面向联邦学习的近似无线通信

马翔*、孙海健†、胡清扬·罗斯*和钱毅‡
*犹他州立大学电气与计算机工程系，洛根，犹他州
†乔治亚大学电气与计算机工程学院，美国佐治亚州雅典
‡内布拉斯加大学林肯分校电气与计算机工程系，林肯，内布拉斯加州 电子邮箱：*{xiang.ma@ieee.org, rose.hu@usu.edu}，†hun@uga,edu，‡ yi.qian@unl.edu

arXiv:2304.03359v1 [cs.DC] 6 Apr 2023

摘要—本文提出了一种用于上行传输中联邦学习（FL）模型聚合的近似无线通信方案。我们考虑了一种现实信道，该信道在无线网络中的联邦学习模型交换期间会产生比特错误。我们的研究表明，模型传输期间的随机比特错误会显著影响联邦学习性能。为克服这一挑战，我们基于数学和统计证明提出了一种近似通信方案，即在一定约束条件下，机器学习（ML）模型梯度是有界的。这一界限使我们能够引入一种新的编码方案，用于梯度值的浮点数到二进制表示及其QAM星座映射。此外，由于联邦学习梯度具有抗误差能力，当信道质量良好时，所提方案会直接传输带有误差的梯度，从而无需大量纠错码和/或重传。其直接优势包括更低的开销和更低的时延。所提方案非常适用于无线网络中的资源受限设备。通过仿真，我们表明，所提方案能够有效减小比特错误对联邦学习性能的影响，并且与采用纠错和重传的传输方式相比，为达到相同的学习性能，至少节省一半时间。此外，我们研究了采用格雷编码时高阶调制中比特保护机制的有效性，发现这种方法能够显著提升学习性能。

索引词—近似通信、联邦学习、无线网络、比特误差率、调制

I. 引言

联邦学习（FL） [1]使本地设备能够执行机器学习（ML）任务，同时受益于模型参数共享所带来的学习泛化能力。它无需在设备与服务器之间共享本地收集的数据，而是仅共享模型参数，从而有效保护数据隐私。联邦学习系统由一个中央参数服务器（PS）和大量智能本地客户端（LCs）组成。学习客户端（LCs）从机载传感器收集数据，并根据参数服务器（PS）广播的全局模型执行预定义的机器学习（ML）任务。计算完成后，每个学习客户端（LC）都会将本地模型发送至参数服务器（PS）进行聚合，然后再将更新后的全局模型重新分发给学习客户端（LCs）。这一过程会不断重复，直至全局模型收敛。

对于作为学习客户端（LC）的无人机等边缘设备，通常采用无线网络将其连接到参数服务器（PS）。然而，无线信道的特性往往会导致信息传输出现错误。为了解决这一问题，现代无线通信采用前向纠错（FEC）方法，例如卷积码和低密度奇偶校验码（LDPC），以检测并纠正接收到的比特错误。FEC 的基本原理是使用冗余信息对消息进行编码，并将其作为纠错码（ECC）。接收机无需知道发射机实际发送的比特，即可纠正出错的比特。当错误数量超过 ECC 的纠错能力时，可以采用数据包重传。尽管前向纠错和数据包重传十分有效，但它们会增加计算开销和通信开销，导致联邦学习（FL）模型聚合期间额外的功耗和传输延迟。在 [2]，中，作者关注了联邦学习中的传输比特错误，但仅限于分组擦除信道。

随机梯度下降（SGD）是分布式机器学习中广泛使用的优化方法。在联邦学习中，每个客户端针对机器学习任务执行随机梯度下降，然后在每个通信轮次中计算单步梯度并发送至中央参数服务器。这种方法称为 FedSGD [3]，，是联邦学习的基线算法。然而，对于拥有数百万个参数的大规模分布式机器学习模型，传输梯度可能会导致较高的延迟。先进的传输方案，例如非正交多址接入（NOMA） [4]，是不错的选择，但需要配备复杂的解码方法。梯度压缩是应对这一挑战的一种有前景的方法，大量研究已表明，梯度稀疏化和量化能够在几乎不损失性能的情况下发挥作用。例如， [5] 中采用了 1 位随机梯度下降来减少梯度传输量，而 [6],则表明可以丢弃 99% 的梯度。因此，本文旨在采用近似无线通信 来传输这些梯度，即允许有损传输（存在误差），以换取低延迟、低开销和更少的前向纠错计算。我们想强调的是，梯度压缩与我们提出的近似无线通信方法有所不同，且二者可以并行使用，尽管两者都可能导致信息误差。梯度量化误差的可容忍性基于这样一个假设：梯度幅值足够小。 [7]，[8]，[9] 中的实证研究表明，梯度近似服从高斯分布，且大多数梯度值落在 $(-1,1)$ 甚至 $(-0.01,0.01)$ 的范围内。 [10]，[11],中提出了用于媒体数据传输的近似无线通信，类似的思想也可应用于联邦学习梯度。

传输。

在本研究中，我们对常用机器学习设置下的有界机器学习梯度进行了理论分析。具体而言，我们证明了在常用条件下，全连接神经网络模型和卷积神经网络模型中的梯度是有界的。基于这一分析，我们为错误梯度设定了一个限值，并结合实际无线网络中的近似传输进行了研究。仿真结果表明，我们提出的方法能够有效减小比特错误对联邦学习性能的影响，并且与采用纠错与重传（ECRT）相比，可节省一半的传输时间。本文其余部分的组织结构如下。第2节介绍无线网络中的联邦学习模型，第3节给出有界梯度的理论分析，第4节介绍所提出的方法，第5节展示仿真结果，第6节总结全文。

II. 系统模型

联邦学习模型如下所述。联邦学习系统由 M 个学习客户端组成，这些客户端通过无线信道连接到参数服务器。总体数据量 D 分布在 M 台设备之间，每台设备 m 包含 D_m 条数据。

A. 联邦学习系统模型

联邦学习是一种迭代式机器学习算法，每轮都会执行本地计算和全局聚合。本地计算之后，学习客户端会上传模型；全局聚合完成后，再将全局模型下载到各个学习客户端。此过程会重复进行，直至模型收敛。联邦学习的目标函数可定义为：

$$\min_{\boldsymbol{w}\in R^d} f(\boldsymbol{w}) \quad \text{where} \quad f(\boldsymbol{w}) \stackrel{\text{def}}{=} \frac{1}{|D|}\sum_{i=1}^{|D|} f_i(\boldsymbol{w}), \tag{1}$$

其中， $|D|$ 是数据集 D的大小。 $f_i(\boldsymbol{w}) = C(\boldsymbol{x_i}, \boldsymbol{y_i}; \boldsymbol{w})$ 是用于衡量数据样本$(\boldsymbol{x_i}, \boldsymbol{y_i})$与模型参数 $\boldsymbol{w}$所做推理之间推理误差的代价函数或损失函数。对于机器学习中的分类问题，通常使用交叉熵函数作为损失函数 C，尤其是在神经网络模型中。在多类分类中，标签 $\boldsymbol{y_i}$ 通常采用独热编码，以确保每个标签的权重相同。

由于数据分布在 M 个学习客户端上，而非同一台设备上，因此需要将目标函数(1)改写如下：

$$f(\boldsymbol{w}) = \sum_{m=1}^{M} \frac{|D_m|}{|D|} F_m(\boldsymbol{w}), \tag{2}$$

其中 $F_m(\boldsymbol{w}) = \frac{1}{|D_m|}\sum_{i\in D_m} f_i(\boldsymbol{w})$。通过将数据和计算分布到多个设备上，传统的集中式机器学习问题可以转化为分布式联邦学习问题。

由于神经网络的代价函数通常是非凸的，因此直接求解并找到全局最小值颇具挑战性。因此，梯度下降法是一种迭代优化算法，在机器学习中常用于寻找局部最小点。随机梯度下降（SGD）是梯度下降法的一种变体，在.....中可能会有所帮助。

通过随机选择数据样本来逃离局部最小值。因此，梯度在学习过程中发挥核心作用。梯度定义为：

$$g = \nabla_{\boldsymbol{w}} C(\boldsymbol{x_i}, \boldsymbol{y_i}; \boldsymbol{w}). \tag{3}$$

每轮中每个 LC 的本地梯度可表示为

$$g_t^m = \nabla F_m(w_t). \tag{4}$$

聚合后的全局梯度为

$$g_t = \sum_{m=1}^{M} \frac{|D_m|}{|D|} g_t^m. \tag{5}$$

参数服务器存储上一轮 w_t 的模型权重，然后按如下方式更新全局模型。

$$w_{t+1} = w_t - \eta g_t. \tag{6}$$

这里， η 是学习率，通常取值范围为 (0,1)。

B. 无线信道模型

联邦学习是一种上层算法，不了解底层梯度传输的细节。当学习客户端是智能传感器或无人机时，传输通常通过无线信道进行。对于从学习客户端到参数服务器的上行信道，我们考虑衰落信道，这可能导致随机比特错误。对于下行信道，我们假设参数服务器能够将全局梯度传输给学习客户端，且误差可以忽略不计；这可以通过参数服务器较高的发射功率（因此具有较高的信噪比）来实现 [2]。

在上行链路中，可以采用时分方案，让每个用户分配到一个特定时隙，同时共享同一信道。参数服务器接收到的信号可表示如下。

$$r_t^m = \sqrt{p_t^m (d^m)^{-\alpha}} h_t^m g_t^m + n_t^m, \tag{7}$$

其中 r_t^m表示从客户端m传输至参数服务器的接收信号。传输功率表示为 p_t^m，小尺度衰落表示为 h_t^m，假设其服从复正态高斯分布，即 $h_t^m \sim \mathcal{CN}(0,1)$。参数服务器与客户端 m 之间的距离表示为d^m，路径损耗指数表示为 α。加性噪声表示为 $n^t \sim \mathcal{CN}(0,\sigma^2)$。参数服务器已知信道增益，即 $c_t^m = \sqrt{p_t^m}(d^m)^{-\alpha} h_t^m$，且只有噪声作为误差源。

整个传输过程可以描述如下。首先，将梯度从十进制格式转换为二进制格式。然后，使用 QAM调制方案将比特映射为符号。接着，这些符号通过无线衰落信道传输。在接收端，使用最大似然估计对信号进行解码，然后解调为星座图中最近的点，

$$\hat{g}_t^m = \arg_{\bar{g}_t^m \in \mathcal{G}} \min ||r_t^m - \sqrt{p_t^m (d^m)^{-\alpha}} h_t^m \bar{g}_t^m||^2, \tag{8}$$

其中 $\mathcal{G}$ 是星座图的符号点集合。

III. 约束下的有界梯度——证明概要

A. 梯度反向传播

在机器学习中，尤其是在深度神经网络中，反向传播广泛用于计算各层的梯度。在全连接神经网络中，每个神经元的前向传播方程可表示为

$$\begin{aligned} z_j^l &= b_j^l + \sum_k w_{jk}^l a_k^{l-1}, \\ a_j^l &= \sigma(z_j^l). \end{aligned} \tag{9}$$

这里， b 是偏置， w 是权重， z 是中间输出， a 是经过激活函数$\sigma(\cdot)$后的最终输出。 l 表示第 l层， j， k 为索引。全连接网络中反向传播对应的四个基本方程是

$$\delta_j^L = \frac{\partial C}{\partial z_j^L} = \frac{\partial C}{\partial a_j^L}\frac{\partial a_j^L}{\partial z_j^L} = \frac{\partial C}{\partial a_j^L}\sigma'(z_j^L), \tag{10a}$$

$$\delta_j^l = \frac{\partial C}{\partial z_j^l} = \sum_k \frac{\partial C}{\partial z_k^{l+1}}\frac{\partial z_k^{l+1}}{\partial a_j^l}\frac{\partial a_j^l}{\partial z_j^l} = \sum_k \delta_k^{l+1} w_{kj}^{l+1}\sigma'(z_j^l), \tag{10b}$$

$$\frac{\partial C}{\partial b_j^l} = \frac{\partial C}{\partial z_j^l}\frac{\partial z_j^l}{\partial b_j^l} = \delta_j^l, \tag{10c}$$

$$\frac{\partial C}{\partial w_{jk}^l} = \frac{\partial C}{\partial z_j^l}\frac{\partial z_j^l}{\partial w_{jk}^l} = \delta_j^l a_k^{l-1}. \tag{10d}$$

这里， L 是神经网络中的最后一层索引，且 δ_j^l是节点 j处第 l 层中定义的“误差”。

为确保梯度 $\nabla C = \frac{\partial C}{\partial w_{jk}^l}$ 有界，有必要根据公式(10d)限制 δ_j^l 和 a_k^{l-1}。这两个项将分别进行讨论。 a_k^{l-1} 是第$(l-1)$ 层神经元 k 的激活函数输出。它取决于所使用的激活函数。例如，无论输入 z_k^{l-1} 如何，Sigmoid 函数都能确保a_k^{l-1} 处于 (0,1) 范围内，而 ReLU激活函数要求输入有界。关于激活函数的进一步讨论和数学表达式可参见 [12]。

δ_j^l 的计算如方程（10b）所述，其中涉及对下一层误差 δ_k^{l+1} 、从第 l 层节点 j 到下一层 w_{kj}^{l+1} 的权重，以及激活函数 $\sigma'(z_j^l)$ 的导数的乘积求和。该方程包含三项，求和要求每层的神经元数量有限。激活函数 $\sigma'(z_j^l)$ 的导数也取决于所使用的激活函数：对于 Sigmoid 函数，导数的取值范围为 (0,0.25)，对于 ReLU 则为 $\{0,1\}$ 。权重 w_{kj}^{l+1} 取决于模型初始化、学习率 η，以及根据方程（6）计算的上一轮梯度。权重初始化方法通常会生成取值范围为 $(-1,1)$ 或更小的随机权重值，此外还有较新的初始化方法，例如 [13] 和 [14]。不失一般性，我们假设权重值 w_{kj}^{l+1} 有界。误差 δ_k^{l+1} 可以用与方程（10b）相同的方式表示，其中包含第 $(l+2)$ 层的元素，并且这一过程会一直反向传播到最后一层。在分类问题中，通常将 softmax 函数用作最后一层的激活函数，以对输出的类别概率进行归一化。使用交叉熵损失函数时，可以将其与 softmax 函数组合使用。对于交叉熵损失函数，

$$C = -\sum_i y_i log(p_i), \tag{11}$$

其中 y_i 是真实标签， p_i 是第 i个类别的 Softmax 概率

$$p_i = \sigma(z_i) = \frac{e^{z_i}}{\sum_k e^{z_k}}, \tag{12}$$

且导数为

$$\frac{\partial p_i}{\partial z_j} = \begin{cases} p_i(1-p_j), & \text{if } i = j; \\ -p_j \cdot p_i, & \text{if } i \neq j. \end{cases} \tag{13}$$

式（10a）可以写为

$$\begin{aligned} \delta_j^L = \frac{\partial C}{\partial p_i^L}\frac{\partial p_i^L}{\partial z_j^L} &= -\sum_i y_i \frac{\partial log(p_i)}{\partial p_i}\frac{\partial p_i}{\partial z_j}, \\ &= -\sum_i y_i \frac{1}{p_i}\frac{\partial p_i}{\partial z_j}, \\ &= -y_j(1-p_j) - \sum_{i\neq j} y_i \frac{1}{p_i}(-p_j \cdot p_i), \\ &= p_j \cdot \sum_i y_i - y_j. \end{aligned} \tag{14}$$

由于 y 是独热编码标签向量，因此 $\sum_i y_i = 1$，也就是说

$$\delta_j^L = p_j - y_j. \tag{15}$$

由于 p_j 的取值介于0和1之间，且 y_j 为0或1，δ_j^L位于区间（-1，1）内。

总而言之，在一个以交叉熵作为代价函数、以Soft max 函数作为最后一层中的激活函数的全连接神经网络中，最后一层的误差 δ_j^L的取值范围为 $(-1,1)$。此外，如果假设权重的取值范围为$(-1,1)$，并且在其他层中使用 Sigmoid 函数作为激活函数，则梯度$\frac{\partial C}{\partial w_{jk}^l}$ 受 l 层之后的神经元数量之和（记为 B^l）的约束。

B. Gradient in Convolutional Neural Network

现代图像识别任务通常采用卷积神经网络（CNN）作为一种先进技术。CNN 是前馈网络的一种特殊变体，由三种类型的层组成：卷积层、池化层和全连接层。CNN 的前馈过程可表示为：

$$z_{j,k}^1 = b_{j,k}^1 + \sum_p \sum_q w_{p,q}^1 x_{j+p,k+q}^0, \tag{16a}$$

$$a_{j,k}^1 = \sigma(z_{j,k}^1), \tag{16b}$$

$$a_{j,k}^2 = \max(a_{2j,2k}^1, a_{2j+1,2k}^1, a_{2j,2k+1}^1, a_{2j+1,2k+1}^1), \tag{16c}$$

$$z_i^3 = b_i^3 + \sum_{j,k} w_{i;j,k}^3 a_{j,k}^2, \tag{16d}$$

$$a_i^3 = \sigma(z_i^3). \tag{16e}$$

为简化起见，我们假设这个卷积神经网络仅包含三层。公式 (16a) 和 (16b) 表示卷积层，公式 (16c) 表示使用 2×2 核的最大池化层，而公式 (16d) 和 (16e) 表示全连接层。这里， p 和 q表示卷积核的索引。

现在，卷积神经网络的反向传播变为

$$\delta_i^3 = \frac{\partial C}{\partial z_i^3} = \frac{\partial C}{\partial a_i^3}\frac{\partial a_i^3}{\partial z_i^3} = \frac{\partial C}{\partial a_i^3}\sigma'(z_i^3), \tag{17a}$$

$$\begin{aligned}\delta_{j,k}^1 = \frac{\partial C}{\partial z_{j,k}^1} &= \sum_i \frac{\partial C}{\partial z_i^3}\frac{\partial z_i^3}{\partial a_{s,t}^2}\frac{\partial a_{s,t}^2}{\partial z_{j,k}^1}, \\ &= \sum_i \delta_i^3 w_{i;s,t}^3 \frac{\partial a_{s,t}^2}{\partial a_{j,k}^1}\frac{\partial a_{j,k}^1}{\partial z_{j,k}^1}, \\ &= \sum_i \delta_i^3 w_{i;s,t}^3 \frac{\partial a_{s,t}^2}{\partial a_{j,k}^1}\sigma'(z_{j,k}^1), \\ &= \begin{cases} \sum_i \delta_i^3 w_{i;s,t}^3 \sigma'(z_{j,k}^1), & \text{if case 1;} \\ 0, & \text{otherwise;} \end{cases}\end{aligned} \tag{17b}$$

$$\frac{\partial C}{\partial w_{i;j,k}^3} = \frac{\partial C}{\partial z_i^3}\frac{\partial z_i^3}{\partial w_{i;j,k}^3} = \delta_i^3 a_{j,k}^2, \tag{17c}$$

$$\frac{\partial C}{\partial w_{p,q}^1} = \frac{\partial C}{\partial z_{j,k}^1}\frac{\partial z_{j,k}^1}{\partial w_{p,q}^1} = \delta_{j,k}^1 x_{j+p,\ k+q}^0. \tag{17d}$$

这里，情况1为 $a_{j,k}^2 = \max(a_{2s,2t}^1, a_{2s+1,2t}^1, a_{2s,2t+1}^1, a_{2s+1,2t+1}^1)$在公式(17b) 中，以及 $s = \frac{j}{2}, n = \frac{k}{2}$。

同样地，当交叉熵作为损失函数且最后一层中的激活函数为 softmax函数时，δ_i^3 的取值范围为（−1,1）。为了界定全连接层中的梯度$\frac{\partial C}{\partial w_{i;j}^3}$，有必要确保$a_j^2$、$_k$ 或 max($a_{2j,2k}^1$,$a_{2j,2k+1}^1$,$a_{2j+1,2k}^1$,$a_{2j+1,2k+1}^1$) 也受到界定。如果第一层使用Sigmoid函数作为激活函数，那么 a_j^2、$_k$ 的取值被限制在（0, 1）范围内，从而使$\frac{\partial C}{\partial w_{i;j}^3}$、$_k$ 的取值被限制在（−1, 1）范围内。通过考虑其中涉及的两个项，可以界定公式（17d）中的梯度$\frac{\partial C}{\partial w_p^1}$、$_q$。首先，$x_{j+p,\ k+q}^0$ 是输入，并且受到界定。其次，δ_j^1、$_k$ 可以表示为 0或$\sum_i \delta_i^3 w_{i;s}^3$、$_t\sigma'(z_j^1$、$_k)$。我们知道， δ_i^3的取值范围为（−1,1），并且如果激活函数为Sigmoid， $\sigma'(z_j^1$、$_k)$的取值范围为（0,0.25）。对于 $w_{i;s}^3$、$_t$，根据公式（6），其取值取决于模型初始化、学习率 η以及上一轮的梯度，正如我们上面所讨论的。假设 $w_{i;s}^3$、$_t$ 在（−1, 1）范围内受到界定，则$\frac{\partial C}{\partial w_p^1}$、^{q}可以由最后一层中的神经元数量界定，该数量也记为 B^l。

IV. 所提方法

在第3节中，我们给出了数学证明，表明在某些条件下，梯度受 B^l 限制。实证研究表明，在 [7], [8], [9] 中，梯度不仅有界，而且还被限制在（−1,1）这一范围内，甚至更小的范围内。这使我们能够对接收到的梯度在统计意义上具有一个期望值，直至参数服务器。相应地，我们首先设计一种 QAM 编码方案对于有界梯度，

A. QAM 编码

在机器学习中，梯度通常以 32 位浮点数表示。这些数遵循 IEEE-754 标准定义的格式：第 1 位为符号位，接下来的 8 位为指数，最后 23 位为尾数。不同位置的位重要性各不相同。符号位控制梯度值的正负，指数部分决定整数和小数的数值。尾数部分只影响小数值，因此指数位比尾数位更重要。此外，指数中位于左侧的位比右侧的位更重要。

在传输过程中，每个位都容易受到噪声影响，从而可能导致损坏。为避免块损坏，我们在发射机处采用交织，并在接收机处采用解交织，从而降低多个误差比特同时发生的可能性。在位表示中，当32 位表示中的第二个位（即指数部分的第一个位）为 1，且其他 31 个位均为0时，十进制值为2。相反，当 32位表示中的第二个位为0，且其他31 个位均为 1时，其幅值小于2。当假设梯度值的幅值阈值为1时，指数部分的第一个位始终为 0。这促使我们在接收机侧，无论梯度的第二个位位置解码出的值是什么，都将其设置为 0，如图 1 所示。



图 1：接收梯度的位表示

此外，我们还观察到，不同的调制方案对位于不同位置的比特具有不同的影响 [11]。这不仅在媒体消息传输中很重要，在机器学习模型参数传输中也同样重要。在无线传输中，传输系统不了解数据比特的相对重要性，并将所有比特一视同仁。当使用QPSK 作为调制方案时，每个符号由 2 个比特组成，比特组合为 00，01，11，10。QPSK中第一个和第二个比特的误码概率相同。相比之下，16-QAM 每个符号包含 4 个比特，其采用格雷码的星座图如下所示。

图 2 中带下划线的比特对应于每个符号中的第一位，即最高有效位（MSB），而第四位或最后一位是最低有效位（LSB）。当每个符号的传输概率相同时，MSB的误码概率高于 LSB。例如，如果符号 s_0 解码出错，则最有可能被解码为 s_1、 s_4 或 s_5。MSB比特保持不变，而LSB改变两次。这总结于表 I 中。其他象限中的符号与第一象限对称，因此结果

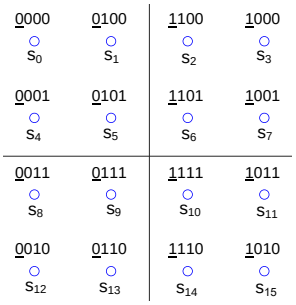


图 2：采用格雷编码的 16-QAM 星座图

是相同的。采用格雷编码的高阶调制方案，为位表示中梯度值的最高有效位提供内置保护。

表 I：16-QAM 最高有效位/最低有效位错误计数

符号	潜在错误符号	最高有效位 误差 计数	最低有效位误差 计数
s_0	s_1, s_4, s_5	0	2
s_1	s_0, s_2, s_4, s_5, s_6	2	3
s_4	s_0, s_1, s_5, s_8, s_9	0	2
s_5	$s_0, s_1, s_2, s_4, s_6, s_8, s_9, s_{10}$	3	3

B. 近似无线传输

为进一步提升无线网络上的梯度交换效率，我们提出了一种近似无线传输方案。本质上，由于梯度具有一定的抗误差能力（现有梯度压缩方法已证明这一点），因此传输的消息（梯度）无需完全准确。因此，当信道信噪比较为理想时，我们会省去前向纠错和重传。虽然具体的信噪比值尚待确定，但我们的实证结果表明，信噪比约为 10–20 dB 时，误码率对联邦学习而言可以接受。请注意，我们的方法不同于用户数据报协议（UDP），后者同样不要求重传。区别在于，UDP工作在较高层，循环冗余校验仅用于检查UDP有效载荷。当错误发生在物理层或MAC层时，仍会进行重传。我们的方法则在较低层（包括物理层和MAC层）同时省去前向纠错和重传。这样做有三方面好处：1）降低通信开销，从而能够传输更多数据位；2）减少前向纠错带来的计算开销，这对边缘设备尤其有利；3）无需重传，因此能够改善时延性能。

V. 仿真结果

本节首先介绍仿真的参数设置。随后，我们给出前文所述无线信道下，误码概率随信噪比（SNR）变化的经验结果。在测试的调制方案中，相同信噪比下，QPSK 的误码率（BER）优于 16-QAM 和 256-QAM。接下来，我们比较三种情形下的联邦学习性能：采用纠错和重传的ECRT传输、朴素错误传输，以及采用所提方案的错误传输。朴素错误传输指无线网络中存在误差且不进行额外操作的传输。与朴素错误传输相比，所提方案能取得较高的测试准确率。此外，与 ECRT传输相比，所提方案用于错误传输时可节省更多时间。最后，我们讨论采用格雷编码的不同调制方案，以展示位表示中对最高有效位的内置保护。

我们在仿真中考虑一种典型的联邦学习设置，其中$M = 100$个学习客户端连接到参数服务器，并且所有学习客户端都参与每个通信轮次的学习过程。学习客户端使用MNIST数据集执行图像分类任务，该数据集由数字0-9的手写数字组成。训练集包含60,000张图像，测试集包含10,000张图像；训练集中每个数字约有6,000张图像，测试集中每个数字约有1,000张图像。为了模拟从环境中收集数据的真实场景，我们以非独立同分布的方式分配数据，每个学习客户端拥有2个数字，每个数字约有300张训练图像。我们使用卷积神经网络（CNN）作为机器学习模型，其中包含2个卷积层，每层的卷积核大小为5；包含2个大小为2的最大池化层，以及2个全连接层。除最后一层使用对数Softmax函数外，所有层均使用ReLU作为激活函数。学习率设为$\eta = 0.01$。

我们将无线信道的路径损耗指数设为$\alpha = 3$，并考虑参数服务器与学习客户端之间的距离为10m。学习客户端处的传输功率归一化为1。我们采用QPSK作为调制方案，除非另有说明，接收机信噪比设为 $\gamma = 10$ dB。

在特定的衰落信道下，在相同信噪比水平下，QPSK 相较于 16-QAM 和 256-QAM 可实现更低的误码率。对于 QPSK，当信噪比为=10 dB 时，误码率约为4×10^{-2}；当信噪比为 20 dB 时，误码率为 5×10^{-3}。

在采用纠错和重传的ECRT方案中，参数服务器（PS）能够正确接收所有比特，但当误差超过前向纠错（FEC）的能力时，需要付出前向纠错（FEC）以及可能进行重传的代价。相比之下，朴素错误传输方案在没有梯度先验知识的情况下传输带有误差的比特，其测试准确率始终稳定在约 10%，如图 3 所示，这与随机猜测类似。这是因为传输误差导致模型无法学到任何信息。相比之下，我们所提方法考虑了梯度值的先验知识，预计梯度值将处于（-1, 1）范围内。这使得所提方案取得了远优于朴素错误传输的结果。

为了量化与ECRT传输相比我们提出的方法所节省的传输时间，我们采用了结合LDPC纠错编码的实用IEEE802.11协议。LDPC是一种很有前景的ECC，可以逼近香农极限。对于不同的编码率，纠错能力与传输开销之间存在权衡。较低的编码率会带来较高的传输开销，但同时具有较强的纠错能力。在此，我们使用 $1/2$ 的编码率来增强纠错能力。根据[15],最小汉明距离为15，对于编码率

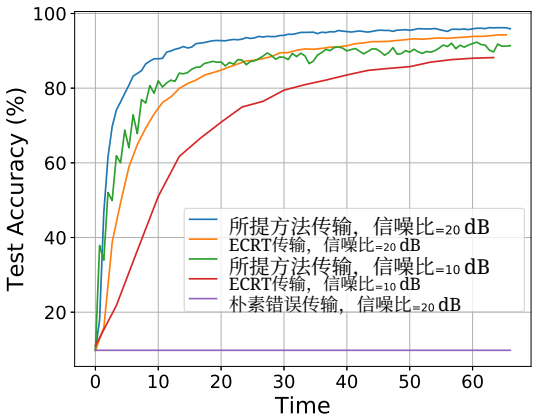
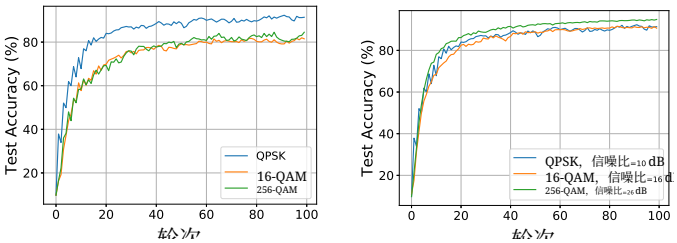


图3：测试准确率与通信时间的关系

当码长为648时的 $1/2$ ，并且我们使用校验矩阵进行搜索。这将得到7比特的纠错能力。在图3中，在信噪比为=20 dB时，采用带重传的LDPC编码进行传输达到80%准确率所需的时间比所提方案多 $2\times$ ，而对于带重传的LDPC编码方案，在信噪比为=10 dB时达到该性能所需的时间超过 $3\times$ 。



(a) 具有相同的测试准确率
信噪比=10 dB

(b) 相同条件下的测试准确率
误码率 $\approx 4\times10^{-2}$

图4：相同信噪比/误码率下的测试准确率

为展示采用格雷编码的高阶调制内置最高有效位保护的有效性，我们首先在图 4(a) 中展示相同信噪比下不同调制方式的测试准确率。当信噪比为 10 dB 时，QPSK、16-QAM 和 256-QAM 的误码率分别约为 4×10^{-2}、10^{-1} 和 3×10^{-1}。由于 QPSK 产生的误差较少，其学习性能优于 16-QAM 和 256-QAM。

在图 4(b) 中，我们展示了一种不同调制方案的误码率相同的场景。为实现这一点，我们将 16-QAM的信噪比提高到 16dB，并将256-QAM的信噪比提高到26 dB。因此，三种调制方案的误码率均为 4×10^{-2}。在此场景下，256-QAM的学习性能显著优于 QPSK，且 256-QAM 的传输误差小于 QPSK。

六、结论

本文提出了一种适用于无线网络的联邦学习参数传输方案。与依赖前向纠错和重传的现有传输方法不同，我们提出了一种基于误差的梯度传输方法，该方法利用梯度值的先验知识。通过数学证明，在特定约束条件下，梯度值处于一个较小的范围内，因此预期接收到的梯度值也会处于该范围内。与朴素错误传输相比，这种方法在存在误差时仍能实现显著更好的学习性能；同时，与 ECRT 传输相比，实现相同学习性能所需的时间至少减少一半。此外，我们还探索了高阶调制，并展示了其带来的学习效果提升。未来，我们计划量化通信错误对联邦学习性能的影响，并研究客户端数量对其的影响。

参考文献

[1] J. Konen、H. B. McMahan、F. X. Yu、P. Richtarik、A. T. Suresh 和 D. Bacon。“联邦学习：提高通信效率的策略”，[在线]: https://arxiv.org/abs/1610.05492，2016年。[2] M. Shirvanimoghaddam、A. Salari、Y. Gao 和 A. Guha，“错误通信链路下的联邦学习”，发表于 *IEEE Commun. Lett.*，第 26 卷，第 6 期，第 1293–1297 页，2022年4月。[3] H. B. McMahan、E. Moore、D. Ramage、S. Hampson 和 H. A. Arcas，“基于去中心化数据的深度网络通信高效学习”，[在线]: https://arxiv.org/abs/1602.05629，2016年。[4] H. Sun、X. Ma、R. Q. Hu，“上行NOMA中的梯度压缩自适应联邦学习”，发表于 *IEEE*车辆技术汇刊，第 69 卷，第 12 期，第 16325–16329 页，2020年。[5] F. Seide、H. Fu、J. Droppo、G. Li 和 D. Yu，“1位随机梯度下降及其在语音深度神经网络数据并行分布式训练中的应用”，发表于 国际语音通信协会第十五届年度会议，2014年。[6] A. F. Aji 和 K. Heafield，“分布式梯度下降的稀疏通信”，[在线]: https://arxiv.org/abs/1704.05021，2017年。[7] W. Wen、C. Xu、F. Yan、C. Wu、Y. Wang、Y. Chen 和 H. Li，“Terngrad：用于减少分布式深度学习通信的三元梯度”，发表于 神经信息处理系统进展，第 30 卷，2017年。[8] A. M. Abdelmoniem、A. Elzanaty、M. S. Alouini 和 M. Canini，“一种用于分布式训练系统的高效基于统计的梯度压缩技术”，发表于 机器学习与系统会议论文集，第 3 卷，第 297–322 页，2021年。[9] B. Guo、Y. Liu 和 C. Zhang，“一种基于分区的分布式训练梯度压缩算法”，发表于 传感器，第 21 卷，第 6 期，第 1943 页。[10]B. Ransford 和 L. Ceze，“SAP：一种用于选择性近似无线通信的架构”，[在线]: https://arxiv.org/abs/1510.03955，2015年。[11] S. Sen、S. Gilani、S. Srinath、S. Schmitt 和 S. Banerjee，“无线媒体应用的‘近似’通信系统的设计与实现”，发表于 *2010*年*ACM SIGCOMM*会议论文集，第 15–26 页，2010年。[12] C. Nwankpa、W. Ijomah、A. Gachagan 和 S. Marshall，“激活函数：深度学习实践与研究趋势比较”，[在线]: https://arxiv.org/abs/1811.03378，2018年。[13] X. Glorot 和 Y. Bengio，“理解训练深度前馈神经网络的难点”，发表于 第十三届人工智能与统计国际会议论文集，第 249–256 页，2010年。[14] K. He、X. Zhang、S. Ren 和 J. Sun，“深入研究整流器：超越人类水平的ImageNet分类性能”，发表于 *IEEE*国际计算机视觉会议论文集，第 1026–1034 页，2015年。[15] B. K. Butler，“IEEE 802通信标准中准循环低密度奇偶校验码的最小距离”，[ ] 1602 02831, 在线: 2016 https://arxiv.org/abs/ . .