

Federated Learning via Plurality Vote

Kai Yue, *Graduate Student Member, IEEE*, Richeng Jin, *Member, IEEE*, Chau-Wai Wong, *Member, IEEE*, and Huaiyu Dai, *Fellow, IEEE*

Abstract—Federated learning allows collaborative clients to solve a machine learning problem while preserving data privacy. Recent studies have tackled various challenges in federated learning, but the joint optimization of communication overhead, learning reliability, and deployment efficiency is still an open problem. To this end, we propose a new scheme named federated learning via plurality vote (FedVote). In each communication round of FedVote, clients transmit binary or ternary weights to the server with low communication overhead. The model parameters are aggregated via weighted voting to enhance the resilience against Byzantine attacks. When deployed for inference, the model with binary or ternary weights is resource-friendly to edge devices. Our results demonstrate that the proposed method can reduce quantization error and converges faster compared to the methods directly quantizing the model updates.

Index Terms—Federated learning, distributed optimization, neural network quantization, efficient communication

I. INTRODUCTION

Federated learning enables multiple clients to solve a machine learning problem under the coordination of a central server [1]. Throughout the training stage, client data will be kept locally and only model weights or model updates will be shared with the server. Federated averaging (FedAvg) [2] was proposed as a generic federated learning solution. Although FedAvg takes advantage of distributed client data while maintaining their privacy, it leaves the following two challenges unsolved. First, transmitting high-dimensional vectors between a client and the server for multiple rounds can incur significant communication overhead. In the federated learning literature, quantization has been directly applied to raw gradients to lower the communication overhead [3, 4]. However, a more sophisticated design of a quantization scheme may provide better trade-offs between communication efficiency and model accuracy. Second, the aggregation rule in FedAvg is vulnerable to Byzantine attacks [5]. Prior works tackled this issue by using robust statistics such as coordinate-wise median and geometric median in the aggregation step [5, 6]. Another strategy is to detect and reject updates from malicious attackers [7, 8]. The robustness of the algorithm is enhanced at the cost of additional computational and algorithmic complexity.

Manuscript received February 17, 2022; revised September 28, 2022 and November 1, 2022; accepted November 22, 2022. This work was supported in part by the US National Science Foundation under grants CNS-1824518 and ECCS-2203214. (Corresponding author: Chau-Wai Wong.)

K. Yue, C.-W. Wong, and H. Dai are with the Department of Electrical and Computer Engineering, NC State University, Raleigh, NC 27695 USA (e-mail: {kyue, chauwai.wong, hdai}@ncsu.edu).

R. Jin is with the College of Information Science and Electronic Engineering, Zhejiang University, the Zhejiang–Singapore Innovation and AI Joint Research Lab, and the Zhejiang Provincial Key Lab of Information Processing, Communication and Networking (IPCAN), Hangzhou, China, 310000 (e-mail: richengjin@zju.edu.cn).

In this paper, we propose a new method called federated learning via plurality vote (FedVote). On the client side, we optimize a neural network with a range normalization function applied to model weights. After local updating, binary/ternary weight vectors are obtained via stochastic rounding and sent to the server. The global model is updated by a voting procedure, and the voting results are sent back to each client for further optimization in the next round. The contributions of the paper are summarized as follows.

- 1) We present FedVote as a novel federated learning solution. By exploiting the quantized model optimization on the client side and aggregation on the server side, we jointly optimize the communication overhead, learning reliability, and deployment efficiency.
- 2) We theoretically and experimentally verify the effectiveness of our FedVote design. In bandwidth-limited scenarios, FedVote is particularly advantageous in simultaneously achieving a high compression ratio and good test accuracy. Given a fixed communication cost, FedVote improves model accuracy on the non-i.i.d. CIFAR-10 dataset by 5–10%, 15–20%, and 25–30% compared to FedPAQ [3], signSGD [9], and FedAvg, respectively.
- 3) We extend FedVote to incorporate reputation-based voting in cross-silo federated learning. The proposed method, Byzantine-FedVote, exhibits much better resilience to Byzantine attacks in the presence of close to half attackers without incurring excessive computation compared with existing algorithms.

II. RELATED WORK

Federated learning serves as a privacy-preserving framework where clients can collaborate without sharing raw data. To improve communication efficiency, various strategies have been proposed. For example, Sattler et al. [10] combined quantization and sparsification tools to lower the communication overhead. Bernstein et al. [9] showed that sign-based gradient descent schemes have good convergence rate in the homogeneous data distribution scenario. This approach is further extended to the heterogeneous data distribution setting [11–13]. FedAvg [2] adopts a periodic averaging scheme and targets at reducing the number of communication rounds. The convergence properties of FedAvg have been verified under different analytical frameworks [14, 15]. Hybrid methods consider simultaneous local updates and accumulative gradient compression [3, 4]. In parallel with the aforementioned studies, cryptographic solutions have been adopted to provide stronger privacy protection, such as secure aggregation [16] and homomorphic encryption [17]. These algorithms may not be easily deployed in federated learning due to their special setups and additional communication and computational overheads.

Meanwhile, there exist many open challenges to federated learning that is resilient to Byzantine adversaries, where arbitrary outputs can be produced. Blanchard et al. [5] showed that FedAvg cannot tolerate a single Byzantine attacker. They proposed to select the gradient from normal clients based on the similarity of local updates. The idea of detecting malicious attackers based on similarity scores has been further developed in follow-up works. Cao et al. [18] calculated the cosine similarity scores between the malicious gradient and reference gradient based on a public small public dataset. Likewise, Shejwalkar et al. [19] assumed a known number of attackers and filtered out malicious updates by computing the similarity score between the gradient and the extracted eigenvector.

Inspired from the work of model quantization [20–23], we improve communication efficiency by using stochastic binary/ternary weights. Our study is orthogonal to existing algorithms that focus on gradient compression. Furthermore, we propose a reputation-based voting strategy for FedVote that is shown to have good convergence performance in the Byzantine setting. Compared to prior defense work, we do not assume a known number of attackers [5, 19] and do not require the availability of a well-distributed public dataset [18].

A few recent work has also conducted case studies of quantized neural network in federated learning. Lin et al. [24] reported the model accuracy of 1-bit quantized neural networks aggregated via ensemble distillation. The aggregation becomes complicated due to the separate optimization stage of knowledge distillation. In addition, their BNN optimization is not tailored to the federated learning setting. Hou et al. [25] theoretically analyzed the convergence of distributed quantized neural networks, which was later implemented in the application of intrusion detection [26]. Compared to [25], we do not assume a convex and twice differentiable objective function and bounded gradients. Therefore, their analysis cannot be directly applied to our study. We take a different perspective from the existing work and demonstrate that model quantization can be a more effective design to improve communication efficiency compared to gradient quantization.

III. PRELIMINARIES

Symbol conventions are as follows. We use $[N]$ to denote the set of integers $\{1, 2, \dots, N\}$. Bold lower cases of letters such as \mathbf{v}_m represent column vectors, and $v_{m,i}$ is the i th entry in the vector. For a scalar function, it applies elementwise operation when a vector input is given. $\mathbf{1} = [1, \dots, 1]^\top$ denotes a vector with all entries equal to 1.

A. Federated Learning

The goal of federated learning is to build a machine learning model based on the training data distributed among multiple clients. To facilitate the learning procedure, a server will coordinate the training without accessing raw data [1]. In a supervised learning scenario, let $\mathcal{D}_m = \{(\mathbf{x}_{m,j}, \mathbf{y}_{m,j})\}_{j=1}^{n_m}$ denote the training dataset on the m th client, with the input $\mathbf{x}_{m,j} \in \mathbb{R}^{d_1}$ and the label $\mathbf{y}_{m,j} \in \mathbb{R}^{d_2}$ in each training pair.

The local objective function f_m with a model weight vector $\boldsymbol{\theta} \in \mathbb{R}^d$ is given by

$$f_m(\boldsymbol{\theta}) \triangleq f_m(\boldsymbol{\theta}; \mathcal{D}_m) = \frac{1}{n_m} \sum_{j=1}^{n_m} \ell(\boldsymbol{\theta}; (\mathbf{x}_{m,j}, \mathbf{y}_{m,j})), \quad (1)$$

where ℓ is a loss function quantifying the error of model $\boldsymbol{\theta}$ predicting the label $\mathbf{y}_{m,j}$ for an input $\mathbf{x}_{m,j}$. A global objective function may be formulated as

$$\min_{\boldsymbol{\theta} \in \mathbb{R}^d} f(\boldsymbol{\theta}) = \frac{1}{M} \sum_{m=1}^M f_m(\boldsymbol{\theta}). \quad (2)$$

B. Quantized Neural Networks

Consider a neural network g with the weight vector $\boldsymbol{\theta} \in \mathbb{R}^d$. A forward pass for an input $\mathbf{x} \in \mathbb{R}^{d_1}$ and a prediction $\hat{\mathbf{y}} \in \mathbb{R}^{d_2}$ can be written as $\hat{\mathbf{y}} = g(\boldsymbol{\theta}, \mathbf{x})$. In quantized neural networks, the real-valued $\boldsymbol{\theta}$ is replaced by $\mathbf{w} \in \mathbb{D}_n^d$, where \mathbb{D}_n is a discrete set with a number n of quantization levels. For example, we may have $\mathbb{D}_2 = \{-1, 1\}$ for a binary neural network. For a given training set $\{(\mathbf{x}_j, \mathbf{y}_j)\}_{j=1}^N$ and the loss function ℓ , the goal is to find an optimal \mathbf{w}^* such that the averaged loss is minimized over a search space of quantized weight vectors:

$$\mathbf{w}^* = \underset{\mathbf{w} \in \mathbb{D}_n^d}{\operatorname{argmin}} \frac{1}{N} \sum_{j=1}^N \ell(\mathbf{w}; (\mathbf{x}_j, \mathbf{y}_j)). \quad (3)$$

Prior studies tried to solve (3) by optimizing a real-valued latent weight vector $\mathbf{h} \in \mathbb{R}^d$. The interpretations of the latent weight vary when viewed from different perspectives. Hubara et al. [20] used the sign operation to quantize the latent weight into two levels during the forward pass. The binary weights can be viewed as an approximation of their latent real-valued counterparts. Shayer et al. [21] trained a stochastic binary neural network, and the normalized latent parameters are interpreted as the Bernoulli distribution parameter ϑ_i :

$$\vartheta_i \triangleq \widehat{\mathbb{P}}(w_i = 1) = S(h_i), \quad w_i \in \{0, 1\}, \quad (4)$$

where $S: \mathbb{R} \rightarrow (0, 1)$ is the sigmoid function. In the forward pass, instead of using the binary vector \mathbf{w} , its expected value,

$$\tilde{\mathbf{w}}_{\text{sto-bnn}} \triangleq \mathbb{E}[\mathbf{w}] = -1 \times [\mathbf{1} - S(\mathbf{h})] + 1 \times S(\mathbf{h}) = 2S(\mathbf{h}) - \mathbf{1}, \quad (5)$$

will participate in the actual convolution or matrix multiplication operations. In other words, the neural network function becomes $\hat{\mathbf{y}} = g(\tilde{\mathbf{w}}_{\text{sto-bnn}}, \mathbf{x})$. Likewise, Gong et al. [22] normalized the latent weight but interpreted it from a non-probabilistic viewpoint. They approximated the staircase quantization function with a differentiable soft quantization (DSQ) function, i.e.,

$$\tilde{\mathbf{w}}_{\text{dsq}} \triangleq \tanh(a\mathbf{h}), \quad (6)$$

where $\tanh: \mathbb{R} \rightarrow (-1, 1)$ is the hyperbolic tangent function, and a controls the shape of the function. The neural network function thus becomes $\hat{\mathbf{y}} = g(\tilde{\mathbf{w}}_{\text{dsq}}, \mathbf{x})$. The binary weights are obtained through the sign operation.

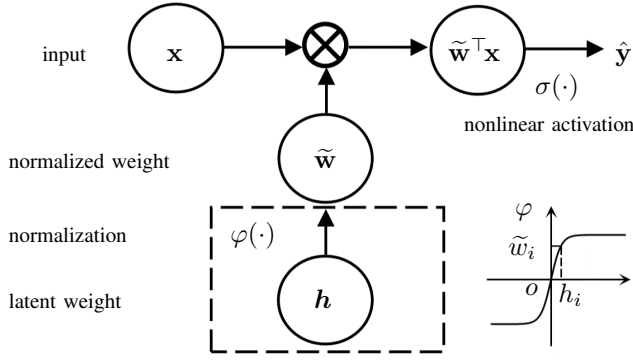


Fig. 1: Example of a single-layer quantized neural network with a latent weight vector $\mathbf{h} \in \mathbb{R}^d$. \mathbf{h} is normalized to generate $\tilde{\mathbf{w}} \in (-1, 1)^d$, and the output is $\hat{\mathbf{y}} = \sigma(\tilde{\mathbf{w}}^T \mathbf{x})$. A binary weight \mathbf{w} can be obtained by thresholding or stochastically rounding $\tilde{\mathbf{w}}$ to the discrete space \mathbb{D}_2^d .

IV. PROPOSED FEDVOTE ALGORITHM

Inspired by prior works, we first present the latent weight-based BNN training methods. We depict an example of a single-layer network in Fig. 1 and give the details as follows. First, a real-valued vector $\mathbf{h} \in \mathbb{R}^d$ is introduced and its range is restricted by using a differentiable and invertible normalization function $\varphi : \mathbb{R} \rightarrow (-1, 1)$, such as the error function $\text{erf}(\cdot)$ or hyperbolic function $\tanh(\cdot)$. The forward pass is then calculated with the normalized weight vector $\tilde{\mathbf{w}}$. The procedure is described as:

$$\hat{\mathbf{y}} = g(\tilde{\mathbf{w}}, \mathbf{x}), \quad \tilde{\mathbf{w}} \triangleq \varphi(\mathbf{h}). \quad (7)$$

Second, in the back propagation, the latent weight vector \mathbf{h} is updated with its gradient, $\mathbf{h}^{(t+1)} = \mathbf{h}^{(t)} - \eta \nabla_{\mathbf{h}} \ell$. Finally, the normalized weight vector $\tilde{\mathbf{w}}$ is mapped to the discrete space to approximate \mathbf{w}^* via thresholding or stochastic rounding.

The separate representation of the quantized weight \mathbf{w} and latent weight \mathbf{h} in the aforementioned model quantization scheme has introduced unique challenges in designing a federated training algorithm. For example, if clients choose to upload only binary weights \mathbf{w} to save bandwidth, the latent weight \mathbf{h} on the server will be out of sync. Besides, the advantages of designing model quantization methods over existing gradient quantization algorithms in federated learning is unexplored. To answer these questions, we present FedVote algorithm with an emphasis on uplink communication efficiency and enhanced Byzantine resilience. We follow the widely adopted analysis framework in wireless communication to investigate only the client uplink overhead, assuming that the downlink bandwidth is much larger and the server will have enough transmission power [27]. To reduce the message size per round, we train a quantized neural network under the federated learning framework. The goal is to find a quantized weight vector \mathbf{w}^* that minimizes the global objective function f formulated in (2),

$$\mathbf{w}^* = \underset{\mathbf{w} \in \mathbb{D}_2^d}{\text{argmin}} f(\mathbf{w}). \quad (8)$$

For the simplicity of presentation, we mainly focus on the BNN case with $\mathbb{D}_2 = \{-1, 1\}$. We illustrate the procedure in

Algorithm 1: Binary-Weight FedVote with/without Byzantine Tolerance

```

1 initialize  $p^{(0)}$  and broadcast
2 for  $k = 0, 1, \dots, N - 1$  do
3   on  $m^{\text{th}}$  worker:
4     receive  $p^{(k)}$  from the server
5     initialize latent weight  $\mathbf{h}_m^{(k,0)} = \varphi^{-1}(2p^{(k)} - 1)$ 
6     for  $t = 0 : \tau - 1$  do
7        $\tilde{\mathbf{g}}_m^{(k,t)} = \nabla_{\mathbf{h}} f_m(\varphi(\mathbf{h}_m^{(k,t)}); \xi_m^{(t,r)})$ 
8        $\mathbf{h}_m^{(k,t+1)} = \mathbf{h}_m^{(k,t)} - \eta^{(k,t)} \tilde{\mathbf{g}}_m^{(k,t)}$ 
9        $\tilde{\mathbf{w}}_m^{(k,\tau)} = \varphi(\mathbf{h}_m^{(k,\tau)})$ 
10       $\mathbf{w}_m^{(k,\tau)} = \text{sto\_rounding}(\tilde{\mathbf{w}}_m^{(k,\tau)}) \triangleright \text{Eq. (11)}$ 
11      send  $\mathbf{w}_m^{(k,\tau)}$  to server
12   on server:
13      $\{\mathbf{w}^{(k+1)}, p^{(k+1)}\} = \text{vote}(\{\mathbf{w}_m^{(k,\tau)}\}_{m=1}^M)$ 
14     broadcast  $p^{(k+1)}$  to workers
15 function vote( $\{\mathbf{w}_m^{(k,\tau)}\}_{m=1}^M$ )
16   for  $i = 1 : d$  do
17      $w_i^{(k+1)} = \text{sign}\left(\sum_{m=1}^M w_{m,i}^{(k,\tau)}\right)$ 
18      $p_i^{(k+1)} = \frac{1}{M} \sum_{m=1}^M \mathbb{1}(w_{m,i}^{(k,\tau)} = 1) \triangleright \text{Option I}$ 
19      $p_i^{(k+1)} = \sum_{m=1}^M \lambda_m^{(k)} \mathbb{1}(w_{m,i}^{(k,\tau)} = 1) \triangleright \text{Option II}$ 
20   return  $\{\mathbf{w}^{(k+1)}, p^{(k+1)}\}$  to the server

```

Fig. 2 and provide the pseudo code in Algorithm 1. Below, we explain each step in more detail.

A. Local Model Training and Transmission

We optimize a neural network with a learnable latent weight vector \mathbf{h} . In the k th communication round, we assume all clients are identically initialized by the server, namely, $\forall m \in [M], \mathbf{h}_m^{(k,0)} = \mathbf{h}^{(k)}$. To reduce the total number of communication rounds, we first let each client conduct local updates to learn the binary weights. For each local iteration step, the local latent weight vector $\mathbf{h}^{(k,t+1)}$ is updated by the gradient descent:

$$\mathbf{h}_m^{(k,t+1)} = \mathbf{h}_m^{(k,t)} - \eta \nabla_{\mathbf{h}} f_m(\varphi(\mathbf{h}_m^{(k,t)}); \xi_m^{(k,t)}), \quad (9)$$

where $\xi_m^{(k,t)}$ is a mini-batch randomly drawn from \mathcal{D}_m at the t th iteration of round k . After updating for τ steps, we obtain $\mathbf{h}_m^{(k,\tau)}$ and the corresponding normalized weight vector $\tilde{\mathbf{w}}_m^{(k,\tau)} \in (-1, 1)^d$ defined as follows:

$$\tilde{\mathbf{w}}_m^{(k,\tau)} \triangleq \varphi(\mathbf{h}_m^{(k,\tau)}). \quad (10)$$

We use the stochastic rounding [28] to draw a randomly quantized version $\mathbf{w}_m^{(k,\tau)}$ using $\tilde{\mathbf{w}}_m^{(k,\tau)}$, i.e.,

$$w_{m,i}^{(k,\tau)} = \begin{cases} +1, & \text{with prob. } \pi_{m,i}^{(k,\tau)} = \frac{1}{2} [\tilde{w}_{m,i}^{(k,\tau)} + 1], \\ -1, & \text{with prob. } 1 - \pi_{m,i}^{(k,\tau)}. \end{cases} \quad (11)$$

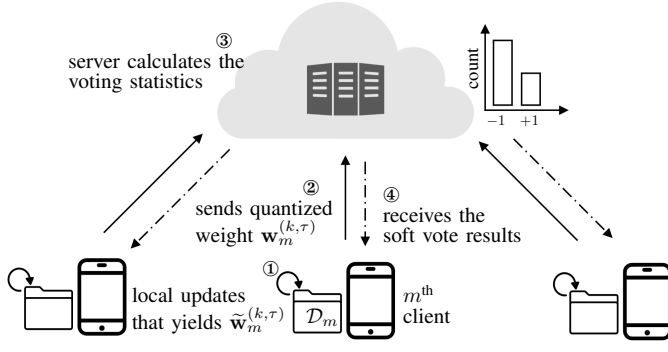


Fig. 2: One round of FedVote is composed of four steps. Each client first updates the local model and then sends the quantized weight $\mathbf{w}_m^{(k,\tau)}$ to the server. Later, the server calculates the voting statistics and sends back the soft voting results $\mathbf{p}^{(k+1)}$ to each client.

It can be shown that the stochastic rounding is an unbiased procedure, i.e., $\mathbb{E}[\mathbf{w}_m^{(k,\tau)} | \tilde{\mathbf{w}}_m^{(k,\tau)}] = \tilde{\mathbf{w}}_m^{(k,\tau)}$. After quantization, the local client will send the binary weights $\mathbf{w}_m^{(k,\tau)}$ to the server for the global model aggregation.

B. Global Model Aggregation and Broadcast

Once the server gathers the binary weights from all clients, it will perform the aggregation via plurality vote, i.e., $\mathbf{w}^{(k+1)} = \text{sign}\left(\sum_{m=1}^M \mathbf{w}_m^{(k,\tau)}\right)$. A tie in vote will be broken randomly. In the following lemma, we show that the probability of error reduces exponentially as the number of clients increases. The proof can be found in Appendix B-A.

Lemma 1 (One-Shot FedVote) Let $\mathbf{w}^* \in \mathbb{D}_2^d$ be the optimal solution defined in (8). For the m th client, $\varepsilon_{m,i} \triangleq \mathbb{P}(w_{m,i}^{(k,\tau)} \neq w_i^*)$ denotes the error probability of the voting result of the i th coordinate. Suppose the error events $\{w_{m,i}^{(k,\tau)} \neq w_i^*\}_{m=1}^M$ are mutually independent, and the mean error probability $s_i = \frac{1}{M} \sum_{m=1}^M \varepsilon_{m,i}$ is smaller than $\frac{1}{2}$. For the voted weight $\mathbf{w}^{(k+1)}$, we have

$$\mathbb{P}(w_i^{(k+1)} \neq w_i^*) \leq [2s_i \exp(1 - 2s_i)]^{\frac{M}{2}}. \quad (12)$$

In practice, the number of available clients may be limited in each round, and the local data distribution is often heterogeneous or even time-variant. To extend the training to multiple communication rounds, we first use the soft voting to build an empirical distribution of global weight \mathbf{w} , i.e.,

$$\hat{\mathbb{P}}(w_i^{(k+1)} = 1) = \frac{1}{M} \sum_{m=1}^M \mathbb{1}(w_{m,i}^{(k,\tau)} = 1), \quad (13)$$

where $\mathbb{1}(\cdot) \in \{0, 1\}$ is the indicator function. Let $p_i^{(k+1)} \triangleq \hat{\mathbb{P}}(w_i^{(k+1)} = 1)$ and $\mathbf{p}^{(k+1)} = [p_1^{(k+1)}, \dots, p_d^{(k+1)}]^\top$. The global latent parameters can be constructed by following (10):

$$\mathbf{h}^{(k+1)} = \varphi^{-1}(2\mathbf{p}^{(k+1)} - 1), \quad (14)$$

where $\varphi^{-1} : (-1, 1) \rightarrow \mathbb{R}$ is the inverse of the normalization function φ . We further apply clipping to restrict the range of the probability, namely, $\text{clip}(p_i^{(k+1)}) = \max(p_{\min}, \min(p_{\max}, p_i^{(k+1)}))$, where $p_{\min}, p_{\max} \in (0, 1)$ are

predefined thresholds. To keep the notation consistent, we denote $\tilde{\mathbf{w}}^{(k+1)} \triangleq \varphi(\mathbf{h}^{(k+1)})$ as the global normalized weight. After broadcasting the soft voting results $\mathbf{p}^{(k+1)}$, all clients are synchronized with the same latent weight $\mathbf{h}^{(k+1)}$ and normalized weight $\tilde{\mathbf{w}}^{(k+1)}$. The learning procedure will repeat until a termination condition is satisfied. We relate FedVote to FedAvg in the following lemma. The detailed proof can be found in Appendix B-B.

Lemma 2 (Relationship with FedAvg) For the normalized weights, FedVote recovers FedAvg in expectation: $\mathbb{E}[\tilde{\mathbf{w}}^{(k+1)}] = \frac{1}{M} \sum_{m=1}^M \tilde{\mathbf{w}}_m^{(k,\tau)}$, where $\tilde{\mathbf{w}}^{(k+1)} = \varphi(\mathbf{h}^{(k+1)})$ and $\tilde{\mathbf{w}}_m^{(k,\tau)} = \varphi(\mathbf{h}_m^{(k,\tau)})$.

C. Reputation-Based Byzantine-FedVote

In this work, we assume a portion of the participants are Byzantine attackers that can access the data of other clients and modify transmitted message. Lemma 2 shows that FedVote is related to FedAvg in expectation. As we have reviewed in Section II, FedAvg cannot tolerate a single Byzantine attacker. It indicates that FedVote will exhibit similar poor performance in the presence of multiple adversaries (see Appendix A-B). We improve the design of FedVote based on a reputation voting mechanism, which is a variant of the weighted soft voting method.

Reputation-based voting was presented in failure-robust large scale grids [29]. Recent studies have also proposed reputation management schemes for federated learning [30, 31]. However, assessing the reputation of different participants is nontrivial. For example, the methods in [30, 31] simplified the attacker model and require a reference to assess the reputation of clients. Instead of building a reference explicitly, FedVote facilitates the reputation assessment by following the majority rule. We modify (13) to $\hat{\mathbb{P}}(w_i^{(k+1)} = 1) = \sum_{m=1}^M \lambda_m^{(k)} \mathbb{1}(w_{m,i}^{(k,\tau)} = 1)$, where $\lambda_m^{(k)}$ is proportional to a credibility score. In Byzantine-resilient FedVote (Byzantine-FedVote), we assume that at least 50% of the clients behave normally and treat the plurality vote result as the correct decision. The credibility score of the m th client is calculated by counting the number of correct votes it makes: $\text{CR}_m^{(k+1)} = \frac{1}{d} \sum_{i=1}^d \mathbb{1}(w_{m,i}^{(k,\tau)} = w_i^{(k+1)})$. Through multiple rounds, we track the credibility of a local client by taking an exponential moving average over the communication rounds, namely, $\nu_m^{(k+1)} = \beta \nu_m^{(k)} + (1 - \beta) \text{CR}_m^{(k+1)}$, where $\beta \in (0, 1)$ is a predefined coefficient. The weight $\lambda_m^{(k)}$ is designed as $\lambda_m^{(k)} = \nu_m^{(k)} / \sum_{m=1}^M \nu_m^{(k)}$.

Although we focus on the binary weights in this section, the scheme can be naturally extended to quantized neural networks of more discrete levels. We will briefly discuss the implementation for ternary weights in Section VI.

V. ANALYSIS OF ALGORITHM

In this section, we present the theoretical analysis of FedVote when local data are independent and identically distributed (i.i.d.). The empirical results in the non-i.i.d. setting are discussed in Section VI. We consider nonconvex

objective functions for neural network optimization. We use the temporal average of the gradient norm as an indicator of convergence, which is commonly adopted in the literature [3, 4]. The algorithm converges to a stationary point when the gradient norm is sufficiently small. We denote the stochastic local gradient by $\tilde{\mathbf{g}}_m^{(k,t)} \triangleq \nabla_{\mathbf{h}} f_m(\varphi(\mathbf{h}_m^{(k,t)}); \xi_m^{(k,t)})$. The local true gradient and global true gradient will be denoted by $\mathbf{g}_m^{(k,t)} \triangleq \mathbb{E}_{\xi}[\tilde{\mathbf{g}}_m^{(k,t)}]$, $\mathbf{g}^{(k)} \triangleq \nabla_{\mathbf{h}} f(\varphi(\mathbf{h}^{(k)}))$, respectively. In addition, let $\zeta_m^{(k)} \triangleq \tilde{\mathbf{w}}_m^{(k,\tau)} - \mathbf{w}_m^{(k,\tau)}$ denote the error introduced by stochastic rounding. According to its unbiased property, $\mathbb{E}_{\pi}[\zeta_m^{(k)}] = \mathbf{0}$. With the aforementioned notations, we state five assumptions for the convergence analysis.

A. Assumptions

Assumption 1 (Lower bound) $\forall \mathbf{h} \in \mathbb{R}^d$, $\tilde{\mathbf{w}} \in (-1, 1)^d$, the objective function is lower bounded by a constant f^* , i.e., $f(\tilde{\mathbf{w}}) \geq f^* = \min_{\mathbf{h} \in \mathbb{R}^d} f(\varphi(\mathbf{h}))$.

Assumption 2 (L-smoothness) $\forall \tilde{\mathbf{w}}_1, \tilde{\mathbf{w}}_2 \in (-1, 1)^d$, $m \in \{1, \dots, M\}$, there exists some nonnegative L such that $\|\nabla f_m(\tilde{\mathbf{w}}_1) - \nabla f_m(\tilde{\mathbf{w}}_2)\|_2 \leq L \|\tilde{\mathbf{w}}_1 - \tilde{\mathbf{w}}_2\|_2$.

Assumptions 1 to 2 are common for necessary analysis [32]. We limit the range of the normalized weight $\tilde{\mathbf{w}}$ while in a typical setting there is no restriction to the model weight.

Assumption 3 The normalization function $\varphi: \mathbb{R} \rightarrow (-1, 1)$ is strictly increasing. In particular, we assume its first derivative is bounded for all $h_{m,i}^{(k,t)}$, i.e., $\frac{d}{dh} \varphi(h_{m,i}^{(k,t)}) \in [c_1, c_2]$, where c_1, c_2 are positive parameters independent of k, t, m , and i .

Assumption 3 is not difficult to satisfy in practice. For example, let $\varphi(h) = \tanh(ah)$, we have $\varphi'(h) = a[1 - \tanh^2(ah)]$, with $c_2 = a$. Note that φ quickly saturates with a large h in the local updating. On the other hand, the empirical Bernoulli parameter p_i will be clipped for stability, which indicates that $h_{m,i}^{(k,t)}$ will be upper bounded by certain h_B . In this sense, we have $c_1 = a[1 - \tanh^2(ah_B)]$. The next two assumptions bound the variance of the stochastic gradient and quantization noise.

Assumption 4 The stochastic gradient has bounded variance, i.e., $\mathbb{E} \|\mathbf{g}_m^{(k,t)} - \tilde{\mathbf{g}}_m^{(k,t)}\|_2^2 \leq \sigma_\varepsilon^2$, where σ_ε^2 is a fixed variance independent of k, t and m .

Assumption 5 The quantization error $\zeta_m^{(k)}$ has bounded variance, i.e., $\mathbb{E} \|\zeta_m^{(k)}\|_2^2 \leq \sigma_k^2$, where σ_k^2 is a fixed variance independent of m .

Note that quantization error is affected by the quantizer type and the corresponding input. For example, if the normalization function φ approximates the sign function very well, the stochastic quantization error will be close to zero. Formally, the upper bound σ_k^2 can be viewed as a function of input dimension d , which we formulate in the following lemma. The proof is in Appendix B-C.

Lemma 3 Suppose we have an input $\mathbf{a} \in (-1, 1)^d$ for the quantizer Q_{sr} defined in (11), then the quantization error satisfies $\mathbb{E} [\|Q_{\text{sr}}(\mathbf{a}) - \mathbf{a}\|_2^2] = d - \|\mathbf{a}\|_2^2$.

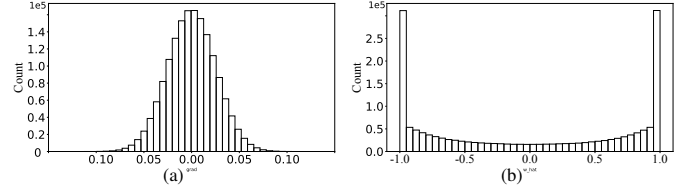


Fig. 3: Histograms of (a) model updates $\delta_{m,i}^{(k)}$ and (b) binary weight probabilities $\pi_{m,i}^{(k,\tau)}$. We trained a LeNet model on the MNIST dataset for a single communication round and inspect the histograms on one client.

For existing algorithms quantizing the model update $\delta_m^{(k)} \triangleq \theta_m^{(k)} - \theta_m^{(k,\tau)}$, the quantizer has the property $\mathbb{E} [\|Q(\mathbf{x}) - \mathbf{x}\|_2^2] \leq q \|\mathbf{x}\|_2^2$. With a fixed quantization step, q increases when the input dimension d increases [33]. We state the result for a widely-used quantizer, QSGD [28], which has been adopted in FedPAQ, in the following lemma.

Lemma 4 Suppose we have an input $\mathbf{x} \in \mathbb{R}^d$ for the QSGD quantizer Q . In the coarse quantization scenario, the quantization error satisfies $\mathbb{E} [\|Q(\mathbf{x}) - \mathbf{x}\|_2^2] = O(d^{\frac{1}{2}}) \|\mathbf{x}\|_2^2$.

B. Convergence Analysis

We state the convergence results in the following theorem. The proof can be found in Appendix B-E.

Theorem 1 For FedVote under Assumptions 1 to 5, let the learning rate $\eta = O\left(\frac{c_1}{c_2^2} \frac{1}{L\tau\sqrt{K}}\right)$, then after K rounds of communication, we have

$$\begin{aligned} \frac{1}{K} \sum_{k=0}^{K-1} c_1^2 \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 &\leq \frac{2[f(\tilde{\mathbf{w}}^{(0)}) - f(\tilde{\mathbf{w}}^*)]}{\eta\tau K} \\ &+ c_2^2 L\eta \left[\frac{1}{M} + \frac{c_1^2 L\eta(\tau-1)}{2} \right] \sigma_\varepsilon^2 \\ &+ \frac{L}{\eta\tau KM} \sum_{k=0}^{K-1} \sigma_k^2 + \frac{2(c_2^2 - c_1^2)}{\tau MK} \sum_{k=0}^{K-1} \sum_{m=1}^M R_m^{(k)}, \quad (15) \end{aligned}$$

where $R_m^{(k)} \triangleq - \sum_{t=0}^{\tau-1} \sum_{i \notin \mathcal{I}_m^{(k,t)}} \mathbb{E} [(\nabla f(\tilde{\mathbf{w}}^{(k)}))_i (\nabla f(\tilde{\mathbf{w}}_m^{(k,t)}))_i]$

and $\mathcal{I}_m^{(k,t)} \triangleq \{i \in [d] | \mathbf{g}_i^{(k)} \mathbf{g}_{m,i}^{(k,t)} \geq 0\}$.

The choice of the learning rate η is discussed in Appendix B-E. We further comment on the result in Theorem 1 below.

Remark 1 When there is no normalization function and quantization, i.e., $\varphi(x) = x$ with $c_1 = c_2 = 1$, $\sigma_k^2 = 0$, Theorem 1 recovers the result obtained in [32].

To discuss the impact of quantization error, consider the distribution of different inputs. For the model update $\delta_m^{(k)}$, we expect the central limit theorem to render its distribution shape, where each entry $\delta_{m,i}^{(k)}$ follows the Gaussian distribution. For the Bernoulli probability $\pi_m^{(k,\tau)}$, we expect the Beta distribution as the conjugate prior to render its distribution shape, where each entry $\pi_{m,i}^{(k,\tau)}$ follows the symmetric Beta distribution. See Fig. 3 for the empirical results.

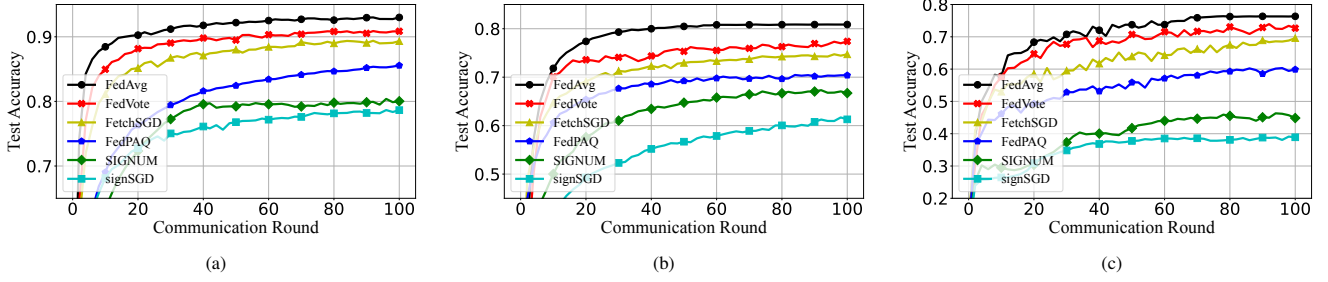


Fig. 4: Test accuracy versus communication round for different communication-efficient methods on (a) cross-device non-i.i.d. FEMNIST with 300 clients, (b) cross-silo non-i.i.d. CIFAR-10 with 31 clients, and (c) cross-device non-i.i.d. CIFAR-10 with 100 clients. FedVote outperforms other communication-efficient methods by achieving the highest accuracy given the communication round.

Remark 2 Following the analysis framework in Theorem 1, the order-wise convergence rate can be formulated as $\frac{1}{K} \sum_{k=0}^{K-1} \mathbb{E} \|\nabla f(\mathbf{w}^{(k)})\|_2^2 = O\left(\frac{1}{\sqrt{K}}\right) + E(d)$, where $E(d)$ is the error introduced by the quantization. For FedVote with the normalized weight $\tilde{\mathbf{w}}_m^{(k,\tau)}$ as the input, when $\pi_{m,i}^{(k,\tau)}$'s follow the symmetric Beta distribution, it can be shown that $\mathbb{E} \|\zeta_m^{(k)}\|_2^2 = O(d)$ based on Lemma 3. For FedPAQ with the model update $\delta_m^{(k)}$ as the input, when $\delta_{m,i}^{(k)}$'s follow the Gaussian distribution, it can be shown that $\mathbb{E} \|Q(\delta_m^{(k)}) - \delta_m^{(k)}\|_2^2 = O(d^{3/2})$ based on Lemma 4. When the weight dimension d is sufficiently large, FedVote converges faster.

Remark 3 The value of the scalar error term $R_m^{(k)}$ in (15) depends on the gradient dissimilarity. If the angle between the local gradient $\nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)})$ and the global one $\nabla f(\tilde{\mathbf{w}}^{(k,t)})$ is not large, $R_m^{(k)}$ can be treated as a bounded variable.

Remark 4 The choice of nonlinear function $\varphi : \mathbb{R}^d \rightarrow (-1, 1)^d$ will affect the convergence. If φ behaves more like the $\text{sign}(\cdot)$ function, e.g., when a increases in $\tanh(ax)$, the quantization error will be reduced. In other words, we expect a smaller σ_k^2 according to Lemma 3, which leads to a tighter bound in (15). Meanwhile, a larger c_2 will negatively influence the convergence.

VI. EXPERIMENTAL RESULTS

Data and Models. We choose image classification datasets, CIFAR-10 [34], FEMNIST [35], and Fashion-MNIST [36]. Suppose each dataset has C label categories. For FEMNIST, the heterogeneity comes from the unique writing styles of clients. We consider two data partition strategies for CIFAR-10 and Fashion-MNIST: (i) i.i.d. setting where the whole dataset is randomly shuffled and assigned to each worker without overlap; (ii) non-i.i.d. setting where we follow [37] and use a Dirichlet distribution to simulate the heterogeneity. In particular, for the m th worker we draw a random vector $\mathbf{q}_m \sim \text{Dir}(\alpha)$, where $\mathbf{q}_m = [q_{m,1}, \dots, q_{m,C}]^\top$ belongs to the standard $(C-1)$ -simplex. We then assign data samples from different classes to the m th worker following the distribution of \mathbf{q}_m . We set $\alpha = 0.5$ unless noted otherwise. We use a LeNet-5 architecture for Fashion-MNIST and a VGG-7 architecture for CIFAR-10 and FEMNIST. Results are obtained over three repetitions.

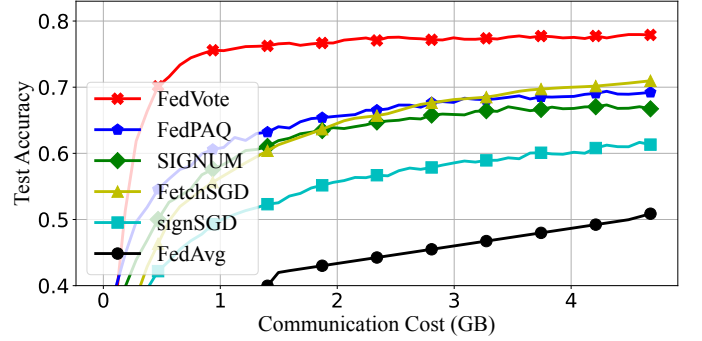


Fig. 5: Test accuracy versus accumulative uplink communication cost on non-i.i.d. CIFAR-10. FedVote outperforms other methods by achieving the highest test accuracy when the communication cost is fixed.

Implementation Details. We provide implementation details in the proposed FedVote design. First, following prior works [21, 22], we keep the weights of the BNN final layer as floating-point values for the sake of the model performance. The weights of the final layer are randomly initialized with a shared seed and will be fixed during the training process. Second, we notice that for quantized neural networks, the batch normalization (BN) [38] after the convolutional layer is necessary to scale the activation. We use the static BN without learnable parameters and local statistics [39] to ensure the voting aggregation of binary weights. For the normalization function, we choose $\varphi(x) = \tanh(3x/2)$ unless noted otherwise. More details can be found in Appendix A-A.

Communication Efficiency and Convergence Rate. We simulate two cross-device settings and one cross-silo setting. For cross-device settings, we set 300 clients in the FEMNIST task and 100 clients in the CIFAR-10 task. We sample 20 of them uniformly at random to simulate partial participation. For the cross-silo setting, we split CIFAR-10 training examples among 31 clients. We compare FedVote with several popular gradient compression methods, including FetchSGD [40], FedPAQ [3], signSGD [9], and SIGNUM [41]. The results are shown in Fig. 4. The three plots reveal that FedVote outperforms gradient compression methods by achieving the highest accuracy in different settings. We plot test accuracy versus accumulative uplink communication cost on non-i.i.d. CIFAR-10 in Fig. 5. FedVote outperforms the gradient quantization methods such as signSGD and SIGNUM that quantize gradients to 1 bit signs, and FedPAQ that quantizes the updates

TABLE I: EFFECT OF THE NORMALIZATION FUNCTION

Fashion-MNIST		a			
		0.5	1.5	2.5	10
i.i.d.	float	90.7%	90.6%	90.0%	88.2%
	binary	88.7%	90.4%	89.9%	88.2%
non-i.i.d.	float	87.3%	86.9%	85.7%	85.0%
	binary	83.3%	85.5%	85.2%	84.6%

to 2 bits integers. It also shows advantage over the count sketch based scheme, FetchSGD, which adopted a special data structure for gradient compression. Compared with FedPAQ, signSGD, and FedAvg, FedVote improves the test accuracy by 5–10%, 15–20%, and 25–30%, respectively, given the fixed communication costs of 1.5–4.7 GB.

Byzantine Resilience. We consider the following three attack methods: (i) inverse sign, where attackers inverse the signs of transmitted weights/gradients; (ii) data poisoning [18], where attackers flip the labels of the training data; (iii) random perturbation, where attackers send random weights/gradients either from a binary uniform distribution or a Gaussian distribution, sharing the same statistics with normal clients. As Byzantine-FedVote needs to maintain the credibility score for each client, we use a cross-silo federated learning setting with full participation. The number of attackers is 15, and the remaining 16 clients are normal participants. We compare the proposed method with coordinate-wise median based gradient descent [6], Krum [5], and signSGD [9] in Fig. 6. Byzantine-FedVote achieves the best resilience among various resilient schemes under different attacks.

Normalization Function. From Remark 4, we know that the normalization function can influence the model convergence. We empirically examine the impact in this experiment. For normalization function $\varphi(x) = \tanh(ax)$, we choose a from $\{0.5, 1.5, 2.5, 10\}$. We test the model accuracy after 20 communication rounds on Fashion-MNIST. The results are shown in TABLE I. As a increases, the linear region of the normalization function shrinks, and the algorithm converges slower due to a larger c_2 . On the other hand, the gap between the model with normalized weight $\tilde{\mathbf{w}}$ and the one with binary weight \mathbf{w} also decreases due to smaller quantization errors.

Ternary Neural Network Extension. In the previous sections, we focus on the BNNs. We extend FedVote to ternary neural networks (TNNs) and empirically verify its performance. Training and transmitting the categorical distribution parameters of the ternary weight may bring additional communication and computation cost to edge devices, we therefore simplify the procedure as follows. For each ternary weight $w_{m,i}^{(k,t)}$, we still keep a latent parameter $h_{m,i}^{(k,t)}$ to optimize. The detail of stochastic rounding can be found in Appendix A-C. The training results are shown in TABLE II. As TNNs can further reduce the quantization error, their performance is better than the BNNs at the cost of additional 1 bit/dimension communication overhead.

Deployment Efficiency. We highlight the advantages of BNNs during deployment on edge devices. In FedVote, we intend to deploy lightweight quantized neural networks on

TABLE II: TEST ACCURACY OF TNN AND BNN

Dataset	Distribution	BNN	TNN
Fashion-MNIST	i.i.d.	91.1%	91.9%
	non-i.i.d.	88.3%	89.4%
CIFAR-10	i.i.d.	80.5%	82.5%
	non-i.i.d.	74.6%	77.6%

TABLE III: FORWARD PASS EFFICIENCY

Neural Net	Weight Type	Adds	Muls	Energy (mJ)
LeNet-5	float	1.7×10^9	1.8×10^9	8.1
	binary	1.7×10^9	1.0×10^5	1.5
VGG-7	float	4.8×10^{10}	5.4×10^{10}	242.9
	binary	4.8×10^{10}	2.1×10^5	43.3

the workers after the training procedure. BNNs require $32 \times$ smaller memory size, which can save storage and energy consumption for memory access [20]. As we do not quantize the activations, the advantage of BNNs inference mainly lies in the replacement of multiplications by summations. Consider the matrix multiplication in a neural network with an input $\mathbf{x} \in \mathbb{R}^{d_1}$ and output $\mathbf{y} \in \mathbb{R}^{d_2}$: $\mathbf{y} = W^\top \mathbf{x}$. For a floating-point weight matrix $W \in \mathbb{R}^{d_1 \times d_2}$, the number of multiplications is $d_1 d_2$, whereas for a binary matrix $W_b \in \mathbb{D}_2^{d_1 \times d_2}$ all multiplication operations can be replaced by an additions. We investigate the number of real multiplications and additions in the forward pass of different models and present the results in TABLE III. We use the CIFAR-10 dataset and set the batch size to 100. As to the energy consumption calculation, we use 3.7 pJ and 0.9 pJ as in [20] for each floating-point multiplication and addition, respectively.

VII. CONCLUSION

In this work, we have proposed FedVote to jointly optimize communication overhead, learning reliability, and deployment efficiency. In FedVote, the server aggregates neural networks with binary/ternary weights via voting. We have verified that FedVote can achieve good model accuracy even in coarse quantization settings. Compared with gradient quantization, model quantization is a more effective design that achieves better trade-offs between communication efficiency and model accuracy. With the voting-based aggregation mechanism, FedVote enjoys the flexibility to incorporate various voting protocols to increase the resilience against Byzantine attacks. We have demonstrated that Byzantine-FedVote exhibits much better Byzantine resilience in the presence of close to half attackers compared to the existing algorithms.

APPENDIX A

SETUP AND ADDITIONAL EXPERIMENTS

A. Hyperparameters

For the clipping thresholds, we set $p_{\min} = 0.001$ and $p_{\max} = 1 - p_{\min}$. The thresholds are introduced for numerical stability and have little impact on performance. We use $\beta = 0.5$ in Byzantine-FedVote. We use the Adam optimizer and search the learning rate η over the set $\{10^{-4}, 3 \times 10^{-4}, 10^{-3}, 3 \times$

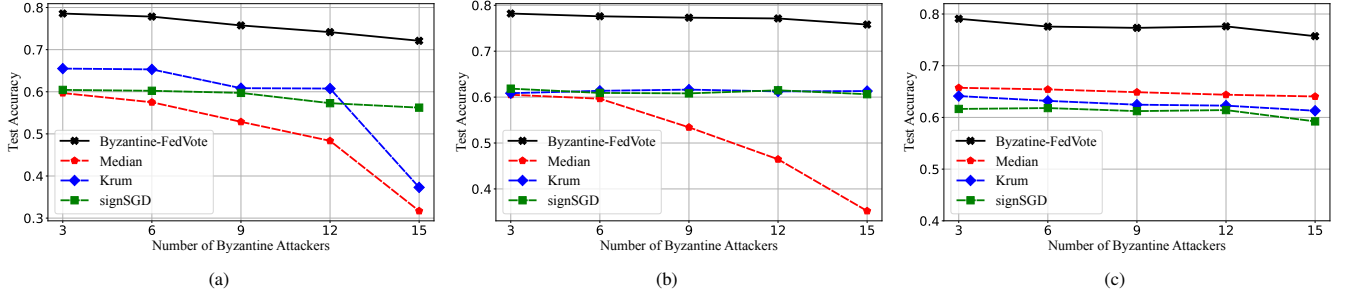


Fig. 6: Test accuracy versus the number of attackers on non-i.i.d. CIFAR-10 with (a) inverse sign attack, (b) data poisoning, and (c) random perturbation. Byzantine-FedVote shows resilience under all types of attack, with less than 7% drop in accuracy.

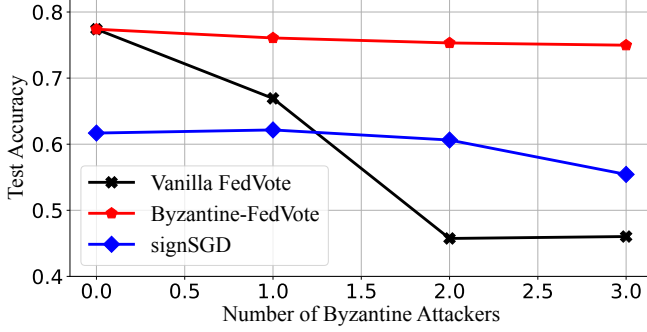


Fig. 7: Test accuracy versus the number of Byzantine workers. As the number of adversaries increases, the test accuracy of FedVote drops rapidly.

$10^{-3}, 10^{-2}, 3 \times 10^{-2}, 10^{-1}, 3 \times 10^{-1}$. We set the number of local iterations τ to 40 and the local batch size to 100. For FetchSGD [40], we set number of sketch columns to 1×10^6 and use $k = 5 \times 10^4$ in Top- k method. Our implementation is available at <https://github.com/KAI-YUE/fedvote>.

B. Comparison of Vanilla FedVote and Byzantine-FedVote

Lemma 2 shows that FedVote is related to FedAvg in expectation. Adversaries sending the opposite results will negatively affect the estimation of the weight distribution and impede the convergence in multiple rounds. We compare the test accuracy of Byzantine-FedVote, Vanilla FedVote, and signSGD on the non-i.i.d. CIFAR-10 dataset with various numbers of omniscient attackers sending the opposite aggregation results. Fig. 7 reveals that the test accuracy of Vanilla FedVote drops severely when the number of adversaries increases, which is consistent with our analysis. In contrast, the drop of accuracy in Byzantine-FedVote is negligible.

C. Extension to Ternary Neural Networks

The stochastic rounding used in the ternary neural networks, $w_i = Q_{sr}(\tilde{w})$, is an extension of (11):

$$w_i = \begin{cases} +1, & \text{with prob. } \pi_1 = \tilde{w}_i \mathbb{1}(\tilde{w}_i > 0), \\ -1, & \text{with prob. } \pi_2 = -\tilde{w}_i \mathbb{1}(\tilde{w}_i < 0), \\ 0, & \text{with prob. } 1 - (\pi_1 + \pi_2). \end{cases} \quad (16)$$

One can modify the normalization function to optimize neural networks with multiple quantization levels.

D. Batch Normalization in FedVote

Below we review the commonly-adopted BN function for convenience of presentation. For a one-dimensional input $x^{(j)}$ from the current batch $\mathcal{B} = \{x^{(1)}, \dots, x^{(n_b)}\}$, the output of BN layer is formulated as

$$y \triangleq \text{BN}_{\gamma, b}(x^{(j)}) = \gamma \frac{x^{(j)} - \mu}{\sqrt{\sigma^2 + \epsilon}} + b, \quad (17)$$

where γ, b are learnable affine transformation parameters, and μ, σ^2 are the mean and variance calculated over the batch samples. Note that the normal BN layer will introduce the real-valued parameters and track the statistics of the input, all of which may cause problems when being binarized in FedVote. Therefore, we choose to set the parameter-free static BN, i.e.,

$$y' \triangleq \text{BN}(x^{(j)}) = \frac{x - \mathbb{E}_{\mathcal{B}}[x^{(j)}]}{\sqrt{\text{Var}_{\mathcal{B}}[x^{(j)}] + \epsilon}}. \quad (18)$$

APPENDIX B MISSING PROOFS

A. Proof of Lemma 1

Proof. Let $X_{m,i} \triangleq \mathbb{1}(w_{m,i}^{(k,\tau)} \neq w_i^*)$, following Bernoulli distribution with parameter $\varepsilon_{m,i}$. Let $Y_i = \sum_{m=1}^M X_{m,i}$, we have

$$\mathbb{P}(w_i^{(k+1)} \neq w_i^*) = \mathbb{P}\left(Y_i \geq \frac{M}{2}\right). \quad (19)$$

With independent vote results from workers, Y_i follows Poisson binomial distribution with mean $\mu_{Y_i} = \sum_{m=1}^M \varepsilon_{m,i}$. $\forall a > 0$, the Chernoff bound can be derived as

$$\mathbb{P}\left(Y_i \geq \frac{M}{2}\right) = \mathbb{P}(e^{aY_i} \geq e^{\frac{aM}{2}}) \quad (20a)$$

$$\stackrel{\textcircled{1}}{\leq} \exp\left(-\frac{aM}{2}\right) \mathbb{E}[e^{aY_i}] \quad (20b)$$

$$= \exp\left(-\frac{aM}{2}\right) \prod_{m=1}^M (1 - \varepsilon_{m,i} + e^a \varepsilon_{m,i}) \quad (20c)$$

$$= \exp\left(-\frac{aM}{2} + \sum_{m=1}^M \ln(1 + \varepsilon_{m,i}(e^a - 1))\right) \quad (20d)$$

$$\stackrel{\textcircled{2}}{\leq} \exp\left(-\frac{aM}{2} + \sum_{m=1}^M \varepsilon_{m,i}(e^a - 1)\right). \quad (20e)$$

where ① is based on Markov's inequality. ② holds due to $\ln(1+x) \leq x$ for all $x \in (-1, \infty)$.

By assumption we have $\mu_{Y_i} < \frac{M}{2}$. Let $a = \ln \frac{M}{2\mu_{Y_i}}$, we have

$$\mathbb{P}\left(Y_i \geq \frac{M}{2}\right) \leq \frac{\exp(-\mu_{Y_i} + \frac{M}{2})}{\left(\frac{M}{2\mu_{Y_i}}\right)^{\frac{M}{2}}} \quad (21a)$$

$$\leq \left(\frac{2\mu_{Y_i}}{M} \exp\left(1 - \frac{2\mu_{Y_i}}{M}\right)\right)^{\frac{M}{2}}. \quad (21b)$$

Let $s_i = \frac{\mu_{Y_i}}{M} = \frac{1}{M} \sum_{m=1}^M \varepsilon_{m,i}$ and substitute it into (21b), the proof is complete. \square

B. Proof of Lemma 2

Proof. From the inverse normalization in (14), we have $\tilde{\mathbf{w}}^{(k+1)} = 2\mathbf{p}^{(k+1)} - 1$. Recall the definition of the empirical Bernoulli parameter $\mathbf{p}^{(k+1)}$ given by (13), we have the elementwise expectation

$$\mathbb{E}_{\pi} [\tilde{w}_i^{(k+1)}] = \frac{1}{M} \sum_{m=1}^M (2\hat{\mathbb{P}}(w_{m,i}^{(k,\tau)} = 1) - 1) \quad (22a)$$

$$\stackrel{\textcircled{1}}{=} \frac{1}{M} \sum_{m=1}^M \varphi(h_{m,i}^{(k,\tau)}), \quad (22b)$$

where ① follows from stochastic rounding defined in (11). Based on the definition of range normalization in (10), for local normalized weight we have $w_{m,i}^{(k,\tau)} = \varphi(h_{m,i}^{(k,\tau)})$. Substituting the result into (22b) we have

$$\mathbb{E}_{\pi} [\tilde{\mathbf{w}}^{(k+1)}] = \frac{1}{M} \sum_{m=1}^M \tilde{\mathbf{w}}_m^{(k,\tau)}, \quad (23)$$

which completes the proof. \square

C. Proof of Lemma 3

Proof. Let $\hat{\mathbf{a}} \triangleq Q_{\text{sr}}(\mathbf{a})$, we have

$$\mathbb{E} [\|Q_{\text{sr}}(\mathbf{a}) - \mathbf{a}\|_2^2 | \mathbf{a}] = \mathbb{E} \left[\sum_{i=1}^d (\hat{a}_i - a_i)^2 | \mathbf{a} \right] \quad (24a)$$

$$= \sum_{i=1}^d (\mathbb{E} [\hat{a}_i^2 | \mathbf{a}] - a_i^2) = d - \|\mathbf{a}\|_2^2. \quad (24b)$$

The proof is complete. \square

D. Proof of Lemma 4

Proof. Consider a QSGD quantizer [28] with $s = 1$. For detailed results of other quantizers, we refer readers to [33].

In particular, we have

$$Q_{\text{qsgd}}(x_i) = \|\mathbf{x}\|_2 \cdot \text{sgn}(x_i) \cdot \xi_i(\mathbf{x}, s), \quad (25)$$

where

$$\xi_i(\mathbf{x}, s)|_{s=1} = \begin{cases} 0 & \text{with prob. } 1 - \frac{|x_i|}{\|\mathbf{x}\|_2}, \\ 1 & \text{with prob. } \frac{|x_i|}{\|\mathbf{x}\|_2}. \end{cases} \quad (26)$$

The variance of quantization error is

$$\mathbb{E} [\|Q(\mathbf{x}) - \mathbf{x}\|_2^2 | \mathbf{x}] = \mathbb{E} \left[\sum_{i=1}^d (\hat{x}_i - x_i)^2 | \mathbf{x} \right] \quad (27a)$$

$$= \sum_{i=1}^d (\mathbb{E} [\hat{x}_i^2 | \mathbf{x}] - x_i^2) = \frac{\|\mathbf{x}\|_2^2}{\|\mathbf{x}\|} \sum_{i=1}^d |x_i| - \|\mathbf{x}\|_2^2 \quad (27b)$$

$$= \|\mathbf{x}\|_2 \|\mathbf{x}\|_1 - \|\mathbf{x}\|_2^2 \leq (\sqrt{d} - 1) \|\mathbf{x}\|_2^2, \quad (27c)$$

which completes the proof. \square

E. Proof of Theorem 1

We first introduce some notations for simplicity. Let $\Delta^{(k)}$ denote the difference between two successive global latent weights, i.e.,

$$\Delta^{(k)} \triangleq \tilde{\mathbf{w}}^{(k)} - \tilde{\mathbf{w}}^{(k+1)}. \quad (28)$$

We use $\varepsilon_m^{(k,t)}$ to denote the stochastic gradient noise, i.e.,

$$\varepsilon_m^{(k,t)} \triangleq \tilde{\mathbf{g}}_m^{(k,t)} - \mathbf{g}_m^{(k,t)}. \quad (29)$$

Finally, we let $\nabla f(\tilde{\mathbf{w}})$ denote the gradient with respect to $\tilde{\mathbf{w}}$. The following five lemmas are presented to facilitate the proof.

Lemma 5 *The global normalized weight $\tilde{\mathbf{w}}^{(k)}$ can be reconstructed as the average of local binary weight, i.e.,*

$$\tilde{\mathbf{w}}^{(k+1)} = \frac{1}{M} \sum_{m=1}^M \mathbf{w}_m^{(k,\tau)}. \quad (30)$$

Proof. See Appendix B-F. \square

Lemma 6 (*Lipschitz continuity*) *Under Assumption 3, $\forall x_1, x_2 \in \mathbb{R}$, we have*

$$|\varphi(x_1) - \varphi(x_2)| \leq c_2 |x_1 - x_2|. \quad (31)$$

Proof. Without loss of generality, suppose $x_1 < x_2$. From the mean value theorem, there exists some $c \in (x_1, x_2)$ such that

$$\varphi'(c) = \frac{\varphi(x_2) - \varphi(x_1)}{x_2 - x_1}. \quad (32)$$

For the monotonically increasing function φ , we have

$$\varphi(x_2) - \varphi(x_1) = \varphi'(c) (x_2 - x_1) \quad (33a)$$

$$\stackrel{\textcircled{1}}{\leq} c_2 (x_2 - x_1), \quad (33b)$$

where ① holds due to Assumption 3. The similar result can be obtained by assuming $x_2 < x_1$, which completes the proof. \square

Lemma 7 (*Bounded weight divergence*) *Under Assumption 4, we have*

$$\mathbb{E} \|\tilde{\mathbf{w}}_m^{(k,\tau)} - \tilde{\mathbf{w}}^{(k)}\|_2^2 \leq (c_2 \eta)^2 \tau \left(\sum_{t=0}^{\tau-1} \mathbb{E} \|\mathbf{g}_m^{(k,t)}\|_2^2 + \sigma_{\varepsilon}^2 \right). \quad (34)$$

Proof. See Appendix B-G. \square

Lemma 8 Under Assumptions 2 to 5, we have

$$\mathbb{E} \langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \Delta^{(k)} \rangle \geq \frac{c_1^2 \eta \tau}{2} \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 \quad (35)$$

$$+ \frac{c_1^2 \eta}{4M} (2 - (c_2 L)^2 \eta^2 \tau (\tau - 1)) \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \|\mathbf{g}_m^{(k,t)}\|_2^2 - \frac{(c_1 c_2 L)^2 \eta^3 \tau (\tau - 1)}{4} \sigma_\varepsilon^2 - \frac{\eta (c_2^2 - c_1^2)}{M} \sum_{m=1}^M R_m^{(k)}, \quad (36)$$

where $R_m^{(k)} \triangleq - \sum_{t=0}^{\tau-1} \sum_{i \notin \mathcal{I}_m^{(k,t)}} \mathbb{E} [(\nabla f(\tilde{\mathbf{w}}^{(k)}))_i (\nabla f(\tilde{\mathbf{w}}_m^{(k,t)}))_i]$

and $\mathcal{I}_m^{(k,t)} \triangleq \{i \in [d] \mid \mathbf{g}_i^{(k)} \mathbf{g}_{m,i}^{(k,t)} \geq 0\}$.

Proof. See Appendix B-H. \square

Lemma 9 Under Assumptions 2 to 5, we have

$$\mathbb{E} \|\Delta^{(k)}\|_2^2 \leq \frac{(c_2 \eta)^2 \tau}{M} \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \|\mathbf{g}_m^{(k,t)}\|_2^2 + \frac{(c_2 \eta)^2 \tau}{M} \sigma_\varepsilon^2 + \frac{1}{M} \sigma_k^2. \quad (37)$$

Proof. See Appendix B-I. \square

We give the proof of Theorem 1 as follows.

Proof. Consider the difference vector $\Delta^{(k)}$ defined in (28), we expand it as

$$\Delta^{(k)} = \tilde{\mathbf{w}}^{(k)} - \tilde{\mathbf{w}}^{(k+1)} \quad (38a)$$

$$\stackrel{\textcircled{1}}{=} \tilde{\mathbf{w}}^{(k)} - \frac{1}{M} \sum_{m=1}^M \mathbf{w}_m^{(k,\tau)} \quad (38b)$$

$$\stackrel{\textcircled{2}}{=} \tilde{\mathbf{w}}^{(k)} - \frac{1}{M} \sum_{m=1}^M \tilde{\mathbf{w}}_m^{(k,\tau)} + \frac{1}{M} \sum_{m=1}^M \zeta_m^{(r)}, \quad (38c)$$

where $\textcircled{1}$ follows from (30), and $\textcircled{2}$ holds by substituting the definition of quantization error. From Assumption 2, we have

$$f(\tilde{\mathbf{w}}^{(k+1)}) - f(\tilde{\mathbf{w}}^{(k)}) \leq - \langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \Delta^{(k)} \rangle + \frac{L}{2} \|\Delta^{(k)}\|_2^2. \quad (39a)$$

Let $\frac{(L\eta)^2 \tau (\tau - 1)}{2} + \frac{L\eta\tau}{c_1^2} \leq \frac{1}{c_2^2}$, take the expectation on both sides, and use Lemmas 8–9:

$$\begin{aligned} \mathbb{E} [f(\tilde{\mathbf{w}}^{(k+1)}) - f(\tilde{\mathbf{w}}^{(k)})] &\leq - \frac{c_1^2 \eta \tau}{2} \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 - \\ &\frac{(c_1 c_2)^2 \eta}{4M} \left(\frac{2}{c_2^2} - L^2 \eta^2 \tau (\tau - 1) - \frac{2L\eta\tau}{c_1^2} \right) \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \|\mathbf{g}_m^{(k,t)}\|_2^2 \\ &+ \frac{(c_2 \eta)^2 L \tau}{4} \left(\frac{2}{M} + c_1^2 L \eta (\tau - 1) \right) \sigma_\varepsilon^2 \\ &+ \frac{\eta (c_2^2 - c_1^2)}{M} \sum_{m=1}^M R_m^{(k)} + \frac{L}{2M} \sigma_k^2 \end{aligned} \quad (40a)$$

$$\stackrel{\textcircled{1}}{\leq} - \frac{c_1^2 \eta \tau}{2} \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 + \frac{(c_2 \eta)^2 L \tau}{4} \left(\frac{2}{M} + c_1^2 L \eta (\tau - 1) \right) \sigma_\varepsilon^2 + \frac{\eta (c_2^2 - c_1^2)}{M} \sum_{m=1}^M R_m^{(k)} + \frac{L}{2M} \sigma_k^2, \quad (40b)$$

where $\textcircled{1}$ follows from the restrictions on learning rate. We rewrite the restriction as

$$\eta \leq \frac{-\frac{L\tau}{c_1^2} + \sqrt{\frac{L^2 \tau^2}{c_1^4} + \frac{2L^2 \tau (\tau - 1)}{c_2^2}}}{L^2 \tau (\tau - 1)} \quad (41a)$$

$$\stackrel{\textcircled{1}}{\leq} \frac{-1 + \sqrt{1 + \frac{2c_1^4}{c_2^2}}}{L(\tau - 1)c_1^2} \stackrel{\textcircled{2}}{\leq} \frac{c_1^2}{L(\tau - 1)c_2^2}, \quad (41b)$$

where in $\textcircled{1}$ we use $\tau(\tau - 1) \leq \tau^2$, and $\textcircled{2}$ holds due to the Bernoulli inequality $(1+x)^{\frac{1}{2}} \leq 1 + \frac{1}{2}x$, $\forall x \in [-1, \infty)$. Based on (41b), we set the learning rate $\eta = O\left(\left(\frac{c_1}{c_2}\right)^2 \frac{1}{L\tau\sqrt{K}}\right)$. The choice of the learning rate η makes the upper bound in (40a) independent of the client local gradient $\mathbf{g}_m^{(k,t)}$. Summing up over K communication rounds yields

$$\begin{aligned} \frac{1}{K} \sum_{k=0}^{K-1} c_1^2 \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 &\leq \frac{2[f(\tilde{\mathbf{w}}^{(0)}) - f(\tilde{\mathbf{w}}^*)]}{\eta \tau K} \\ &+ c_2^2 L \eta \left[\frac{1}{M} + \frac{c_1^2 L \eta (\tau - 1)}{2} \right] \sigma_\varepsilon^2 + \frac{L}{\eta \tau K M} \sum_{k=0}^{K-1} \sigma_k^2 \\ &+ \frac{2(c_2^2 - c_1^2)}{\tau M K} \sum_{k=0}^{K-1} \sum_{m=1}^M R_m^{(k)}. \end{aligned} \quad (42a)$$

\square

F. Proof of Lemma 5

Proof. From the reconstruction rule (14), we have

$$\tilde{\mathbf{w}}^{(k+1)} = 2\mathbf{p}^{(k+1)} - 1. \quad (43)$$

The i th entry of $\mathbf{p}^{(k)}$ is defined in (13), i.e.,

$$p_i^{(k+1)} = \frac{1}{M} \sum_{m=1}^M \mathbb{1}(\hat{w}_{m,i}^{(k,\tau)} = 1). \quad (44)$$

Substituting (44) into (43) yields

$$w_i^{(k+1)} = \frac{1}{M} \sum_{m=1}^M (2 \cdot \mathbb{1}(\hat{w}_{m,i}^{(k,\tau)} = 1) - 1). \quad (45)$$

Note that

$$2 \cdot \mathbb{1}(\hat{w}_{m,i}^{(k,\tau)} = 1) - 1 = \begin{cases} +1, & \hat{w}_m^{(k,\tau)} = +1, \\ -1, & \hat{w}_m^{(k,\tau)} = -1, \end{cases} \quad (46)$$

we have

$$w_i^{(k+1)} = \frac{1}{M} \sum_{m=1}^M \hat{w}_i^{(k)}, \quad (47)$$

which completes the proof. \square

G. Proof of Lemma 7

Proof. With the local initialization and update method described in Algorithm 1, we have

$$\mathbb{E} \|\tilde{\mathbf{w}}_m^{(k,\tau)} - \tilde{\mathbf{w}}^{(k)}\|_2^2 = \mathbb{E} \|\varphi(\mathbf{h}_m^{(k,\tau)}) - \varphi(\mathbf{h}_m^{(k,0)})\|_2^2 \quad (48a)$$

$$\stackrel{\textcircled{1}}{\leq} c_2^2 \mathbb{E} \|\mathbf{h}_m^{(k,\tau)} - \mathbf{h}_m^{(k,0)}\|_2^2 = c_2^2 \mathbb{E} \left\| \sum_{t=0}^{\tau-1} -\eta \tilde{\mathbf{g}}_m^{(k,t)} \right\|_2^2. \quad (48b)$$

where ① comes from the Lipschitz condition in Lemma 6. By decomposing $\tilde{\mathbf{g}}_m^{(k,t)}$ into $\mathbf{g}_m^{(k,t)} + \boldsymbol{\varepsilon}_m^{(k,t)}$, we have

$$\mathbb{E} \left\| \tilde{\mathbf{w}}_m^{(k,\tau)} - \tilde{\mathbf{w}}_m^{(k)} \right\|_2^2 = (c_2\eta)^2 \left(\mathbb{E} \left\| \sum_{t=0}^{\tau-1} \mathbf{g}_m^{(k,t)} \right\|_2^2 + \mathbb{E} \left\| \sum_{t=0}^{\tau-1} \boldsymbol{\varepsilon}_m^{(k,t)} \right\|_2^2 \right) \quad (49a)$$

$$\leq (c_2\eta)^2 \tau \left(\sum_{t=0}^{\tau-1} \mathbb{E} \left\| \mathbf{g}_m^{(k,t)} \right\|_2^2 + \sigma_\varepsilon^2 \right), \quad (49b)$$

which completes the proof. \square

H. Proof of Lemma 8

Proof. We have

$$\mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \Delta^{(k)} \right\rangle = \mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \tilde{\mathbf{w}}^{(k)} - \frac{1}{M} \sum_{m=1}^M \tilde{\mathbf{w}}_m^{(k,\tau)} + \frac{1}{M} \sum_{m=1}^M \boldsymbol{\zeta}_m^{(k)} \right\rangle \quad (50a)$$

$$= \mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \frac{1}{M} \sum_{m=1}^M \varphi(\mathbf{h}^{(k)}) - \varphi(\mathbf{h}_m^{(k,\tau)}) \right\rangle \quad (50b)$$

From the mean value theorem, for $h_i^{(k)}, h_{m,i}^{(k,\tau)} \in \mathbb{R}$, there exists a point $c_{m,i}^{(k)} \in \mathbb{H}_{m,i}^{(r)}$ such that

$$f'(c_{m,i}^{(k)}) = \frac{\varphi(h_i^{(k)}) - \varphi(h_{m,i}^{(k,\tau)})}{h_i^{(k)} - h_{m,i}^{(k,\tau)}}, \quad (51)$$

where $\mathbb{H}_{m,i}^{(r)}$ is an open interval with endpoints $h_i^{(k)}$ and $h_{m,i}^{(k,\tau)}$, i.e.,

$$\mathbb{H}_{m,i}^{(r)} = \begin{cases} (h_i^{(k)}, h_{m,i}^{(k,\tau)}), & \text{if } h_i^{(k)} < h_{m,i}^{(k,\tau)}, \\ (h_{m,i}^{(k,\tau)}, h_i^{(k)}), & \text{otherwise.} \end{cases} \quad (52)$$

Let $C_m^{(k)} = \text{diag} \left(\frac{d\varphi}{dc_{m,1}^{(k,\tau)}}, \dots, \frac{d\varphi}{dc_{m,d}^{(k,\tau)}} \right)$, we have

$$\varphi(\mathbf{h}^{(k)}) - \varphi(\mathbf{h}_m^{(k,\tau)}) = C_m^{(k)} (\mathbf{h}^{(k)} - \mathbf{h}_m^{(k,\tau)}) \quad (53a)$$

$$= \eta C_m^{(k)} \sum_{t=0}^{\tau-1} (\mathbf{g}_m^{(k,t)} + \boldsymbol{\varepsilon}_m^{(k,t)}), \quad (53b)$$

Substituting (53b) into (50b) yields

$$\mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \Delta^{(k)} \right\rangle = \frac{\eta}{M} \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), C_m^{(k)} \mathbf{g}_m^{(k,t)} \right\rangle. \quad (54)$$

According to the chain rule, $\mathbf{g}_m^{(k,t)}$ can be written as

$$\mathbf{g}_m^{(k,t)} = \nabla_{\mathbf{h}} f_m(\varphi(\mathbf{h}_m^{(k,t)})) = D_m^{(k,t)} \nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}), \quad (55)$$

where $D_m^{(k,t)} = \text{diag} \left(\frac{d\varphi}{dh_{m,1}^{(k,t)}}, \dots, \frac{d\varphi}{dh_{m,d}^{(k,t)}} \right)$. To simplify the notations, let $B_m^{(k,t)} = C_m^{(k)} D_m^{(k,t)}$. Note that $B_m^{(k,t)}$ is still a diagonal matrix, where the i th diagonal element $b_{m,i}^{(k,t)}$ is

$$b_{m,i}^{(k,t)} \triangleq (B_m^{(k,t)})_{i,i} = \frac{d\varphi}{dc_{m,i}^{(k,\tau)}} \cdot \frac{d\varphi}{dh_{m,i}^{(k,t)}}. \quad (56)$$

Substituting (55) into (54) we have

$$\mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \Delta^{(k)} \right\rangle = \frac{\eta}{M} \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), B_m^{(k,t)} \nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}) \right\rangle. \quad (57)$$

We first focus on the following inner product:

$$\begin{aligned} & \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), B_m^{(k,t)} \nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}) \right\rangle \\ &= \sum_{i=1}^d (\nabla f(\tilde{\mathbf{w}}^{(k)}))_i \times b_{m,i}^{(k,t)} (\nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}))_i, \end{aligned} \quad (58)$$

where $(\nabla f)_i$ denotes the i th entry of the gradient vector. We consider the set $\mathcal{I}_m^{(k,t)}$ defined as

$$\mathcal{I}_m^{(k,t)} \triangleq \left\{ i \in [d] \mid (\nabla f(\tilde{\mathbf{w}}^{(k)}))_i \cdot (\nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}))_i \geq 0 \right\}, \quad (59)$$

Let $\mathcal{I}_m^{-(k,t)}$ denote the complement of $\mathcal{I}_m^{(k,t)}$. The result in (58) can be bounded as

$$\mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), B_m^{(k,t)} \nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}) \right\rangle \quad (60a)$$

$$\begin{aligned} & \stackrel{\textcircled{1}}{\geq} c_1^2 \sum_{i \in \mathcal{I}_m^{(k,t)}} \mathbb{E} \left[(\nabla f(\tilde{\mathbf{w}}^{(k)}))_i \cdot (\nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}))_i \right] + \\ & c_2^2 \sum_{i \in \mathcal{I}_m^{-(k,t)}} \mathbb{E} \left[(\nabla f(\tilde{\mathbf{w}}^{(k)}))_i \cdot (\nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}))_i \right] \end{aligned} \quad (60b)$$

$$\begin{aligned} &= c_1^2 \mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}) \right\rangle + \\ & (c_2^2 - c_1^2) \sum_{i \in \mathcal{I}_m^{-(k,t)}} \mathbb{E} \left[(\nabla f(\tilde{\mathbf{w}}^{(k)}))_i \cdot (\nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}))_i \right], \end{aligned} \quad (60c)$$

where ① follows from Assumption 3. To simplify the notation, let $R_m^{(k)}$ denote the accumulated gradient divergence, namely,

$$R_m^{(k)} \triangleq - \sum_{t=0}^{\tau-1} \sum_{i \in \mathcal{I}_m^{-(k,t)}} \mathbb{E} \left[(\nabla f(\tilde{\mathbf{w}}^{(k)}))_i (\nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}))_i \right]. \quad (61)$$

The expected inner product in (62) can be bounded as

$$\begin{aligned} \mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \Delta^{(k)} \right\rangle & \geq \frac{c_1^2 \eta}{M} \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \left\langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \right. \\ & \left. \nabla f_m(\tilde{\mathbf{w}}_m^{(k,t)}) \right\rangle - \frac{\eta(c_2^2 - c_1^2)}{M} \sum_{m=1}^M R_m^{(k)}. \end{aligned} \quad (62)$$

By rewriting the inner product term in (62) according to $2\langle \mathbf{a}, \mathbf{b} \rangle = \|\mathbf{a}\|_2^2 + \|\mathbf{b}\|_2^2 - \|\mathbf{a} - \mathbf{b}\|_2^2$, we have

$$\begin{aligned} & \mathbb{E} \langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \Delta^{(k)} \rangle \\ & \geq \frac{c_1^2 \eta}{2M} \sum_{m=1}^M \sum_{t=0}^{\tau-1} \left(\mathbb{E} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 + \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}_m^{(k,t)})\|_2^2 \right. \\ & \quad \left. - \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}_m^{(k,t)}) - \nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 \right) - \frac{\eta(c_2^2 - c_1^2)}{M} \sum_{m=1}^M R_m^{(k)} \end{aligned} \quad (63a)$$

$$\begin{aligned} & \stackrel{\textcircled{1}}{\geq} \frac{c_1^2 \eta \tau}{2} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 + \frac{c_1^2 \eta}{2M} \sum_{m=1}^M \sum_{t=0}^{\tau-1} \left(\mathbb{E} \|\nabla f(\tilde{\mathbf{w}}_m^{(k,t)})\|_2^2 \right. \\ & \quad \left. - L^2 \mathbb{E} \|\tilde{\mathbf{w}}_m^{(k,t)} - \tilde{\mathbf{w}}^{(k)}\|_2^2 \right) - \frac{\eta(c_2^2 - c_1^2)}{M} \sum_{m=1}^M R_m^{(k)}, \end{aligned} \quad (63b)$$

where ① holds due to Assumption 2 of Lipschitz smoothness for the objective function. From Lemma 7, we can show that

$$\mathbb{E} \|\tilde{\mathbf{w}}_m^{(k,t)} - \tilde{\mathbf{w}}^{(k)}\|_2^2 \leq (c_2 \eta)^2 t \left(\sum_{n=0}^{t-1} \|\mathbf{g}^{(k,n)}\|_2^2 + \sigma_\varepsilon^2 \right), \quad (64)$$

where $t = 1, \dots, \tau - 1$. Substituting (64) in (63b) yields

$$\begin{aligned} & \mathbb{E} \langle \nabla f(\tilde{\mathbf{w}}^{(k)}), \Delta^{(k)} \rangle \\ & \geq \frac{c_1^2 \eta \tau}{2} \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 + \frac{c_1^2 \eta}{2M} \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}_m^{(k,t)})\|_2^2 \\ & \quad - \frac{(c_1 c_2 L)^2 \eta^3}{4M} \sum_{m=1}^M \sum_{n=0}^{\tau-1} (\tau(\tau-1) - n(n+1)) \mathbb{E} \|\mathbf{g}^{(k,n)}\|_2^2 \\ & \quad - \frac{(c_1 c_2 L)^2 \eta^3 \tau(\tau-1)}{4} \sigma_\varepsilon^2 - \frac{\eta(c_2^2 - c_1^2)}{M} \sum_{m=1}^M R_m^{(k)} \end{aligned} \quad (65a)$$

$$\begin{aligned} & \stackrel{\textcircled{1}}{\geq} \frac{c_1^2 \eta \tau}{2} \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 + \frac{c_1^2 \eta}{2M} \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}_m^{(k,t)})\|_2^2 \\ & \quad - \frac{\eta}{4M} (c_1 c_2 L)^2 \eta^2 \tau(\tau-1) \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \|\mathbf{g}_m^{(k,t)}\|_2^2 \\ & \quad - \frac{(c_1 c_2 L)^2 \eta^3 \tau(\tau-1)}{4} \sigma_\varepsilon^2 - \frac{\eta(c_2^2 - c_1^2)}{M} \sum_{m=1}^M R_m^{(k)} \end{aligned} \quad (65b)$$

$$\begin{aligned} & \stackrel{\textcircled{2}}{\geq} \frac{c_1^2 \eta \tau}{2} \mathbb{E} \|\nabla f(\tilde{\mathbf{w}}^{(k)})\|_2^2 \\ & \quad + \frac{c_1^2 \eta}{4M} (2 - (c_2 L)^2 \eta^2 \tau(\tau-1)) \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \|\mathbf{g}_m^{(k,t)}\|_2^2 \\ & \quad - \frac{(c_1 c_2 L)^2 \eta^3 \tau(\tau-1)}{4} \sigma_\varepsilon^2 - \frac{\eta(c_2^2 - c_1^2)}{M} \sum_{m=1}^M R_m^{(k)} \end{aligned} \quad (65c)$$

where ① follows from $\tau(\tau-1) - n(n+1) \leq \tau(\tau-1)$; ② holds due to the chain rule in (55) and Assumption 3. \square

I. Proof of Lemma 9

Proof. We have

$$\mathbb{E} \|\Delta^{(k)}\|_2^2 = \mathbb{E} \left\| \tilde{\mathbf{w}}^{(k)} - \frac{1}{M} \sum_{m=1}^M \tilde{\mathbf{w}}_m^{(k,\tau)} + \frac{1}{M} \sum_{m=1}^M \zeta_m^{(k)} \right\|_2^2 \quad (66a)$$

$$= \mathbb{E} \left\| \frac{1}{M} \sum_{m=1}^M \varphi(\mathbf{h}^{(k)}) - \varphi(\mathbf{h}_m^{(k,\tau)}) + \frac{1}{M} \sum_{m=1}^M \zeta_m^{(k)} \right\|_2^2 \quad (66b)$$

$$\begin{aligned} & = \mathbb{E} \left\| \frac{1}{M} \sum_{m=1}^M \varphi(\mathbf{h}^{(k)}) - \varphi(\mathbf{h}_m^{(k,\tau)}) \right\|_2^2 + \mathbb{E} \left\| \frac{1}{M} \sum_{m=1}^M \zeta_m^{(k)} \right\|_2^2 \\ & \quad + 2\mathbb{E} \left\langle \frac{1}{M} \sum_{m=1}^M \varphi(\mathbf{h}^{(k)}) - \varphi(\mathbf{h}_m^{(k,\tau)}), \frac{1}{M} \sum_{m=1}^M \zeta_m^{(k)} \right\rangle \end{aligned} \quad (66c)$$

$$\stackrel{\textcircled{1}}{=} \mathbb{E} \left\| \frac{1}{M} \sum_{m=1}^M \varphi(\mathbf{h}^{(k)}) - \varphi(\mathbf{h}_m^{(k,\tau)}) \right\|_2^2 + \mathbb{E} \left\| \frac{1}{M} \sum_{m=1}^M \zeta_m^{(k)} \right\|_2^2. \quad (66d)$$

where ① comes from Assumption 5. For the first term in (66d),

$$\begin{aligned} & \mathbb{E} \left\| \frac{1}{M} \sum_{m=1}^M (\varphi(\mathbf{h}^{(k)}) - \varphi(\mathbf{h}_m^{(k,\tau)})) \right\|_2^2 \\ & \leq \frac{1}{M} \sum_{m=1}^M \mathbb{E} \|\varphi(\mathbf{h}^{(k)}) - \varphi(\mathbf{h}_m^{(k,\tau)})\|_2^2 \end{aligned} \quad (67a)$$

$$\stackrel{\textcircled{1}}{\leq} \frac{c_2^2}{M} \sum_{m=1}^M \|\mathbf{h}^{(k)} - \mathbf{h}_m^{(k,\tau)}\|_2^2 \quad (67b)$$

$$\stackrel{\textcircled{2}}{=} \frac{(c_2 \eta)^2}{M} \sum_{m=1}^M \left\| -\eta \sum_{t=0}^{\tau-1} \tilde{\mathbf{g}}_m^{(k,t)} \right\|_2^2 \quad (67c)$$

$$\stackrel{\textcircled{3}}{\leq} \frac{(c_2 \eta)^2 \tau}{M} \sum_{m=1}^M \sum_{t=0}^{\tau-1} \mathbb{E} \|\mathbf{g}_m^{(k,t)}\|_2^2 + \frac{(c_2 \eta)^2 \tau}{M} \sigma_\varepsilon^2, \quad (67d)$$

where ① is due to Lemma 6 ③ follows from Assumption 4. For the second term in (66d) we have

$$\mathbb{E} \left\| \frac{1}{M} \sum_{m=1}^M \zeta_m^{(k)} \right\|_2^2 \leq \frac{1}{M} \sigma_\zeta^2. \quad (68)$$

Combing the results of (67d) and (68) completes the proof. \square

REFERENCES

- [1] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings *et al.*, “Advances and open problems in federated learning,” *Foundations and Trends in Machine Learning*, vol. 14, no. 1-2, pp. 1–210, 2021.
- [2] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in *International Conference on Artificial Intelligence and Statistics*, 2017, pp. 1273–1282.

- [3] A. Reisizadeh, A. Mokhtari, H. Hassani, A. Jadbabaie, and R. Pedarsani, "FedPAQ: A communication-efficient federated learning method with periodic averaging and quantization," in *International Conference on Artificial Intelligence and Statistics*, 2020, pp. 2021–2031.
- [4] F. Haddadpour, M. M. Kamani, A. Mokhtari, and M. Mahdavi, "Federated learning with compression: Unified analysis and sharp guarantees," in *International Conference on Artificial Intelligence and Statistics*, 2021, pp. 2350–2358.
- [5] P. Blanchard, R. Guerraoui, J. Stainer *et al.*, "Machine learning with adversaries: Byzantine tolerant gradient descent," in *Advances in Neural Information Processing Systems*, 2017.
- [6] D. Yin, Y. Chen, R. Kannan, and P. Bartlett, "Byzantine-robust distributed learning: Towards optimal statistical rates," in *International Conference on Machine Learning*, 2018, pp. 5650–5659.
- [7] L. Muñoz-González, K. T. Co, and E. C. Lupu, "Byzantine-robust federated machine learning through adaptive model averaging," *arXiv preprint arXiv:1909.05125*, 2019.
- [8] F. Sattler, K.-R. Müller, T. Wiegand, and W. Samek, "On the byzantine robustness of clustered federated learning," in *International Conference on Acoustics, Speech and Signal Processing*, 2020, pp. 8861–8865.
- [9] J. Bernstein, Y.-X. Wang, K. Azizzadenesheli, and A. Anandkumar, "SignSGD: Compressed optimisation for non-convex problems," in *International Conference on Machine Learning*, 2018, pp. 560–569.
- [10] F. Sattler, S. Wiedemann, K.-R. Müller, and W. Samek, "Robust and communication-efficient federated learning from non-iid data," *IEEE transactions on neural networks and learning systems*, 2019.
- [11] X. Chen, T. Chen, H. Sun, S. Z. Wu, and M. Hong, "Distributed training with heterogeneous data: Bridging median- and mean-based algorithms," in *Neural Information Processing Systems*, 2020, pp. 21 616–21 626.
- [12] R. Jin, Y. Huang, X. He, H. Dai, and T. Wu, "Stochastic-sign sgd for federated learning with theoretical guarantees," *arXiv preprint arXiv:2002.10940*, 2020.
- [13] M. Safaryan and P. Richtarik, "Stochastic sign descent methods: New algorithms and better theory," in *International Conference on Machine Learning*, 2021, pp. 9224–9234.
- [14] B. Huang, X. Li, Z. Song, and X. Yang, "FL-NTK: A neural tangent kernel-based framework for federated learning convergence analysis," *arXiv preprint arXiv:2105.05001*, 2021.
- [15] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang, "On the convergence of fedavg on non-iid data," *International Conference on Learning Representations*, 2020.
- [16] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. Brendan McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for federated learning on user-held data," 2016.
- [17] C. Zhang, S. Li, J. Xia, W. Wang, F. Yan, and Y. Liu, "BatchCrypt: Efficient homomorphic encryption for cross-silo federated learning," in *USENIX Annual Technical Conference*, 2020, pp. 493–506.
- [18] X. Cao, M. Fang, J. Liu, and N. Z. Gong, "Fltrust: Byzantine-robust federated learning via trust bootstrapping," *Network and Distributed System Security Symposium*, 2020.
- [19] V. Shejwalkar and A. Houmansadr, "Manipulating the byzantine: Optimizing model poisoning attacks and defenses for federated learning," in *Network and Distributed System Security Symposium*, 2021.
- [20] I. Hubara, M. Courbariaux, D. Soudry, R. El-Yaniv, and Y. Bengio, "Binarized neural networks," in *Advances in Neural Information Processing Systems*, 2016, pp. 4114–4122.
- [21] O. Shayer, D. Levi, and E. Fetaya, "Learning discrete weights using the local reparameterization trick," in *International Conference on Learning Representations*, 2018.
- [22] R. Gong, X. Liu, S. Jiang, T. Li, P. Hu, J. Lin, F. Yu, and J. Yan, "Differentiable soft quantization: Bridging full-precision and low-bit neural networks," in *International Conference on Computer Vision*, 2019, pp. 4852–4861.
- [23] H. Qin, R. Gong, X. Liu, X. Bai, J. Song, and N. Sebe, "Binary neural networks: A survey," *Pattern Recognition*, p. 107281, 2020.
- [24] T. Lin, L. Kong, S. U. Stich, and M. Jaggi, "Ensemble distillation for robust model fusion in federated learning," in *Advances in Neural Information Processing Systems*, 2020, pp. 2351–2363.
- [25] L. Hou, R. Zhang, and J. T. Kwok, "Analysis of quantized models," in *International Conference on Learning Representations*, 2019.
- [26] Q. Qin, K. Poularakis, K. K. Leung, and L. Tassiulas, "Line-speed and scalable intrusion detection at the network edge via federated learning," in *International Federation for Information Processing Networking Conference*, 2020, pp. 352–360.
- [27] N. H. Tran, W. Bao, A. Zomaya, M. N. Nguyen, and C. S. Hong, "Federated learning over wireless networks: Optimization model design and analysis," in *International Conference on Computer Communications*, 2019.
- [28] D. Alistarh, D. Grubic, J. Li, R. Tomioka, and M. Vojnovic, "QSGD: Communication-efficient SGD via gradient quantization and encoding," in *Advances in Neural Information Processing Systems*, 2017, pp. 1709–1720.
- [29] A. Bendahmane, M. Essaïdi, A. El Moussaoui, and A. Younes, "The effectiveness of reputation-based voting for collusion tolerance in large-scale grids," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 665–674, 2014.
- [30] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Reliable federated learning for mobile networks," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 72–80, 2020.
- [31] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet of Things Journal*, vol. 6,

no. 6, pp. 10 700–10 714, 2019.

- [32] J. Wang and G. Joshi, “Cooperative SGD: A unified framework for the design and analysis of communication-efficient sgd algorithms,” in *ICML Workshop on Coding Theory for Machine Learning*, 2019.
- [33] D. Basu, D. Data, C. Karakus, and S. N. Diggavi, “Qsparse-local-SGD: Distributed SGD with quantization, sparsification, and local computations,” *IEEE Journal on Selected Areas in Information Theory*, vol. 1, no. 1, pp. 217–226, 2020.
- [34] A. Krizhevsky, “Learning multiple layers of features from tiny images,” *Master thesis, Dept. of Comput. Sci., Univ. of Toronto, Toronto, Canada*, 2009.
- [35] S. Caldas, S. M. K. Duddu, P. Wu, T. Li, J. Konečný, H. B. McMahan, V. Smith, and A. Talwalkar, “Leaf: A benchmark for federated settings,” *arXiv preprint arXiv:1812.01097*, 2018.
- [36] H. Xiao, K. Rasul, and R. Vollgraf, “Fashion-MNIST: a novel image dataset for benchmarking machine learning algorithms,” *arXiv preprint arXiv:1708.07747*, 2017.
- [37] T.-M. H. Hsu, H. Qi, and M. Brown, “Measuring the effects of non-identical data distribution for federated visual classification,” *arXiv preprint arXiv:1909.06335*, 2019.
- [38] S. Ioffe and C. Szegedy, “Batch normalization: Accelerating deep network training by reducing internal covariate shift,” *arXiv preprint arXiv:1502.03167*, 2015.
- [39] E. Diao, J. Ding, and V. Tarokh, “HeteroFL: Computation and communication efficient federated learning for heterogeneous clients,” in *International Conference on Learning Representations*, 2021.
- [40] D. Rothchild, A. Panda, E. Ullah, N. Ivkin, I. Stoica, V. Braverman, J. Gonzalez, and R. Arora, “Fetchsgd: Communication-efficient federated learning with sketching,” in *International Conference on Machine Learning*. PMLR, 2020, pp. 8253–8265.
- [41] J. Bernstein, J. Zhao, K. Azizzadenesheli, and A. Anandkumar, “signsgd with majority vote is communication efficient and fault tolerant,” in *International Conference on Learning Representations*, 2019.



Kai Yue (Graduate Student Member, IEEE) received his B.E. degree (with honors) in electronic and information engineering from the University of Science and Technology of China, Hefei, China, in 2020. He is currently working toward the Ph.D. degree in Electrical Engineering at the North Carolina State University. His research interests include federated learning, image processing, and video coding.



Richeng Jin (Member, IEEE) received the B.S. degree in information and communication engineering from Zhejiang University, Hangzhou, China, in 2015, and the Ph.D. degree in electrical engineering from North Carolina State University, Raleigh, NC, USA, in 2020.

He was a Postdoctoral Researcher in electrical and computer engineering at North Carolina State University, Raleigh, NC, USA, from 2021 to 2022. He is currently a faculty member of the department of information and communication engineering with Zhejiang University, Hangzhou, China. His research interests are in the general area of wireless AI, game theory, and security and privacy in machine learning/artificial intelligence and wireless networks.



Chau-Wai Wong (Member, IEEE) received his B.Eng. and M.Phil. degrees in electronic and information engineering from The Hong Kong Polytechnic University, in 2008 and 2010, and the Ph.D. degree in electrical engineering from the University of Maryland, College Park, MD, USA, in 2017. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, the Forensic Sciences Cluster, and the Secure Computing Institute, North Carolina State University. He was a data scientist at Origin Wireless, Inc., Greenbelt,

MD, USA. His research interests include multimedia forensics, statistical signal processing, machine learning, data analytics, and video coding. Dr. Wong received a Top-Four Student Paper Award, Future Faculty Fellowship, HSBC Scholarship, and Hitachi Scholarship. He was the General Secretary of the IEEE PolyU Student Branch from 2006 to 2007. He was involved in organizing the third edition of the IEEE Signal Processing Cup in 2016 on electric network frequency forensics.



Huaiyu Dai (Fellow, IEEE) received the B.E. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 1996 and 1998, respectively, and the Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ in 2002.

He was with Bell Labs, Lucent Technologies, Holmdel, NJ, in summer 2000, and with AT&T Labs-Research, Middletown, NJ, in summer 2001. He is currently a Professor of Electrical and Computer Engineering with NC State University, Raleigh, holding the title of University Faculty Scholar. His research interests are in the general areas of communications, signal processing, networking, and computing. His current research focuses on machine learning and artificial intelligence for communications and networking, multilayer and interdependent networks, dynamic spectrum access and sharing, as well as security and privacy issues in the above systems.

He has served as an area editor for IEEE Transactions on Communications, a member of the Executive Editorial Committee for IEEE Transactions on Wireless Communications, and an editor for IEEE Transactions on Signal Processing. Currently he serves as an area editor for IEEE Transactions on Wireless Communications. He was a co-recipient of best paper awards at 2010 IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS 2010), 2016 IEEE INFOCOM BIGSECURITY Workshop, and 2017 IEEE International Conference on Communications (ICC 2017). He received Qualcomm Faculty Award in 2019.