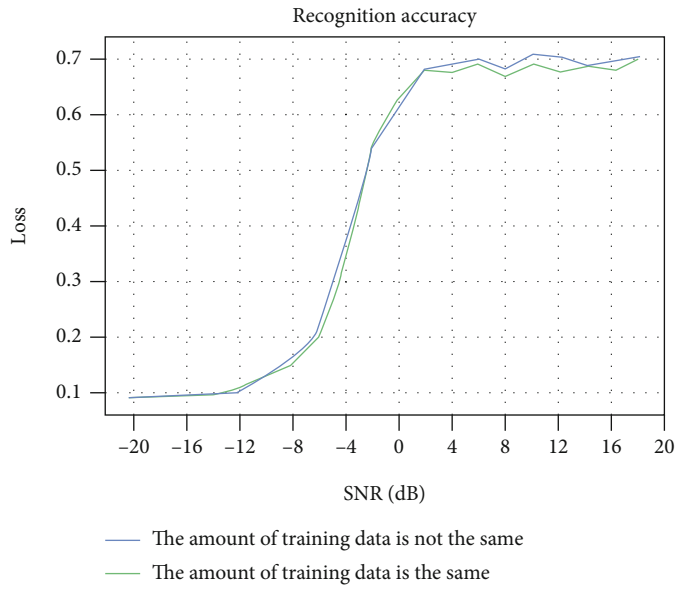

Figure 9: Recognition accuracy (different amounts of training data).

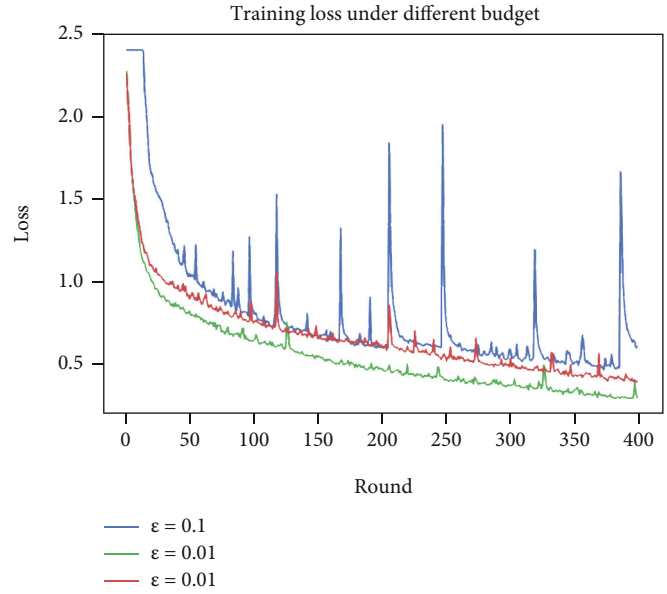

Figure 10: Training loss under different privacy budget.

We demonstrate that the loss of training is significantly greater and constant at 2.39 under the conditions of low SNR. The training loss is comparable, at at least 0.44, in high SNR circumstances. The training loss can reach at least 0.54 in the 0 dB SNR situation. This shows that in the low SNR setting, the training performance is poor. Noise and interference can be caused by disguising the signal properties in a low SNR situation. But our system training performance has increased significantly in the 0 dB SNR or greater SNR environment.

4.2. Recognition Accuracy of Test Data with Different SNRs. Consider that 10 training devices are available, and the training data of each device contains all modulation types. Each device has 900 signals and is adjusted to +18 dB for the quantity of training data. Following 20 training rounds, the accuracy of the test data accuracy of various SNRs is displayed in Figure 6.

Experimental results indicate that the accuracy of the modulation recognition is 62.96% at 0 dB SNR, and the accuracy of the identification drops quickly at the SNR of 0 dB. The accuracy of identification may reach 70.61% in the high-SNR situation. This is equivalent to the results of the proposed approach [1].

4.3. The Impact of Different Numbers of the Training Device on Federated Learning Performance. We assume next that each device's training data includes all modulation modules

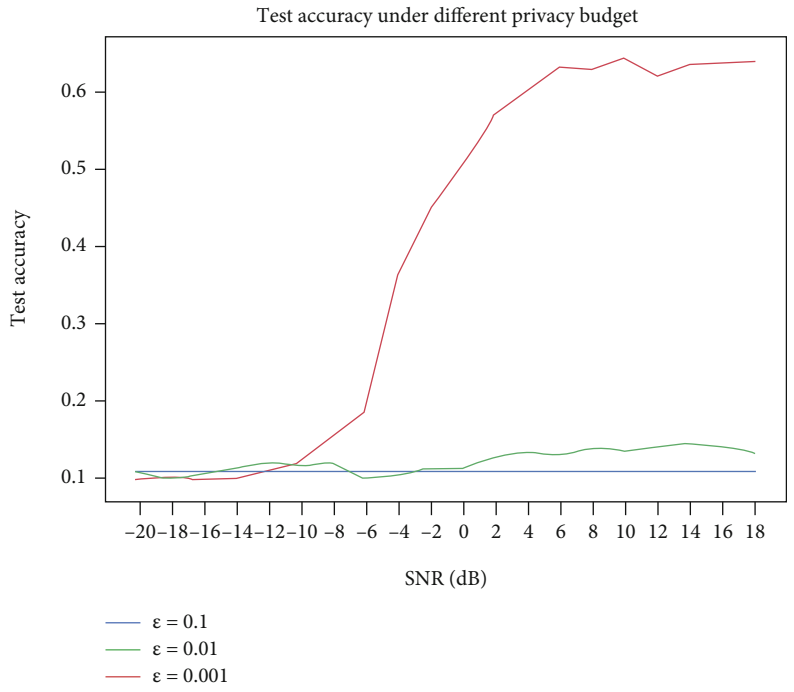

Figure 11: Test accuracy under different privacy budgets.

while each device has the same quantity of training data and the SNR is set at +18 dB. The number of trainers is 5, 10, and 20, and the accuracy of the detection curve is given in Figure 7 after 20 training rounds. The accuracy curve of recognition shows that the training performance of a federated learning system with diverse training equipment ranges from -20 dB to +12 dB of SNR which is practically equal. The federated learning system with five training devices is subject to SNR = +6 dB and has the best accuracy in accuracy which is 71.98%.

With SNR +18 dB, the 20 training devices in the federated learning system had the highest accuracy (69.19%). This demonstrates that the higher the training devices, the better the training performance; the varied number of equipment may be employed for training in various settings. For example, five equipment can be selected for training in an environment where the SNR is +6 dB, to minimize the training costs while obtaining greater precision. If greater precision is needed at higher SNRs, 20 training devices will be selected. If the criteria for precision are not severe, 5 equipment can be taught to attain the necessary precision.

4.4. The Impact of Different Amounts of Training Data on Performance. Next, we investigate a case in which each device's training data covers all forms of modulation and sets the SNR at +18 dB. However, there is no difference in the amount of data on the devices. The loss curves and the detection precision curves under different SNRs are, respectively, presented in Figures 8 and 9 after 20 rounds on 10 devices.

The results of the simulation show that if the quantity of training data from the device is identical, the formation loss is smaller, because the local model update is comparable in

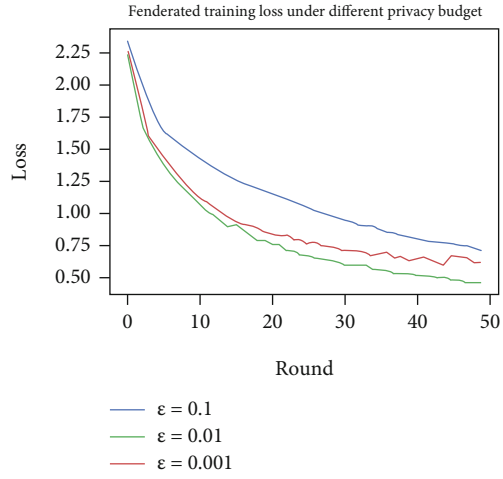

Figure 12: Federated training loss under different privacy budgets.

this scenario. The accuracy of recognition obtained by federated learning systems with diverse training data, however, is considerably higher than that of the former low SNR circumstances. The discrepancies between the training data can be caused. Some data, for example, have fewer characteristics while some have more features. Thus, it can increase the performance of federated learning to choose how much training data is.

4.5. Performance Comparison of Differential Privacy Centralized CNN and Differential Privacy Federated CNN

4.5.1. Performance of Differential Privacy Centralized CNN. According to the global sensitivity definition mentioned above, the global sensitivity of the original dataset used in

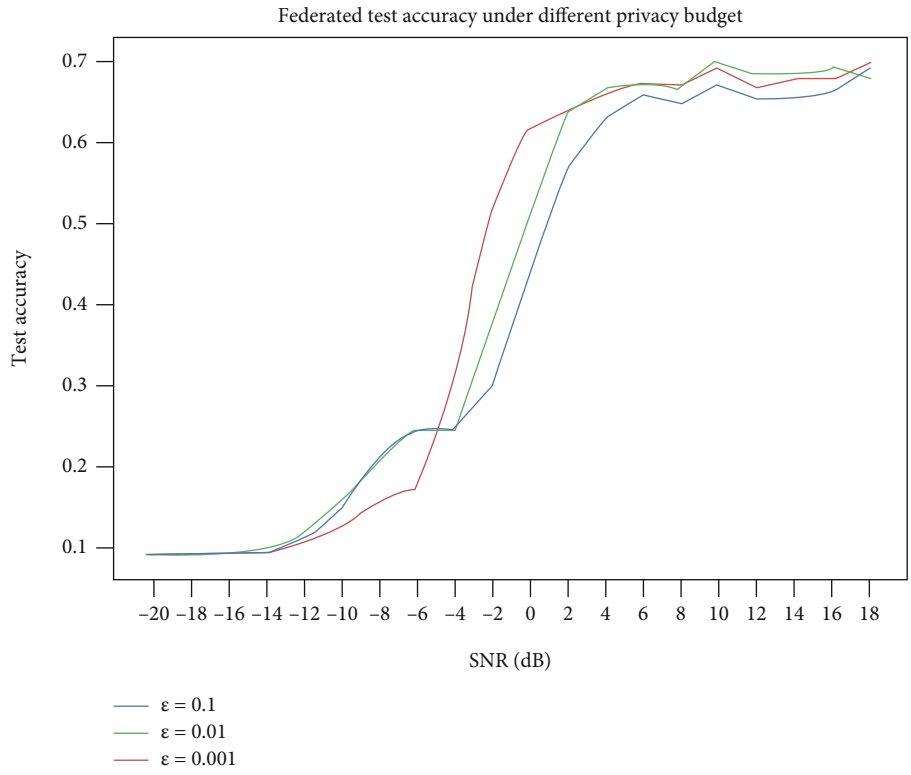

Figure 13: Federated test accuracy under different privacy budgets.

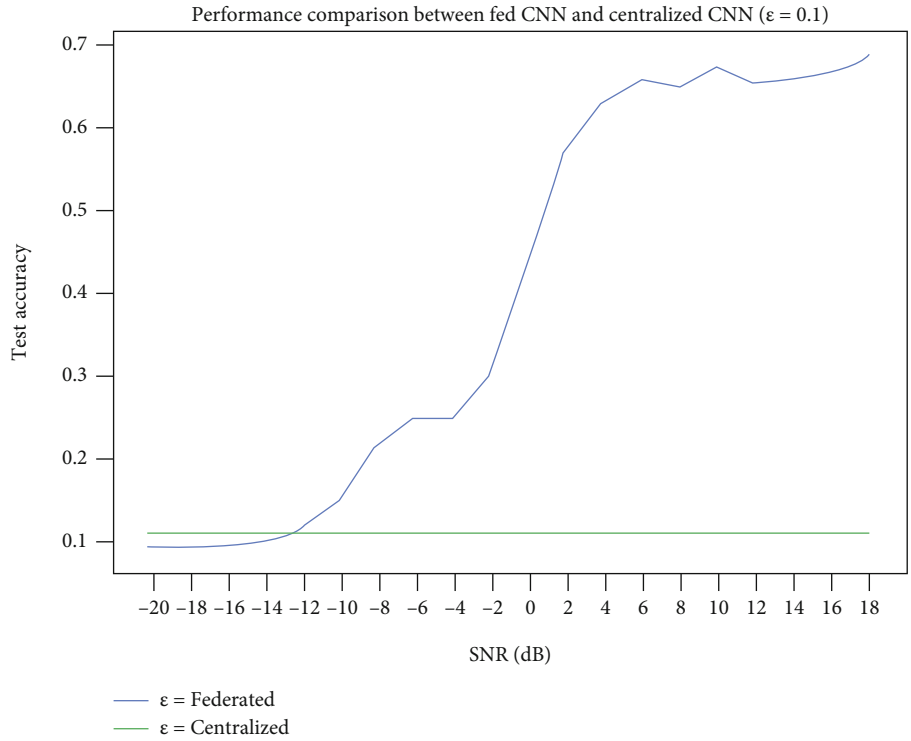

Figure 14: Performance comparison between federated CNN and centralized CNN ($\varepsilon = 0.1$).

this article is 0.417. For the convenience of calculation, we take the global sensitivity as 0.5. When ε is 0.1, 0.01, and 0.001, the differential privacy budgets are 5, 50, and 500, respectively. We first conducted experiments on the differential privacy dataset on a centralized CNN. The training loss curve and test accuracy curve under different privacy

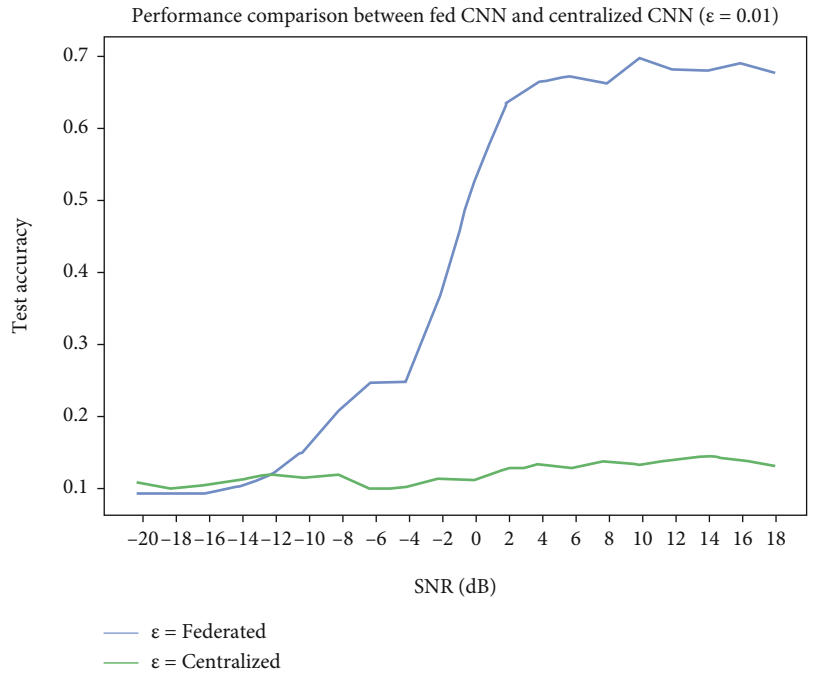

Figure 15: Performance comparison between federated CNN and centralized CNN ($\varepsilon = 0.01$).

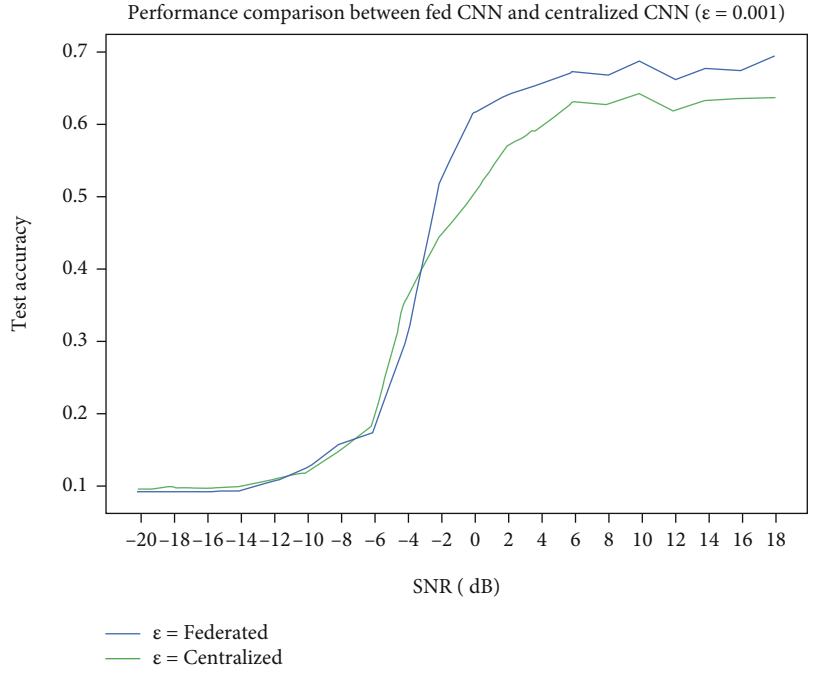

Figure 16: Performance comparison between federated CNN and centralized CNN ($\varepsilon = 0.001$).

budgets after 400-round training are shown in Figures 10 and 11, respectively.

It can be seen from the experimental results that as the privacy budget increases, the performance of the centralized CNN improves, but when the privacy budget is 5 and 50, the performance of the centralized CNN is very poor; that is, the utility of the dataset is very low. When the privacy budget is 500, the performance of the centralized CNN is acceptable, with the highest recognition accuracy rate of 63.9%.

4.5.2. Performance of Differential Privacy Federated CNN. Next, we conducted a differential privacy dataset experiment on federated CNN. The same as above, when epsilon is 0.1, 0.01, and 0.001, the differential privacy budget is 5, 50, and

500, respectively. Based on the above experimental results, we fixed the number of devices in the federated learning framework to 5, and each device dataset has the same size. After 50 rounds of federated training, the differential privacy federated training loss curve and test accuracy curve are shown in Figures 12 and 13, respectively.

The experimental results show that when the privacy budget is 50, the performance of the differential privacy federated CNN is the best, with the highest test accuracy rate of 69.9%. The performance when the privacy budget is 5 and 500 is close to the performance when the privacy budget is 50. Among them, the performance of the two at a low signal-to-noise ratio is better than the performance of privacy budget of 50, and at a high signal-to-noise ratio, the performance of the former two is slightly worse than the performance of privacy budget of 50.It proves that the differential privacy dataset has high data utility in the federated learning framework.

4.5.3. Performance of Differential Privacy Federated CNN. Finally, we compare the performance of federated CNN and centralized CNN under different privacy budgets. When the privacy budget is 5, 50, and 500, the test accuracy curves of federated CNN and centralized CNN are shown in Figures 14–16, respectively.

From the experimental results, it can be found that the differential privacy federated learning framework proposed in this paper has better performance than centralized differential privacy learning. When the privacy budget is 5 and 50, the performance of differential privacy federated learning is significantly higher than that of centralized differential privacy learning. Compared with nondifferential privacy federated learning, differential privacy federated learning can effectively protect data privacy and security, while also achieving a comparable recognition accuracy rate, ensuring high data utility.

5. Conclusion

In this article, we examined the federated learning and the feasibility of federated learning-based signal modulation recognition. On this basis, the signal modulation recognition based on differential privacy federated learning is studied. Federated learning performance has been assessed via simulation in five situations. It obtained a recognition rate of more than 70% under the premise of safeguarding privacy and security. This demonstrates the enormous potential of federated learning for signal processing. Federated learning is being implemented in more areas with more and more emphasis devoted to the security of data privacy worldwide.

Data Availability

The RML2016.10a data used to support the findings of this study may be released upon application to the DEEPSIG, who can be contacted at info@deepsig.io.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61771154) and the Fundamental Research Funds for the Central Universities (3072021CF0815). 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. A preprint has previously been published [23]. We added discussion and experimental verification on differential privacy content.

References

[1] T. J. O'Shea, J. Corgan, and T. Charles Clancy, "Convolutional radio modulation recognition networks," in *Engineering Applications of Neural Networks*, pp. 213–226, Springer, Cham, 2016.

[2] Y. Tu, Y. Lin, J. Wang, and J. Kim, "Semi-supervised learning with generative adversarial networks on digital signal modulation classification," *CMC-Computers Materials & Continua*, vol. 55, no. 2, pp. 243–254, 2019.

[3] Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. Zhou, "The individual identification method of wireless device based on dimensionality reduction and machine learning," *The Journal of Supercomputing*, vol. 75, no. 6, pp. 3010–3027, 2019.

[4] Y. Wang, M. Liu, J. Yang, and G. Gui, "Data-driven deep learning for automatic modulation recognition in cognitive radios," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 4074–4077, 2019.

[5] Z. Zhang, X. Guo, and Y. Lin, "Trust management method of D2D communication based on RF fingerprint identification," *IEEE Access*, vol. 6, pp. 66082–66087, 2018.

[6] Y. Tu, Y. Lin, C. Hou, and S. Mao, "Complex-valued networks for automatic modulation classification," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 10085–10089, 2020.

[7] Y. Lin, Y. Tu, Z. Dou, L. Chen, and S. Mao, "Contour Stella image and deep learning for signal recognition in the physical layer," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 1, pp. 34–46, 2021.

[8] Y. Lin, Y. Tu, and Z. Dou, "An improved neural network pruning technology for automatic modulation classification in edge devices," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5703–5706, 2020.

[9] Y. Wang, G. Gui, H. Gacanin, T. Ohtsuki, H. Sari, and F. Adachi, "Transfer learning for semi-supervised automatic modulation classification in ZF-MIMO systems," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 10, no. 2, pp. 231–239, 2020.

[10] M. Liu, K. Yang, N. Zhao, Y. Chen, H. Song, and F. Gong, "Intelligent signal classification in industrial distributed wireless sensor networks based industrial Internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4946–4956, 2021.

[11] M. Wang, Y. Lin, Q. Tian, and G. Si, "Transfer learning promotes 6G wireless communications: recent advances and future challenges," *IEEE Transactions on Reliability*, vol. 70, no. 2, pp. 790–807, 2021.

[12] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 126–132, 2020.

[13] Y. Lin, H. Zhao, X. Ma, Y. Tu, and M. Wang, "Adversarial attacks in modulation recognition with convolutional neural networks," *IEEE Transactions on Reliability*, vol. 70, no. 1, pp. 389–401, 2021.

[14] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

[15] N. H. Tran, W. Bao, A. Zomaya, M. N. H. Nguyen, and C. S. Hong, "Federated learning over wireless networks: optimization model design and analysis," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 1387–1395, Paris, France, 2019.

[16] J. Konečný, H. McMahan, F. Yu, P. Richtárik, A. Suresh, and D. Bacon, "Federated learning: strategies for improving communication efficiency," https://arxiv.org/abs/1610.05492.

[17] K. Yang, T. Jiang, Y. Shi, and Z. Ding, "Federated learning based on over-the-air computation," in *ICC 2019-2019 IEEE international conference on communications (ICC)*, pp. 1–6, Shanghai, China, 2019.

[18] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of cryptography*, Springer, Berlin, Heidelberg, 2006.

[19] L. Xie, K. Lin, S. Wang, F. Wang, and J. Zhou, "Differentially private generative adversarial network," 2018, https://arxiv.org/abs/1802.06739.

[20] J. Lee and D. Kifer, "Concentrated differentially private gradient descent with adaptive periteration privacy budget," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery& Data Mining*, pp. 1656–1665, London, United Kingdom, 2018.

[21] Y. Yan, L. Zhang, Q. Z. Sheng, B. Wang, X. Gao, and Y. Cong, "Dynamic release of big location data based on adaptive sampling and differential privacy," *IEEE Access*, vol. 7, pp. 164962–164974, 2019.

[22] Y. Yan, B. Wang, Q. Z. Sheng, A. Mahmood, T. Feng, and P. Xie, "Modelling the publishing process of big location data using deep learning prediction methods," *Electronics*, vol. 9, no. 3, p. 420, 2020.

[23] J. Shi, H. Zhao, M. Wang, and Q. Tian, "Signal recognition based on federated learning," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1105–1110, Toronto, ON, Canada, 2020.

[24] K. Bonawitz, V. Ivanov, B. Kreuter et al., "Practical secure aggregation for federated learning on user-held data," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1175–1191, Dallas Texas, USA, 2017.

[25] S. Wang, T. Tuor, T. Salonidis et al., "Adaptive federated learning in resource constrained edge computing systems," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205–1221, 2019.

[26] G. Gong, C. Lessoy, C. Lu, and K. Lv, "Differential privacy spatial decomposition via flattening Kd-tree," *International Journal of Performability Engineering*, vol. 16, no. 7, pp. 1058–1066, 2020.

[27] D. Bhavana, K. Kishore Kumar, M. Bipin Chandra, P. V. S. K. Bhargav, D. J. Sanjana, and G. M. Gopi, "Hand sign recognition using CNN," *International Journal of Performability Engineering*, vol. 17, no. 3, pp. 314–321, 2021.