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—Distributed optimization, efficient communication, federated learning, neural network quantization.

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.

In this article, 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 article 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 nonindependent and identically distributed (i.i.d.) Canadian Institute For Advanced Research (CIFAR-10) dataset by 5%–10%, 15%–20%, and 25%–30% compared to Federated learning method with periodic averaging and quantization (FedPAQ) [3], sign stochastic gradient descent (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 of 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 a good convergence rate in the homogeneous data distribution scenario. This approach is further extended to the heterogeneous data distribution setting [11], [12], [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 and Houmansadr [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], [21], [22], [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 works have also conducted case studies of quantized neural networks 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 binary neural network (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 \([1, 2, \ldots, N]\). Bold lower cases of letters such as \(v_m\) 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. \(I = [1, \ldots, 1]^{\top}\) 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 \(D_m = \{(x_{m,j}, y_{m,j})\}_{j=1}^{n_m}\) denote the training dataset on the \(m\)th client, with the input \(x_{m,j} \in \mathbb{R}^{d_i}\) and the label \(y_{m,j} \in \mathbb{R}^{d_i}\) in each training pair. The local objective function \(f_m\) with a model weight vector \(\theta \in \mathbb{R}^d\) is given by

\[
    f_m(\theta) \triangleq f_m(\theta; D_m) = \frac{1}{n_m} \sum_{j=1}^{n_m} \ell(\theta; (x_{m,j}, y_{m,j}))
\]

where \(\ell\) is a loss function quantifying the error of model \(\theta\) predicting the label \(y_{m,j}\) for an input \(x_{m,j}\). A global objective function may be formulated as

\[
    \min_{\theta \in \mathbb{R}^d} f(\theta) = \frac{1}{M} \sum_{m=1}^{M} f_m(\theta).
\]

#### B. Quantized Neural Networks

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

\[
    w^* = \text{argmin}_{w \in \mathbb{D}_q^n} \frac{1}{N} \sum_{j=1}^{N} \ell(w; (x_j, y_j)).
\]

Prior studies tried to solve (3) by optimizing a real-valued latent weight vector \(h \in \mathbb{R}^d\). 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 BNN, and the normalized latent parameters are interpreted as the Bernoulli distribution parameter \(\vartheta\)

\[
    \vartheta_i \triangleq \mathbb{P}(w_i = 1) = S(h_i), \quad w_i \in \{0, 1\}
\]

where \(S : \mathbb{R} \to (0, 1)\) is the sigmoid function. In the forward pass, instead of using the binary vector \(w\), its expected value \(\mathbb{E}_{\text{sto-bnn}}[w] = -1 \times [1 - S(h)] + 1 \times S(h) = 2S(h) - 1\) will participate in the actual convolution or matrix multiplication operations. In other words, the neural network function

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
becomes \( \hat{\mathbf{y}} = g(\mathbf{w}_{\text{dsq}}, \mathbf{x}) \). Likewise, Gong et al. [22] normalized the latent weight but interpreted it from a nonprobabilistic viewpoint. They approximated the staircase quantization function via thresholding or stochastic rounding.

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 \( \hat{\mathbf{y}} = g(\mathbf{w}_{\text{dsq}}, \mathbf{x}) \). The binary weights are obtained through the sign operation.

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 \( \mathbf{\bar{w}} \).

\[
\mathbf{\bar{w}}_{\text{dsq}} \triangleq \tanh(a\mathbf{h}) \quad (6)
\]

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 \( \hat{\mathbf{y}} = g(\mathbf{w}_{\text{dsq}}, \mathbf{x}) \). The binary weights are obtained through the sign operation.

\[
\hat{\mathbf{y}} = g(\mathbf{\bar{w}}, \mathbf{x}), \quad \mathbf{\bar{w}} \triangleq \varphi(\mathbf{h}) \quad (7)
\]

Second, in the back-propagation, the latent weight vector \( \mathbf{h} \) is updated with its gradient, \( \mathbf{h}^{(t+1)} = \mathbf{h}^{(t)} - \eta \nabla \mathcal{L} \). Finally, the normalized weight vector \( \mathbf{\bar{w}} \) 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 are unexplored. To answer these questions, we present the 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)

\[
\mathbf{w}^* = \arg\min_{\mathbf{w} \in \mathbb{F}_2} f(\mathbf{w}). \quad (8)
\]

For the simplicity of presentation, we mainly focus on the BNN case with \( \mathbb{F}_2 = (-1, 1) \). We illustrate the procedure in Fig. 2 and provide the pseudocode 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 that all clients are identically initialized by the server, namely, \( \forall m \in [M], \mathbf{h}^{(0)}_{m} = \mathbf{h}^{(k)} \). 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

\[
\mathbf{h}^{(k,t+1)} = \mathbf{h}^{(k,t)} - \eta \nabla_{\mathbf{h}} f_m(\varphi(\mathbf{h}^{(k,t)}); \mathbf{z}_{m}^{(k,t)}) \quad (9)
\]

where \( \mathbf{z}_{m}^{(k,t)} \) is a mini-batch randomly drawn from \( \mathcal{D}_m \) at the \( t \)th iteration of round \( k \). After updating for \( t \) steps, we obtain \( \mathbf{h}^{(k,t)} \) and the corresponding normalized weight vector \( \mathbf{\bar{w}}^{(k,t)} \).
Fig. 2. One round of FedVote is composed of four steps. Each client first
updates the local model and then sends the quantized weight

\[ \text{Fig. 2. One round of FedVote is composed of four steps. Each client first}
\]
\[ \text{updates the local model and then sends the quantized weight}
\]
\[ \text{to the server. Later, the server calculates the voting statistics and sends back the soft}
\]
\[ \text{vote results to each client.}
\]

\[ (-1, 1)^d \text{ defined as follows:}
\]
\[ \tilde{w}_m^{(k,t)} \triangleq \varphi(h_m^{(k,t)}), \]
\[ \text{(10)} \]

We use the stochastic rounding [28] to draw a randomly quantized version \( w_m^{(k,t)} \) using \( \tilde{w}_m^{(k,t)} \), that is,

\[ w_{m,i}^{(k,t)} = \begin{cases} +1, & \text{with prob. } P_{m,j}^{(k,t)} = \frac{1}{2}\left[ \tilde{w}_{m,j}^{(k,t)} + 1 \right] \\ -1, & \text{with prob. } 1 - P_{m,j}^{(k,t)} \end{cases} \]
\[ \text{(11)} \]

It can be shown that stochastic rounding is an unbiased procedure, that is, \( \mathbb{E}[w_m^{(k,t)}|\tilde{w}_m^{(k,t)}] = \tilde{w}_m^{(k,t)} \). After quantization, the local client will send the binary weights \( w_m^{(k,t)} \) 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, that is, \( w^{(k+1)} = \text{sign}(\sum_{m=1}^{M} w_m^{(k,t)}) \). 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 \( \mathbf{w}^* \in \mathbb{D}^d \) be the optimal solution defined in (8). For the \( m^{th} \) client, \( e_{m,i} = P(w_{m,i}^{(k,t)} \neq w_i^*) \) denotes the error probability of the voting result of the \( i^{th} \) coordinate. Suppose the error events \( \{w_{m,i}^{(k,t)} \neq w_i^*\}_{m=1}^{M} \) are mutually independent, and the mean error probability \( s_i = (1/M) \sum_{m=1}^{M} e_{m,i} \) is smaller than (1/2). For the local weight \( w^{(k+1)} \), we have

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

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 soft voting to build an empirical distribution of global weight \( \mathbf{w} \), that is,

\[ \mathbb{P}(w_i^{(k+1)} = 1) = \frac{1}{M} \sum_{m=1}^{M} \mathbb{I}(w_{m,i}^{(k,t)} = 1) \]
\[ \text{(13)} \]

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

\[ h^{(k+1)} = \varphi^{-1}(2\mathbf{p}^{(k+1)} - 1) \]
\[ \text{(14)} \]

where \( \varphi^{-1} : (-1, 1) \to \mathbb{R} \) is the inverse of the normalization function \( \varphi \). We further apply clipping to restrict the range of the probability, namely, \( \text{clip}(p_i^{(k+1)}) = \max(p_{\text{min}}, \min(p_{\text{max}}, p_i^{(k+1)})), \) where \( p_{\text{min}}, p_{\text{max}} \in (0, 1) \) are predefined thresholds. To keep the notation consistent, we denote \( \tilde{w}^{(k+1)} = \varphi(h^{(k+1)}) \) as the global normalized weight. After broadcasting the soft voting results \( \mathbf{p}^{(k+1)} \), all clients are synchronized with the same latent weight \( h^{(k+1)} \) and normalized weight \( \tilde{w}^{(k+1)} \). 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: \( \mathbb{E}[\tilde{w}^{(k+1)}] = (1/M) \sum_{m=1}^{M} \tilde{w}_m^{(k,t)} \), where \( \tilde{w}^{(k+1)} = \varphi(h^{(k+1)}) \) and \( \tilde{w}_m^{(k,t)} = \varphi(h_m^{(k,t)}) \).

**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 the 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] and [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 \( \mathbb{P}(w_i^{(k+1)} = 1) = \sum_{m=1}^{M} \lambda_m^{(k)} (w_{m,i}^{(k,t)} = 1) \), 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:

\[ \text{CR}_m^{(k+1)} = (1/d) \sum_{i=1}^{d} w_{m,i}^{(k,t)} = w_i^{(k+1)} \].

Through multiple rounds, we track the credibility of a local client by taking an exponential moving average over the communication rounds, namely, \( v_m^{(k)} = \beta v_m^{(k-1)} + (1 - \beta) \text{CR}_m^{(k+1)} \), where \( \beta \in (0, 1) \) is a predefined coefficient. The weight \( \lambda_m^{(k)} \) is designed as \( \lambda_m^{(k)} = v_m^{(k)} / \sum_{m=1}^{M} v_m^{(k)} \).

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 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 ̂h = ∇hf(m)(h(k); z(m)). The local true gradient and global true gradient will be denoted by ̂h = ∇hf(m)(h(k); z(m)). In addition, let ̂θ(k, i) = wθ(k, i) − ŵθ(k, i) denote the error introduced by stochastic rounding. According to its unbiased property, Eξ|x = ξ ≈ f(x).

Assumption 1 (Lower Bound): ∀ h ∈ R, ̂w ∈ (−1, 1), the objective function is lower bounded by a constant f∗, that is, f(̂w) ≥ f∗ = minh∈R f(ϕ(h)).

Assumption 2 (L-Smoothness): ∀ ̂w1, ̂w2 ∈ (−1, 1), there exist some nonnegative L such that ∥∇f(m)(̂w1) − ∇f(m)(̂w2)∥ ≤ L ∥̂w1 − ̂w2∥. Assumptions 1–2 are common for necessary analysis [32].

Assumption 3: The normalization function ϕ : R → (−1, 1) is strictly increasing. In particular, we assume its first derivative is bounded for all h ∈ [c1, c2], that is, (d/dh)ϕ(h) ∈ [c1, c2], where c1, c2 are positive parameters independent of k, t, m, and i. Assumption 3 is not difficult to satisfy in practice. For example, let ϕ(h) = tanh(ah), we have ϕ′(h) = a[1 − tanh2(ah)], with c2 = a. Note that ϕ quickly saturates with a large h in the local updating. On the other hand, the empirical Bernoulli parameter pθ will be clipped for stabilization, which indicates that hθ(k, i) will be upper bounded by certain hB. In this sense, we have c1 = a[1 − tanh2(abh)]). The next two assumptions bound the variance of the stochastic gradient and quantization noise.

Assumption 4: The stochastic gradient has bounded variance, that is, E∥gθ(k, i) − hθ(k, i)∥2 ≤ σ2, where σ2 is a fixed variance independent of k, t, and m.

Assumption 5: The quantization error ξ(k, i) has bounded variance, that is, E∥ξ(k, i)∥2 ≤ σ2, where σ2 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 σ2 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 a ∈ (−1, 1) for the quantizer Q defined in (11), then the quantization error satisfies E∥Qa − a∥2 ≤ d − |a|2.

For existing algorithms quantizing the model update δ(m) = θ(k, i) − θθ(k, i, τ)2, the quantizer has the property E∥Q(x) − x∥2 ≤ q|x|2, with a fixed quantization step, q increases when the input dimension d increases [33]. We state the result for a widely used quantizer, quantized stochastic gradient descent (QSGD) [28], which has been adopted in FedPAQ, in the following lemma.

Lemma 4: Suppose we have an input x ∈ R for the QSGD quantizer Q. In the coarse quantization scenario, the quantization error satisfies E∥Q(x) − x∥2 ≤ O(d1/2)|x|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 η = O(c1/c2(1/θ√K)), then after K rounds of communication, we have

\[
\frac{1}{K} \sum_{k=0}^{K-1} c_2^2 E \| \nabla f(\tilde{w}(k)) \|^2_2 \leq \frac{2 [f(\tilde{w}(0)) − f(\tilde{w}^*)]}{\eta K} + c_2^2 \frac{L}{\eta \tau K M} \sum_{k=0}^{K-1} \sum_{m=1}^{M} R_m^{(k)} + c_2 \frac{2}{\tau M K} \sum_{k=0}^{K-1} \sum_{m=1}^{M} R_m^{(k)} (15)
\]

where R_m^{(k)} \preceq − \sum_{i=0}^{M} \sum_{j=1}^{M} [E[\langle \nabla f(\tilde{w}(k)) \rangle_i, \langle \nabla f(\tilde{w}(k)) \rangle_j]] and T_m^{(k)} \preceq \{ i \in [d] | g_i \cdot R_m^{(k)} \geq 0 \}.

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

Remark 1: When there is no normalization function and quantization, that is, ϕ(x) = x with c1 = c2 = 1, σ2 = 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 gθ(k, i), we expect the central limit theorem to render its distribution shape, where each entry δθ(k, i, τ) follows the Gaussian distribution. For the Bernoulli probability π(k, i), we expect the Beta distribution as the conjugate before rendering its distribution shape, where each entry πθ(k, i, τ) follows the symmetric Beta distribution. See Fig. 3 for the empirical results.

Remark 2: Following the analysis framework in Theorem 1, the order-wise convergence rate can be formulated.
as \((1/K) \sum_{k=0}^{K-1} \mathbb{E} \| \nabla f_m(\tilde{w}_m^{(k)}) \|_2^2 = O(1/\sqrt{K}) + E(d)\), where \(E(d)\) is the error introduced by the quantization. For FedVote with the normalized weight \(\tilde{w}_m^{(k,r)}\) as the input, when \(\pi_{m,j}\)’s follow the symmetric Beta distribution, it can be shown that \(\mathbb{E} \| \xi_m^{(k)} \|_2^2 = O(d)\) based on Lemma 3. For FedPAQ with the model update \(\delta_m^{(k)}\) as the input, when \(\delta_m^{(k)}\)’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 \(\nabla f_m(\tilde{w}_m^{(k)})\) and the global one \(\nabla f(\tilde{w}^{(k)})\) is not large, \(R_m^{(k)}\) can be treated as a bounded variable.

Remark 4: The choice of nonlinear function \(\phi : \mathbb{R}^d \rightarrow (-1, 1)^d\) will affect the convergence. If \(\phi\) behaves more like the sign(\cdot) function, for example, when \(a\) increases in tanh(\(ax\)), the quantization error will be reduced. In other words, we expect a smaller \(c_2^2\) 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

A. Data and Models

We choose image classification datasets, CIFAR-10 [34], Federated extended modified National Institute of Standards and Technology (FEMNIST) [35], and Fashion-Modified National Institute of Standards and Technology (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: 1) i.i.d. setting where the whole dataset is randomly shuffled and assigned to each worker without overlap and 2) 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 \(q_m \sim \text{Dir}(\alpha)\), where \(q_m = [q_{m,1}, \ldots, q_{m,C}]^\top\) belongs to the standard \((C-1)\)-simplex. We then assign data samples from different classes to the \(m\)th worker following the distribution of \(q_m\). We set \(\alpha = 0.5\) unless noted otherwise. We use a LeNet-5 architecture for Fashion-MNIST and a Visual Geometry Group (VGG)-7 architecture for CIFAR-10 and FEMNIST. Results are obtained over three repetitions.

B. Implementation Details

We provide implementation details in the proposed FedVote design. First, following prior works [21] and [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, 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 \(\phi(x) = \tanh(3x/2)\) unless noted otherwise. More details can be found in Appendix A-A.

C. 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. FedVote outperforms other methods by achieving the highest test accuracy when the communication cost is fixed.
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.

D. Byzantine Resilience

We consider the following three attack methods: 1) inverse sign, where attackers inverse the signs of transmitted weights/gradients; 2) data poisoning [18], where attackers flip the labels of the training data; and 3) 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.

E. Normalization Function

From Remark 4, we know that the normalization function can influence the model convergence. We empirically examine the impact of 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 cost. On the other hand, the gap between the model with normalized weight \( \tilde{w} \) and the one with binary weight \( w \) also decreases due to smaller quantization errors.

F. Ternary Neural Network (TNN) Extension

In Section IV, we focus on the BNNs. We extend FedVote to TNNs and empirically verify its performance. Training and transmitting the categorical distribution parameters of the ternary weight may bring additional communication and computation costs to edge devices, we, therefore, simplify the procedure as follows. For each ternary weight \( w_{(m,i)} \), we still keep a latent parameter \( h_{(m,i)}^{(l,t)} \) 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 an additional 1 bit/dimension communication overhead.

G. Deployment Efficiency

We highlight the advantages of BNNs during deployment on edge devices. In FedVote, we intend to deploy lightweight quantized neural networks on 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 \( x \in \mathbb{R}^{d_1} \) and output \( y \in \mathbb{R}^{d_2} \): \( y = W^T x \). 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 \( W_b \in \mathbb{D}_{d_1 \times d_2}^2 \) all multiplication operations can be replaced by an addition. 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 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 tradeoffs between communication efficiency and model accuracy. With the voting-based aggregation mechanism, FedVote enjoys the flexibility to incorporate various voting protocols to increase resilience against Byzantine attacks. We have
demonstrated that Byzantine-FedVote exhibits much better Byzantine resilience in the presence of close to half of attackers compared to the existing algorithms.

APPENDIX A
SETUP AND ADDITIONAL EXPERIMENTS
A. Hyperparameters
For the clipping thresholds, we set \( p_{\text{min}} = 0.001 \) and \( p_{\text{max}} = 1 - p_{\text{min}} \). 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 and use \( k \) and \( \tau \) for the current batch \( B \) to 40 and the local batch size to 100. For FetchSGD [40], we set the number of sketch columns to \( 1 \times 10^6 \) and use \( k = 5 \times 10^6 \) 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 in accuracy in Byzantine-FedVote is negligible.

C. Extension to TNNs
The stochastic rounding used in the TNNs, \( w_i = Q_{st}(\tilde{w}) \), is an extension of (11)

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

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

APPENDIX B
MISSING PROOFS
A. Proof of Lemma 1
Proof: Let \( X_{m,i} \triangleq \mathbb{1}(w_{m,i}^{(k+1)} \neq w_i^*) \), following Bernoulli distribution with parameter \( \epsilon_{m,i} \). Let \( Y_i = \sum_{m=1}^{M} X_{m,i} \), we have

\[
\mathbb{P}(w_i^{(k+1)} \neq w_i^*) = \mathbb{P}(Y_i \geq \frac{M}{2}).
\]
With independent vote results from workers, \( Y_i \) follows Poisson binomial distribution with mean \( \mu_{Y_i} = \sum_{m=1}^{M} e_{m,i} \), \( \forall \, a > 0 \), the Chernoff bound can be derived as

\[
\mathbb{P}
\left(
Y_i \geq \frac{M}{2}
\right)
\leq
\exp\left(-\frac{a M}{2}ight) \mathbb{E}[e^{aY_i}]
\leq \exp\left(-\frac{a M}{2}\right) \prod_{m=1}^{M} (1 - e_{m,i} + e^{a e_{m,i}})
\leq \exp\left(-\frac{a M}{2} \sum_{m=1}^{M} (e^{a e_{m,i}} - 1)\right)
\]

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

By assumption we have \( \mu_{Y_i} < (M/2) \). Let \( a = \ln(M/2\mu_{Y_i}) \), we have

\[
\mathbb{P}
\left(
Y_i \geq \frac{M}{2}
\right)
\leq \exp\left(-\frac{\mu_{Y_i} + M}{2}\right) \left(\frac{\mu_{Y_i}}{\mu_{Y_i}}\right)^{\frac{M}{2}}
\leq \left(\frac{2 \mu_{Y_i}}{M} \exp\left(1 - \frac{2 \mu_{Y_i}}{M}\right)\right)^{\frac{M}{2}}
\]

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

**B. Proof of Lemma 2**

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

\[
\mathbb{E}_x \left[ w_{m,i}^{(k+1)} \right] = \frac{1}{M} \sum_{m=1}^{M} \left( 2 \bar{p}_{m,i}^{(k+1)} - 1 \right)
= \frac{1}{M} \sum_{m=1}^{M} \phi \left( h_{m,i}^{(k)} \right)
\]

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

\[
\mathbb{E}_x \left[ \bar{w}_{m,i}^{(k+1)} \right] = \frac{1}{M} \sum_{m=1}^{M} \bar{w}_{m,i}^{(k+1)}
\]

which completes the proof.

**C. Proof of Lemma 3**

**Proof:** Let \( \hat{a} \triangleq Q_{\nu}(a) \), we have

\[
\mathbb{E}[\|Q_{\nu}(a) - a\|_2^2] = \mathbb{E}\left[ \sum_{i=1}^{d} (\hat{a}_i^2 - a_i^2) \right] = \sum_{i=1}^{d} (\mathbb{E}[\hat{a}_i^2] - a_i^2) = d - \|a\|_2^2.
\]

The proof is complete.

**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

\[
Q_{\text{qsgd}}(x_i) = \|x\|_2 \cdot \text{sgn}(x_i) \cdot \xi_i(x_i, s)
\]

where

\[
\xi_i(x_i, s) = \begin{cases} 
0, & \text{with prob. } 1 - \frac{|x_i|}{\|x\|_2} \\[1em]
1, & \text{with prob. } \frac{|x_i|}{\|x\|_2}.
\end{cases}
\]

The variance of quantization error is

\[
\mathbb{E}[\|Q(x) - x\|_2^2| x] = \mathbb{E}\left[ \sum_{i=1}^{d} (\hat{\xi}_i - x_i)^2 \right] = \mathbb{E}\left[ \sum_{i=1}^{d} (\hat{\xi}_i^2 | x) - x_i^2 \right] = \|x\|_2^2 \sum_{i=1}^{d} |x_i| - \|x\|_2^2 = \|x\|_2 \|x\|_1 - \|x\|_2^2 \leq (\sqrt{d} - 1) \|x\|_2^2
\]

which completes the proof.

**E. Proof of Theorem 1**

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

\[
\Delta^{(k)} \triangleq \bar{w}^{(k)} - \bar{w}^{(k+1)}.
\]

We use \( \varepsilon^{(k)} \) to denote the stochastic gradient noise, that is,

\[
\varepsilon^{(k)} \triangleq \bar{g}^{(k)} - g^{(k)}.
\]

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

**Lemma 5:** The global normalized weight \( \bar{w}^{(k+1)} \) can be reconstructed as the average of local binary weight, i.e.,

\[
\bar{w}^{(k+1)} = \frac{1}{M} \sum_{m=1}^{M} w_{m,i}^{(k)}.
\]

**Proof:** See Appendix B-F.

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

\[
|\varphi(x_1) - \varphi(x_2)| \leq c_2 |x_1 - x_2|.
\]
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

\[
\phi'(c) = \frac{\phi(x_2) - \phi(x_1)}{x_2 - x_1}.
\]

(32)

For the monotonically increasing function \( \phi \), we have

\[
\phi(x_2) - \phi(x_1) = \phi'(c)(x_2 - x_1)
\]

(33a)

\[\triangleright= c_2(x_2 - x_1)\]

(33b)

where \( \triangleright \) holds due to Assumption 3. A 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

\[
E\|\overline{\omega}_{m}^{(k),r} - \overline{\omega}^{(k)}\|_2^2 \leq (c_2\eta^2)^2 \left( \sum_{t=0}^{t-1} E\|g_m^{(k,t)}\|_2^2 + \sigma_c^2 \right).
\]

(34)

Proof: See Appendix B-G. \( \square \)

Lemma 8: Under Assumptions 2–5, we have

\[
E(\nabla f(\overline{w}^{(k)}), \Delta^{(k)}) \geq \frac{c_1^2\eta^2}{2} E\|\nabla f(\overline{w}^{(k)})\|_2^2
\]

+ \[
\frac{c_1^2\eta}{4M} (2 - (c_2L)^2\eta^2\tau(\tau - 1)) \sum_{m=1}^{M} \sum_{t=0}^{t-1} E\|g_m^{(k,t)}\|_2^2
\]

- \[
\frac{(c_1c_2L)^2\eta^2\tau(\tau - 1)}{4} \sigma_c^2 - \frac{\eta^2(c_2^2 - c_1^2)M}{4} \sum_{m=1}^{M} R_m^{(k)}
\]

(35)

where \( R_m^{(k)} \triangleq - \sum_{t=0}^{t-1} \sum_{m=0}^{d-1} \mathbb{E}[E(\nabla f(\overline{w}^{(k)}), \nabla f(\overline{w}^{(k,m,t)}))] \) and \( T_m^{(k,t)} \triangleq \{i \in [d] | g_{m,i}^{(k,t)} > 0\} \).

Proof: See Appendix B-H. \( \square \)

Lemma 9: Under Assumptions 2–5, we have

\[
E\|\Delta^{(k)}\|_2^2 \leq \frac{(c_2\eta^2)^2}{M} \left( \sum_{m=1}^{M} \sum_{t=0}^{t-1} E\|g_m^{(k,t)}\|_2^2 \right)
\]

+ \[
\frac{(c_2\eta^2)^2}{M} \sigma_c^2 + \frac{1}{M} \sigma_k^2
\]

(36)

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

\[
\Delta^{(k)} = \overline{w}^{(k)} - \overline{w}^{(k+1)}
\]

(37)

\[\triangleright \overline{w}^{(k)} - \frac{1}{M} \sum_{m=1}^{M} \overline{w}_{m}^{(k),r}\]

(38a)

\[\triangleright \overline{w}^{(k)} - \overline{w}^{(k)} = \frac{1}{M} \sum_{m=1}^{M} \overline{w}_{m}^{(k),r} + \frac{1}{M} \sum_{m=1}^{M} \xi^{(k)}
\]

(38b)

where \( \triangleright \) follows from (30), and \( \triangleright \) holds by substituting the definition of quantization error. From Assumption 2, we have

\[
f(\overline{w}^{(k+1)}) - f(\overline{w}^{(k)}) \leq -\langle \nabla f(\overline{w}^{(k)}), \Delta^{(k)} \rangle + \frac{L}{2}\|\Delta^{(k)}\|_2^2.
\]

(39a)

Let \( ((L\eta^2(\tau - 1)/2) + (L\eta/c_1^2) \leq (1/c_2^2) \), take the expectation on both sides, and use Lemmas 8 and 9

\[
E\left[ f(\overline{w}^{(k+1)}) - f(\overline{w}^{(k)}) \right] \leq -\frac{c_1^2\eta^2}{2} E\|\nabla f(\overline{w}^{(k)})\|_2^2 - \frac{(c_1c_2^2)^2\eta}{4M}
\]

\[
+ \frac{(c_1^2\eta)^2L\tau}{4} \sum_{m=1}^{M} R_m^{(k)} + \frac{L}{2M}\sigma_c^2
\]

(40a)

where \( \triangleright \) follows from the restrictions on the learning rate. We rewrite the restriction as

\[
\eta \leq \frac{L\tau}{(L(\tau - 1)c_1^2)} \leq \frac{c_1^2}{L(\tau - 1)c_2^2}
\]

(40b)

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

\[
\frac{1}{K} \sum_{k=0}^{K-1} c_1^2 E\|\nabla f(\overline{w}^{(k)})\|_2^2
\]

\[
\leq \frac{2\left( f(\overline{w}^{(0)}) - f(\overline{w}^{*}) \right)\eta \tau K}{c_1^2}
\]

\[
+ c_1^2\eta \left[ \frac{1}{M} + \frac{c_1^2\eta^2(\tau - 1)}{2} \right] \sigma_c^2 + \frac{L}{\eta \tau KM} \sum_{k=0}^{K-1} \sigma_k^2
\]

(41a)

\[
+ \frac{2(c_2^2 - c_1^2)}{\tau MK} \sum_{k=0}^{K-1} R_m^{(k)}
\]

(42a)

\( \square \)

F. Proof of Lemma 5

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

\[
\widehat{w}_{m}^{(k+1)} = 2p_{m}^{(k+1)} - 1.
\]

(43)

The \( i \)th entry of \( p_{i}^{(k)} \) is defined in (13), that is,

\[
p_{i}^{(k+1)} = \frac{1}{M} \sum_{m=1}^{M} \mathbb{I}\left( \widehat{w}_{m}^{(k+1)} = 1 \right).
\]

(44)
Substituting (44) into (43) yields
\[ w_i^{(k+1)} = \frac{1}{M} \sum_{m=1}^{M} \left( 2 \cdot \mathbb{1}(\omega_{m,i}^{(k,r)} = 1) - 1 \right). \] (45)

Note that
\[ 2 \cdot \mathbb{1}(\omega_{m,i}^{(k,r)} = 1) - 1 = \begin{cases} +1, & \omega_{m,i}^{(k,r)} = 1 \\ -1, & \omega_{m,i}^{(k,r)} = -1 \end{cases} \] (46)
we have
\[ w_i^{(k+1)} = \frac{1}{M} \sum_{m=1}^{M} \omega_{m,i}^{(k,r)} \] (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
\[ \mathbb{E} \left\| \hat{w}_m^{(k,r)} - \tilde{w}_m^{(k)} \right\|_2^2 \\
= \mathbb{E} \left\| \varphi(h_m^{(k,r)}) - \varphi(h_m,0_m) \right\|_2^2 \] (48a)
\[ \overset{\odot}{\leq} c_2^2 \mathbb{E} \left\| h_m^{(k,r)} - h_m(0) \right\|_2^2 = c_2^2 \mathbb{E} \left\| \sum_{t=0}^{r-1} - \eta \hat{g}_m^{(k)}[k,t] \right\|_2^2 \] (48b)
where \( \odot \) comes from the Lipschitz condition in Lemma 6. By decomposing \( \hat{g}_m^{(k,r)} \) into \( h_m^{(k,r)} + e_m^{(k,r)} \), we have
\[ \mathbb{E} \left\| \hat{w}_m^{(k,r)} - \tilde{w}_m^{(k)} \right\|_2^2 = (c_2^2 \nu) \left( \mathbb{E} \left\| \sum_{t=0}^{r-1} g_m^{(k,t)} \right\|_2^2 + \mathbb{E} \left\| \sum_{t=0}^{r-1} e_m^{(k,t)} \right\|_2^2 \right) \] (49a)
\[ \overset{\odot}{\leq} (c_2^2 \nu) \left( \sum_{t=0}^{r-1} \mathbb{E} \left\| g_m^{(k,t)} \right\|_2^2 + \sigma_e^2 \right) \] (49b)
which completes the proof. \[ \square \]

H. Proof of Lemma 8

Proof: We have
\[ \mathbb{E} \langle \nabla f(\tilde{w}^{(k)}), \Delta^{(k)} \rangle \\
= \mathbb{E} \langle \nabla f(\tilde{w}^{(k)}), \tilde{w}^{(k)} - \frac{1}{M} \sum_{m=1}^{M} \tilde{w}_m^{(k)} + \frac{1}{M} \sum_{m=1}^{M} \xi_m^{(k)} \rangle \\
= \mathbb{E} \langle \nabla f(\tilde{w}^{(k)}), \frac{1}{M} \sum_{m=1}^{M} \varphi(h_m^{(k)}) - \varphi(h_m^{(k,r)}) \rangle. \] (50a)

From the mean value theorem, for \( h_i^{(k)}, h_m^{(k,r)} \in \mathbb{R} \), there exists a point \( c_{m,i}^{(k)} \in \mathbb{H}_{m,i}^{(k,r)} \) such that
\[ f'(c_{m,i}^{(k)}) = \frac{\phi(h_i^{(k)}) - \phi(h_m^{(k,r)})}{h_i^{(k)} - h_m^{(k,r)}} \] (51)
where \( \mathbb{H}_{m,i}^{(k,r)} \) is an open interval with endpoints \( h_i^{(k)} \) and \( h_m^{(k,r)} \), that is,
\[ \mathbb{H}_{m,i}^{(k,r)} = \begin{cases} (h_i^{(k)}, h_m^{(k,r)}), & \text{if } h_i^{(k)} < h_m^{(k,r)} \\ (h_m^{(k,r)}, h_i^{(k)}), & \text{otherwise}. \end{cases} \] (52)

Let \( C_m^{(k)} = \text{diag}((d\varphi/dh_m^{(k,r)}),\ldots,(d\varphi/dh_m^{(k,r)})) \), we have
\[ \phi(h_m^{(k)}) - \phi(h_m^{(k,r)}) = C_m^{(k)}(h_m^{(k)} - h_m^{(k,r)}) \] (53a)
\[ \overset{\odot}{=} \eta C_m^{(k)} \sum_{t=0}^{r-1} (g_m^{(k,t)} + e_m^{(k,t)}). \] (53b)

Substituting (53b) into (50b) yields
\[ \mathbb{E} \langle \nabla f(\tilde{w}^{(k)}), \Delta^{(k)} \rangle \\
= \frac{\mu}{M} \sum_{m=1}^{M} \sum_{t=0}^{r-1} \mathbb{E} \langle \nabla f(\tilde{w}^{(k)}), C_m^{(k)} g_m^{(k,t)} \rangle. \] (54)

According to the chain rule, \( g_m^{(k,t)} \) can be written as
\[ g_m^{(k,t)} = \nabla_k f_m(\varphi(h_m^{(k,t)})) = D_m^{(k)} \nabla f_m(\tilde{w}_m^{(k,t)}) \] (55)
where \( D_m^{(k)} = \text{diag}((d\varphi/dh_m^{(k,r)}),\ldots,(d\varphi/dh_m^{(k,r)})) \). To simplify the notations, let \( B_m^{(k,t)} = C_m^{(k)} D_m^{(k)} \). Note that \( B_m^{(k,t)} \) is still a diagonal matrix, where the \( i \)th diagonal element \( b_{m,i}^{(k,t)} \) is
\[ b_{m,i}^{(k,t)} \overset{\odot}{=} (B_m^{(k,t)})_{i,i} = \frac{d\varphi}{dh_m^{(k,t)}} \cdot \frac{d\varphi}{dh_m^{(k,t)}}. \] (56)

Substituting (55) into (54), we have
\[ \mathbb{E} \langle \nabla f(\tilde{w}^{(k)}), \Delta^{(k)} \rangle \\
= \frac{\mu}{M} \sum_{m=1}^{M} \sum_{t=0}^{r-1} \mathbb{E} \langle \nabla f(\tilde{w}^{(k)}), B_m^{(k,t)} \nabla f_m(\tilde{w}_m^{(k,t)}) \rangle. \] (57)

We first focus on the following inner product:
\[ \langle \nabla f(\tilde{w}^{(k)}), B_m^{(k,t)} \nabla f_m(\tilde{w}_m^{(k,t)}) \rangle \\
= \sum_{i=1}^{d} \langle \nabla f(\tilde{w}^{(k)}), h_i^{(k,t)}, \nabla f_m(\tilde{w}_m^{(k,t)}) \rangle_i \] (58)
where \( \langle \nabla f \rangle_i \) denotes the \( i \)th entry of the gradient vector.
We consider the set \( \mathcal{I}_m^{(k,t)} \) defined as
\[ \mathcal{I}_m^{(k,t)} = \{ i \in [d] | \langle \nabla f(\tilde{w}^{(k,t)}) \rangle_i \cdot \langle \nabla f_m(\tilde{w}_m^{(k,t)}) \rangle_i \geq 0 \}. \] (59)

Let \( \mathcal{I}_m^{(k,t)} \) denote the complement of \( \mathcal{I}_m^{(k,t)} \). The result in (58) can be bounded as
\[ \mathbb{E} \langle \nabla f(\tilde{w}^{(k)}), B_m^{(k,t)} \nabla f_m(\tilde{w}_m^{(k,t)}) \rangle \\
\overset{\odot}{=} c_1^t \sum_{i \in \mathcal{I}_m^{(k,t)}} \mathbb{E} \left[ \langle \nabla f(\tilde{w}^{(k,t)}) \rangle_i \cdot \langle \nabla f_m(\tilde{w}_m^{(k,t)}) \rangle_i \right] \\
+ c_2^t \sum_{i \not\in \mathcal{I}_m^{(k,t)}} \mathbb{E} \left[ \langle \nabla f(\tilde{w}^{(k,t)}) \rangle_i \cdot \langle \nabla f_m(\tilde{w}_m^{(k,t)}) \rangle_i \right]. \] (60b)
\[ c_1^2 \mathbb{E}(\nabla f(\tilde{w}(k)), \nabla f_m(\tilde{w}_m^{(k,l)})) + \]
\( (c_2^2 - c_1^2) \sum_{i \in I_{n^{(k,l)}}} \mathbb{E}(\nabla f(\tilde{w}(k)), (\nabla f_m(\tilde{w}_m^{(k,l)}))) \] (60c)

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

\[ R_m^{(k)} = \sum_{t=0}^{\tau - 1} \sum_{m=t} \mathbb{E}(\nabla f(\tilde{w}(k)), (\nabla f_m(\tilde{w}_m^{(k,l)}))) \] (61)

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

\[ \mathbb{E}(\nabla f(\tilde{w}[k]), \Delta[k]) \geq \frac{c_1^2 \eta}{2M} \sum_{m=1}^{M} \sum_{t=0}^{\tau - 1} (\mathbb{E}\|\nabla f(\tilde{w}(k))\|_2^2 + \mathbb{E}\|\nabla f_m(\tilde{w}_m^{(k,l)})\|_2^2)
\]

\[ - \mathbb{E}\|\nabla f(\tilde{w}_m^{(k,l)}) - \nabla f(\tilde{w}(k))\|_2^2
\]

\[ - \eta(c_2^2 - c_1^2) \sum_{m=1}^{M} R_m^{(k)} \] (63a)

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

\[ \mathbb{E}(\nabla f(\tilde{w}(k)), \Delta[k]) \geq \frac{c_1^2 \eta}{2M} \sum_{m=1}^{M} \sum_{t=0}^{\tau - 1} (\mathbb{E}\|\nabla f(\tilde{w}(k))\|_2^2 + \mathbb{E}\|\nabla f_m(\tilde{w}_m^{(k,l)})\|_2^2)
\]

\[ - \mathbb{E}\|\nabla f(\tilde{w}_m^{(k,l)}) - \nabla f(\tilde{w}(k))\|_2^2
\]

\[ - \eta(c_2^2 - c_1^2) \sum_{m=1}^{M} R_m^{(k)} \] (63b)

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

\[ \mathbb{E}\|\tilde{w}_m^{(k,l)} - \tilde{w}(k)\|_2^2 \leq (c_2\eta)^2 \tau \left( \sum_{n=0}^{\tau - 1} \|g_m^{(k,n)}\|_2^2 + \sigma_c^2 \right) \] (64)

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

\[ \mathbb{E}(\nabla f(\tilde{w}[k]), \Delta[k]) \geq \frac{c_1^2 \eta \tau}{2M} \mathbb{E}\|\nabla f(\tilde{w}(k))\|_2^2 + \frac{c_1^2 \eta}{2M} \sum_{m=1}^{M} \sum_{t=0}^{\tau - 1} \mathbb{E}\|\nabla f_m(\tilde{w}_m^{(k,l)})\|_2^2
\]

\[ - \frac{(c_1c_2L)^2 \eta \tau}{4M} \sum_{m=1}^{M} \sum_{t=0}^{\tau - 1} (\tau(n + 1)) \mathbb{E}\|g_m^{(k,n)}\|_2^2
\]

\[ - \frac{(c_1c_2L)^2 \eta \tau}{4} \mathbb{E}\|\nabla f(\tilde{w}(k))\|_2^2 - \frac{(c_2^2 - c_1^2)}{M} \sum_{m=1}^{M} R_m^{(k)} \] (65a)

where \( \square \) follows from Assumption 5. For the first term in (66d)

\[ \mathbb{E}\|\tilde{w}_m^{(k,l)} - \tilde{w}(k)\|_2^2 \leq (c_2\eta)^2 \tau \left( \sum_{n=0}^{\tau - 1} \|g_m^{(k,n)}\|_2^2 + \sigma_c^2 \right) \] (64)

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

\[ \mathbb{E}(\nabla f(\tilde{w}[k]), \Delta[k]) \geq \frac{c_1^2 \eta \tau}{2M} \mathbb{E}\|\nabla f(\tilde{w}(k))\|_2^2 + \frac{c_1^2 \eta}{2M} \sum_{m=1}^{M} \sum_{t=0}^{\tau - 1} \mathbb{E}\|\nabla f_m(\tilde{w}_m^{(k,l)})\|_2^2
\]

\[ - \frac{(c_1c_2L)^2 \eta \tau}{4M} \sum_{m=1}^{M} \sum_{t=0}^{\tau - 1} (\tau(n + 1)) \mathbb{E}\|g_m^{(k,n)}\|_2^2
\]

\[ - \frac{(c_1c_2L)^2 \eta \tau}{4} \mathbb{E}\|\nabla f(\tilde{w}(k))\|_2^2 - \frac{(c_2^2 - c_1^2)}{M} \sum_{m=1}^{M} R_m^{(k)} \] (65a)

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
where 1 is due to Lemma 6 ③ follows from Assumption 4. For the second term in (66d) we have

$$E\|1/M\sum_{m=1}^{M} \xi_m^{(k)}\|^2_2 \leq 1/M^2 \zeta^2.$$  (68)

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

REFERENCES

[1] P. Kairouz et al., “Advances and open problems in federated learning,” Found. Trends Mach. Learn., vol. 14, nos. 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 Proc. Int. Conf. Artif. Intell. Statist., 2017, pp. 1273–1282.
[3] A. Reisizadeh, A. Mokhtari, H. Hassani, A. Jadbabaie, and R. Pedarsani, “FedAvg: A communication-efficient federated learning method with periodic averaging and quantization,” in Proc. Int. Conf. Artif. Intell. Statist., 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 Proc. Int. Conf. Artif. Intell. Statist., 2021, pp. 2350–2358.
[5] P. Blanchard et al., “Machine learning with adversaries: Byzantine tolerant gradient descent,” in Proc. Adv. Neural Inf. Process. Syst., 2017, pp. 1–15.
[6] D. Yin, Y. Chen, R. Kannan, and P. Bartlett, “Byzantine-robust distributed learning: Towards optimal statistical rates,” in Proc. Int. Conf. Mach. Learn., 2018, pp. 5650–5659.
[7] L. Muñoz-González, K. T. Co, and E. C. Lupu, “Byzantine-robust federated machine learning through adaptive model averaging,” 2019, arXiv:1909.05135.
[8] F. Sattler, K.-R. Müller, T. Wiegand, and W. Samek, “On the Byzantine robustness of clustered federated learning,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), May 2020, pp. 8861–8865.
[9] J. Bernstein, Y.-X. Wang, K. Azizzadenesheli, and A. Anandkumar, “SignSGD: Compressed optimisation for non-convex problems,” in Proc. Int. Conf. Mach. Learn., 2018, pp. 560–569.
[10] F. Sattler, S. Wiedemann, K.-R. Müller, and W. Samek, “Robust and communication-efficient federated learning from non-i.id. Data,” IEEE Trans. Neural Netw. Learn. Syst., vol. 31, no. 9, pp. 3400–3413, Sep. 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 Proc. Neural Inf. Process. Syst., 2020, pp. 21616–21626.
[12] R. Jin, Y. Huang, X. He, H. Dai, and T. Wu, “Stochastic-sign SGD for federated learning with theoretical guarantees,” 2020, arXiv:2002.10940.
[13] M. Safaryan and P. Richtarik, “Stochastic sign descent methods: New algorithms and better theory,” in Proc. Int. Conf. Mach. Learn., 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,” 2021, arXiv:2105.05001.
[15] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang, “On the convergence of fedavg on non-iID data,” in Proc. Int. Conf. Learn. Represent., 2020, pp. 1–26.
[16] K. Bonawitz et al., “Practical secure aggregation for federated learning on user-held data,” 2016, arXiv:1611.04842.
[17] C. Zhang, S. Li, J. Xia, W. Wang, F. Yan, and Y. Liu, “BatchCrypt: Efficient homomorphic encryption for cross-silo federated learning,” in Proc. USENIX Annu. Tech. Conf., 2020, pp. 493–506.
[18] X. Cao, M. Fang, J. Liu, and N. Z. Gong, “FLTrust: Byzantine-robust federated learning via trust bootstrapping,” in Proc. New. Distrib. Syst. Symp., 2021, pp. 1–18.
[19] V. Shejwalkar and A. Houmansadr, “Manipulating the Byzantine: Optimizing model poisoning attacks and defenses for federated learning,” in Proc. New. Distrib. Syst. Secur. Symp., 2021, pp. 1–19.
[20] I. Hubara, M. Courbariaux, D. Soudry, R. El-Yaniv, and Y. Bengio, “Binarized neural networks,” in Proc. Adv. Neural Inf. Process. Syst., 2016, pp. 4114–4122.
[21] O. Shayev, D. Levi, and E. Fetaya, “Learning discrete weights using the local reparameterization trick,” in Proc. Int. Conf. Learn. Represent., 2018, pp. 1–12.
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 Post-Doctoral Researcher in electrical and computer engineering at North Carolina State University from 2021 to 2022. He is currently a Faculty Member with the Department of Information and Communication Engineering, Zhejiang University. 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 the B.Eng. and M.Phil. degrees in electronic and information engineering from The Hong Kong Polytechnic University, Hong Kong, in 2008 and 2010, respectively, and the Ph.D. degree in electrical engineering from the University of Maryland, College Park, MD, USA, in 2017.

He was a Data Scientist at Origin Wireless Inc., Greenbelt, MD, USA. 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, Raleigh, NC, USA. His research interests include multimedia forensics, statistical signal processing, machine learning, data analytics, and video coding.

Dr. Wong received the Top-Four Student Paper Award, the Future Faculty Fellowship, the HSBC Scholarship, and the 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.

Huaiku 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, USA, in 2002.

He was with Bell Labs, Lucent Technologies, Holmdel, NJ, USA, in the Summer of 2000, and with AT&T Labs-Research, Middletown, NJ, USA, in the Summer of 2001. He is currently a Professor of electrical and computer engineering with NC State University, Raleigh, NC, USA, 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.

Dr. Dai was a co-recipient of Best Paper Awards at the 2010 IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS 2010), the 2016 IEEE INFOCOM BigSecurity Workshop, and the 2017 IEEE International Conference on Communications (ICC 2017). He received the Qualcomm Faculty Award in 2019. He 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.