Secure Federated Learning over Wireless Communication Networks with Model Compression

DING Yahao[1], Mohammad SHIKH-BAHAEI[1],
YANG Zhaohui[2], HUANG Chongwen[2], YUAN Weijie[3]

(1. King's College London, London WC2R 2LS, U.K.;
2. Zhejiang University, Hangzhou 310058, China;
3. Southern University of Science and Technology, Shenzhen 518055, China)

DOI: 10.12142/ZTECOM.202301006

https://kns.cnki.net/kcms/detail/34.1294.TN.20230314.1752.002.html, published online March 16, 2023

Manuscript received: 2023-02-11

Abstract: Although federated learning (FL) has become very popular recently, it is vulnerable to gradient leakage attacks. Recent studies have shown that attackers can reconstruct clients' private data from shared models or gradients. Many existing works focus on adding privacy protection mechanisms to prevent user privacy leakages, such as differential privacy (DP) and homomorphic encryption. These defenses may cause an increase in computation and communication costs or degrade the performance of FL. Besides, they do not consider the impact of wireless network resources on the FL training process. Herein, we propose weight compression, a defense method to prevent gradient leakage attacks for FL over wireless networks. The gradient compression matrix is determined by the user's location and channel conditions. We also add Gaussian noise to the compressed gradients to strengthen the defense. This joint learning of wireless resource allocation and weight compression matrix is formulated as an optimization problem with the objective of minimizing the FL loss function. To find the solution, we first analyze the convergence rate of FL and quantify the effect of the weight matrix on FL convergence. Then, we seek the optimal resource block (RB) allocation by exhaustive search or ant colony optimization (ACO) and then use the CVX toolbox to obtain the optimal weight matrix to minimize the optimization function. The simulation results show that the optimized RB can accelerate the convergence of FL.

Keywords: federated learning (FL); data leakage from gradient; resource block (RB) allocation

Citation (IEEE Format): Y. H. Ding, M. Shikh-Bahaei, Z. H. Yang, et al., "Secure federated learning over wireless communication networks with model compression," *ZTE Communications*, vol. 21, no. 1, pp. 46 – 54, Mar. 2022. doi: 10.12142/ZTECOM.202301006.

1 Introduction

Federated learning (FL) [1], an emerging distributed learning algorithm, has received much attention in recent years due to its data protection property[2]. This algorithm has been extensively employed in applications where preserving user privacy is of utmost importance, such as in the case of hospital data[3]. FL allows clients to utilize private sensitive data to collaboratively train a machine learning model locally without explicitly sharing individual sensitive data. In the context of wireless networks with limited bandwidth and latency requirements, the advantages of FL are even more pronounced, especially when there are a large number of users and data. This is because only models or gradients are transmitted, which not only enhances the privacy of the data but also significantly improves communication efficiency.

Although FL offers default data privacy by avoiding the exchange of raw data between participants and a server, recent studies have noted that FL faces various attacks such as membership inference attacks[4], generative adversarial network attacks[5 – 6], gradient leakage attacks[7 – 10], model inversion attacks[11], model poisoning, data poisoning and free-riding attack during the training process[12]. These attacks will expose users' private data, such as the location of confidential sites, and the condition of patients, or corrupt the global model and affect the performance of the model. One of the most advanced privacy leakage techniques is gradient leakage, where an honest-but-curious server could illegally reconstruct the user's privacy data by performing gradient leakage attacks on the client's uploaded model weights or gradients. Furthermore, even if the federated server is reliable, gradient leakage can occur by eavesdroppers near the clients or server in the wireless network. Therefore, tackling the gradient leakage issue is essential for promoting FL in practical applications, such as edge computing and UAV swarms.

The related work is as follows.

1) Gradient leakage attacks: Gradient leakage attacks are used to reconstruct training input data (e.g., images or text) and labels through shared gradients or weights. The work in Ref. [7] first discussed the recovery of image data from gradients in neural networks and demonstrated the feasibility of reconstructing data from a single neuron or linear layer net-

works. In Ref. [6], a single image was reconstructed from a 4-layer CNN comprising a significantly large fully-connected layer. ZHU et al. in Ref. [8] proposed the deep leakage from gradient (DLG) algorithm. In particular, it yields dummy gradients by randomly generating dummy data and dummy labels, then minimizing the difference between the dummy gradient and the original gradient, which in turn makes the dummy input close to the original input, and finally recovering the original data. They successfully reconstructed training data and ground-truth labels from a 4-layer CNN. Moreover, they demonstrated that it is indeed possible to recover multiple images from their averaged gradients (maximum batch size of 8). Following up Ref. [8], due to the difficulties of DLG in convergence performance and extracting ground truth labels consistently, the improved deep leakage from gradient (iDLG) algorithm was proposed in 2020[9] as a simple and effective method to recover the original data and discover ground truth labels. GEIPING et al.[13] studied the reconstruction of multiple images from their averaged gradients, where they used cosine similarity as a cost function and optimized the sign of the gradient. The simulations show that it only reconstructs single images from gradients. Furthermore, the work in Ref. [10] introduced a GradInversion method to recover training image batches by inverting averaged gradients.

2) Defense methods for privacy leakage: Recently, a number of studies have focused on defense strategies for privacy leakage in FL. These methods can be categorized into four types: homomorphic encryption[7, 14 – 15], multi-party computation[16 – 17], differential privacy (DP)[18 – 20], and gradient compression. Homorphic encryption and multi-party computation incur a significant extra computational cost, thus it is not suitable for wireless network scenarios with limited communication resources and delay requirements. For the DP method, it is to add Gaussian noise or Laplacian noise to the gradient before transmission, which can mitigate privacy leakage, but it also negatively affects the training process and model performance[21]. Gradient compression defends against data leakage by pruning gradients with small magnitudes to zero so that eavesdroppers cannot match the original gradients. The work in Ref. [8] demonstrated that it is not possible to prevent leakage when the sparsity is less than 10%, but when the compression rate is more than 20%, the recovered image is no longer recognizable, and the leakage is successfully prevented. However, excessive compression may affect the model's performance. Overall, these defense approaches achieve adequate defense either by incurring significant overhead or by compromising the accuracy of the model and they are not specifically designed to defend against data leakage on a gradient[22]. Unlike the general-purpose protection mentioned above, the studies in Refs. [22 – 24] focus on defending against gradient leakage attacks. SUN et al. in Ref. [22] observed that the class-wise data presentations of each client's data are embedded in shared local model updates, which is why privacy can be inferred from the gradient, and the proposed Soteria could effectively protect training data via perturbing data presentation in an FC layer. In PRECODE[23], variational modeling is used to disguise the original latent feature space susceptible to privacy leakage by DLG attacks. Moreover, WANG et al.[24] proposed a lightweight defense mechanism against data leakage from gradients. They used the sensitivity of gradient changes w.r.t. the input data to quantify the leakage risk and perturb gradients according to leakage risk. In addition, global correlations of gradients are applied to compensate for this perturbation. These three methods provide a significant defense against DLG attacks and have little effect on model performance. However, one essential part, wireless network resources (e.g., bandwidth and power), are not considered in these defense frameworks.

Although the aforementioned methods (Soteria, PRE CODE, and a lightweight defense mechanism) have been successful in defending against DLG attacks, all the proposed defense methods focus solely on the theoretical process of FL training and only the server or participants are considered malicious attackers. To the best of our knowledge, there is a lack of research on defending against DLG attacks for FL in wireless networks. The fact is that the convergence and performance of FL may be affected by bandwidth, noise, delay, power, etc. in dynamic wireless networks. Therefore, to fill in the blank, we propose a novel defensive mechanism, weight compression for gradients, to protect data privacy from DLG attacks in FL. Moreover, we consider external eavesdroppers, such as users around the clients or servers who are not involved in FL training. Key contributions of this work include:

• We propose a novel defensive framework, weight compression, for protecting the data privacy of FL over wireless networks by considering FL and wireless metrics and factors. This defense is implemented by compressing the local gradient by taking into account the user's location and channel quality. In addition, Gaussian artificial noise is added to the compressed gradients for further defense.

• We formulate this joint resource allocation and weight compression matrix for FL as an optimization problem with the goal of minimizing the training loss while satisfying the delay and leakage requirement. Thus, our defensive mechanism jointly considers learning and wireless network metrics.

The rest of this paper is organized as follows. The system model and problem formulation are analyzed in Section 2. The analysis of the FL convergence rate is presented in Section 3. In Section 4, the joint optimization problem is simplified and solved. Then, the simulation result and analysis are described in Section 5. Finally, conclusions are summarized in Section 6.

2 System Model and Problem Formulation

In this paper, we consider a small network consisting of one server and a set of N clients to jointly train an FL model for task inference in a wireless environment, which includes an

eavesdropper, as shown in Fig. 1.

2.1 Federated Learning Model

In the FL model, the training data as input of the FL algorithm collected by each client i is denoted as $\boldsymbol{X}_i = \left[\boldsymbol{x}_{i1}, \cdots, \boldsymbol{x}_{iK_i}\right]$, where K_i is the number of samples collected by client i and each element $\boldsymbol{x}_{ik}$ denotes the K-th sample of client i. The matrix $\boldsymbol{y}_i = \left[y_{i1}, \cdots, y_{iK_i}\right]$ is the corresponding labels of training data $\boldsymbol{X}_i$. After collecting data, each client i trains its local model using $\left(\boldsymbol{X}_i, \boldsymbol{y}_i\right)$ and the server aggregates received local models to update the global model for the next round of training. The main objective of the FL training process is to find optimal model parameters $\boldsymbol{w}^*$ that minimize the global loss function and the training process can be considered as solving an optimization problem, defined as:

$$\min_{\boldsymbol{w}_1, \cdots, \boldsymbol{w}_N} \frac{1}{K} \sum_{i=1}^{N} \sum_{k=1}^{K_i} f\left(\boldsymbol{w}_i, \boldsymbol{x}_{ik}, y_{ik}\right), \tag{1}$$

where $K = \sum_{i=1}^{N} K_i$ is the total size of the training data of all clients; $\boldsymbol{w}_i$ is a vector that represents the local model of each client i; $f\left(\boldsymbol{w}_i, \boldsymbol{x}_{ik}, y_{ik}\right)$ is the loss function of the i-th client with one data sample. $F_i\left(\boldsymbol{w}_i, \boldsymbol{x}_{i1}, y_{i1}, \cdots, \boldsymbol{x}_{iK_i}, y_{iK_i}\right)$ is the total loss function of the i-th client with the whole data sample, which is abbreviated as $F_i\left(\boldsymbol{w}_i\right)$. Moreover, the expression of $f(\cdot)$ is application-specific.

In general, Eq. (1) could be solved by performing gradient descent in each client periodically. The detailed training process consists of the following three steps:

1) Training initialization: The server first initiates a global model $\boldsymbol{w}^0$ and sets up hyperparameters of training processes, e. g., the number of epochs and learning rate. The initialized global model $\boldsymbol{w}^0$ is broadcast to clients in the first round. The clients start local model training after receiving $\boldsymbol{w}^0$.

2) Local training and updating: At each step j, after receiving the global weight $\boldsymbol{w}^j$ from the server, each client i samples a batch from their own dataset to compute the updated local gradients $\boldsymbol{g}_i^j$.

$$\boldsymbol{g}_i^j = \frac{1}{B} \sum_{k \in K_i^{j+1}} \frac{\partial f\left(\boldsymbol{w}^j, \boldsymbol{x}_{ik}, y_{ik}\right)}{\partial \boldsymbol{w}^j}, \tag{2}$$

where K_i^j is a randomly selected subset of B training data samples from user i's training dataset K_i at the j-th training round.

3) Model aggregation and download: Once the server receives all local gradients from N clients, it combines them to update the global gradients $\boldsymbol{g}_g^j$. Then, the weights $\boldsymbol{w}^{j+1}$ are updated and sent back to the clients for the next training round. The update of the global gradient vector and weights is given by[25]:

$$\boldsymbol{g}_g^j = \frac{1}{K} \sum_{i=1}^{N} K_i \boldsymbol{g}_i^j, \tag{3}$$

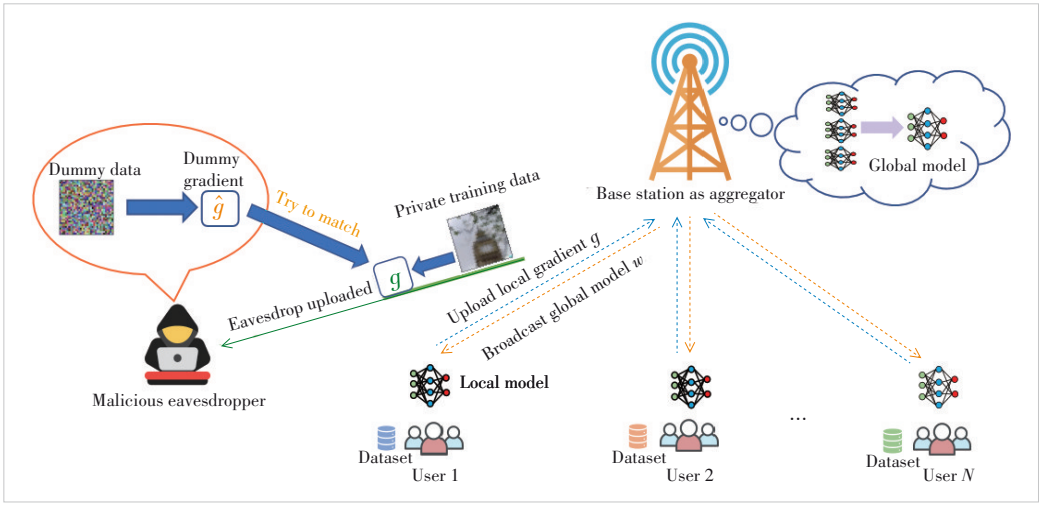
$$\boldsymbol{w}^{j+1} = \boldsymbol{w}^j - \eta \boldsymbol{g}_g^j, \tag{4}$$

where η is the learning rate. Finally, processes 2 and 3 are iterated until the global loss function converges or achieves the desired accuracy.

2.2 Threat Model

In this work, we consider the DLG attack[8] performed by the eavesdropper on the uplink and downlink to recover the original private data from the client. The DLG attack is conducted by making the gap between the generated dummy gradient and the eavesdropped local FL gradient smaller and smaller through multiple iterations, so that the corresponding dummy data become more and more similar to the original data.

We assume that the eavesdropper taps only one nearby client i at a time, eavesdropping on the last updated local gradient $(\boldsymbol{g}_i^J)$ of the uplink transmission and the weight $(\boldsymbol{w}^J)$ from the downlink, where J is the number of iterations for FL to reach convergence. After that, the eavesdropper randomly generates a set of dummy inputs $\hat{\boldsymbol{x}} = \left[\hat{\boldsymbol{x}}_1, \cdots, \hat{\boldsymbol{x}}_B\right]$ and $\hat{\boldsymbol{y}} = \left[\hat{y}_1, \cdots, \hat{x}_B\right]$, which are initialized as random noise and optimized toward the ground truth data $\boldsymbol{x}^*$. These dummy data and labels are updated by the difference between the dummy gradient and the original gradi-



▲Figure 1. Architecture of FL algorithm with one eavesdropper in wireless networks

ent in each loop. Finally, the privacy data are recovered by minimizing the following objective[10, 26].

$$\hat{\boldsymbol{x}}^*, \hat{\boldsymbol{y}}^* = \arg\min_{\hat{\boldsymbol{x}}, \hat{\boldsymbol{y}}} \left\| \hat{\boldsymbol{g}} - \boldsymbol{g}_i^J \right\|_2, \tag{5}$$

$$\hat{\boldsymbol{g}} = \frac{1}{B} \sum_{b=1}^{B} \frac{\partial f\left(\boldsymbol{w}^J, \hat{\boldsymbol{x}}_b, \hat{y}_b\right)}{\partial \boldsymbol{w}^J}, \tag{6}$$

where $\hat{\boldsymbol{x}}$ and $\hat{\boldsymbol{y}}$ are the synthetic dummy data and labels, respectively; $\boldsymbol{x}^*$ and $\boldsymbol{y}^*$ are the ground truth data and labels corresponding to the eavesdropped gradient $\boldsymbol{g}_i^J$; $\hat{\boldsymbol{x}}^*$ and $\hat{\boldsymbol{y}}^*$ are the recovered data and labels. If $B = 1$, Eq. (5) can be expressed as

$$\hat{\boldsymbol{x}}^*, \hat{y}^* = \arg\min_{\hat{\boldsymbol{x}}, \hat{y}} \left\| \frac{\partial f\left(\boldsymbol{w}^J, \hat{\boldsymbol{x}}, \hat{y}\right)}{\partial \boldsymbol{w}^J} - \boldsymbol{g}_i^J \right\|_2. \tag{7}$$

2.3 Defense Method

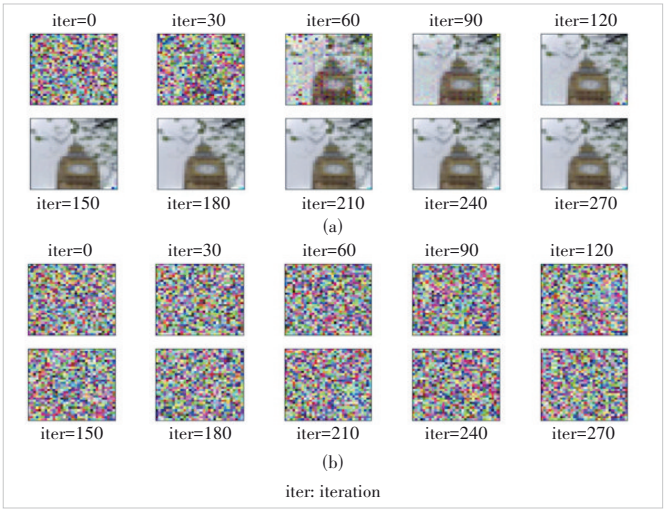
Data leakage is mainly caused by the leakage of the gradient transmitted in the wireless network. Therefore, it can be considered to compress or encrypt the gradient on the client side to make it difficult for eavesdroppers to recover private data. In this section, we propose a defense method against data leakage called weight compression. The weight compression scheme belongs to gradient compression, which is based on the user's location and channel quality to determine the compression matrix. Local gradients are divided into several parts by the compression matrix and only some of the gradients are sent to the server at a time for aggregation. Moreover, we add Gaussian noise to compressed gradients as the second defense strategy to strengthen the defense. Fig. 2 shows the result of applying DP to defend against DLG attacks. Fig. 2(a) illustrates that DLG can recover the original image easily without adding any defense methods and Fig. 2(b) demonstrates its effectiveness with the addition of the Gaussian noise defense approach.

We define u_i^j as the weight matrix of client i at the j-th iteration. To further prevent privacy data leakage, we add artificial Gaussian noise to the compressed gradient, and then the selected partial local gradient is given as:

$$\tilde{\boldsymbol{g}}_i^j = \boldsymbol{g}_i^j \odot \boldsymbol{u}_i^j + \boldsymbol{n}_i^j, \tag{8}$$

where $\boldsymbol{g}_i^j = \left[g_{i,1}^j, \cdots, g_{i,M}^j\right]$ and $\boldsymbol{u}_i^j = \left[u_{i,1}^j, \cdots, u_{i,M}^j\right]$, M refers to the number of gradients, and $\odot$ is the dot product. In Eq. (8), the first part $\boldsymbol{g}_i^j \odot \boldsymbol{u}_i^j$ represents the selected partial gradient, and the second part represents the addition of Gaussian noise, where $n \sim N\left(0, \sigma^2\right)$. An example is shown in Fig. 3. Moreover, the compression ratio is controlled by α, i. e., $\sum_{m=1}^{M} u_{i,m}^j \leqslant \alpha_i M, u_{i,m}^j \in \{0, 1\}$.

In this work, we define Eq. (9) to restrict the leakage of gradients[27].



▲Figure 2. Illustration of the differential privacy (DP) method to protect the privacy of federated learning (FL)

User 1		User 2		User 3	
Original gradients g_1	Transmitted gradients $\tilde{g}_1$	Original gradients g_2	Transmitted gradients $\tilde{g}_2$	Original gradients g_3	Transmitted gradients $\tilde{g}_3$
1	0	0.8	0.8	−2	0
1	1	0.3	0	1.5	0
−1	0	0.7	0.7	−1	0
1	0	2	0	3	3
−1	−1	−1	0	−0.4	0
−1	0	−0.5	0	2	2

Selected partial gradients

$g_i \odot u_i + n_i = \tilde{g}_i$

▲Figure 3. An example of proposed weight compression

$$\sum_{m=1}^{M} \rho_{i,m} u_{i,m} \leqslant DP_0, \tag{9}$$

where $\rho_{i,m} = 1/(K_i \sigma^2)$ stands for the data leakage level of each gradient and DP_0 denotes the maximum amount of gradient leakage.

2.4 Transmission Model

In the FL training process, all clients upload their local FL gradient to the BS via orthogonal frequency domain multiple access (OFDMA). For the uplink, the upper bound of the transmission rate of client i can be given by:

$$r_i^U = b_i B_0 \log_2\left(1 + \frac{P_i h_i}{N_0 B_0}\right), \tag{10}$$

where $b_i = \sum_{q=1}^{Q} b_{i,q}$ is the number of RBs allocated to client i. Note that we assume that all clients participate in the FL training, so $b_i \geqslant 1$. Q is the total number of RBs, B_0 is the bandwidth of each RB, and $\sum_{i=1}^{N} b_i B_0 \leqslant B$, where B is the total

bandwidth. P_i is the transmit power of client i, h_i is the channel gain between client i and the BS. N_0 is the Gaussian noise power spectral density.

According to the data rate of the uplink in Eq. (10), the transmission delay between client i and the BS on the uplink can be expressed by:

$$t_i^U = \frac{Z(\tilde{\boldsymbol{g}}_i)}{r_i^U}, \tag{11}$$

where the function $Z(\tilde{\boldsymbol{g}}_i)$ denotes the size of the data transmitted by each client i to the BS, i.e., the number of bits corresponding to the selected local gradients. We set $Z(\tilde{\boldsymbol{g}}_i) = C\sum_m^M u_{i,m} + 1\sum_m^M(1 - u_{i,m})$, where C denotes the number of bits per selected gradient.

2.5 Problem Formulation

In order to prevent eavesdroppers from recovering the private data of clients and to guarantee FL model convergence, we propose a defense method called weight compression to compress the transmission gradient and formulate an optimization problem to implement this joint-designed defense method and the FL algorithm. The objective is to minimize data leakage with limited iterations or delays by optimizing the portion selection of the local FL gradient for transmission. The optimization function is defined by

$$\min_{\boldsymbol{u},\boldsymbol{b}} \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K_i} f(\boldsymbol{w}_i, \boldsymbol{x}_{ik}, y_{ik}), \tag{12}$$

$$\text{s.t. } b_i = \sum_{q=1}^{Q} b_{i,q} \geqslant 1, \forall i \in N, \tag{12a}$$

$$\sum_{i=1}^{N} b_i B_0 \leqslant B, \forall i \in N, \tag{12b}$$

$$u_{i,m} \in \{0,1\}, \forall i \in N, \tag{12c}$$

$$\sum_{m=1}^{M} u_{i,m} \leqslant \alpha_i M, \forall i \in N, \tag{12d}$$

$$\sum_{m=1}^{M} \rho_{i,m} u_{i,m} \leqslant DP_0, \forall i \in N, \tag{12e}$$

$$t_i^U(b_i, \boldsymbol{u}_i) \leqslant \tau, \forall i \in N, \tag{12f}$$

where B_0 is the bandwidth of each RB, B is the total uplink bandwidth, τ is the requirement for uplink transmission delay, and DP_0 is the constraint of gradient leakage. Eq. (12c) shows the sum of the bandwidth allocated to each user is less than or equal to the total bandwidth of the uplink. Eq. (12e) indicates the compression requirement for the number of valid gradients uploaded by each user.

3 Analysis of FL Convergence Rate

Since we add defense methods to the original FL algorithm, we need to investigate how transmitting compressed gradient affects the performance of FL to solve Eq. (12). Therefore, in this section, we derive the upper bound on the optimality gap of the defense-added FL algorithm.

We assume that $F(\boldsymbol{w}) = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K_i} f(\boldsymbol{w}^j, \boldsymbol{x}_{ik}, y_{ik})$ and $F_i(\boldsymbol{w}) = \sum_{k=1}^{K_i} f(\boldsymbol{w}^j, \boldsymbol{x}_{ik}, y_{ik})$. Based on Eq. (4), the updated global FL model $\boldsymbol{w}$ at step j will be

$$\boldsymbol{w}^{j+1} = \boldsymbol{w}^j - \eta\left(\nabla F(\boldsymbol{w}^j) - \boldsymbol{o}\right), \tag{13}$$

where $\boldsymbol{o} = \nabla F(\boldsymbol{w}^j) - \frac{\sum_{i=1}^{N}\sum_{k=1}^{K_i} \boldsymbol{u}_i \odot \nabla f(\boldsymbol{w}, \boldsymbol{x}_{ik}, y_{ik})}{\sum_{i=1}^{N} K_i}$.

Before deriving the convergence rate of FL, we first make the following assumptions, the same as Ref. [28].

• A1: We assume that the gradient $\nabla F(\boldsymbol{w})$ of $F(\boldsymbol{w})$ is uniformly Lispschitz continuous with respect to w, such that

$$\left\| \nabla F(\boldsymbol{w}^{j+1}) - \nabla F(\boldsymbol{w}^j) \right\| \leqslant L \left\| \boldsymbol{w}^{j+1} - \boldsymbol{w}^j \right\|, \tag{14}$$

where L is a positive constant which is determined by the loss function and $\|\cdot\|$ presents the two-norm.

• A2: We assume that $F(\boldsymbol{w})$ is the μ-strongly convex, such that

$$F(\boldsymbol{w}^{j+1}) \geqslant F(\boldsymbol{w}^j) + (\boldsymbol{w}^{j+1} - \boldsymbol{w}^j)^T \nabla F(\boldsymbol{w}^j) + \frac{\mu}{2}\left\| \boldsymbol{w}^{j+1} - \boldsymbol{w}^j \right\|^2. \tag{15}$$

• A3: We assume that $F(\boldsymbol{w})$ is twice continuously differentiable. Based on A1 and A2, we have

$$\mu I \leq \nabla^2 F(\boldsymbol{w}) \leq LI. \tag{16}$$

• A4: we assume that $\left\| \nabla f(\boldsymbol{w}^j, \boldsymbol{x}_{ik}, y_{ik}) \right\|^2 \leqslant \delta_1 + \delta_2 \left\| \nabla F(\boldsymbol{w}^j) \right\|^2$ with $\delta_1, \delta_2 \geqslant 0$.

Theorem 1: If we run the FL algorithm with the weight matrix $\boldsymbol{u}$, optimal global model $\boldsymbol{w}^*$ and learning rate $\eta = 1/L$, we have

$$F(\boldsymbol{w}^{j+1}) - F(\boldsymbol{w}^*) \leqslant A^t\left(F(\boldsymbol{w}^0) - F(\boldsymbol{w}^*)\right) + \frac{2\delta_1}{LK}\sum_{m=1}^{M}\sum_{i=1}^{N} K_i(1 - u_{i,m})\frac{A^t - 1}{A - 1}, \tag{17}$$

where $A = 1 - \frac{\mu}{L} + \frac{4\mu\delta_2}{LK}\sum_{m=1}^{M}\sum_{i=1}^{N} K_i(1 - u_{i,m})$ and the

proof process of $F\left(\boldsymbol{w}^{j+1}\right)-F\left(\boldsymbol{w}^{*}\right)$ is shown below.

According to the second-order Taylor expansion, $F\left(\boldsymbol{w}^{j+1}\right)$ can be rewritten as

$$F\left(\boldsymbol{w}^{j+1}\right)=F\left(\boldsymbol{w}^{j}\right)+\left(\boldsymbol{w}^{j+1}-\boldsymbol{w}^{j}\right)^{T}\nabla F\left(\boldsymbol{w}^{j}\right)+\frac{1}{2}\left(\boldsymbol{w}^{j+1}-\boldsymbol{w}^{j}\right)^{T}\nabla^{2}F\left(\boldsymbol{w}\right)\left(\boldsymbol{w}^{j+1}-\boldsymbol{w}^{j}\right)\leqslant F\left(\boldsymbol{w}^{j}\right)+\left(\boldsymbol{w}^{j+1}-\boldsymbol{w}^{j}\right)^{T}\nabla F\left(\boldsymbol{w}^{j}\right)+\frac{L}{2}\left\|\boldsymbol{w}^{j+1}-\boldsymbol{w}^{j}\right\|^{2}. \tag{18}$$

Based on Eq. (13) and given the learning rate $\eta=1/L$, the $F\left(\boldsymbol{w}^{j+1}\right)$ can be expressed as

$$F\left(\boldsymbol{w}^{j+1}\right)\leqslant F\left(\boldsymbol{w}^{j}\right)-\eta\left(\nabla F\left(\boldsymbol{w}^{j}\right)-\boldsymbol{o}\right)^{T}\nabla F\left(\boldsymbol{w}^{j}\right)+\frac{L\eta^{2}}{2}\left\|\nabla F\left(\boldsymbol{w}^{j}\right)-\boldsymbol{o}\right\|^{2}=F\left(\boldsymbol{w}^{j}\right)-\frac{1}{2L}\left\|\nabla F\left(\boldsymbol{w}^{j}\right)\right\|^{2}+\frac{1}{2L}\left\|\boldsymbol{o}\right\|^{2}. \tag{19}$$

Next, we derive $\left\|\boldsymbol{o}\right\|^{2}$, and the derivation is given as follows:

$$\left\|\boldsymbol{o}\right\|^{2}=\sum_{m=1}^{M}\left\|\boldsymbol{o}_{m}\right\|^{2}=\left\|\nabla F\left(\boldsymbol{w}^{j}\right)-\frac{\sum_{i=1}^{N}\sum_{k=1}^{K_i}\boldsymbol{u}_{i}\odot\nabla f\left(\boldsymbol{w},\boldsymbol{x}_{ik},y_{ik}\right)}{\sum_{i=1}^{N}K_i}\right\|^{2}=\sum_{m=1}^{M}\left\|\nabla F\left(\boldsymbol{w}^{j}\right)-\frac{\sum_{i=1}^{N}\sum_{k=1}^{K_i}u_{i,m}\nabla f_{m}\left(\boldsymbol{w},\boldsymbol{x}_{ik},y_{ik}\right)}{\sum_{i=1}^{N}K_iu_{i,m}}\right\|^{2}=\sum_{m=1}^{M}\left\|-\frac{\left(K-\sum_{i=1}^{N}K_iu_{i,m}\right)\sum_{i\in\mathcal{D}_{1,m}}\sum_{k=1}^{K_i}\nabla f_{m}\left(\boldsymbol{w},\boldsymbol{x}_{ik},y_{ik}\right)}{K\sum_{i=1}^{N}K_iu_{i,m}}+\frac{\sum_{i\in\mathcal{D}_{0,m}}\sum_{k=1}^{K_i}\nabla f_{m}\left(\boldsymbol{w},\boldsymbol{x}_{ik},y_{ik}\right)}{K}\right\|^{2}\leqslant\sum_{m=1}^{M}\left(\frac{\left(K-\sum_{i=1}^{N}K_iu_{i,m}\right)\sum_{i\in\mathcal{D}_{1,m}}\sum_{k=1}^{K_i}\left\|\nabla f_{m}\left(\boldsymbol{w},\boldsymbol{x}_{ik},y_{ik}\right)\right\|}{K\sum_{i=1}^{N}K_iu_{i,m}}+\frac{\sum_{i\in\mathcal{D}_{0,m}}\sum_{k=1}^{K_i}\left\|\nabla f_{m}\left(\boldsymbol{w},\boldsymbol{x}_{ik},y_{ik}\right)\right\|}{K}\right)^{2}, \tag{20}$$

where $\mathcal{D}_{1,m}$ is the set of users with $u_{i,m}=1$ and $\mathcal{D}_{0,m}$ is the set of users with $u_{i,m}=0$; the inequality equation is realized based on the triangle inequality. According to A4, $\left\|\boldsymbol{o}\right\|^{2}$ can be expressed by

$$\left\|\boldsymbol{o}\right\|^{2}\leqslant\sum_{m=1}^{M}\left(\frac{4}{K^{2}}\left(K-\sum_{i=1}^{N}K_iu_{i,m}\right)^{2}\left(\delta_1+\delta_2\left\|\nabla F\left(\boldsymbol{w}^{j}\right)\right\|^{2}\right)\right). \tag{21}$$

Since $0\leqslant K-\sum_{i=1}^{N}K_iu_{i,m}\leqslant K$, we have

$$\left\|\boldsymbol{o}\right\|^{2}\leqslant\sum_{m=1}^{M}\left(\frac{4}{K}\left(K-\sum_{i=1}^{N}K_iu_{i,m}\right)\left(\delta_1+\delta_2\left\|\nabla F\left(\boldsymbol{w}^{j}\right)\right\|^{2}\right)\right)\leqslant\frac{4}{K}\sum_{m=1}^{M}\left(\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)\left(\delta_1+\delta_2\left\|\nabla F\left(\boldsymbol{w}^{j}\right)\right\|^{2}\right)\right). \tag{22}$$

Substituting Eq. (22) into Eq. (19), we have

$$F\left(\boldsymbol{w}^{j+1}\right)\leqslant F\left(\boldsymbol{w}^{j}\right)+\frac{2\delta_1}{LK}\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)-\frac{1}{2L}\left(1-\frac{4\delta_2}{K}\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)\right)\left\|\nabla F\left(\boldsymbol{w}^{j}\right)\right\|^{2}, \tag{23}$$

$$F\left(\boldsymbol{w}^{j+1}\right)-F\left(\boldsymbol{w}^{*}\right)\leqslant\left(F\left(\boldsymbol{w}^{j}\right)-F\left(\boldsymbol{w}^{*}\right)\right)+\frac{2\delta_1}{LK}\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)-\frac{1}{2L}\left(1-\frac{4\delta_2}{K}\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)\right)\left\|\nabla F\left(\boldsymbol{w}^{j}\right)\right\|^{2}. \tag{24}$$

Based on Eq.(15) and Eq.(16), we get

$$\left\|\nabla F\left(\boldsymbol{w}^{j}\right)\right\|^{2}\geqslant 2\mu\left(F\left(\boldsymbol{w}^{j}\right)-F\left(\boldsymbol{w}^{*}\right)\right), \tag{25}$$

$$F\left(\boldsymbol{w}^{j+1}\right)-F\left(\boldsymbol{w}^{*}\right)\leqslant\frac{2\delta_1}{LK}\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)+A\left(F\left(\boldsymbol{w}^{j}\right)-F\left(\boldsymbol{w}^{*}\right)\right), \tag{26}$$

where $A=1-\frac{\mu}{L}+\frac{4\mu\delta_2}{LK}\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)$. Applying Eq. (26) recursively, we have

$$F\left(\boldsymbol{w}^{j+1}\right)-F\left(\boldsymbol{w}^{*}\right)\leqslant A^{t}\left(F\left(\boldsymbol{w}^{0}\right)-F\left(\boldsymbol{w}^{*}\right)\right)+\frac{2\delta_1}{LK}\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)\frac{A^{t}-1}{A-1}. \tag{27}$$

This completes the proof.

According to Theorem 1, we obtain the gap between $F\left(\boldsymbol{w}^{j+1}\right)$ and $F\left(\boldsymbol{w}^{*}\right)$. Next, we derive the conditions for δ_2 that guarantees the convergence of FL and simplify the optimization problem in Eq. (12). In Theorem 1, if we set $A<1$ and $A^{t}=0$, we can get $F\left(\boldsymbol{w}^{j+1}\right)-F\left(\boldsymbol{w}^{*}\right)=\sum_{m=1}^{M}\sum_{i=1}^{N}K_i$ (1 –

$u_{i,m}\right)\frac{A^t-1}{A-1}$ and FL converges. Therefore, we only need to make $A=1-\frac{\mu}{L}+\frac{4\mu\delta_2}{LK}\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)<1$ to ensure FL convergence. Moreover, we can get the relationship between μ and L, $\mu<L$, from Eq. (16). Hence, we get $\delta_2<K\Big/4\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)$. In addition, since δ_2 satisfies the assumption A4, we have

$$0<\delta_2<\frac{K}{\max\limits_{\boldsymbol{u},\boldsymbol{b}}\ 4\sum\limits_{m=1}^{M}\sum\limits_{i=1}^{N}K_i\left(1-u_{i,m}\right)}. \tag{28}$$

4 Optimization of Training Loss

In this section, we aim to minimize the training loss of FL by optimizing the weight compression matrix and RB allocation and considering the constraints under the wireless network. We first simplify the objective function in Eq. (12). From Theorem 1 and the analysis of FL convergence conditions in Section 3, we see that if we want to minimize the training loss of FL, we only need to minimize the gap between $F\left(\boldsymbol{w}^{j+1}\right)$ and $F\left(\boldsymbol{w}^{*}\right)$, under the condition that $A<1$. Then we get

$$\frac{2\delta_1}{LK}\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)\frac{A^t-1}{A-1}=\frac{\frac{2\delta_1}{LK}\sum\limits_{m=1}^{M}\sum\limits_{i=1}^{N}K_i\left(1-u_{i,m}\right)}{\frac{\mu}{L}-\frac{4\mu\delta_2}{LK}\sum\limits_{m=1}^{M}\sum\limits_{i=1}^{N}K_i\left(1-u_{i,m}\right)}. \tag{29}$$

It is obvious to find that to minimize Eq. (29), only $\sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right)$ needs to be minimized, so the optimization problem can be simplified as

$$\min_{\boldsymbol{u},\boldsymbol{b}}\ \sum_{m=1}^{M}\sum_{i=1}^{N}K_i\left(1-u_{i,m}\right), \tag{30}$$

$$\text{s.t. } b_i=\sum_{q=1}^{Q}b_{i,q}\geqslant 1, \tag{30a}$$

$$\sum_{i=1}^{N}b_iB_0\leqslant B,\forall i\in N, \tag{30b}$$

$$u_{i,m}\in\{0,1\},\forall i\in N, \tag{30c}$$

$$\sum_{m=1}^{M}u_{i,m}\leqslant\alpha_iM,\forall i\in N, \tag{30d}$$

$$\sum_{m=1}^{M}\rho_{i,m}u_{i,m}\leqslant DP_0,\forall i\in N, \tag{30e}$$

$$t_i^U\left(b_i,\boldsymbol{u}_i\right)\leqslant\tau,\forall i\in N. \tag{30f}$$

Next, we aim to find the optimal RB allocation and weight compression matrix for each user. To accomplish this, we utilize ant colony optimization (ACO) for a large number of RBs and exhaustive search for a small number of RBs.

5 Simulation Results and Analysis

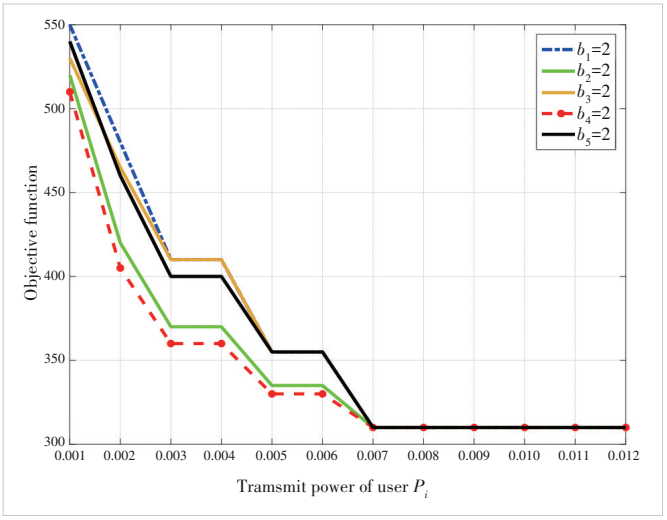
For our simulations, we investigate how the wireless network parameters $\left(P_i,\boldsymbol{b}\right)$, user sample size K_i and gradient compression restrictions α_i affect the convergence rate under the premise that FL can converge. This simulation topology is a circular wireless network area with a central base station serving $N=5$ uniformly distributed users with $d=30$ m. Specifically, we consider only six RBs and five users, first finding all solutions for $\boldsymbol{b}$ by exhaustive search (at most one user is assigned two RBs), and then we solve the optimization problem by using a CVX (a Matlab-based modeling system for convex optimization) toolbox and MOSEK solver in MATLAB. Other key parameters used in this simulation are listed in Table 1.

Fig. 4 shows how the change of P_i and the allocation of RB

▼Table 1. Simulation Parameters

Description	Parameter	Value
Total bandwidth of uplink	B	20 MHz
Bandwidth of each RB	B_0	3.33 MHz
Noise power spectral density	N_0	−174 dBm/MHz
Total number of training samples for user	K_i	[10, 20, 15, 25, 10]
Gradient compression ratio of user	α_i	$\left[\frac{3}{9},\frac{6}{9},\frac{4}{9},\frac{6}{9},\frac{5}{9}\right]$
Number of gradients for each user	M	9
Delay requirement of uplink	τ	2 s
Distance between user and BS	d	30 m
Number of RBs	Q	6
Transmit power of user	P_i	0.001 – 0.012 W

BS: base station RB: resource block



▲Figure 4. Objective function as user power and resource block (RB) allocation varies

change the objective function value, i.e., the convergence rate of the FL algorithm. As can be seen from Fig. 4, with the increase of P_i, the objective function first decreases and then tends to remain unchanged. This is because when the user power increases, the uplink transmission rate of the user becomes larger, allowing the user to upload more gradients, thus accelerating the convergence speed and optimizing the objective function. However, when P_i is very large, the optimal number of gradients that users can upload is already saturated due to DP_0 constraints, so the objective function cannot continue to decline.

Different RB allocations also affect the convergence speed of FL at the same P_i, and here we analyze three cases. The objective function value of the red line in Fig. 4 is the smallest, which is because the number of samples K_4 and the compression ratio α_4 of user 4 are the largest. Therefore, assigning more RBs to the user with more samples and larger α_i can increase the transmission rate of that user and reduce the total delay of uplink transmission, thereby accelerating the convergence speed. When K_i is the same but α_i is different, that is, the blue line and the black line, the larger α_i is, the smaller the value of the objective function is. The reason is that if α_i is large, more gradients can be transmitted, so assigning more RBs to it will result in faster convergence. When α_i is the same and K_i is different, i.e., green and red lines, the larger K_i is, the smaller the value of the objective function is. This is because the larger K_i is, the smaller DP_0 is and the smaller $\rho_{i,m}$ is. According to Constraint (30e), more $u_{i,m}$ can be taken as 1, resulting in a smaller objective function and better performance. Overall, optimizing $\boldsymbol{b}$ can make the convergence faster given a fixed P_i.

6 Conclusions

In this work, we propose a novel defensive framework to protect data privacy from DLG attacks in wireless networks. We jointly optimize RBs allocations and weight compression matrix to minimize FL training loss. We first formulate this optimization problem and simplify it by finding the relationship between the weight matrix and FL convergence rate. Optimal RB allocation is solved by ACO for a large number of RBs and exhaustive search for a small number of RBs. The optimal weight matrix is solved by the CVX toolbox. The simulation results illustrate that optimizing RBs can effectively improve the convergence speed given fixed user power.

References

[1] YANG Q, LIU Y, CHEN T J, et al. Federated machine learning: concept and applications [J]. ACM transactions on intelligent systems and technology, 2019, 10 (2): 1 – 19. DOI: 10.1145/3298981
[2] JOCHEMS A, DEIST T M, VAN SOEST J, et al. Distributed learning: developing a predictive model based on data from multiple hospitals without data leaving the hospital—a real life proof of concept [J]. Radiotherapy and oncology, 2016, 121(3): 459 – 467. DOI: 10.1016/j.radonc.2016.10.002
[3] BONAWITZ K, EICHNER H, GRIESKAMP W, et al. Towards federated learning at scale: system design [C]//Conference on machine learning and systems. MLSys, 2019: 374 – 388
[4] SHOKRI R, STRONATI M, SONG C Z, et al. Membership inference attacks against machine learning models [C]//IEEE Symposium on Security and Privacy (SP). IEEE, 2017: 3 – 18. DOI: 10.1109/SP.2017.41
[5] HITAJ B, ATENIESE G, PEREZ-CRUZ F. Deep models under the GAN: information leakage from collaborative deep learning [C]//ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017: 603 – 618. DOI: 10.1145/3133956.3134012
[6] WANG Z B, SONG M K, ZHANG Z F, et al. Beyond inferring class representatives: user-level privacy leakage from federated learning [C]//IEEE Conference on Computer Communications. IEEE, 2019: 2512 – 2520. DOI: 10.1109/INFOCOM.2019.8737416
[7] PHONG L T, AONO Y, HAYASHI T, et al. Privacy-preserving deep learning via additively homomorphic encryption [J]. IEEE transactions on information forensics and security, 2017, 13(5): 1333 – 1345. DOI: 10.1109/TIFS.2017.2787987
[8] ZHU L G, LIU Z J, HAN S. Deep leakage from gradients [C]//33rd Conference on Neural Information Processing Systems. NeurIPS, 2019: 8389
[9] ZHAO B, MOPURI K R, BILEN H. iDLG: improved deep leakage from gradients [EB/OL]. [2020-01-08]. https://arxiv.org/abs/2001.02610
[10] YIN H X, MALLYA A, VAHDAT A, et al. See through gradients: image batch recovery via GradInversion [C]//IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2021: 16332 – 16341. DOI: 10.1109/CVPR46437.2021.01607
[11] CHEN S, JIA R X, QI G J. Improved techniques for model inversion attack [EB/OL]. [2021-08-19]. https://arxiv.org/abs/2010.04092v1
[12] JERE M S, FARNAN T, KOUSHANFAR F. A taxonomy of attacks on federated learning [J]. IEEE security privacy, 2021, 19(2): 20 – 28. DOI: 10.1109/MSEC.2020.3039941
[13] GEIPING J, BAUERMEISTER H, DRÖGE H, et al. Inverting gradients: how easy is it to break privacy in federated learning? [C]//34th International Conference on Neural Information Processing Systems. NeurIPS, 2020: 16937 – 16947
[14] ZHANG C L, LI S Y, XIA J Z, et al. BatchCrypt: efficient homomorphic encryption for cross-silo federated learning [C]//USENIX Conference on Usenix Annual Technical Conference. ACM, 2020: 493 – 506. DOI: 10.5555/3489146.3489179
[15] CHENG K W, FAN T, JIN Y L, et al. SecureBoost: a lossless federated learning framework [J]. IEEE intelligent systems, 2021, 36(6): 87 – 98. DOI: 10.1109/MIS.2021.3082561
[16] MOHASSEL P, ZHANG Y P. Secureml: a system for scalable privacy-preserving machine learning [C]//IEEE Symposium on Security and Privacy (SP). IEEE, 2017: 19 – 38. DOI: 10.1109/SP.2017.12
[17] BONAWITZ K, IVANOV V, KREUTER B, et al. Practical secure aggregation for privacy-preserving machine learning [C]//ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017: 1175 – 1191. DOI: 10.1145/3133956.3133982
[18] GEYER R C, KLEIN T, NABI M. Differentially private federated learning: a client level perspective [EB/OL]. [2022-03-01]. https://arxiv. org/abs/1712.07557
[19] MCMAHAN H B, RAMAGE D, TALWAR K, et al. Learning differentially private recurrent language models [EB/OL]. [2022-02-24]. https://arxiv. org/abs/1710.06963
[20] WEI K, LI J, DING M, et al. Federated learning with differential privacy: algorithms and performance analysis [J]. IEEE transactions on information forensics and security, 2020, 15: 3454 – 3469. DOI: 10.1109/TIFS.2020.2988575
[21] WEI W Q, LIU L, LOPER M, et al. A framework for evaluating gradient leakage attacks in federated learning [EB/OL]. [2021-04-23]. https://arxiv.org/abs/2004.10397
[22] SUN J W, LI A, WANG B H, et al. Soteria: provable defense against privacy leakage in federated learning from representation perspective [C]//IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2021: 9307 – 9315. DOI: 10.1109/CVPR46437.2021.00919

[23] SCHELIGA D, MÄDER P, SEELAND M. Precode—a generic model extension to prevent deep gradient leakage [C]//IEEE/CVF Winter Conference on Applications of Computer Vision (WACV). IEEE, 2022: 3605 – 3614. DOI: 10.1109/WACV51458.2022.00366
[24] WANG J X, GUO S, XIE X, et al. Protect privacy from gradient leakage attack in federated learning [C]//IEEE Conference on Computer Communications. IEEE, 2022: 580 – 589. DOI: 10.1109/INFOCOM48880.2022.9796841
[25] KONEČNÝ J, MCMAHAN H B, RAMAGE D, et al. Federated optimization: distributed machine learning for on-device intelligence [EB/OL]. [2021-10-08]. https://arxiv.org/abs/1610.02527
[26] HATAMIZADEH A, YIN H X, MOLCHANOV P, et al. Do gradient inversion attacks make federated learning unsafe? [EB/OL]. [2022-02-14]. https://arxiv.org/abs/2202.06924
[27] TAVANGARAN N, CHEN M Z, YANG Z H, et al. On differential privacy for federated learning in wireless systems with multiple base stations [EB/OL]. [2022-08-25]. https://arxiv.org/abs/2208.11848
[28] CHEN M Z, YANG Z H, SAAD W, et al. A joint learning and communications framework for federated learning over wireless networks [J]. IEEE transactions on wireless communications, 2021, 20(1): 269 – 283. DOI: 10.1109/TWC.2020.3024629

Biographies

DING Yahao received her master's degree in communications and signal processing from Imperial College London, U.K. in 2020. She is currently pursuing her PhD degree in information and communication engineering with King's College London, U.K. Her current research interests include federated learning, security, and UAV swarms.

Mohammad SHIKH-BAHAEI received his BSc degree from the University of Tehran, Iran in 1992, MSc degree from the Sharif University of Technology, Iran in 1994, and PhD degree from King's College London, U.K. in 2000. He has worked for two start-up companies and for National Semiconductor Corporation, USA (now part of Texas Instruments Inc.). In 2002, he joined King's College London, where he is currently a full professor. Since then, he has authored numerous journals and conference papers and worked as an expert consultant to a number of international high-tech companies and legal firms. His research interests are secure communications and connected intelligence, full-duplex and cognitive dense networks, visual data communications over the IoT, applications of wireless communications in healthcare, and communication protocols for autonomous vehicle/drone networks. He has been the founder and the chair of the Wireless Advanced (formerly SPWC) Annual International Conference from 2003 to 2018.

YANG Zhaohui received his PhD degree from Southeast University, China in 2018. From 2018 to 2020, he was a postdoctoral research associate with the Center for Telecommunications Research, Department of Informatics, King's College London, U.K. From 2020 to 2022, he was a research fellow with the Department of Electronic and Electrical Engineering, University College London, U.K. He is currently a young professor with the College of Information Science and Electronic Engineering, Zhejiang Key Laboratory of Information Processing Communication and Networking, Zhejiang University, China, and also a research scientist with Zhejiang Laboratory. His research interests include joint communication, sensing and computation, federated learning, and semantic communications. He is an associate editor for *IEEE Communications Letters*, *IET Communications*, and *EURASIP Journal on Wireless Communications and Networking*. He was the guest editor of several journals, including *JSAC*, *WCM* and *CM*. He was the co-chair for international workshops with more than ten times, including ICC, GLOBECOM, WCNC, PIMRC and INFOCOM.

HUANG Chongwen (chongwenhuang@zju. edu. cn) received his BSc degree from the Binhai College, Nankai University, China in 2010, and MSc degree from the University of Electronic Science and Technology of China (UESTC), China in 2013. He has been joining the Institute of Electronics, Chinese Academy of Sciences (IECAS) as a research engineer, since July 2013. Since September 2015, he has been starting his PhD journey with the Singapore University of Technology and Design (SUTD), Singapore and CentraleSupélec University, Paris, France under the supervision of Prof. Chau YUEN and Prof. Mérouane DEBBAH. From October 2019 to September 2020, he was a post-doctoral researcher at SUTD. Since September 2020, he has been joining Zhejiang University as a Tenure-Track Young Professor. His main research interests include holographic MIMO surface/reconfigurable intelligent surface, B5G/6G wireless communications, mmWave/THz communications, and deep learning technologies for wireless communications. He was a recipient of the IEEE Marconi Prize Paper Award in Wireless Communications in 2021. He was also a recipient of the Singapore Government PhD Scholarship and received PHC Merlion PhD Grant (2016 – 2019) for studying in CentraleSupélec, France. He has been serving as an editor of *IEEE Communications Letter*, *Signal Processing* (Elsevier), *EURASIP Journal on Wireless Communications and Networking*, and *Physical Communication* since 2021. In addition, he has served as the chair of several wireless communications flagship conferences, including the session chair of 2021 IEEE WCNC, 2021 IEEE VTC-Fall, and the symposium chair of IEEE WCSP 2021.

YUAN Weijie received his BE degree from the Beijing Institute of Technology, China in 2013, and PhD degree from the University of Technology Sydney, Australia in 2019. In 2016, he was a visiting PhD student with the Institute of Telecommunications, Vienna University of Technology, Austria. He was a research assistant with the University of Sydney, Australia, a visiting associate fellow with the University of Wollongong, Australia and a visiting fellow with the University of Southampton, U.K. from 2017 to 2019. From 2019 to 2021, he was a research associate with the University of New South Wales, Australia. He is currently an assistant professor with the Department of Electrical and Electronic Engineering, Southern University of Science and Technology, China. He was a recipient of the Best PhD Thesis Award from the Chinese Institute of Electronics and an Exemplary Reviewer from IEEE TCOM/WCL. He currently serves as an associate editor of *IEEE Communications Letters*, an associate editor and an award committee member of *EURASIP Journal on Advances in Signal Processing*. He has led the guest editorial teams for three special issues in *IEEE Communications Magazine*, *IEEE Transactions on Green Communications and Networking*, and *China Communications*. He was an organizer/the chair of several workshops and special sessions on orthogonal time frequency space and integrated sensing and communication in flagship IEEE and ACM conferences, including IEEE ICC, IEEE/CIC ICCC, IEEE SPAWC, IEEE VTC, IEEE WCNC, IEEE ICASSP, and ACM MobiCom. He is the founding chair of the IEEE ComSoc Special Interest Group on Orthogonal Time Frequency Space.