Spectrum Sensing Based on Federated Learning with Value Evaluation Mechanism

Zheng Liu[1(✉)], Junsheng Mu[1], Fangpei Zhang[2], Xiaojun Jing[1], and Bohan Li[3]

[1] Beijing University of Posts and Telecommunications, Beijing, China
{l_z,mujs,jxiaojun}@bupt.edu.cn
[2] Information Science Academy of China Electronics Technology Group Corporation, Beijing, China
[3] University of Southampton, Southampton, UK
Bohan.Li@soton.ac.uk

Abstract. In the Internet of things (IoT), the extensive use of IoT devices makes the problem of spectrum sharing among devices increasingly prominent. Spectrum sensing is very significant to promote spectrum efficiency in IoT. However, due to network security and industry privacy issues, it is difficult to obtain large-scale data sets needed for spectrum sensing. Therefore, federated learning (FL) is an effective technique to solve the problems that may be encountered in the establishment of data sets and the problem of data leakage. In this paper, FL is utilized to study the problem of spectrum sensing, and a value evaluation mechanism of IoT devices is proposed to improve the performance of FL and resist poisoning attacks. Simulation shows that the proposed value evaluation mechanism can make the global model of FL converge more quickly and stably, and at the same time it is almost unaffected by malicious nodes when poisoning attacks occur.

Keywords: Spectrum sensing · Federated learning · Value evaluation mechanism · Poisoning attack

1 Introduction

With the popularity of 5G technology, the IoT paradigm and a variety of emerging applications (such as smart home, industrial IoT, etc.) are developing rapidly. During this period, the number of connections between smart devices and terminals increased explosively. In any case, the rapid growth in the number of connections in the IoT is bound to take up all the 5G spectrum. Therefore, both now and in the future, it is an important challenge for the network to improve spectrum efficiency. In this regard, cognitive radio is regarded as a potential solution [1–3]. Cognitive radio technology can monitor the spectrum utilization in real-time and dynamically adjust the devices accessing the spectrum [4, 5].

Before spectrum allocation, it is necessary to determine whether the target spectrum is available or not. Recently, machine learning has been used in spectrum sensing [6]. Sarikhani et al. [7] have proposed Deep Reinforcement Learning based cooperative

S. Sun et al. (Eds.): ICSINC 2021, LNEE 895, pp. 80–87, 2022.
https://doi.org/10.1007/978-981-19-4775-9_10

spectrum sensing algorithm. Zheng et al. [8] have proposed a sensing method based on deep learning classification.

However, in these methods combined with machine learning, it is troublesome to build a centralized dataset containing a large number of samples. At present, some people have proposed methods to expand the data set [9, 10]. However, if the data sets in the IoT devices are required to be transmitted to the cloud to build a large data set, which is then used to train machine learning models, it may lead to serious network security or user privacy problems [11]. FL [12] solved this problem. In FL, IoT devices train the model independently, and then the central node aggregates the local model to get the global model. Google proposed a FederatedAveraging algorithm [13], which averages the neural network parameters of each edge device to improve the global model. However, the average aggregation method can not resist poisoning attacks. Therefore, this paper proposes a value evaluation mechanism, which can accurately evaluate the effectiveness of IoT devices and resist poisoning attacks.

This paper is organized as follows. Section 2 introduces the framework of FL and the system model. In Sect. 3, the workflow of the model and the value evaluation mechanism of IoT devices are introduced. The simulation and analysis are conducted in Sect. 4. Finally, conclusions are drawn in Sect. 5.

2 System Work

In this paper, the OFDM signal is used as the signal of the primary user (PU). Different Internet of things devices will correspond to different signal acquisition devices, so they will produce their own local data sets that are different from other devices. The device D_i regards the spectrum sensing problem as a binary classification problem and uses local data sets to train the local model. The system model is shown in Fig. 1.

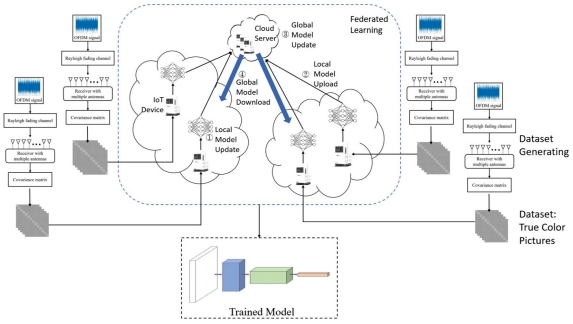

Fig. 1. System model

The essence of FL a distributed machine learning. FL mainly includes IoT devices and cloud servers. IoT devices jointly train the model under the coordination of the cloud server (CS). Each of these IoT devices has a copy of the global model, which is called the local model. IoT devices use their local data to update the local model, and the cloud server aggregates all the local models to get a global model ω, which is similar to the

result of centralized machine learning after many iterations. In this way, problems such as data leakage can be effectively avoided.

However, if there is a device D_j that maliciously uses the wrong dataset to update the model, the effectiveness of the global model may be seriously affected.

In FL, the collection of devices can be defined as $D = \{D_1, D_2, \ldots, D_{N_D}\}$, where $D_i (i = 1, 2, \ldots, N_D)$ represents the i-th device, $N_D = |D|$ indicates the total number of devices. Each device stores its own local dataset. The local dataset of the device D_i is represented as S_i, where $|S_i| = N_i$.

The model of device D_i utilizes an M_i-element antenna system to receive signals based on N_i observation vectors, then get the dataset by the method in [14]. Then we use mathematical methods to calculate the covariance matrix and finally get true color pictures as dataset S_i [9].

3 Spectrum Sensing Based on FL

3.1 Work Flow

As shown in Fig. 2, the operation at the l-th epoch consists of the following five moves:

a. Get and store datasets. Follow the method in Sect. 2 to create a dataset S_i for device D_i;
b. Global model distribution. The CS sends the global model ω^{l-1} to each device;
c. Edge model update. The device D_i updates the edge model based on the global model ω^{l-1}. Then the parameter $\omega_i^{(m,l)}$ of the m-th iteration of the local model at the l-th epoch can be expressed as

$$\omega_i^{(m,l)} = \omega_i^{(m-1,l)} - \gamma \nabla F_i\left(\omega_i^{(m,l)}\right) \tag{1}$$

where γ represents the learning rate, $F_i\left(\omega_i^{(m,l)}\right)$ is the loss function. The final parameter is taken as the local model parameter ω_i^l of the l-th epoch.
d. Local model upload. the device D_i upload the parameter ω_i^l of the updated edge model to the CS.
e. Global model aggregation. In FL, the aggregation at the l-th epoch can be expressed as

$$\omega^l = \sum\nolimits_{i=1}^{N_D} \alpha_i \omega_i^l. \tag{2}$$

where $\alpha_i = \frac{ST_i}{ST}$ is the weight of the device D_i, ST_i indicates the score of the device D_i, ST represents the total score of all devices.

Repeat these steps until the global model converges or the model reaches the required accuracy.

3.2 Value Evaluation Mechanism of Parameters

Because of the long distance between edge devices, there are many difficulties in the correct dissemination of information. There are even some devices that tamper with an edge or global model during move e. Therefore, it is very significant to make a complete effectiveness evaluation of the parameters uploaded by the equipment. At present, many objective weighting methods are widely used to determine the weight [15, 16].

The CRITIC weight method is an objective weighting method. It is based on the contrast intensity of indicators and the conflict between the indicators to comprehensively measure the objective weight of indicators.

In this paper, we use several indicators to evaluate the score of the parameter, such as the size of the dataset, the correlation with the global model, and the accuracy of the local model. The CRITIC weight method is utilized to evaluate the weight of the indicators. The score for the edge device is generated during the global model aggregation. The score affects the weight of the parameters of the local model in FL. Due to the complexity of deep learning, it is difficult to assess the validity of parameters by simply comparing the accuracy of local models. Therefore, we determine the local training performance by calculating the correlation between the parameters of the edge model and the global model.

Suppose $\omega_i = \{\omega_{i1}, \omega_{i2}, \ldots, \omega_{iP}\}$, $(i = 1, 2, \ldots, N_D)$ are all the parameters of the local model uploaded by the device D_i, $\omega' = \left\{\omega'_1, \omega'_2, \ldots, \omega'_P\right\}$ are all parameters of the global model. We use Pearson product-moment correlation coefficient (PPMCC) to represent the degree of correlation between the edge model and the global model:

$$r_i = \frac{\sum_{j=1}^{P}\left(\omega_{ij} - \overline{\omega_i}\right)\left(\omega'_j - \overline{\omega'}\right)}{\sqrt{\sum_{j=1}^{P}\left(\omega_{ij} - \overline{\omega_i}\right)^2}\sqrt{\sum_{j=1}^{P}\left(\omega'_j - \overline{\omega'}\right)^2}} \tag{3}$$

The larger the r_i, the greater the correlation between the edge model and the global model. In addition, we can make further improvements to r_i,

$$r_j = \begin{cases} r_j \ if \ \ r_j > 0 \\ 0 \ if \ \ r_j \leq 0 \end{cases} \tag{4}$$

CRITIC Weight Method

The number of dataset in the device D_j is N_j, the accuracy of edge model ω_j is A_j, and the correlation between the local parameter ω_j and the global parameter ω' is r_j. In the following sections, we use $x_{ij}(i = 1, 2, 3, \ \ j = 1, 2, \ldots, N_T)$ to denote N_j, A_j and r_j, that is, $x_{1j} = N_j, x_{2j} = A_j, x_{3j} = r_j$.

Then the proportion of x_{ij} can be expressed as

$$P_{ij} = \frac{x_{ij}}{\sum_{j=1}^{N_T} x_{ij}} \tag{5}$$

First of all, we use the standard deviation SD_i to express the contrast intensity of the i-th indicator. First calculate the mean value $\overline{x_i} = \frac{1}{n}\sum_{j=1}^{N_T} x_{ij}$, and then the standard

deviation of the i-th indicator is obtained,

$$SD_i = \sqrt{\frac{\sum_{j=1}^{N_T} \left(x_{ij} - \overline{x_i}\right)^2}{n-1}} \tag{6}$$

Secondly, the correlation coefficient R_i is used to express the conflict of the indicators. First of all, we need to calculate the correlation degree r_{ik} between different indicators. According to PPMCC,

$$r_{ik} = \frac{\sum_{j=1}^{N_D}(x_{ij} - \overline{x_i})(x_{kj} - \overline{x_k})}{\sqrt{\sum_{j=1}^{N_D}(x_{ij} - \overline{x_i})^2}\sqrt{\sum_{j=1}^{N_D}(x_{kj} - \overline{x_k})^2}} \tag{7}$$

Then

$$R_i = \sum_{k=1}^{3}(1 - r_{ik}) \tag{8}$$

Then the amount of information C_i of the i-th indicator is calculated according to the standard deviation SD_i and the correlation coefficient R_i.

$$C_i = SD_i \times \sum_{k=1}^{3}(1 - r_{ik}) = SD_i \times R_i. \tag{9}$$

So the objective weight of the i-th indicator is

$$W_i = \frac{C_i}{\sum_1^3 C_i} \tag{10}$$

Therefore, the score of the device D_i can be expressed as

$$ST_j = \sum_{i=1}^{3} W_i \times P_{ij}. \tag{11}$$

After the above steps, we adjust the weight of each edge device in the model aggregation to prevent the bad model uploaded by malicious nodes from affecting the accuracy of the global model. This method significantly improves the accuracy, convergence and anti-interference of the global model.

4 Numerical Result

In this paper, we set up 10 nodes in FL and establish local datasets for each node under different signal-to-noise ratios (SNR). At the same time, two cases are set, one is that there is no malicious node in 10 nodes, and the other is that there are two malicious nodes in 10 nodes, which is called a poisoning attack. The dataset of the malicious node is wrong, and the distribution of the wrong dataset is opposite to that of the normal dataset. As a result, the local model of the malicious node has the opposite effect on the aggregation of FL. At the same time, we compare the performance of average aggregation, called FLavg, and weighted aggregation with value evaluation mechanism, called FLvem, under different

SNR. The probability of detection (PD) and probability of false alarm (PFA) are shown in Fig. 2.

When there are no malicious nodes, the performance of FLavg is almost the same as that of FLvem. with the increase of SNR, PD increases and PFA decreases. However, when subjected to poisoning attacks, the performance of FLvem is almost unchanged under most SNR, while the performance of FLavg degrades sharply.

At the same time, we can also see the advantages of FLvem from loss function. Figure 3 shows the loss function of FLavg and FLvem when subjected to poisoning attacks under SNR $= -2$ dB, respectively. It can be seen that the loss function of FLavg can not always decrease steadily, but will increase when it decreases to a certain extent, which shows that the malicious nodes have a serious impact on the global model, and the loss function of the global model is difficult to converge to the lowest value. However, the loss function of FLvem can maintain a steady and continuous decline, and its global model can gradually converge to the lowest value, which indicates that malicious nodes have almost no effect on the global model.

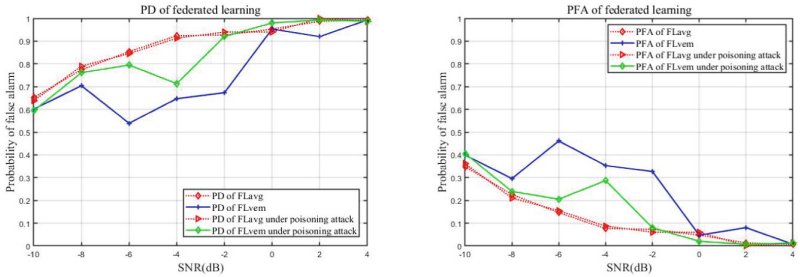

Fig. 2. The probability of detection and the probability of false alarm

In fact, not only in the case of poisoning attack, the performance of FLvem is superior, but also the loss function of FLvem converges faster when there is no poisoning attack.

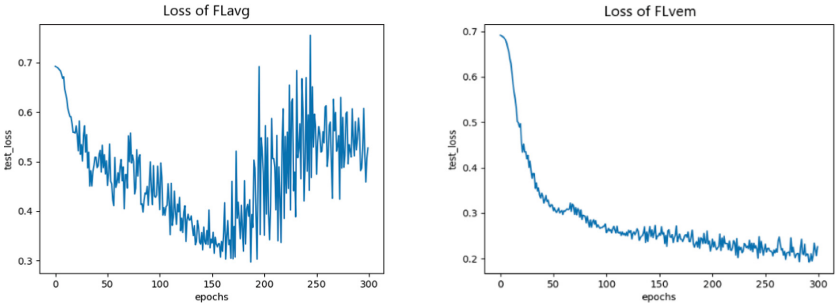

Fig. 3. The loss function of FLavg and FLvem

5 Conclusion

In summary, we design a spectrum sensing framework based on federated learning in IoT. At the same time, in federated learning, we propose a value evaluation mechanism for IoT devices, which can effectively strengthen the positive role of beneficial nodes and weaken the impact of malicious nodes. In federation learning, this mechanism not only plays a significant role in making the model converge more quickly and stably but also can effectively resist poisoning attacks.

References

1. Boccardi, F., Heath, R.W., Lozano, A., Marzetta, T.L., Popovski, P.: Five disruptive technology directions for 5G. IEEE Commun. Mag. **52**(2), 74–80 (2014). https://doi.org/10.1109/MCOM.2014.6736746
2. El Tanab, M., Hamouda, W.: Resource allocation for underlay cognitive radio networks: a survey. IEEE Commun. Surv. Tut. **19**(2), 1249–1276 (2017). https://doi.org/10.1109/COMST.2016.2631079
3. Yang, C., Li, J., Guizani, M., Anpalagan, A., Elkashlan, M.: Advanced spectrum sharing in 5G cognitive heterogeneous networks. IEEE Wirel. Commun. **23**(2), 94–101 (2016). https://doi.org/10.1109/MWC.2016.7462490
4. Mitola, J., Maguire, G.Q.: Cognitive radio: making software radios more personal. IEEE Pers. Commun. **6**(4), 13–18 (1999). https://doi.org/10.1109/98.788210
5. Haykin, S.: Cognitive radio: brain-empowered wireless communications. IEEE J. Sel. Areas Commun. **23**(2), 201–220 (2005). https://doi.org/10.1109/JSAC.2004.839380
6. Gao, N., Jin, S., Li, X., Matthaiou, M.: Aerial RIS-assisted high altitude platform communications. IEEE Wirel. Commun. Lett. **10**(10), 2096–2100 (2021). https://doi.org/10.1109/LWC.2021.3091164
7. Sarikhani, R., Keynia, F.: Cooperative spectrum sensing meets machine learning: deep reinforcement learning approach. IEEE Commun. Lett. **24**(7), 1459–1462 (2020). https://doi.org/10.1109/LCOMM.2020.2984430
8. Zheng, S., Chen, S., Qi, P., Zhou, H., Yang, X.: Spectrum sensing based on deep learning classification for cognitive radios. China Commun. **17**(2), 138–148 (2020). https://doi.org/10.23919/JCC.2020.02.012
9. Davaslioglu, K., Sagduyu, Y.E.: Generative adversarial learning for spectrum sensing. In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6 (2018).https://doi.org/10.1109/ICC.2018.8422223
10. Liu, Z., Jing, X., Zhang, R., Mu, J.: Spectrum sensing based on deep convolutional generative adversarial networks. Int. Wirel. Commun. Mob. Comput. (IWCMC) **2021**, 796–801 (2021). https://doi.org/10.1109/IWCMC51323.2021.9498871
11. Zhao, J., Chen, Y., Zhang, W.: Differential privacy preservation in deep learning: challenges, opportunities and solutions. IEEE Access **7**, 48901–48911 (2019). https://doi.org/10.1109/ACCESS.2019.2909559
12. Konečný, J., McMahan, B., Ramage, D.: Federated optimization: distributed optimization beyond the datacenter. arXiv preprint arXiv:1511.03575 (2015)
13. McMahan, H.B., et al.: Communication-efficient learning of deep networks from decentralized data. arXiv preprint arXiv:1602.05629 (2016)
14. Gao, N., Li, X., Jin, S., Matthaiou, M.: 3-D deployment of UAV swarm for massive MIMO communications. IEEE J. Sel. Areas Commun. **39**(10), 3022–3034 (2021). https://doi.org/10.1109/JSAC.2021.3088668

15. Lu, C., Li, L., Wu, D.: Application of combination weighting method to weight calculation in performance evaluation of ICT. In: 2015 IEEE 15th International Conference on Advanced Learning Technologies, pp. 258–259 (2015). https://doi.org/10.1109/ICALT.2015.15
16. Lee, D., Lee, J.: Incremental receptive field weighted actor-critic. IEEE Trans. Industr. Inf. **9**(1), 62–71 (2013). https://doi.org/10.1109/TII.2012.2209660