

A Bargaining Game for Personalized, Energy Efficient Split Learning over Wireless Networks

Minsu Kim, Alexander DeRieux, and Walid Saad

Wireless@VT, Bradley Department of Electrical and Computer Engineering, Virginia Tech, Arlington, VA, USA.

Emails: {msukim, acd1797, walids}@vt.edu.

Abstract—Split learning (SL) is an emergent distributed learning framework which can mitigate the computation and wireless communication overhead of federated learning. It splits a machine learning model into a device-side model and a server-side model at a cut layer. Devices only train their allocated model and transmit the activations of the cut layer to the server. However, SL can lead to data leakage as the server can reconstruct the input data using the correlation between the input and intermediate activations. Although allocating more layers to a device-side model can reduce the possibility of data leakage, this will lead to more energy consumption for resource-constrained devices and more training time for the server. Moreover, non-iid datasets across devices will reduce the convergence rate leading to increased training time. In this paper, a new personalized SL framework is proposed. For this framework, a novel approach for choosing the cut layer that can optimize the tradeoff between the energy consumption for computation and wireless transmission, training time, and data privacy is developed. In the considered framework, each device personalizes its device-side model to mitigate non-iid datasets while sharing the same server-side model for generalization. To balance the energy consumption for computation and wireless transmission, training time, and data privacy, a multiplayer bargaining problem is formulated to find the optimal cut layer between devices and the server. To solve the problem, the Kalai-Smorodinsky bargaining solution (KSBS) is obtained using the bisection method with the feasibility test. Simulation results show that the proposed personalized SL framework with the cut layer from the KSBS can achieve the optimal sum utilities by balancing the energy consumption, training time, and data privacy, and it is also robust to non-iid datasets.

I. INTRODUCTION

Federated learning (FL) is a promising solution for distributed inference as it enables multiple devices and a server to train a shared model without revealing private data [1]. Since each device trains a whole model and transmits it to the server iteratively, significant wireless communication and computation overhead can exist on devices. To mitigate this challenge, split learning (SL) was proposed in [2]. In SL the model is split into two separate portions, which are a device-side model and a server-side model, at the cut layer. The devices and the server communicate over a wireless channel. A device only needs to train its allocated model and transmit the activations of the cut layer to the server. Then, the server with more computing resources trains the remaining model based on the received information. However, the server can still reconstruct the private data of the devices from the received activations due to the high correlation between the activations

and the input when the allocated device-side model is too shallow [3], [4]. Although one can reduce the possibility of data leakage by increasing the device-side model, the training will become computationally intensive for resource-constrained devices. In addition, this will increase the training time as the server should wait until devices finish processing their models. Moreover, non-iid datasets across devices will increase the training time by reducing the convergence rate. Thus, it is important to find the optimal cut layer by balancing the energy consumption related to computation and wireless transmission, training time, and data privacy and to develop an algorithm for robust performance over non-iid datasets.

Several prior works [3]–[6] studied the problems of data privacy and non-iid datasets in SL scenarios over communication networks. In [5], the authors proposed SplitFed in which device-side training was parallelized and differential privacy was incorporated to improve data privacy. The work in [3] demonstrated that data leakage can happen when training convolutional neural networks in SL. In [4], the authors proposed a novel SL algorithm to enhance data privacy by minimizing the distance correlation between the intermediate activations and the input data. Meanwhile, in [6], the authors studied the use of SL at inference stage over wireless networks and the impact of non-iid datasets on its performance.

However, these works [3]–[6] did not consider the impact of the cut layer on energy consumption, training time, and data privacy. Only few works such as [7] and [8] considered the optimal cut layer in terms of training latency. The work in [7] developed a local-loss-based training for SL and derived the optimal cut layer to minimize the training latency. In [8], cluster-based parallel SL was proposed along with a resource management algorithm to minimize its training time by optimizing the cut layer selection. To the best of our knowledge, there are no prior works on SL that jointly consider energy consumption for computation and communication, training time, and data privacy to obtain the optimal cut layer for devices and the server.

The main contribution of this paper is a novel personalized SL framework that can handle heterogeneous datasets and that is equipped with a new approach to find the optimal cut layer between devices and the server¹. In our personalized SL model, the learning model is divided into two separate portions: a device-side model and a server-side model. Each device personalizes its own device-side model while sharing

This work was supported by the U.S. National Science Foundation under Grant CNS-2114267.

¹The source code is publicly available on <https://github.com/news-vt>.

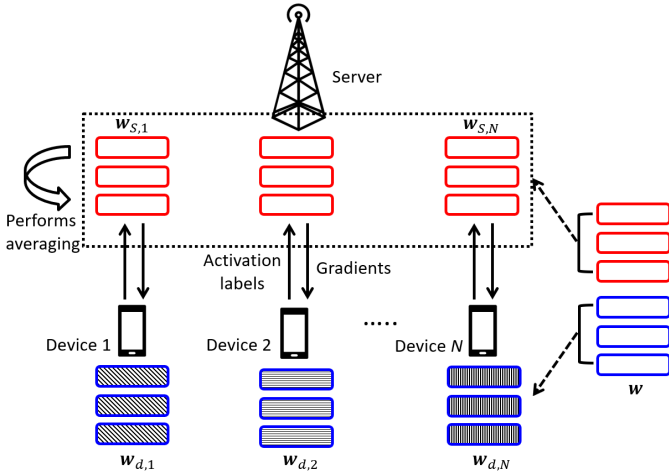


Fig. 1: An illustration of the personalized SL system over wireless networks.

the same server-side model. At the beginning of the learning, each device performs forward propagation on its allocated model in parallel and transmits the activations of the cut layer to the server. Then, the server completes the forward propagation with each device's activations and performs back propagation on its model separately, in parallel. The server transmits the gradients of its last layer to the corresponding devices so that they can finish back propagation. Subsequently, the server performs FedAvg on its updated models to generate a new server-side model. We then formulate utility functions for the devices and the server by capturing energy consumption of computation and communication, training time, and data privacy. In particular, devices can reduce energy consumption by choosing a shallow cut layer. However, this can result in data leakage due to the high correlation between the cut layer's activations and the input data. Meanwhile, the server may want to choose the shallow cut layer so that it can leverage its computing capability to minimize the training time. To capture this conflict over the cut layer between devices and the server, we formulate a multiplayer bargaining problem whose goal is to maximize the utilities of devices and the server. To solve the problem, we obtain the Kalai-Smorodinsky bargaining solution (KSBS) using the bisection method with the feasibility test. Simulation results show that personalized SL with the optimal cut layer from the KSBS can achieve robust performance over non-iid datasets with fast convergence while achieving the best sum utilities by balancing the energy consumption, training time, and data privacy.

The rest of this paper is organized as follows. Section II presents the system model. In Section III, we formulate the bargaining problem. Section IV provides simulation results. Finally, conclusions are drawn in Section V.

II. SYSTEM MODEL

We consider a personalized SL system, in which one server and a set of devices \mathcal{N} with $|\mathcal{N}| = N$ (e.g. mobile or Internet of Things (IoT) devices) collaboratively train a machine learning (ML) model to execute a certain data analysis task.

All devices have their personalized layers while sharing the same subsequent layers with the server as shown in Fig. 1. The server generates an ML model w for an image classification task. Let $|w|$ be the number of model parameters in the generated model. For device k , we define $w_{d,k}$ as the device-side model, $\forall k \in \mathcal{N}$ and w_S as the server-side model. We use α such that $0 \leq \alpha \leq 1$ to allocate $|w_{d,k}| = \alpha|w|$, $\forall k \in \mathcal{N}$, model parameters to a device-side model and $|w_S| = (1-\alpha)|w|$ model parameters to the server-side model. Note that all device-side models share the same architecture while they are personalized to each device. The main goal of the personalized SL system is to solve the following problem:

$$\min_{w_d, w_S} \frac{1}{D} \sum_{k \in \mathcal{N}} \sum_{l \in \mathcal{D}_k} \ell(w_{d,k}, w_S, x_{kl}, y_{kl}), \quad (1)$$

where $w_d = (w_{d,1}, \dots, w_{d,N})$, \mathcal{D}_k is the input dataset of device k with $|\mathcal{D}_k| = D_k$, $D = \sum_{k \in \mathcal{N}} D_k$ is the total number of data samples across devices, and $\ell(\cdot, \cdot, \cdot, \cdot)$ is a loss function for a given sample. We assume that all devices use the same loss function. x_{kl} is an input vector l of device k , and y_{kl} is the corresponding output with $l = \{1, \dots, D_k\}$. Without loss of generality, we consider unbalanced and non-iid dataset \mathcal{D}_k across devices.

A. Proposed Personalized SL algorithm

We now describe the proposed algorithm to solve problem (1). The server uses FedAvg [1] to train w_S while each device updates its personalized layers using a gradient based algorithm. For a given α , each device $k \in \mathcal{N}$ receives its device-side model $w_{d,k}$ from the server and initializes it. The server also generates $w_{S,k}, \forall k \in \mathcal{N}$. Motivated by [5] and [9], we assume that each device $k \in \mathcal{N}$ performs forward propagation in parallel on $w_{d,k}$ at each local step using mini-batch ξ_k . Then, device $k \in \mathcal{N}$ transmits the intermediate outputs, i.e., activations, $a_{d,k}$ and the corresponding labels $Y_k \in \xi_k$ to the server. Based on the received information, the server can finish forward propagation and perform back propagation on $w_{S,k}(t)$. Subsequently, it transmits the gradients of its last layer to the corresponding device. Then, device k can update $w_{d,k}(t)$ using the received gradients. After I local steps, the server perform FedAvg on $w_{S,k}(t), \forall k \in \mathcal{N}$, to generate $w_S(t+1) = \sum_{k \in \mathcal{N}} \frac{D_k}{\sum_{k \in \mathcal{N}} D_k} w_{S,k}(t)$. Then, at the next global round $t+1$, the server sets $w_{S,k}(t+1) = w_S(t+1), \forall k \in \mathcal{N}$. We summarize the aforementioned algorithm in Algorithm 1.

B. Wireless Transmission and Computing Model

1) *Wireless transmission model:* After device k finishes forward propagation on $w_{d,k}$, it transmits activations $a_{d,k}$ and the corresponding labels Y_k to the server using orthogonal frequency domain multiple access (OFDMA). Then, the achievable rate of device k can be given by

$$R_k = W \log_2 \left(1 + \frac{P_k h_k}{N_0 W} \right), \quad (2)$$

where W is the bandwidth allocated to device k , h_k is the channel gain between device k and the server, P_k is the

Algorithm 1: Proposed Personalized SL Algorithm

```

1 while global round  $t \neq R$  do
2   if  $t = 0$  then
3     Initialize  $\mathbf{w}_{d,k}(0)$  and  $\mathbf{w}_{S,k}(0) \forall k \in \mathcal{N}$ ;
4   Sample a set of devices  $\mathcal{N}$ ;
5   for device  $k \in \mathcal{N}$  do
6     while local step  $i \neq I$  do
7       /* Forward Propagation */
8       Device  $k$  samples mini-batch  $\xi_k$ ;
9        $a_{d,k} \leftarrow \text{forward}(\mathbf{w}_{d,k}(t), \xi_k)$ ;
10      Device  $k$  transmits  $a_{d,k}$  and label  $Y_k$  to server;
11       $\hat{y}_k \leftarrow \text{forward}(\mathbf{w}_{S,k}(t), a_{d,k})$ ;
12
13      /* Backward Propagation */
14       $\ell_k(t) \leftarrow \text{loss}(Y_k, \hat{y}_k)$ ;
15      Server computes  $\nabla \ell_k(\mathbf{w}_{S,k}(t))$ ;
16       $\mathbf{w}_{S,k}(t) \leftarrow \mathbf{w}_{S,k}(t) - \eta \nabla \ell_k(\mathbf{w}_{S,k}(t))$ ;
17      Server transmits gradient of its last layer  $da_{d,k}(t)$  to device
18       $k$ ;
19      Using  $da_{d,k}(t)$ , device  $k$  updates
20       $\mathbf{w}_{d,k}(t) \leftarrow \mathbf{w}_{d,k}(t) - \eta \nabla \ell_k(\mathbf{w}_{d,k}(t))$ 
21
22   /* FedAvg */
23    $\mathbf{w}_S(t+1) \leftarrow \sum_{k \in \mathcal{N}} \frac{D_k}{\sum_{k \in \mathcal{N}} D_k} \mathbf{w}_{S,k}(t)$ ;
24   Set  $\mathbf{w}_{S,k}(t+1) = \mathbf{w}_S(t+1), \forall k \in \mathcal{N}$ ;

```

transmission power, N_0 is the power spectral density of white Gaussian noise. Then, the transmission time to upload $a_{d,k}$ and Y_k will be

$$\tau_k = \frac{|a_{d,k}| + |Y_k|}{R_k}. \quad (3)$$

Then, the energy consumption to transmit $a_{d,k}$ and Y_k to the server is $E_k^U = \tau_k P_k$. Since the server usually has a high transmission power and large bandwidth for the downlink, we neglect the energy and the time to transmit the gradients of its last layer [10].

2) *Computing model*: Let f_k be the CPU frequency of device k . Then the energy consumption to train $\mathbf{w}_{d,k}$ for one global round using \mathcal{D}_k will be given by [7]

$$E_k^C(\alpha) = \kappa \alpha D_k L_k f_k^2, \quad (4)$$

where κ is the effective capacitance coefficient of CPU [11], L_k is the number of required CPU cycles to process one data sample. Note that $E_k^C(\alpha)$ is a function of α since device k processes $\mathbf{w}_{d,k}$, which has $\alpha|\mathbf{w}|$ number of model parameters. The computation time will be

$$T_k(\alpha) = \frac{\alpha L_k D_k}{f_k}. \quad (5)$$

Similarly, we can define the energy consumption of the server for one global round t as $E_S(\alpha) = \sum_{k \in \mathcal{N}} D_k (1 - \alpha) \kappa L_S f_S^2$, where L_S is the number of requires CPU cycles to process one data sample for the server and f_S is its CPU frequency. Then, the computation time of the server will be $T_S(\alpha) = \max_{k \in \mathcal{N}} D_k (1 - \alpha) L_S / f_S$. Since the server processes $\mathbf{w}_{S,k}, \forall k \in \mathcal{N}$ in parallel, $T_S(\alpha)$ will be determined by the largest computation time.

C. Utility Functions

Now, we define the utility functions of each device and the server. Since the server usually has a strong computing

capability, it may want to set α small so as to reduce the elapsed time during training. For devices, the optimal α should neither be too small because of the possibility of data leakage nor too large because of the energy consumption for training. Specifically, there exists high probability of data leakage when device-side models are shallow. As α decreases, the correlation between the input data and an intermediate layer output, i.e., activations $a_{d,k}$, increases. Hence, it is possible to reconstruct input data from activations as shown in [3] and [4]. In other words, an honest-but-curious server can do model inversion attack during training to restore private input data [12]. However, training a large device-side model would be also infeasible for resource-constrained devices since training a deep neural network consumes significant energy.

To capture this tradeoff between privacy and energy consumption for devices, we define the utility function of each device $k \in \mathcal{N}$ for one global round as follows

$$U_{d,k}(\alpha) = \underbrace{c_k f_k}_{(a)} - \underbrace{(E_k^C(\alpha) + I E_k^U)}_{(b)} + \underbrace{\lambda_k \log_2(1 + \alpha)}_{(c)}, \quad (6)$$

where (a) is the received reward from the server for the allocated computing resources with payoff c_k , (b) is the energy consumption for training $\mathbf{w}_{d,k}$ and transmitting the intermediate outputs to the server, and (c) is a function to measure privacy protection with coefficient λ_k to capture the preference of data privacy. Note that as α increases the correlation between input data and the intermediate outputs become decreased [4]. We then define the utility function of the server for one global round as below

$$U_S(\alpha) = B - \left[\underbrace{\sum_{k \in \mathcal{N}} c_k f_k}_{(a)} + \underbrace{\gamma E_S(\alpha)}_{(b)} + (1 - \gamma) \underbrace{\left\{ T_S(\alpha) + \max_{k \in \mathcal{N}} T_k(\alpha) + I \mathbb{E}[\tau_k] \right\}}_{(c)} \right], \quad (7)$$

where B is the available budget of the server, (a) is the amount of payoff for devices, (b) is the energy consumption for training $\mathbf{w}_{S,k}, \forall k \in \mathcal{N}$, (c) is the elapsed time to compute $\mathbf{w}_{S,k}, \forall k$ and the elapsed time to wait for the slowest device to finish computing its model, $\mathbb{E}(\cdot)$ is with respect to h_k and γ is a parameter to balance the interests between the energy consumption and the training time. We assume that the server can control c_k so that $U_S(\alpha)$ and $U_{d,k}(\alpha), \forall k$ can be larger than zero.

From the above utility functions, we can see that devices and the server have conflicting interests over α . If the server prioritizes minimizing training time, then it will try to set α as a low value so as to leverage its high computing power. However, when α is low, there exists high probability of data leakage for the devices. Hence, they need to reach a certain agreement for α to initiate personalized SL. This situation can be modeled as a bargaining game between devices and the server as they can mutually benefit from reaching the optimal α^* while conflict exists on the terms of the agreement [13].

In the following section, we obtain the KSBS to find the optimal split.

III. PERSONALIZED SL AS A BARGAINING GAME

We formulate a bargaining game to reach an agreement over α . We first define the set of all feasible utility functions as:

$$\mathcal{U} = \{U_{d,1}(\alpha), \dots, U_{d,N}(\alpha), U_S(\alpha) \mid 0 \leq \alpha \leq 1\}. \quad (8)$$

Let $\phi = \{\phi_{d,1}, \dots, \phi_{d,N}, \phi_S\}$ be the disagreement point, which is a set of utilities when devices and the server fail to come to an agreement. Then, our bargaining game can be defined as the pair (\mathcal{U}, ϕ) , and the bargaining solution is a function f that maps (\mathcal{U}, ϕ) to a unique outcome $f(\mathcal{U}, \phi) \in \mathcal{U}$. Our bargaining solution should prioritize a device with important or private-sensitive dataset so that it can achieve a higher utility than devices with less important datasets. Therefore, while there are many bargaining approaches (e.g., Nash bargaining, etc.), we choose the KSBS [13]. This is because the monotonicity axiom of the KSBS can capture the aforementioned benefit since a device with a stronger privacy preference λ_k will be able to get a larger achievable maximum utility and a larger utility set. Thus, it can have stronger bargaining power than others leading to a better output α^* .

It is known that the KSBS is the largest element in \mathcal{U} that is on the line connecting ϕ and $\mathbf{U}^{\text{ideal}}$, where $\mathbf{U}^{\text{ideal}}$ is the vector of individually maximized utilities. The KSBS point is essentially the solution to the following optimization problem:

$$\max \beta \quad (9)$$

$$\text{s.t. } \phi + \beta(\mathbf{U}^{\text{ideal}} - \phi) \in \mathcal{U}. \quad (10)$$

For the disagreement point ϕ , we can set $\phi = 0$ because the server cannot initiate the learning if devices and the server fail to negotiate on α . Then, we can simplify the problem as

$$\max \beta \quad (11)$$

$$\text{s.t. } \beta \mathbf{U}^{\text{ideal}} \in \mathcal{U}. \quad (12)$$

Now, the KSBS will lie on the line connecting the origin point and $\mathbf{U}^{\text{ideal}}$. To solve problem (11), we use the bisection method with a feasibility test to tackle constraint (12). Firstly, we characterize $\mathbf{U}^{\text{ideal}} = (U_{d,1}^{\text{ideal}}, U_{d,2}^{\text{ideal}}, \dots, U_{d,N}^{\text{ideal}}, U_S^{\text{ideal}})$. From (6), it is straightforward to see that $U_{d,k}(\alpha)$ is concave with respect to α as $\frac{\partial^2 U_{d,k}(\alpha)}{\partial \alpha^2} = -\frac{\lambda_k \log 2}{(1+\alpha)^2} < 0$. Hence, we can obtain $U_{d,k}^{\text{ideal}}$ from the first derivative test as below

$$\frac{\partial U_{d,k}(\alpha)}{\partial \alpha} = \frac{\lambda_k}{\log 2 \times (1+\alpha)} - \kappa D_k L_k f_k^2 = 0. \quad (13)$$

Then, the solution of the above equation can be given by

$$\hat{\alpha}_k = \frac{\lambda_k}{\log 2 \times \kappa L_k D_k f_k^2} - 1. \quad (14)$$

From (14), we can see that the optimal split ratio $\hat{\alpha}_k$ for device k increases as the preference of data protection λ_k increases. For the $U_S(\alpha)$, its first derivative can be given by

$$\frac{\partial U_S(\alpha)}{\partial \alpha} = \gamma \sum_{k \in \mathcal{N}} \kappa D_k L_S f_S^2 + (1-\gamma) \max_{k \in \mathcal{N}} \left[\frac{D_k L_S}{f_S} - \frac{D_k L_k}{f_k} \right], \quad (15)$$

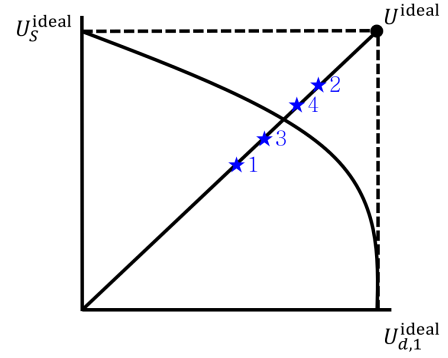


Fig. 2: An illustration of the Algorithm 2 for the two player case.

Algorithm 2: Algorithm for the KSBS

```

1 Set  $\beta_{\min} = 0$  and  $\beta_{\max} = 1$ ;
2 while  $|\beta_{\max} - \beta_{\min}| < \epsilon$  do
3    $\beta \leftarrow \frac{\beta_{\max} + \beta_{\min}}{2}$ ;
4   Solve the feasibility problem (16);
5   if  $\beta$  is feasible then
6      $\beta_{\min} \leftarrow \beta$ ;
7   else
8      $\beta_{\max} \leftarrow \beta$ ;

```

where the first term is the energy consumption for training w_S and the second term is related to the elapsed time during one global epoch. Hence, depending on the balancing parameter γ , the optimal fraction $\hat{\alpha}_S$ will be either zero or one. From (14) and (15), we can obtain $\mathbf{U}^{\text{ideal}}$. Then, for a given β , we can formulate the feasibility problem as follows

$$\text{Find } \alpha \quad (16)$$

$$\text{s.t. } \beta \mathbf{U}^{\text{ideal}} = (U_{d,1}(\alpha), \dots, U_{d,N}(\alpha), U_S(\alpha)). \quad (17)$$

Since $U_{d,k}(\alpha)$ and $U_S(\alpha)$ are a concave and a linear function with respect to α , respectively, it is straightforward to find α such that $U_{d,k}(\alpha) = \beta U_{d,k}^{\text{ideal}}, \forall k$ and $U_S(\alpha) = \beta U_S^{\text{ideal}}$ using a software solver.

We now obtain the KSBS by using the bisection method with the feasibility problem (16) as shown in Fig. 2 [14]. We first set $\beta_{\max} = 1$, $\beta_{\min} = 0$, and $\beta = \frac{\beta_{\min} + \beta_{\max}}{2}$. Then, at iteration n , we solve the feasibility problem (16) for $\beta(n)$. If it is feasible, we set $\beta_{\min} = \beta(n)$. Otherwise, we set $\beta_{\max} = \beta(n)$. We repeat this iteration until a certain stopping criteria becomes satisfied. The summary of our approach is provided in Algorithm 2. The key complexity of Algorithm 2 stems from solving the feasibility problem (16). Since we should solve N equations in (16), the complexity of Algorithm 2 will be proportional to the total number of devices N .

In practice, we can assume that the devices send their channel information, hardware information, size of dataset, and preference toward privacy to the server through the designated interface. Then, the server can perform Algorithm 2.

IV. SIMULATION RESULTS

For our simulations, we distribute $N = 10$ devices uniformly over a 50 m \times 50 m square area and locate the server

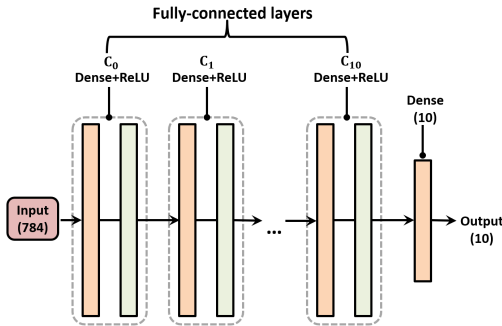


Fig. 3: MLP model architecture with one input layer, 11 fully connected layers, and one output layer.

Algorithms	MNIST	FMNIST
Proposed	93.52%	92.01%
SplitFed	92.90%	79.65%

TABLE I: Performance of different algorithms on test dataset

at the center. We adopt a Rayleigh fading channel model with a path loss exponent of 4 between the devices and the server. For a default setting, we use $P_k = 100$ mW, $W = 10$ MHz, $N_0 = -174$ dBm, and $\kappa = 2 \times 10^{-28}$. f_k follows uniform distribution between (1.5, 2.4) GHz, λ_k is uniformly distributed between (25, 30), and c_k follows uniform distribution between $(10^{-8}, 10^{-7})$. We also set $L_k = L_S = 10^3$, $\forall k$, $B = 1215$, $\gamma = 0.01$, and $f_S = 4$ GHz [11] [10]. We use multi-layer perceptron (MLP) model to classify 10 digits and clothes in the MNIST and FMNIST datasets, respectively. The model consists of one input layer, 11 fully-connected layers blocks, C_0, C_1, \dots, C_{10} , and one classification layer as shown in Fig. 3. Each block C_k consists of one dense layer and ReLU activation. The total number of model parameters is $|\mathbf{w}| = 287955$. We split both the MNIST/FMNIST dataset into 55000 samples for training, 5000 samples for validation, and 10000 samples for testing. We distribute the training dataset over devices in non-iid fashion. We choose two major and eight minor labels for each device. Then, we allocate 40% of each major label and 5% of each minor label to a device. We also distribute the validation/test datasets over devices using the same method as the training dataset [15]. We use Adam optimizer with learning rate 0.01 and mini-batch size is 256. For each global round, each device runs $I = 25$ local steps.

From the given setting, our KSBS is $\alpha^* = 0.379$ and this corresponds to C_3 , which becomes the cut layer. Hence, the input layer up to the cut layer C_3 will be assigned to the device-side model $\mathbf{w}_{d,k}, \forall k$ with $|\mathbf{w}_{d,k}| = 117135$, and all subsequent layers are assigned to the server-side model \mathbf{w}_S with $|\mathbf{w}_S| = 170820$. All statistical results are averaged over a large number of independent runs.

To benchmark our proposed learning algorithm, we use SplitFed [5] as a baseline. In SplitFed, FedAvg is performed on both device-side models and server-side models for every global round while our proposed algorithm only averages the server-side models. Specifically, after the server performs FedAvg on $\mathbf{w}_{S,k}(t), \forall k$, each device k transmits its device-

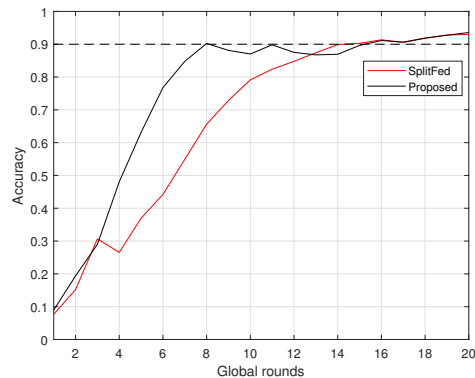


Fig. 4: Validation accuracy of the proposed algorithm and SplitFed on non-iid MNIST dataset

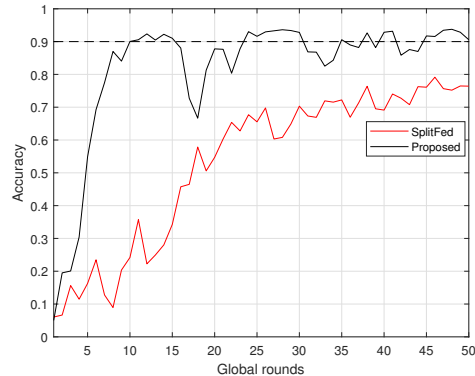
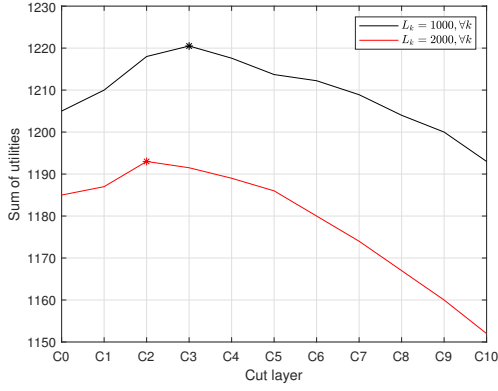


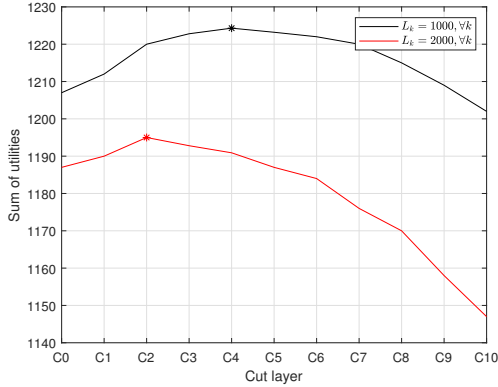
Fig. 5: Validation accuracy of the proposed algorithm and SplitFed on non-iid FMNIST dataset

side model $\mathbf{w}_{d,k}(t)$ to an edge server for averaging. Note that the edge server only does FedAvg on $\mathbf{w}_{d,k}(t)$ and does not perform forward/back propagation. Subsequently, the Fed server generates $\mathbf{w}_d(t+1) = \frac{1}{N} \sum_{k \in \mathcal{N}} \mathbf{w}_{d,k}(t)$ and broadcasts it to devices. Then, devices set $\mathbf{w}_{d,k}(t+1) = \mathbf{w}_d(t+1)$ for the next global round.

Figures 4 and 5 show the accuracy on the MNIST/FMNIST validation datasets as a function of global rounds for our algorithm and SplitFed. In Figs. 4 and 5, we can see that the proposed algorithm converges faster than the baseline on both datasets. From Table I, we observe that, although the baseline achieves similar performance with the proposed algorithm on the MNIST test dataset, it does not perform well on more difficult dataset, which is FMNIST. Meanwhile, our algorithm shows more robust accuracy on both non-iid datasets. This is because the proposed algorithm can mitigate discrepancies among the individual device optimum via personalization. Unlike the baseline, our algorithm only averages the server-side models while keeping the device-side models personalized. Then, each device-side model can move toward its local optimum during training. Therefore, it can achieve fast convergence as well as generalization through the server-side models. Meanwhile, SplitFed averages all layers and then moves toward the average of all individual optimum points



(a) $\lambda \sim U(25, 30)$



(b) $\lambda \sim U(30, 35)$

Fig. 6: Sum of utilities with different privacy parameter distributions

resulting in slow convergence [16].

Figure 6 presents the sum of utilities for each cut layer with different distribution of privacy parameters $\lambda = \{\lambda_1, \dots, \lambda_N\}$. From Fig. 6a, we can clearly see that our cut layer C_3 , which is obtained from the KSBS, can achieve the best sum of utilities. Moreover, as the number of required CPU cycles to process one data sample L_k increases, we can see that the optimal cut layer decreases. This is because devices have to spend more energy for training, so having a large device-side model is not beneficial. This also corroborates (14), which shows that the optimal cut layer for each device is a decreasing function of L_k . In Fig. 6b, $\lambda_k, \forall k$ follows uniform distribution between $[30, 35]$ resulting in a stronger privacy preference for all devices than Fig. 6a. From the given setting, the KSBS is found to be 0.506, and this corresponds to C_4 for the cut layer. We can see that the optimal cut layer increased to C_4 from C_3 . This is because devices now have a stronger preference for data protection and have more bargaining power due to the monotonicity axiom of the KSBS.

V. CONCLUSION

In this paper, we have studied the problem of finding the optimal split on a neural network in a personalized SL over wireless networks. We have presented the training algorithm

for the proposed personalized SL to tackle non-iid datasets. We also have introduced utility functions by considering energy consumption, training time, and data privacy during training. Then, we have formulated a multiplayer bargaining problem to find the optimal cut layer between devices and the server to maximize their utilities. To solve the problem, we have obtained the KSBS using the bisection method and the feasibility test. Our simulation results have shown that the proposed learning algorithm can converge faster than the baseline and the KSBS can provide the best sum utilities. Moreover, we have shown that the proposed algorithm can achieve significantly higher accuracy in non-iid datasets.

REFERENCES

- [1] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, "Communication-efficient learning of deep networks from decentralized data," *arXiv preprint arXiv:1602.05629*, 2017.
- [2] A. Singh, P. Vepakomma, O. Gupta, and R. Raskar, "Detailed comparison of communication efficiency of split learning and federated learning," *arXiv preprint arXiv:1909.09145*, 2019.
- [3] S. Abuadba, K. Kim, M. Kim, C. Thapa, S. A. Camtepe, Y. Gao, H. Kim, and S. Nepal, "Can we use split learning on 1d cnn models for privacy preserving training?" in *Proc. of the ACM Asia Conference on Computer and Communications Security*, Taipei, Taiwan, Oct.
- [4] P. Vepakomma, O. Gupta, A. Dubey, and R. Raskar, "Reducing leakage in distributed deep learning for sensitive health data," *arXiv preprint arXiv:1812.00564*, 2019.
- [5] C. Thapa, P. C. M. Arachchige, S. Camtepe, and L. Sun, "Splitfed: When federated learning meets split learning," in *Proc. of Association for the Advancement of Artificial Intelligence (AAAI)*, vol. 36, no. 8, Mar. 2022.
- [6] M. Chen, D. Gündüz, K. Huang, W. Saad, M. Bennis, A. V. Feljan, and H. V. Poor, "Distributed learning in wireless networks: Recent progress and future challenges," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 12, pp. 3579–3605, Dec. 2021.
- [7] D.-J. Han, H. I. Bhatti, J. Lee, and J. Moon, "Accelerating federated learning with split learning on locally generated losses," in *Proc. of International Conference on Machine Learning (ICML), Workshop on Federated Learning for User Privacy and Data Confidentiality*, Virtual, Jul. 2021.
- [8] W. Wu, M. Li, K. Qu, C. Zhou, W. Zhuang, X. Li, W. Shi *et al.*, "Split learning over wireless networks: Parallel design and resource management," *arXiv preprint arXiv:2204.08119*, 2022.
- [9] M. G. Arivazhagan, V. Aggarwal, A. K. Singh, and S. Choudhary, "Federated learning with personalization layers," *arXiv preprint arXiv:1912.00818*, 2019.
- [10] Z. Yang, M. Chen, W. Saad, C. S. Hong, and M. Shikh-Bahaei, "Energy efficient federated learning over wireless communication networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1935–1949, Mar. 2021.
- [11] N. H. Tran, W. Bao, A. Zomaya, M. N. H. Nguyen, and C. S. Hong, "Federated learning over wireless networks: Optimization model design and analysis," in *Proc. of IEEE Conf. on Computer Commun.*, Paris, France, May 2019.
- [12] Z. He, T. Zhang, and R. B. Lee, "Model inversion attacks against collaborative inference," in *Proc. of the Annual Computer Security Applications Conference*, NY, USA, Dec. 2019.
- [13] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, "Game Theory in Wireless and Communication Networks: Theory, Models, and Applications". Cambridge University Press, 2011.
- [14] M. Nokleby and A. L. Swindlehurst, "Bargaining and the miso interference channel," *EURASIP J. Appl. Signal Process*, vol. 2009, pp. 1–13, Apr. 2009.
- [15] A. Fallah, A. Mokhtari, and A. Ozdaglar, "Personalized federated learning: A meta-learning approach," *arXiv preprint arXiv:2002.07948*, 2020.
- [16] S. P. Karimireddy, S. Kale, M. Mohri, S. Reddi, S. Stich, and A. T. Suresh, "Scaffold: Stochastic controlled averaging for federated learning," in *Proc. of International Conference on Machine Learning (ICML)*, Virtual, Jul. 2020.