FedBIAD: Communication-Efficient and Accuracy-Guaranteed Federated Learning with Bayesian Inference-Based Adaptive Dropout

Jingjing Xue*[†], Min Liu*^{†‡}, Sheng Sun*, Yuwei Wang*, Hui Jiang*[†], and Xuefeng Jiang*[†]

*Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China

[†]University of Chinese Academy of Sciences, Beijing, China

Email: {xuejingjing20g, liumin, sunsheng, ywwang, jianghui, jiangxuefeng21b}@ict.ac.cn

Abstract—Federated Learning (FL) emerges as a distributed machine learning paradigm without end-user data transmission, effectively avoiding privacy leakage. Participating devices in FL are usually bandwidth-constrained, and the uplink is much slower than the downlink in wireless networks, which causes a severe uplink communication bottleneck. A prominent direction to alleviate this problem is federated dropout, which drops fractional weights of local models. However, existing federated dropout studies focus on random or ordered dropout and lack theoretical support, resulting in unguaranteed performance. In this paper, we propose Federated learning with Bayesian Inference-based Adaptive Dropout (FedBIAD), which regards weight rows of local models as probability distributions and adaptively drops partial weight rows based on importance indicators correlated with the trend of local training loss. By applying FedBIAD, each client adaptively selects a high-quality dropping pattern with accurate approximations and only transmits parameters of nondropped weight rows to mitigate uplink costs while improving accuracy. Theoretical analysis demonstrates that the convergence rate of the average generalization error of FedBIAD is minimax optimal up to a squared logarithmic factor. Extensive experiments on image classification and next-word prediction show that compared with status quo approaches, FedBIAD provides $2\times$ uplink reduction with an accuracy increase of up to 2.41% even on non-Independent and Identically Distributed (non-IID) data, which brings up to 72% decrease in training time.

Index Terms—federated learning, communication bottleneck, adaptive dropout, Bayesian inference

I. INTRODUCTION

The increased prevalence of smart end-user devices has led to the significant growth of the data generated by edge networks. To utilize such decentralized data without possible leakage of end-user privacy, Federated Learning (FL) [1, 2] has emerged as a distributed paradigm for training a global model over massive devices without raw data transmission. In particular, participating end devices (i.e., clients) train locally on their own data and periodically upload local model updates to a central server for global aggregation [3].

The clients in FL are usually limited by lower bandwidth in wireless networks, whereas millions of model parameters have to be uploaded. For example, a large model with 488.08 MegaByte (MB) weights is trained for speech recognition [4]. After hundreds of iterations, the total communication of every client can grow to more than a PetaByte (PB) [5]. The mismatch between communication resources and transmission



Fig. 1: Comparison of dropout, where blue shading is importance of weight rows, and yellow masks denote dropped rows.

demand constitutes the communication bottleneck of FL. As the uplink is typically much slower than the downlink, e.g., the T-Mobile 5G wireless network at 110.6 Mbps down vs. 14.0Mbps up [6], it is indispensable to design communicationefficient FL schemes for mitigating uplink overhead.

Several pioneering studies have attempted to alleviate the uplink burden [7–10]. A feasible solution is to transmit compressed parameters *after* local training (i.e., sketched compression [7]), which learns a *full* model update and compresses it. Yet this method inevitably introduces the noise to models, and the noise is accumulated over long-term learning, leading to accuracy degradation [7, 11]. Another solution is model compression *in* local training, where clients train on local *shrunk* models. It is flexible for clients to adjust compressed model structures based on local data. Federated Dropout (FD) [12–15] is a prominent approach for model compression in local training, which dynamically drops fractional neurons for each client. It implies that fractional rows or columns of weight matrices are zeroed and not uploaded to the server.

However, existing FD works still face two challenges: unguaranteed accuracy and lack of theoretical analysis. Firstly, current mainstream FD researches concentrate on random dropout (such as FedDrop [12, 13]) or ordered dropout (such as Fjord [14], which drops partial back rows in weight matrices). They ignore the different importance of weights, meaning that some significant weights are dropped (see Fig. 1) at the expense of accuracy. AFD [15] advances federated dropout by designing score maps in the server to determine dropping structures, while clients cannot adjust dropping structures during local training, leading to less flexibility for dropout. In addition, FedDrop and AFD are limited in the application scope. They have not extended to recurrent connections of



Fig. 2: Comparison of test results for different methods.

Recurrent Neural Networks (RNN), where the deviation introduced by dropout is amplified in long sequences [16], resulting in poor performance [17]. Empirically, we execute next-word prediction using a Long Short-Term Memory (LSTM) model on the PTB dataset [18]. As shown in Fig. 2, FedDrop, AFD, and Fjord all reveal worse performance than a basic FL algorithm, FedAvg. Furthermore, there is no theoretical explanation provided in existing FD works. It is not convincing without error bound and convergence proof. Thus, there is a need for a novel dropout strategy with guaranteed accuracy and theoretical interpretation in federated settings.

Motivated by research at the intersection of Bayesian inference and deep learning [19], the dropout can be interpreted by the spike-and-slab distribution-based Bayesian inference, where each row of weight matrices in the Deep Neural Network (DNN) follows an independent spike-and-slab prior [20]. As stated in [21], spike-and-slab distributions zero out partial weight rows and sample the remaining rows from Gaussian [22, 23], equivalent to dropouts of corresponding activations in DNN. However, existing Bayesian interpretations of dropout [16, 21] focus on centralized training. For boosting federated dropout, it is crucial to embrace spike-and-slab distributionbased Bayesian inference in distributed FL scenarios.

In light of the above observations, we propose Federated learning with Bayesian Inference-based Adaptive Dropout (FedBIAD), which enables uplink overhead mitigation while improving performance and guaranteeing convergence. Specifically, we introduce Bayesian inference with spike-and-slab prior into local models, which infuses probabilistic distributions into models and is robust to overfitting on limited client data. On this basis, FedBIAD allows clients to adopt adaptive dropout based on importance indicators that evaluate the effect of each weight row on training loss, aiming at exploring a high-quality dropout for each client to enhance accuracy. Consequently, each client adaptively picks the sub-model structure with more accurate approximations and only transfers the corresponding parameters of the sub-model. Moreover, the extension of Bayesian inference provides a novel insight into the application of federated dropout to recurrent connections, and FedBIAD can empirically combine with existing sketched compressions, further alleviating the communication burden.

Our main contributions can be summarized as follows:

- Considering constrained uplink communication resources and unguaranteed performance, we propose a novel FL algorithm, FedBIAD, which allows clients to adaptively drop partial weight rows based on the trend of training loss. In FedBIAD, we additionally devise an importance indicator that measures the importance of weight rows for each client. This indicator contributes to looking for a high-quality dropout with performance improvement.
- To obtain theoretical support, we perform a formal analysis of the generalization error bound and convergence property. Theoretical results demonstrate that the convergence rate of the average generalization error of FedBIAD is minimax optimal up to a squared logarithmic factor.
- We conduct extensive experiments on image classification and next-word prediction. The results show that FedBIAD outperforms baselines in uplink costs and test accuracy even on non-IID datasets. Compared to status quo approaches, FedBIAD provides 2× reduction in uplink costs with an accuracy increase of up to 2.41%, further shortening the training time by up to 72%. We empirically combine FedBIAD with a sketched compression, DGC [4], which reduces up to 2× uplink costs while improving accuracy by up to 2.26% compared with naive DGC.

II. RELATED WORK

The communication bottleneck of FL has attracted tremendous attention, and some efforts have been devoted to solving this challenge, which is roughly divided into two directions: decreasing the total communication rounds and reducing transmitted parameters per round.

Decreasing communication rounds. FedAvg [1] performs multiple local training iterations in a round to reduce communication frequency. Yu and Jin [24] find that the dynamic increase of batch size is beneficial for fast convergence to reduce communication rounds. Stremmel and Singh [25] propose that pretraining models could speed up convergence and lessen rounds. However, these approaches cannot avoid the simultaneous transmission of a huge number of parameters in the wireless communication link for each round, leading to network exhaustion and transmission deceleration.

Reducing transmitted parameters. There are mainly two strategies. The first type is reducing the number of clients that upload parameters to the server. For example, CMFL [8] excludes the clients with irrelevant updates from parameter uploading, and FedMed [26] considers that only clients with lower training loss are allowed to transmit parameters. Although the above methods mitigate uplink costs, they waste computation resources of devices that train locally but do not participate in global aggregation. The second type is reducing the transmitted parameters of each client. SignSGD [11] and FedPAQ [9] quantize weights into low-precision values to reduce communication volume. DGC [4] and SmartIdx [10] propose to transfer fractional gradients with higher magnitudes. These sketched approaches compress weights after local training, inevitably pulling noise into models. The noise is accumulated in the long training, adversely affecting model accuracy. Besides, low rank [7] enforces every weight matrix as the product of two low-rank matrices, one of which is fixed and the other is trained and transmitted. This fixed structure restricts model updates [15], resulting in poor performance [7].

Instead of the fixed structure, federated dropout [12, 13] dynamically selects smaller models by the dropout of neurons to alleviate the communication burden. Caldas et al. [12] first extend dropout to FL, which randomly drops a fixed number of neurons for each participant client. This random dropout ignores the importance of weights, so some significant weights are discarded, resulting in the sacrifice of accuracy. More recently, FjORD [14] proposes ordered dropout that directly drops adjacent neurons of models. It assumes that partial back rows in the weight matrix of each model layer have less effect on accuracy, which can be dropped. However, this ordered theory has only been proved in linear mapping and has not been derived in non-linear DNN. Besides, FedMP [27] directly prunes weights with lower magnitudes in clients without considering their effect on training loss. These methods also cannot achieve satisfying performance. Furthermore, although existing works have been evaluated through extensive experiments, there is no theoretical analysis to guarantee reliability. Without error bound and convergence proof, we cannot trust them to achieve consistent performance in FL.

Different from the above methods, this work studies federated learning with adaptive dropout, where each client adaptively drops weight rows based on the importance indicator correlated with the local loss changes. Furthermore, considering the generalization properties of Bayesian inference, the convergence of average generalization error can be proven.

III. BAYESIAN INTERPRETATION OF DROPOUT

A. Formulations for Deep Neural Network

Deep Learning (DL) constructs an input-output mapping through a Deep Neural Network (DNN). Given a dataset (X, Y), for any $(x, y) \in (X, Y)$, there is an input x and an unknown true function f_0 such that $y = f_0(x)$. The goal of DL is to learn a DNN model f_{θ} such that $f_{\theta}(x) \approx f_0(x)$, where θ denotes the set of weights in the model.

We consider two types of commonly used DNNs: the nonrecurrent neural network and the Recurrent Neural Network (RNN). Starting by a non-recurrent neural network with Llayers, $f_{\theta} : \mathbb{R}^d \to \mathbb{R}$ is written recursively as:

$$x_{l} = \rho(W_{l}x_{l-1}), \ f_{\theta}(x) = x_{L} \text{ for } l = 1, \dots, L$$

where $x_0 = x$, ρ is an activation function, and W_l is the weight matrix in the *l*-th layer of DNN such that $\theta = \{W_1, \ldots, W_L\}$. The input dimension is *d*. For ease of analysis, we use an equal-width DNN as [21] and [28], i.e., the number of units in each hidden layer is equal to *D*, where $d \leq D$.

For sequence learning tasks, such as time series forecasting and next-word prediction, the RNN with memory correlation ability is more effective. In this case, the input is a sequence of feature vectors $[x_1, \ldots, x_L], x_l \in \mathbb{R}^d$, and f_θ can be expressed in a different form. The input sequence is mapped by

$$h_l = \varrho(W_x x_l + W_h h_{l-1}), \ f_\theta(x) = \phi(h_L) \text{ for } l = 1, \dots, L$$

with $h_0 = \overrightarrow{0}$. $W_x \in \mathbb{R}^{D \times d}$ is the input-hidden weight matrix, and $W_h \in \mathbb{R}^{D \times D}$ is the hidden-hidden weight matrix (denoted recurrent connections of RNN) such that $\theta = \{W_x, W_h\}$. Besides, ϱ and ϕ are activation functions.

We set N as the total number of weights in θ and J as the number of rows in all weight matrices. The \mathbf{w}_j denotes the *j*-th row of weight matrices. The unsparse number S is the number of nonzero weights in θ . In this way, the model architecture is determined by (S, L, D). $\Theta_{S,L,D}$ represents the solution space composed of all feasible weights.

B. Variational Bayesian Inference

From the Bayesian perspective, we consider θ as random variables following prior π . Given the dataset (X, Y), we aim to find out the posterior $\pi(\theta|X, Y)$, which is usually intractable because the posterior is high-dimensional and non-convex in DNN [29]. Variational Inference (VI) [30] is one of the most efficient solutions for the posterior studied in the last decade [31–33], which searches for a variational approximation to estimate $\pi(\theta|X, Y)$. Based on VI, [34] considers that the likelihood $p(y|x, \theta)$ could be replaced by $[p(y|x, \theta)]^{\alpha}$ for any $\alpha \in (0, 1)$, leading to the tempered posterior

$$\pi_{m,\alpha} \propto \sum_{i=1}^{m} \alpha \ln p(y_i | \boldsymbol{x}_i, \theta) \pi(\mathrm{d}\theta), \tag{1}$$

where *m* is the number of samples. The proof of concentration of the tempered posterior $\pi_{m,\alpha}$ needs fewer assumptions than $\pi(\theta|X, Y)$ [34]. Following it, we pay attention to a variational approximation $\tilde{\pi}$ of the tempered posterior $\pi_{m,\alpha}$.

For any $(x_i, y_i) \in (X, Y)$, $i \in \{1, ..., m\}$, the $p(y_i | x_i, \theta)$ follows a Gaussian with a likelihood variance σ^2 . Our objective is to explore a variational approximation $\tilde{\pi}$ to estimate the tempered posterior $\pi_{m,\alpha}$ for minimizing the loss function

$$\mathcal{L}(\tilde{\pi}) = \frac{\alpha}{2\sigma^2} \sum_{i=1}^{m} \int \left(y_i - f_{\theta}(\boldsymbol{x}_i) \right)^2 \tilde{\pi}(\mathrm{d}\theta) + KL(\tilde{\pi} \| \pi).$$
(2)

The second item from the right in (2) has been proven to approximate L2 regularisation [16, 22]. Hence, variational Bayesian inference avoids overfitting and easily learns from small samples. Inspired by [21], Definition 1 gives an expression for the generalization error of variational approximation.

Definition 1. The generalization error of the variational approximation $\tilde{\pi}$ is $G_e(\tilde{\pi}) = \mathbb{E} \left[\int \|f_{\theta} - f_0\|_2^2 \tilde{\pi}(\mathrm{d}\theta) \right].$

C. Bayesian Inference-based Dropout

The Bayesian inference with spike-and-slab distribution can act as a relevant proxy of the dropout [21]. As mentioned in [13], the dropout technique zeros out a fixed number of weights, while the idea of setting a subset of weights to zero can be realized by placing spike-and-slab distributions over weights [22]. Motivated by [16] and [22], we define the spikeand-slab distributions to factorize over the weight matrices, where each weight row \mathbf{w}_i follows

$$\tilde{\pi}(\mathbf{w}_j) = p\delta(0) + (1-p)\mathcal{N}(\boldsymbol{\mu}_j, \tilde{s}^2 I),$$
(3)

with dropout rate p given in advance, the variational parameter (row vector) μ_j learned in the local training, and posterior variance \tilde{s}^2 . Here, $\delta(0)$ is an impulse function. We suppose that posterior variance \tilde{s}^2 is constant for any weight rows, which is common in Bayesian variational inference, as referred to [16, 21]. The precise setting of the posterior variance \tilde{s}^2 for FedBIAD will be detailed in Section IV-F. Based on the setting of constant posterior variance, we conduct extensive experiments, and the results are shown in Section V-B.

For better characterizing the spike-and-slab distributions of weight rows, we define a binary vector $\boldsymbol{\beta} = [\beta_1, \dots, \beta_J]^\top \in \{0, 1\}^J$ as the dropping pattern to represent whether weight rows are dropped. If the dropping label β_j of the *j*-th row is zero, then \mathbf{w}_j is dropped; otherwise, \mathbf{w}_j is held for training. Given dropout rate *p*, we compute the unsparse number $S = (1 - p)J \times D$ and determine the set of all possible dropping patterns \mathcal{Z}_N^S . Sampling $\boldsymbol{\beta}$ from \mathcal{Z}_N^S , the spike-and-slab distribution of \mathbf{w}_j is rewritten as

$$\tilde{\pi}(\mathbf{w}_j) = \beta_j \mathcal{N}(\boldsymbol{\mu}_j, \tilde{s}^2 I) + (1 - \beta_j) \delta(0), \tag{4}$$

where $j \in \{1, ..., J\}$. This work looks for high-quality dropping patterns based on importance indicators of weight rows to reduce uplink costs while achieving excellent performance.

IV. FEDERATED LEARNING WITH BAYESIAN INFERENCE-BASED ADAPTIVE DROPOUT (FEDBIAD)

In this section, we first provide the problem formulation. Then, we elaborate on the details of FedBIAD, where each client adaptively drops fractional weight rows based on training loss changes and maintains an importance indicator, aiming at finding an effective dropping pattern to decrease loss. Moreover, we theoretically analyze the convergence of the average generalization error of FedBIAD.

A. Problem Formulation

Given K devices formed a set \mathcal{K} , each device $k \in \mathcal{K}$ owns its data \mathcal{D}^k and true function f_0^k such that $y^k = f_0^k(\boldsymbol{x}^k)$ for any $(\boldsymbol{x}^k, y^k) \in \mathcal{D}^k$. We aim to look for a global variational approximation $\tilde{\pi}^g = \mathcal{N}(U, \tilde{s}^2 I)$ from a variational set [21] $\mathcal{F}_{S,L,D} \subseteq \Theta_{S,L,D}$ to minimize the average loss over all clients:

$$\mathcal{L}^* = \min_{\tilde{\pi}^g \in \mathcal{F}_{S,L,D}} \left\{ \frac{1}{K} \sum_{k=1}^K \frac{\mathcal{L}^k(\tilde{\pi}^g)}{|\mathcal{D}^k|} \right\}.$$
 (5)

Here, \mathcal{L}^k denotes the loss of the k-th client over \mathcal{D}^k that can be calculated by (2), in which m is replaced by $|\mathcal{D}^k|$.

Instead of using weights, we learn the variational approximation distribution in optimization problem (5) of average loss minimization. Each client k owns its local variational approximation $\tilde{\pi}^k$, which is determined by the dropping pattern β^k , local variational parameters $U^k = [\mu_1^k, \ldots, \mu_J^k]^\top$, and the posterior variance \tilde{s}^2 . As stated above, we assume that \tilde{s}^2 is a constant, so client k learns U^k and explores β^k during local training. In this setting, client k needs to transmit nonzero elements of $\beta^k \circ U^k$ to the server, where we define

$$\boldsymbol{\beta}^{k} \circ U^{k} = [\beta_{1}^{k} \boldsymbol{\mu}_{1}^{k}, \dots, \beta_{J}^{k} \boldsymbol{\mu}_{J}^{k}]^{\top}.$$
 (6)



Fig. 3: An overview of FedBIAD.

Concretely, for any $j \in \{1, ..., J\}$, the variational parameter μ_i^k will be transmitted only if $\beta_i^k \neq 0$.

B. Overview of FedBIAD

As shown in Fig. 3, the procedure of FedBIAD in global round r is as follows:

- Step 1: The server selects the client set C_r and sends global variational parameters U_{r-1} to each client k ∈ C_r.
- Step 2: For each client k ∈ C_r, the local model is initialized by θ^{k,0}_r ~ N(U_{r-1}, š²I). Then, fractional weight rows of the local model are dropped according to the dropping pattern β^k_r, and the remaining sparse model is updated on local data. During local iterative training, the dropping pattern is adaptively adjusted based on changing trends of training loss. The experience of dropout is recorded in the weight score vector to characterize the importance of weight rows, which contributes to looking for a powerful dropping pattern for the client.
- Step 3: After V training iterations, client k ∈ C_r uploads nonzero elements of variational parameters and binary dropping pattern (much less than variational parameters and can even be ignored in uplink costs) to the server.
- Step 4: The server reconstructs complete variational parameters based on the received binary dropping pattern for client k ∈ C_r, and performs global aggregation to calculate new global variational parameters U_r (§IV-E).

Specifically, FedBIAD is divided into two stages by a preset boundary R_b of the global round. The difference between the two stages is the determination schemes of dropping patterns. In stage one (i.e., global round $r \leq R_b$), each client randomly samples the initial dropping pattern from \mathcal{Z}_N^S , and then adaptively adjusts the dropping pattern based on the trend of training loss (§IV-C) to find a better dropping pattern during training. If global round $r > R_b$, FedBIAD enters stage two, where the dropping pattern is determined by the experiencebased importance indicator (§IV-D).

C. Adaptive Dropout Correlated to Loss Trend

Our main idea is to explore the dropping pattern based on the trend of local training loss. As different weight rows have different effects on loss, we should drop the rows that cannot



Fig. 4: The dropout based on the importance indicator. The blue shades are the normalized importance of weight rows. The green and yellow masks indicate that they are zeroed.

facilitate loss reduction. Firstly, we preset the dropout rate p, which determines the unsparse number $S = (1 - p)J \times D$. Given S, the set \mathcal{Z}_N^S is specific. The $\beta_r^{k,0} = [\beta_{r,1}^{k,0}, \dots, \beta_{r,J}^{k,0}]^\top$ is defined as an initial dropping pattern of client k in round r.

After receiving global variational parameters U_{r-1} , client k initializes the local model $\theta_r^{k,0} \sim \mathcal{N}(U_{r-1}, \tilde{s}^2 I)$, randomly samples the dropping pattern $\beta_r^{k,0}$ from \mathcal{Z}_N^S , and then zeros out each weight row \mathbf{w}_j whose dropping label $\beta_{r,j}^{k,0} = 0$ in local model $\theta_r^{k,0}$. Subsequently, the remaining sparse model is trained locally. For the v-th iteration, the dropping pattern is denoted as $\beta_r^{k,v} = [\beta_{r,1}^{k,v}, \dots, \beta_{r,J}^{k,v}]^\top$, $v \in \{1, \dots, V\}$, and the variational parameters $U_r^{k,v} = [\boldsymbol{\mu}_{r,1}^{k,v}, \dots, \boldsymbol{\mu}_{r,J}^{k,v}]^\top$ update by

$$U_r^{k,v+1} = U_r^{k,v} - \eta \big[\boldsymbol{\beta}_r^{k,v} \circ \nabla_U \mathcal{L}^k \big(\tilde{\pi}_r^{k,v} (\boldsymbol{\beta}_r^{k,v}, U_r^{k,v}) \big) \big], \quad (7)$$

where η is the learning rate and $\tilde{\pi}_{r}^{k,v} = \beta_{r}^{k,v} \circ \mathcal{N}(U_{r}^{k,v}, \tilde{s}^{2}I).$

During training, client k calculates the loss gap between adjacent τ iterations, described as:

$$\Delta \mathcal{L}_{r}^{k,v} = \bar{\mathcal{L}}_{r}^{k,v} - \bar{\mathcal{L}}_{r}^{k,v-\tau}, \ v \ge 2\tau,$$
(8)

where $\bar{\mathcal{L}}_{r}^{k,v} = \sum_{i=v-\tau+1}^{v} \mathcal{L}^{k}(\tilde{\pi}_{r}^{k,i})$ is the average loss of the $(v-\tau+1)$ -th iteration to the *v*-th iteration in the global round r. If $\Delta \mathcal{L}_{r}^{k,v} \leq 0$, the current dropping pattern $\beta_{r}^{k,v}$ is favorable for loss decrease, which is used for the next τ iterations; otherwise, client k resamples $\beta_{r}^{k,v+1} = \ldots = \beta_{r}^{k,v+\tau}$ from \mathcal{Z}_{N}^{S} for training in the next τ iterations. After V iterations, client k drops zero row vectors, and transfers the variational parameters of the remaining weight rows to the server. Through dropout, clients can reduce transmitted parameter size so the uplink overhead can be alleviated. Note that, the amount of reduction in uplink costs is determined by the preset dropout rate p.

An intuitive dropout example for CNNs. In the above description, we elaborated on the dropout for fully connected neural networks and RNNs, where the weight matrix for each model layer is two-dimensional, and we can view weights by rows [16, 22]. Extending to Convolutional Neural Networks (CNNs), we view weights by filters and dropout is filter-wise, as referred to [12, 27]. Each client k possesses a filter-wise dropping pattern $\beta_{r,v}^{k,v} = [\beta_{r,1}^{k,v}, \ldots, \beta_{r,J}^{k,v}]^{\top}$ for the local CNN in round r. For each convolutional layer in CNN, if the j-th filter has the dropping label $\beta_{r,j}^{k,v} = 0$, all weights in this

Algorithm 1: FedBIAD

Input: dropout rate p, client selection fraction κ , the number of local iterations V, boundary of stages R_b . **Initialize:** global variational parameters U_0 , the number of selected clients $c \leftarrow \max(|\kappa \cdot K|, 1)$, the dropping pattern set \mathcal{Z}_N^S , posterior variance \tilde{s}^2 **Aggregate:** // Run on the server 1: for each round r = 1, 2, ..., R do 2: $C_r \leftarrow (\text{random set of } c \text{ clients})$ Send global U_{r-1} to client $k \in C_r$ 3: for each client $k \in C_r$ in parallel do $\beta_r^{k,V}, \{\mu_{r,j}^{k,V}\} \leftarrow \text{ClientUpdate}(U_{r-1}, r)$ 4: 5: 6: Reconstruct $\beta_r^{k,V} \circ U_r^{k,V}$ and calculate U_r by (10) 7: 8: end for ClientUpdate (U_{r-1}, r) : // Done by clients 9: Initialize $U_r^{k,0} \leftarrow U_{r-1}$ and $\theta_r^{k,0} \sim \mathcal{N}(U_r^{k,0}, \tilde{s}^2 I)$ 10: if $r \leq R_b$ then $\beta_r^{\overline{k,0}} = \ldots = \beta_r^{k,2\tau} \leftarrow \text{Randomly sample from}$ 11: // stage one 12: else $\beta_r^{k,0} = \ldots = \beta_r^{k,V} \leftarrow \text{Initialize based on weight}$ score vector E^k // stage two 13: 14: end if 15: for each iteration v = 0, 1, ..., V - 1 do $\begin{array}{l} U_r^{k,v} \sim \tilde{\pi}_r^{k,v} = \beta_r^{k,v} \circ \mathcal{N}(U_r^{k,v}, \tilde{s}^2 I) \\ U_r^{k,v+1} \leftarrow U_r^{k,v} - \eta \big[\beta_r^{k,v} \circ \nabla_U \mathcal{L}^k(\tilde{\pi}_r^{k,v}) \big] \\ \text{if } r \leq R_b \text{ and } v > \tau \text{ and } v \, \% \, \tau = 0 \text{ then} \end{array}$ 16: 17: 18: Calculate $\Delta \mathcal{L}_{r}^{k,v}$ using (8) if $\Delta \mathcal{L}_{r}^{k,v} > 0$ then $\beta_{r}^{k,v+1} = \ldots = \beta_{r}^{k,v+\tau} \leftarrow$ Randomly sample from \mathcal{Z}_{N}^{S} 19: 20: 21: else 22: $\boldsymbol{\beta}_{r}^{k,v+1} = \ldots = \boldsymbol{\beta}_{r}^{k,v+\tau} \leftarrow \boldsymbol{\beta}_{r}^{k,v}$ 23: end if 24: 25: end if // only execute in stage one Update weight score vector E^k by (9) 26: 27: end for 28: return $\beta_{r}^{k,V}$, $\{\mu_{r,j}^{k,V} | \mu_{r,j}^{k,V} \in U_{r}^{k,V}, \beta_{r,j}^{k,V} \neq 0\}$

filter are zeroed out, meaning that the *j*-th filter is dropped. During local training, each client adaptively adjusts the filterwise dropping pattern according to the loss gap calculated by (8), as mentioned above. After that, the dropped filters in the local CNN will not be transmitted to the server.

D. Experience-based Importance Indicator

We design the weight score vector $E^k = [E_1^k, \ldots, E_J^k]$ for each client k, which is row-wise for fully connected neural networks or RNNs, but filter-wise for CNNs. In the training process described in Section IV-C, client k records adaptive dropout times of each weight row for fully connected neural networks or RNNs in E^k . While for CNN, client k reports the adaptive dropout times of each filter in E^k . Assuming that



Fig. 5: FedBIAD with a sketched compression - each client (1) drops partial rows, (2) compresses variational parameters of the remaining rows, and (3) uploads compressed variational parameters. The server (4) decompresses and (5) reconstructs weight matrices, and aggregates recovered variational parameters, which are sent to the newly selected clients (6). And then, clients repeat dropping and compression in the next round as (7) and (8). Green and yellow masks indicate that rows are zeroed out.

client k holds the j-th weight row/filter \mathbf{w}_j in the v-th iteration, the score E_i^k of \mathbf{w}_j is updated iteratively by

$$E_j^k = \begin{cases} E_j^k + 1, & \text{if } \Delta \mathcal{L}_r^{k,v} \le 0, \\ E_j^k + e_j, & \text{if } \Delta \mathcal{L}_r^{k,v} > 0. \end{cases}$$
(9)

If the dropping label $\beta_j^{k,v+1} = 1$ for the weight row \mathbf{w}_j , then $e_j = 1$; otherwise, $e_j = 0$.

As FL progresses until global round $r > R_b$, FedBIAD enters stage two, where the accumulated dropout experiences are enough to be regarded as the importance indicator. This experience-based importance indicator can guide the client to select an effective dropping pattern, which is beneficial for loss reduction. Hence, in stage two, client k can set the dropping pattern based on E^k instead of random sampling, as shown in Fig. 4. The weight score vector determines the dropping pattern as follows. If global round $r > R_b$, client k calculates the threshold λ_r^k that is the p-quantile of E^k . If the score $E_j^k > \lambda_r^k$, then the dropping label $\beta_{r,j}^{k,0} = \ldots = \beta_{r,j}^{k,V} = 1$ for the j-th weight row/filter; otherwise, $\beta_{r,j}^{k,0} = \ldots = \beta_{r,j}^{k,V} = 0$.

E. Global Aggregation

After V training iterations on local data, each client $k \in C_r$ transmits nonzero elements of the latest variational parameters $\{\boldsymbol{\mu}_{r,j}^{k,V} | \boldsymbol{\mu}_{r,j}^{k,V} \in U_r^{k,V}, \beta_{r,j}^{k,V} \neq 0, \text{ for } j = 1, \dots, J\}$ and the dropping pattern $\beta_r^{k,V}$ to the server. Subsequently, the server reconstructs complete variational parameters $\beta_r^{k,V} \circ U_r^{k,V}$ based on the received $\beta_r^{k,V}$, and performs global aggregation by averaging variational parameters [35]:

$$U_r = \frac{\sum_{k \in \mathcal{C}_r} |\mathcal{D}^k| \beta_r^{k,V} \circ U_r^{k,V}}{\sum_{k \in \mathcal{C}_r} |\mathcal{D}^k|}.$$
 (10)

Essentially, the global variational approximation $\tilde{\pi}^g_r$ in round r can be denoted as

$$\theta_r \sim \tilde{\pi}_r^g = \mathcal{N}(U_r, \tilde{s}^2 I),$$
(11)

where θ_r is the global weights in round r.

The entire process of FedBIAD is summarized in Algorithm 1, and Fig. 5 briefly depicts the iterative procedure. Moreover, inspired by [15], we can employ FedBIAD in combination with existing sketched compression methods to further lighten the communication burden. As shown in Fig. 5, variational parameters are compressed in steps (2) and (8).

F. Convergence Analysis

Based on Section III-B, FedBIAD explores a global variational approximation $\tilde{\pi}^g$ to estimate the tempered posteriors of client-side data. Considering a global model f_{θ} with L layers whose weights θ follow $\tilde{\pi}^g$, we define the unsparse number Sas the number of nonzero weights in θ and D as the dimension of hidden layers in the global model. In this way, the global model is determined by (S, L, D), and $\Theta_{S,L,D}$ represents the solution space composed of all feasible weights. The input dimension of the global model is d. As discussed in Section IV-A, each device $k \in \mathcal{K}$ owns its data \mathcal{D}^k and unknown true function f_0^k such that $y^k = f_0^k(\boldsymbol{x}^k)$ for any $(\boldsymbol{x}^k, y^k) \in \mathcal{D}^k$.

We define m as the client-side total input data, which is associated with the training round r. Considering that different clients have different amounts of local data, after r rounds, the minimum amount of client-side total input data is denoted as $m_r = r \times V \times \min\{|\mathcal{D}^1|, \ldots, |\mathcal{D}^K|\}$, where V is the number of training iterations in each round. To analyze the convergence of the average generalization error in FedBIAD, we start with some assumptions.

Assumption 1. The activation functions ρ , ρ , and ϕ are 1-Lipschitz continuous.

Assumption 2. The absolute values of all weights in optimal global model θ^* have an upper bound of $B \ge 2$.

Assumption 1 and 2 are common in Bayesian convergence analysis works [21, 28], which are realistic. The activation functions (i.e., relu function ρ , tanh function ρ , sigmoid function ϕ) we used are actually 1-Lipschitz continuous. Besides, the optimal global model is denoted by $\theta^* =$ $\arg\min_{\theta\in\Theta_{S,L,D}} \frac{1}{K} \sum_{k=1}^{K} ||f_{\theta} - f_{0}^{k}||_{2}^{2}$, which is fixed. Hence, the absolute values of all weights in θ^{*} are fixed, and they must have an upper bound.

Based on [21, 28] and Definition 1, the average generalization error of global model learned by FedBIAD is the expected average of the squared L2-distance between the global model f_{θ} and local unknown true functions $\{f_0^k | k \in \mathcal{K}\}$, denoted by:

$$\mathbb{E}\bigg[\frac{1}{K}\sum_{k=1}^{K}\int \|f_{\theta} - f_{0}^{k}\|_{2}^{2}\tilde{\pi}^{g}(\mathrm{d}\theta)\bigg].$$
(12)

The constant posterior variance is set to

$$\tilde{s}^{2} = \frac{S}{16md^{2}}\log(3D)^{-1}(2BD)^{-2L}$$
(13)
$$\left\{ \left(d+1+\frac{1}{BD-1}\right)^{2} + \frac{1}{(BD)^{2}-1} + \frac{2}{(BD-1)^{2}} \right\}^{-1}.$$

In FedBIAD, the posterior variances of local variational approximations on clients and the global variational approximation on the server are the same in each round. Hence, clients and the server do not exchange posterior variances \tilde{s}^2 and only compute \tilde{s}^2 via (13), which is beneficial for communication efficiency. Based on the setting of posterior variance in (13), we can derive the upper bound of the average generalization error expressed by (12) for FedBIAD in Theorem 1.

Theorem 1. Let Assumption 1 and 2 hold, considering different numbers of local data in different clients such that the minimum amount of client-side total input data up to round r is denoted as $m_r = r \times V \times \min\{|\mathcal{D}^1|, \ldots, |\mathcal{D}^K|\}$, for any $\alpha \in (0, 1)$, we obtain the average generalization error of global model f_{θ} learned by FedBIAD in the server:

$$\mathbb{E}\left[\frac{1}{K}\sum_{k=1}^{K}\int \|f_{\theta} - f_{0}^{k}\|_{2}^{2}\tilde{\pi}^{g}(\mathrm{d}\theta)\right]$$
$$\leq \frac{2\sigma^{2}}{\alpha(1-\alpha)}(1+\frac{\alpha}{\sigma^{2}})\varepsilon_{m_{r}}^{S,L,D} + \frac{2}{K(1-\alpha)}\sum_{k=1}^{K}\xi^{k} \quad (14)$$

with

$$\varepsilon_{m_r}^{S,L,D} = \frac{SL}{m_r} \log(2BD) + \frac{3S}{m_r} \log(LD) + \frac{SB^2}{2m_r} + \frac{2S}{m_r} \log\left(4d \max(\frac{m_r}{S}, 1)\right)$$
(15)

and

$$\xi^{k} = \inf_{\theta^{*} \in \Theta_{S,L,D}} \|f_{\theta^{*}} - f_{0}^{k}\|_{\infty}^{2},$$
(16)

where θ is the global weights computed by (11) and σ^2 is the likelihood variance defined in Section III-B.

Through Theorem 1, we get the upper bound of the average generalization error of global model, which can ensure convergence of FedBIAD. Referring to [21], if local true functions $\{f_0^k | k \in \mathcal{K}\}$ are actually neural networks with structure (S, L, D), the term ξ^k denoted by (16) on the right-hand side of (14) vanishes. Then, we only need to analyze the first term on the right-hand side of (14), where $\varepsilon_{m,L,D}^{S,L,D}$ is calculated

by (15). According to (15), $\varepsilon_{m_r}^{S,L,D}$ apparently declines with the increasing of client-side total input data m_r . While m_r increases with the growth of training round r. Therefore, as the round grows, the upper bound of the generalization error of FedBIAD decreases, and FedBIAD gradually converges.

However, if local true functions $\{f_0^k | k \in \mathcal{K}\}\$ are not neural networks with structure (S, L, D) like the global model f_{θ} , we have to consider the term ξ^k . Motivated by [28, 36], we assume that $\{f_0^k | k \in \mathcal{K}\}\$ are γ -Hölder smooth functions with $0 < \gamma < d$. According to Lemma 5.1 in [36] and Corollary 3 in [21], there exist constants C, C' such that $\xi^k \leq Cm_r^{\frac{-2\gamma}{2\gamma+d}} \cdot \log^2 m_r$ and $\varepsilon_{m_r}^{S,L,D} \leq C'm_r^{\frac{-2\gamma}{2\gamma+d}} \cdot \log^2 m_r$. Then, we have

$$\mathbb{E}\left[\frac{1}{K}\sum_{k=1}^{K}\int \|f_{\theta} - f_{0}^{k}\|_{2}^{2}\tilde{\pi}^{g}(\mathrm{d}\theta)\right] \leq C_{1}m_{r}^{\frac{-2\gamma}{2\gamma+d}} \cdot \log^{2}m_{r},$$
(17)

where $C_1 > 0$ is a constant. In addition, based on Theorem 8 in [37], there exists a constant $C_2 > 0$ such that

$$\inf_{\theta} \sup_{\{f_0^k\}_{k=1}^K} \frac{1}{K} \sum_{k=1}^K \int \|f_{\theta} - f_0^k\|_2^2 \tilde{\pi}^g(\mathrm{d}\theta) \ge C_2 m_r^{\frac{-2\gamma}{2\gamma+d}}.$$
 (18)

The (17) gives an upper bound of generalization error for Fed-BIAD with γ -Hölder smooth functions, while (18) provides the minimax lower bound [28, 37] of generalization error for FedBIAD. Both (17) and (18) have the same term of $m_r^{\frac{-2\gamma}{2\gamma+d}}$, through which we can derive the average generalization error of FedBIAD converges at the minimax rate $m_r^{\frac{-2\gamma}{2\gamma+d}}$ up to a squared logarithmic factor for the expected L_2 -distance.

Note that, the setting of posterior variance can affect the generalization error bound. The optimal variance is derived in (13), which is used to derive the minimum generalization error bound in (14). Furthermore, FedBIAD only exchanges variational model parameters without sharing client-side data. Therefore, it does not introduce extra privacy concerns and existing FL privacy-preserving methods can be directly applied.

V. EXPERIMENT EVALUATION

In this section, extensive experiments are conducted on five datasets for image classification and next-word prediction tasks to evaluate the performance of FedBIAD compared to the state-of-the-art methods.

A. Experimental Settings

Datasets. We consider five datasets for the experiment evaluation: MNIST [38], Fashion-MNIST (FMNIST) [39], Penn TreeBank (PTB) [18], WikiText-2 [40], and Reddit [41].

MNIST and FMNIST are 10-class image datasets containing 60,000 training data and 10,000 test data. MNIST is for digital handwriting classification, while FMNIST consists of pictures of fashion clothes, and its task is more challenging than simple MNIST. For MNIST and FMNIST, the number of clients is 1000, and we utilize the non-IID partitioning strategy in [28].

PTB, WikiText-2, and Reddit are three English datasets widely used for next-word prediction [41, 42]. The PTB has a 5.1M training corpus, smaller than most modern datasets. The

WikiText-2 is over 2 times larger than the PTB, featuring a vocabulary of more than 30,000 words. Both of them are IID. We randomly sample data without overlap and allocate them to 100 clients. For Reddit, the data are non-IID and the top 100 users with more data are chosen as clients, so that different clients have different sample sizes. The data in clients are split into the training set, validation set, and test set.

Baselines. We compare with the following baselines:

- FedAvg [1]: FedAvg is a pioneering work of FL, where each participating client periodically transmits all weights of the local model to the server.
- FedDrop [12]: Each client randomly drops partial units of DNN, which applies to convolutional and Fully Connected (FC) layers and does not extend to recurrent layers.
- AFD [15]: AFD builds upon FedDrop and proposes to train and transmit only the necessary weights that are not affected by the dropout, but the dropout is only applied to non-recurrent connections of models.
- FedMP [27]: FedMP assumes that small weights have a weak effect on model accuracy, where each client prunes weights with lower absolute values.
- Fjord [14]: Each client extracts the lower footprint submodel by ordered dropout, which preferentially drops the right-most adjacent neurons of each layer. The left-most neurons are used by more clients during training.
- HeteroFL [43]: HeteroFL reduces the number of local weights by shrinking the width of hidden layers, where different clients could adopt different shrinkage ratios.

Simulation Parameters. In terms of parameter settings, we mainly refer to [44] for image classification tasks and [42, 45] for next-word prediction tasks. Concretely, we adopt a fully connected model that uses a hidden layer, a ReLU activation function, and a softmax layer for image classification. The number of hidden units is set to 128 on MNIST and 256 on FMNIST. We conduct various experiments with stochastic gradient descent (SGD) optimizer. Under next-word prediction tasks, the model consists of an embedding layer with 300 units, a two-layer LSTM with 300 hidden units, and a Fully Connected (FC) layer. We use the SGD optimizer with the clipped gradient norm. The iteration interval is set to $\tau = 3$, and the client selection ratio is $\kappa = 0.1$. All methods execute 60 global rounds, and the boundary of the stage is $R_b = 55$.

Dropout rate settings. Referring to [15], empirical dropout rates are between 0.1 to 0.5, which are associated with model scales. Different datasets require different-scale models [13]. For example, PTB is more challenging than simple MNIST, so the model for training PTB is bigger than MNIST. Large-scale models are often possible to use higher dropout rates [15]. For small-scale models (such as 531KB for MNIST), high rates make shrinking models unable to extract accurate features, degrading accuracy [13]. For MNIST, if dropout rate p = 0.5, the accuracy results of FedDrop, AFD, FedMP, and *FedBIAD* are 94.45, 94.26, 94.45, and 94.69, lower than p = 0.2 (see Table I). Thus, different dropout rates are necessary for different datasets requiring different model scales. Motivated

TABLE I: Test accuracy (i.e., 'Acc') and per-round upload parameter size (i.e., 'Upload Size') of different methods.

Dataset	Method	Acc (%)	Upload Size	Save Ratio
	FedAvg	95.06±0.03	531KB	1 ×
MNIST	FedDrop	$95.03 {\pm} 0.05$	424KB	1.25 ×
	AFD	$94.49 {\pm} 0.10$	424KB	1.25 ×
	FedMP	$95.09 {\pm} 0.03$	477KB	1.10 ×
	FjORD	$94.93{\scriptstyle\pm0.08}$	437KB	1.21 ×
	HeteroFL	$94.98{\scriptstyle\pm0.06}$	432KB	1.23 ×
	FedBIAD	95.20±0.11	424KB	1.25 ×
	FedAvg	81.18±1.09	1.1MB	1 ×
	FedDrop	81.12 ± 0.47	530KB	2 ×
	AFD	$82.37 {\pm} 0.37$	530KB	2 ×
FMNIST	FedMP	82.40 ± 0.26	862KB	1.3 ×
	FjORD	82.64 ± 0.10	718KB	1.5 ×
	HeteroFL	82.68 ± 0.51	685KB	1.6 ×
	FedBIAD	83.59±0.13	530KB	2 ×
	FedAvg	$28.54{\pm}0.15$	29.8MB	1 ×
	FedDrop	27.81 ± 0.21	23.8MB	1.25 ×
	AFD	$28.67 {\pm} 0.03$	22.4MB	1.3 ×
PTB	FedMP	28.76 ± 0.20	22.7MB	1.3 ×
	FjORD	27.88 ± 0.18	21.4MB	1.4 ×
	HeteroFL	26.80 ± 0.42	20.4MB	1.5 ×
	FedBIAD	29.85 ±0.15	16.4MB	2 ×
	FedAvg	$31.86{\pm}0.05$	75.3MB	1 ×
WikiText-2	FedDrop	32.02 ± 0.55	57.9MB	1.3 ×
	AFD	31.20 ± 0.64	56.5MB	1.3 ×
	FedMP	32.53 ± 1.48	59.1MB	1.3 ×
	FjORD	31.16 ± 0.03	54.0MB	1.4 ×
	HeteroFL	31.84 ± 0.64	52.9MB	1.4 ×
	FedBIAD	33.16 ±0.97	39.1MB	2 ×
Reddit	FedAvg	$31.68{\scriptstyle\pm0.54}$	29.8MB	1 ×
	FedDrop	31.84 ± 0.08	24.1MB	1.25 ×
	AFD	32.26 ± 0.11	22.5MB	1.3 ×
	FedMP	31.06 ± 0.19	22.7MB	1.3 ×
	FjORD	31.35 ± 0.38	21.4MB	1.4 ×
	HeteroFL	31.24 ± 0.11	20.4MB	1.5 ×
	FedBIAD	33.93±0.28	16.4MB	2 ×

by [13, 15], we set lower dropout rate p = 0.2 for MNIST with small-scale model (< 1M), while other four datasets requiring large-scale models (\geq 1M) use the same dropout rate p = 0.5. This selection strategy for dropout rates is feasible in practice.

B. Experimental Results

Performance Comparison. Table I shows the performance results of different methods on test data, where 'Save Ratio' is the saving multiples in upload parameter size per round compared to FedAvg, and the results are obtained in a NVIDIA Tesla V100 GPU with 32GB. Besides, 'Upload Size' in Table I has included the size of transmitted binary dropping pattern β . Although each hidden layer has an independent row/filter size, the number of dropping labels for these rows/filters in all hidden layers is much less than the number of model weights. Besides, each dropping label is 1bit, while each weight is 32bit. Therefore, the size of β is much smaller than the model weights. For example, β in the Reddit dataset is 0.3KB, much smaller than the original model size of 29.8MB. Note that, for next-word prediction, we follow [2] to regard top-3 accuracy as the evaluation metric of model performance because mobile keyboards generally include three candidates, while the

TABLE II	: The comparison	between sketched	compression	methods and	l FedBIAD	combined	with DGC	on five	datasets.
----------	------------------	------------------	-------------	-------------	-----------	----------	----------	---------	-----------

Method	s / Metrics	FedPAQ [9]	SignSGD [11]	STC [5]	DGC [4]	AFD+DGC [15]	Fjord+DGC [14]	FedBIAD+DGC
MNIST	Accuracy (%)	94.90 ±0.09	92.04 ±0.55	90.56±0.17	94.84±0.11	94.39±0.20	94.93±0.03	95.22±0.11
	Upload size	129KB	16KB	3KB	3KB	2KB	2KB	2KB
	Save ratio	4 ×	33 ×	177 ×	177 ×	265 ×	265 ×	265 ×
FMNIST	Accuracy (%) Upload Size Save Ratio	$ \begin{array}{c c} 78.64 \pm 0.02 \\ 258 \text{KB} \\ 4 \times \end{array} $	76.57±0.43 33KB 34 ×	81.13±0.43 6KB 188 ×	80.64±0.09 4KB 281 ×	81.96±0.43 3KB 375 ×	82.16±0.56 3KB 375 ×	82.96 ±0.03 3KB 375 ×
РТВ	Accuracy (%) Upload Size Save Ratio	$\begin{array}{c c} 28.60 \pm 0.01 \\ \hline 7.1 \text{MB} \\ 4 \times \end{array}$	23.76±0.24 908KB 33 ×	24.42±0.46 148KB 206 ×	28.10±0.33 95KB 321 ×	27.74±0.10 71KB 429 ×	27.50±0.24 71KB 429 ×	28.77±0.05 53KB 575 ×
WikiText-2	Accuracy (%)	32.04±0.02	30.62±0.42	28.92 ±0.91	31.58±0.06	31.24±0.16	30.92±0.25	33.78±0.43
	Upload Size	18.8MB	2.4MB	374KB	215KB	180KB	179KB	126KB
	Save Ratio	4 ×	32 ×	206 ×	359 ×	428 ×	430 ×	612 ×
Reddit	Accuracy (%)	32.36±0.13	29.86±0.06	30.22±0.08	31.23±0.48	32.19±0.28	30.85±0.28	32.51±0.06
	Upload Size	7.1MB	960KB	148KB	97KB	88KB	86KB	52KB
	Save Ratio	4 ×	32×	206 ×	314 ×	346 ×	355 ×	587 ×



Fig. 6: Training loss and test accuracy versus rounds on MNIST and WikiText-2.

evaluation metric of the image classification is top-1 accuracy. As shown in Table I, FedBIAD achieves consistent state-ofthe-art accuracy with minimal per-round upload parameters across all datasets. For image classification, FedBIAD reduces $2 \times$ uplink costs while improving accuracy by 2.41% on FMNIST compared to FedAvg. In terms of MNIST and FMNIST, the model architecture consists of several FC layers. Because both FedDrop and AFD can apply dropout to all FC layers, FedBIAD does not significantly outperform FedDrop and AFD in communication efficiency. However, for MNIST, FedBIAD increases accuracy by 0.17% and 0.71% compared to FedDrop and AFD. Similarly, FedBIAD shows 2.47% and 1.22% accuracy improvements on FMNIST.

We also observe from Table I that on next-word prediction, FedBIAD outperforms other baselines in both uplink communication efficiency and test accuracy, achieving a 2× reduction of uplink costs and up to 1.45% accuracy increase compared to FedAvg. Because FedDrop and AFD cannot be applied to recurrent connections of RNN models, both show smaller save ratios, meaning less reduction in uplink overhead. FedBIAD adaptively drops partial weight rows for recurrent connections, which provides more uplink savings with higher accuracy. Thus, FedBIAD has better communication efficiency than AFD and FedDrop when using LSTM (a typical RNN) layers on next-word prediction. Compared with FedDrop, FedBIAD provides a $1.6 \times$ reduction in uplink costs while increasing accuracy by 1.37% on Reddit. In comparison to AFD, Fed-BIAD compresses uplink costs by $1.5 \times$ with 0.97% accuracy improvement. Besides, FedBIAD reduces $1.4 \times$ uplink costs and is 2.17% more accurate than Fjord on Reddit.

Motivated by [15], we empirically combine FedBIAD with a sketched compression method, DGC [4], further alleviating communication overhead. We also compare FedBIAD with DGC against other sketched compression approaches, among which SignSGD [11] and FedPAQ [9] compress parameters via 1-bit and 8-bit quantizers, respectively. STC [5] integrates sparsification and quantization into a compression framework. Both STC and DGC require clients to upload the positions of compressed parameters. For fairness, we adopt the same position representation approach, where the position representation of each parameter occupies 64 bits [4]. The performance results are presented in Table II. We notice that FedBIAD with DGC consistently achieves the highest accuracy with the least uplink overhead than other methods. Compared to FedAvg, which does not involve any compression strategies, FedBIAD with DGC achieves up to $612 \times$ reduction in uplink overhead while improving accuracy by up to 2.43%. In addition, Fed-BIAD with DGC gives up to $3 \times$ better uplink compression



Fig. 7: Comparison of Local Training Time in a Round (LTTR) and Time-To-Accuracy (TTA) on different datasets.

than STC with up to 8.07% accuracy improvement. The uplink communication volume of FedBIAD with DGC is about $2\times$ less than that of naive DGC, and FedBIAD with DGC is 2.26% more accurate than naive DGC. Furthermore, we combine AFD, Fjord with DGC, respectively. Both show lower model accuracy and more uplink costs than FedBIAD with DGC.

Convergence Comparison. To evaluate the convergence of FedBIAD, we report the average training loss and test accuracy of MNIST and WikiText-2 datasets varying with rounds in Fig. 6. Fig. 6a shows the convergence curves of MNIST. We observe that FedBIAD quickly converges to higher accuracy than other baselines. Additionally, FedBIAD nearly achieves the lowest training loss and the highest test accuracy in each round on MNIST. Fig. 6b presents the convergence curves of WikiText-2. For clarity, the curves are smoothed by the moving average, which will cause a few precision biases. As shown in Fig. 6b, although FedBIAD does not provide the lowest training loss, it converges to the best test accuracy, which indicates that FedBIAD avoids overfitting on training data and outperforms other baselines on test data.

C. Training Time Analysis

The Local Training Time in a Round (LTTR) can be used to characterize the local computation costs. Fig. 7a and Fig. 7b show the LTTR of different datasets, in which time is gained from the end-user device of Macbook Pro 2019 with 32G RAM. We note that FedBIAD increases local computation costs, which is apparent on WikiText-2. Concretely, Fed-BIAD increases LTTR by 3.4 seconds (8.81%), 1.99 seconds (5.16%), and 6.1 seconds (15.81%) on WikiText-2 compared to FedDrop, AFD, and Fjord.

FedBIAD reduces uplink communication costs with accuracy improvement, so it can accelerate global models to achieve target accuracy. As shown in Fig. 6a and Fig. 6b, under the same number of rounds, FedBIAD can generally achieve higher accuracy, which means that FedBIAD consumes much fewer communication rounds to reach a pre-defined target accuracy. For example, FedBIAD can obtain an accuracy of 31% after 4 rounds on WikiText-2, while Fjord needs 7 rounds and AFD needs 13 rounds. Motivated by [46], we utilize Time-To-Accuracy (TTA) to measure the total training time required to achieve target accuracy, which comprises local running time, parameter transmission time, and parameter aggregation time.



Fig. 8: The results for different dropout rates on Reddit.

To simulate parameter transmission time, we utilize the T-Mobile 5G network with a download speed of 110.6 Megabits per second (Mbps) and an upload speed of 14.0 Mbps [6]. The target accuracies are 90%, 80%, 31%, and 30% for MNIST, FMNIST, WikiText-2, and Reddit, respectively. Then, we calculate the TTA of different datasets, and the results are shown in Fig. 7c and Fig. 7d. We observe that on four datasets, FedBIAD consistently takes the shortest time to achieve the target accuracy compared with baselines. Although FedBIAD increases LTTR by 6.1 seconds on WikiText-2, it reduces uplink costs and the number of rounds, so the TTA of FedBIAD is 205.1 seconds shorter than Fjord. Specifically, FedBIAD reduces 66.67%, 72.00%, and 43.61% TTA on WikiText-2 compared to FedDrop, AFD, and Fjord, respectively. For FMNIST, the reductions are 29.64%, 23.91%, and 21.54%.

D. Effect of Dropout rate

To investigate the effect of dropout rate *p*, we measure accuracy and TTA for different dropout rates on Reddit. As shown in Fig 8a, the results of FedAvg without dropout remain constant as it is not affected by dropout rates. We notice that compared with the other three baselines, FedBIAD provides the highest accuracy at different dropout rates. As shown in Fig. 8b, the TTA decreases as the dropout rate increases, and the TTA of FedBIAD is always shorter than other baselines. It indicates that FedBIAD achieves the goal of efficient communication and guaranteed performance in FL.

VI. CONCLUSION

In this paper, we propose federated learning with Bayesian inference-based adaptive dropout (FedBIAD) to improve communication efficiency while guaranteeing accuracy. In FedBIAD, we introduce Bayesian inference and adaptively drop weight rows of local models based on the training loss to mitigate uplink overhead. Each client also maintains an importance indicator contributing to finding a high-quality dropping pattern for performance improvement. Theoretical analysis demonstrates that the convergence rate of generalization error of FedBIAD is minimax optimal up to a squared logarithmic factor. Experimental results show that FedBIAD provides up to $2 \times$ reduction in uplink costs with an accuracy increase of up to 2.41%, which shortens 72% training time compared to status quo approaches. FedBIAD focuses enough on communication efficiency, and we intend to further explore saving local computation in future work. Another future direction involves the adaptive adjustment of dropout rates based on the changes in communication conditions and device capabilities.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China (No. 62072436) and the National Key Research and Development Program of China (2021YFB2900102).

APPENDIX

A. Proof of Theorem 1

We want to analyze the upper bound on the generalization error of global variational approximation $\tilde{\pi}^g$ (see Definition 1 in the paper). Based on Theorem 2 in [21], we can obtain generalization properties of a fully connected DNN, where for any client k, the global model f_{θ} satisfies

$$\mathbb{E}\left[\|f_{\theta} - f_{0}^{k}\|_{2}^{2}\tilde{\pi}^{g}(\mathrm{d}\theta)\right] \\
\leq \frac{2}{(1-\alpha)} \inf_{\theta^{*} \in \Theta_{S,L,D}} \|f_{\theta^{*}} - f_{0}^{k}\|_{\infty}^{2} \\
+ \frac{2}{(1-\alpha)}(1 + \frac{\sigma^{2}}{\alpha})\varepsilon_{m}^{S,L,D}$$
(19)

with

$$\varepsilon_m^{S,L,D} = \frac{SL}{m} \log(2BD) + \frac{S}{4m} \left(12 \log(LD) + B^2 \right) + \frac{S}{m} \log\left(11d \max(\frac{m}{S}, 1) \right).$$
(20)

In the proof process, A. Chérief [21] introduce the optimal posterior variance $\tilde{s}_m^2 = \frac{S}{16m_2} \log(3D)^{-1} (2BD)^{-2L} \{ (d+1+\frac{1}{BD-1})^2 + \frac{1}{(2BD)^{2-1}} + \frac{(2BD-1)^2}{(2BD-1)^2} \}^{-1}$.

Then, we derive the upper bound on the global generalization error of a sparse single-layer RNN that is detailed in Section III-A. We start with the variant inequality of theorem 2.6 in [34]. Given the variational set $\mathcal{F}_{S,T,D}$ of tempered posterior, if there is $q^* \in \mathcal{F}_{S,T,D}$ and $\varepsilon_m > 0$ such that

$$KL(q^* \| \tilde{\pi}^g) \le m \varepsilon_m \tag{21}$$

and

$$\int \|f_{\theta} - f_{\theta^*}\|_2^2 q^*(d\theta) \le \varepsilon_m, \tag{22}$$

then for any $\alpha \in (0,1)$, we get the upper bound on the generalization error of Bayesian variational inference:

$$\mathbb{E}\left[\int \|f_{\theta} - f_{0}^{k}\|_{2}^{2}\tilde{\pi}_{m,\alpha}(d\theta)\right]$$

$$\leq \frac{2}{1-\alpha} \left(\inf_{\theta^{*}\in\Theta_{S,T,D}} \|f_{\theta^{*}} - f_{0}^{k}\|_{2}^{2} + \varepsilon_{m}\right) + \frac{2\sigma^{2}\varepsilon_{m}}{\alpha(1-\alpha)}.$$
(23)

We can prove that our RNN model satisfies Inequality (21) and (22) with $q^*(\theta)$ following the distribution of

$$\tilde{\pi}_{m,\alpha}^*(\theta_n) = \beta_n^* \mathcal{N}(\theta_n^*, \tilde{s}^2) + (1 - \beta_n^*) \delta(0) \quad \text{for } n = 1, ..., N,$$

and

$$\varepsilon_m = \frac{SL}{m} \log(2BD) + \frac{S}{m} \log(2D^2) + \frac{S}{2m} \log\log(3D) + \frac{SB^2}{2m} + \frac{S}{2m} \log\left(\frac{69md^2}{S}\right) \leq \frac{SL}{m} \log(2BD) + \frac{SB^2}{2m} + \frac{5S}{2m} \log(2D) + \frac{S}{m} \log\left(9d\max(\frac{m}{S}, 1)\right)$$
(24)

Here, β_n^* is the optimal dropping label of the *n*-th parameter θ_n , and the posterior variance \tilde{s}^2 satisfies

$$\tilde{s}^{2} = \frac{S}{16md^{2}}\log(3D)^{-1}(2BD)^{-2L}$$

$$\left\{ \left(d + 1 + \frac{1}{BD - 1} \right)^{2} + \frac{1}{(BD)^{2} - 1} + \frac{2}{(BD - 1)^{2}} \right\}^{-1}.$$
(25)

Our posterior variance \tilde{s}^2 calculated by (25) is larger than \tilde{s}_m^2 used in [21]. Thus, (19) still holds with \tilde{s}^2 calculated by (25).

Consequently, we integrate the derivations on the fully connected DNN and single-layer RNN and extend them to our federated architecture. Combining (20) and 24, we obtain

$$\varepsilon_{m_r}^{S,L,D} = \frac{SL}{m_r} \log(2BD) + \frac{3S}{m_r} \log(LD) + \frac{SB^2}{2m_r} + \frac{2S}{m_r} \log\left(4d \max(\frac{m_r}{S}, 1)\right), \quad (26)$$

where we consider the different numbers of local data in different clients such that the minimum amount of clientside total input data up to round r is denoted as $m_r =$ $r \times V \times \min\{|\mathcal{D}^1|, \ldots, |\mathcal{D}^K|\}$. The $\varepsilon_{m_r}^{S,L,D}$ denoted as (26) is larger than (20) and (24) with the same number of input data. Based on (26), we can derive the average generalization error of global model f_{θ} learned by FedBIAD in the server:

$$\mathbb{E}\left[\frac{1}{K}\sum_{k=1}^{K}\int \|f_{\theta} - f_{0}^{k}\|_{2}^{2}\tilde{\pi}^{g}(\mathrm{d}\theta)\right] \\
\leq \frac{2}{K(1-\alpha)}\sum_{k=1}^{K}\inf_{\theta^{*}\in\Theta_{S,L,D}}\|f_{\theta^{*}} - f_{0}^{k}\|_{\infty}^{2} \\
+ \frac{2\sigma^{2}}{\alpha(1-\alpha)}(1+\frac{\alpha}{\sigma^{2}})\varepsilon_{m_{r}}^{S,L,D}.$$
(27)

Therefore, we prove Theorem 1.

REFERENCES

- B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas. Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2017.
- [2] A. Hard, K. Rao, R. Mathews, S. Ramaswamy, F. Beaufays, S. Augenstein, H. Eichner, C. Kiddon, and D. Ramage. Federated learning for mobile keyboard prediction. arXiv preprint arXiv:1811.03604, 2018.
- [3] L. Wang, Y. Xu, H. Xu, J. Liu, Z. Wang, and L. Huang. Enhancing federated learning with in-cloud unlabeled data. In 2022 IEEE 38th International Conference on Data Engineering (ICDE), 2022.
- [4] Y. Lin, S. Han, H. Mao, Yu Y. Wang, and W. J. Dally. Deep gradient compression: Reducing the communication bandwidth for distributed training. In *The International Conference on Learning Representations* (*ICLR*), 2018.
- [5] K. R. Müller F. Sattler, S. Wiedemann and W. Samek. Robust and communication-efficient federated learning from non-i.i.d. data. *IEEE Transactions on Neural Networks and Learning Systems*, 31(9):3400– 3413, 2020.
- [6] USA mobile network experience report January 2022. https://www. opensignal.com/reports/2022/01/usa/mobile-network-experience.
- [7] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon. Federated learning: Strategies for improving communication efficiency. In *NIPS Workshop on Private Multi-Party Machine Learning*, 2016.
- [8] L. Wang, W. Wang, and B. Li. CMFL: Mitigating communication overhead for federated learning. In *IEEE 39th International Conference* on Distributed Computing Systems (ICDCS), 2019.
- [9] A. Reisizadeh, A. Mokhtari, H. Hassani, A. Jadbabaie, and R. Pedarsani. FedPAQ: A communication-efficient federated learning method with periodic averaging and quantization. In *Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics* (AISTATS), 2020.
- [10] D. Wu, X. Zou, S. Zhang, H. Jin, W. Xia, and B. Fang. Smartidx: Reducing communication cost in federated learning by exploiting the cnns structures. In *Proceedings of the AAAI Conference on Artificial Intelligence*, 2022.
- [11] J. Bernstein, Y. Wang, K. Azizzadenesheli, and A. Anandkumar. signSGD: Compressed optimisation for non-convex problems. In Proceedings of the 35th International Conference on Machine Learning (ICML), 2018.
- [12] S. Caldas, J. Konečný, H. B. McMahan, and A. Talwalkar. Expanding the reach of federated learning by reducing client resource requirements. *arXiv preprint arXiv*:1812.07210, 2019.
- [13] D. Wen, K. J. Jeon, and K. Huang. Federated dropout a simple approach for enabling federated learning on resource constrained devices. *IEEE Wireless Communications Letters*, 11(5):923–927, 2022.
- [14] H. Samuel, L. Stefanos, A. Mario, L. Ilias, V. Stylianos, and D. L. Nicholas. FjORD: Fair and accurate federated learning under heterogeneous targets with ordered dropout. *Advances in Neural Information Processing Systems (NeurIPS)*, 2021.
- [15] N. Bouacida, J. Hou, H. Zang, and X. Liu. Adaptive federated dropout: Improving communication efficiency and generalization for federated learning. In *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2021.
- [16] Y. Gal and Z. Ghahramani. A theoretically grounded application of dropout in recurrent neural networks. Advances in Neural Information Processing Systems 29 (NeurIPS), 2016.
- [17] J. Bayer, C. Osendorfer, N. Chen, S. Urban, and P. van der Smagt. On fast dropout and its applicability to recurrent networks. arXiv preprint arXiv:1311.0701, 2014.
- [18] M. P. Marcus, B. Santorini, and M. A. Marcinkiewicz. Building a large annotated corpus of English: The Penn Treebank. *Computational Linguistics*, 1993.
- [19] Y. Gal and Z. Ghahramani. Dropout as a bayesian approximation: Representing model uncertainty in deep learning. In *Proceedings of the* 33rd International Conference on International Conference on Machine Learning (ICML), 2016.
- [20] I. Castillo, Johannes S. H., and A. van der Vaart. Bayesian linear regression with sparse priors. arXiv preprint arXiv:1403.0735, 2014.
- [21] E. Badr A. Chérief. Convergence rates of variational inference in sparse deep learning. In *Proceedings of the 37th International Conference on Machine Learning (ICML)*, 2020.

- [22] Y. Gal. Uncertainty in deep learning. PhD thesis, University of Cambridge, 2016.
- [23] E. Lobacheva, N. Chirkova, and D. Vetrov. Bayesian sparsification of recurrent neural networks. In Workshop on Learning to Generate Natural Language, ICML, 2017.
- [24] H. Yu and R. Jin. On the computation and communication complexity of parallel SGD with dynamic batch sizes for stochastic non-convex optimization. In *Proceedings of the 36th International Conference on Machine Learning (ICML)*, 2019.
- [25] J. Stremmel and A. Singh. Pretraining federated text models for next word prediction. arXiv preprint arXiv:2005.04828, 2020.
- [26] X. Wu, Z. Liang, and J. Wang. Fedmed: A federated learning framework for language modeling. *Sensors*, 2020.
- [27] Z. Jiang, Y. Xu, H. Xu, Z. Wang, C. Qiao, and Y. Zhao. FedMP: Federated learning through adaptive model pruning in heterogeneous edge computing. In *IEEE 38th International Conference on Data Engineering (ICDE)*, 2022.
- [28] X. Zhang, Y. Li, W. Li, K. Guo, and Y. Shao. Personalized federated learning via variational Bayesian inference. In *Proceedings of the 39th International Conference on Machine Learning (ICML)*, 2022.
- [29] P. Izmailov, S. Vikram, M. D. Hoffman, and A. G. Wilson. What are bayesian neural network posteriors really like? In *Proceedings of the* 38th International Conference on Machine Learning (ICML), 2021.
- [30] A. Graves. Practical variational inference for neural networks. Advances in Neural Information Processing Systems (NeurIPS), 2011.
- [31] M. Welling and Y. W. Teh. Bayesian learning via stochastic gradient langevin dynamics. In *Proceedings of the 28th international conference* on machine learning (ICML), 2011.
- [32] A. Kendall and Y. Gal. What uncertainties do we need in bayesian deep learning for computer vision? Advances in Neural Information Processing Systems (NeurIPS), 2017.
- [33] A. Garriga-Alonso and V. Fortuin. Exact langevin dynamics with stochastic gradients. In *Third Symposium on Advances in Approximate Bayesian Inference*, 2021.
- [34] P. Alquier and J. Ridgway. Concentration of tempered posteriors and of their variational approximations. arXiv preprint arXiv:1706.09293, 2019.
- [35] A. Ozer, K. B. Buldu, A. Akgül, and G. Unal. How to combine variational bayesian networks in federated learning. arXiv preprint arXiv:2206.10897, 2022.
- [36] N. G. Polson and V. Ročková. Posterior concentration for sparse deep learning. NIPS'18, 2018.
- [37] R. Nakada and M. Imaizumi. Adaptive approximation and generalization of deep neural network with intrinsic dimensionality. *The Journal of Machine Learning Research*, 21(1), 2020.
- [38] Y. LeCun. The MNIST database of handwritten digits. http://yann.lecun. com/exdb/mnist/, 1998.
- [39] X. Han, R. Kashif, and V. Roland. Fashion-MNIST: a novel image dataset for benchmarking machine learning algorithms. arXiv preprint arXiv:1708.07747, 2017.
- [40] S. Merity, C. Xiong, J. Bradbury, and R. Socher. Pointer sentinel mixture models. arXiv preprint arXiv:1609.07843, 2016.
- [41] S. Caldas, S. M. K. Duddu, P. Wu, T. Li, J. Konečný, B. McMahan, V. Smith, and A. Talwalkar. LEAF: A benchmark for federated settings. arXiv preprint arXiv:1812.01097, 2019.
- [42] S. Ji, S. Pan, G. Long, X. Li, J. Jiang, and Z. Huang. Learning private neural language modeling with attentive aggregation. In *International Joint Conference on Neural Networks (IJCNN)*, 2019.
- [43] E. Diao, J. Ding, and V. Tarokh. HeteroFL: Computation and communication efficient federated learning for heterogeneous clients. In International Conference on Learning Representations (ICLR), 2021.
- [44] C. T. Dinh, N. H. Tran, and T. D. Nguyen. Personalized federated learning with moreau envelopes. Advances in Neural Information Processing Systems (NeurIPS), 2020.
- [45] S. Merity, N. S. Keskar, and R. Socher. Regularizing and optimizing LSTM language models. arXiv preprint arXiv:1708.02182, 2017.
- [46] J. Wolfrath, N. Sreekumar, D. Kumar, Y. Wang, and A. Chandra. HACCS: Heterogeneity-aware clustered client selection for accelerated federated learning. In *IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, 2022.