物联网环境中基于深度学习的差分隐私预算优化方法

罗丹，徐茹枝，关志涛
（华北电力大学控制与计算机工程学院，北京 102206）

摘 要：为有效处理物联网大规模应用所带来的海量数据，深度学习在物联网环境中得到广泛应用。然而，深度模型在训练过程中，存在推理攻击、模型逆向攻击等安全威胁，这会导致输入模型中的原始数据泄露。应用差分隐私对深度模型训练过程的参数进行保护，是解决该问题的有效方式。基于此提出一种物联网环境中基于深度学习的差分隐私预算优化方法，根据参数迭代变化规律，自适应地分配不同预算；为避免噪声过大的问题，引入正则化项对扰动项进行约束，既防止神经网络过拟合，又有助于学习模型的显著特征。实验表明，所提方法可有效增强模型的泛化能力；随着模型迭代次数增加，加噪后训练得到的模型，与使用原始数据训练得到的模型，二者精度差值低于0.5%。因此，所提方法既可实现用户隐私保护，同时有效保证模型可用性，实现了隐私性和可用性的平衡。

关键词：物联网；差分隐私；正则化；深度学习；隐私预算
中图分类号：TP391
文献标志码：A
doi: 10.11959/j.issn.2096−3750.2022.00264

Differential privacy budget optimization based on deep learning in IoT

LUO Dan, XU Ruzhi, GUAN Zhitao
School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China

Abstract: In order to effectively process the massive data brought by the large-scale application of the internet of things (IoT), deep learning is widely used in IoT environment. However, in the training process of deep learning, there are security threats such as reasoning attacks and model reverse attacks, which can lead to the leakage of the original data input to the model. Applying differential privacy to protect the training process parameters of the deep model is an effective way to solve this problem. A differential privacy budget optimization method was proposed based on deep learning in IoT, which adaptively allocates different budgets according to the iterative change of parameters. In order to avoid the excessive noise, a regularization term was introduced to constrain the disturbance term. Preventing the neural network from over fitting also helps to learn the salient features of the model. Experiments show that this method can effectively enhance the generalization ability of the model. As the number of iterations increases, the accuracy of the model trained after adding noise is almost the same as that obtained by training using the original data, which not only achieves privacy protection, but also guarantees the availability, which means balance the privacy and availability.

Key words: IoT, differential privacy, regularization, deep learning, privacy budget

0 引言

近年来，物联网技术快速发展，在可穿戴设备、环境监测、物流管理、虚拟现实、智能家居、智能电网、智慧城市和公共服务等诸多场景得到广泛应用，将数字世界和物理世界紧密相连，加速万物互联的时代到来。随着物联网的大规模应用，个人用电信息、健康信息、行动轨迹等涉及个人隐私的海

收稿日期：2021−09−22；**修回日期**：2022−03−07
通信作者：关志涛，guanzhitao@126.com
基金项目：国家自然科学基金资助项目（No.61972148）
Foundation Item: The National Natural Science Foundation of China (No. 61972148)

量数据将被物联网终端记录采集。为有效处理物联网应用所带来的海量数据，深度学习被广泛应用在物联网场景下的一些模型训练中，这也带来一些隐私泄露的隐患。在模型训练过程中，模型参数信息可能会遭到推理攻击、模型逆向攻击等安全威胁，进而输入模型中的原始数据可以被反推出来，造成隐私信息泄露。针对上述问题，本文考虑保护模型训练过程的参数信息。常用的深度学习隐私保护方案主要基于差分隐私或同态加密方法。同态加密不会对模型的精度造成影响，但加密会产生密文膨胀的问题，在传输过程中带来较大的通信开销，不适用于物联网场景。本文采用差分隐私方法，通过损失微小的精度实现对模型的隐私保护。如何实现模型精度和隐私保护这二者之间的平衡，是需要考虑的问题。差分隐私方法所添加的扰动大小和隐私预算直接相关，本文通过合理分配隐私预算来调整噪声大小，实现用户隐私保护，同时保证模型的可用性。

1 相关工作

针对隐私泄露的问题[1]，已经有很多相关的保护方法，文献[2]提出了基于动态污点跟踪的隐私保护方法，文献[3]提出了加权贝叶斯网络的隐私数据保护方法。

深度学习中常用的隐私保护方法主要有同态加密和差分隐私，对于同态加密，Li 等[4]通过掩码技术与 Paillier 同态加密技术保护训练集及训练模型的隐私，并建立非交互式的联合学习框架避免数据拥有者和训练者之间的多轮交互。Zhang 等[5]使用 Paillier 加密实现梯度的安全聚合，并利用同态散列改进双线性聚合签名验证聚合结果的正确性。Suh 等[6]考虑了一种基于同态加密的保密云控制综合体系结构，在强化学习体系结构下说明了 Cheon-Kim-Kim-Song（CKKS）加密方案下加密噪声对模型收敛性的影响。Wang 等[7]将深度学习与同态加密算法相结合，并设计了基于安全多方的深度学习网络模型。虽然同态加密不会影响模型的精度，但在物联网这种资源受限以及需要反复交互的环境，同态加密会带来很大的通信开销，尤其对于训练数据量大以及神经网络比较复杂的情况，会造成更高的复杂度。

而差分隐私对计算的需求较低，其通过数学定义对隐私性和可用性进行量化分析且不需要考虑攻击者拥有的背景知识，即可以假设攻击者除特定目标外了解全部内容。对于差分隐私的应用，也有很多相关工作，Ye 等[8]提出一种基于 Order- Pre-serving 加密的云外包差分隐私数据查询方法，云服务器在适当的隐私预算范围内进行一些查询。Bu 等[9]提出一个通用框架理解差分隐私深度学习网络结构的损失函数，该框架建立了每个样本裁剪和 NTK 矩阵之间的关系。Bu 等[10]使用 Johnson-Lindenstrauss（JL）投影快速逼近样本梯度，而不需要精确计算。Chen 等[11]提出一种基于扰动的技术，可以在梯度分布高度不对称的情况下修正裁剪偏差。Koskela 等[12]提出 numerical accountant 评估一维输出算法的隐私损失，通过离散积分和快速傅里叶变换，在给出精确隐私预算和松弛项值的情况下计算离散卷积积分公式的数值近似。Ghazi 等[13]提出一种新的算法来训练具有标签差分隐私的深度神经网络。Yuan 等[14]提出了结合安全多方和差分隐私的新协议，在安全多方计算过程中释放差分隐私信息，以减少训练时间，减少复杂性。以上文献主要在训练过程分配固定隐私预算。

然而，由噪声随机梯度下降模型 NoisySGD[15]可知，引入随机噪声的量和隐私预算随着训练时期数量的增加而保持增加，但隐私预算通常是有限的，因此需要合理分配。此外，以往的方法不管不同参数在现有差分隐私深度学习技术中的重要性如何，噪声量都保持不变。然而，在深度学习模型训练早期阶段，随机初始化的网络权重离局部最优解较远，梯度较大，事实上可以分配更少的隐私预算，即向梯度添加更多的噪声，然而随着训练次数增加，越逼近最优解，对梯度的处理需要越精细，基于该思想，本文提出一种优化的隐私预算分配方法。

2 隐私保护技术及优化模型

2.1 差分隐私

差分隐私通过添加噪声对数据进行扰动。该技术主要基于相邻数据集，即两个数据集中仅有一条记录不同的情况。在进行扰动后，攻击者不能区分该条记录是否存在于某个数据集中。

定义 1 差分隐私[16]

对于一个随机算法 K，S 为经算法 K 处理，可以输出的所有值的集合的任意子集。若对于任意的一对相邻数据集 D_1 和 D_2，算法 K 满足式(1)则称算法 K 满足 ε-差分隐私。

$$\Pr\left[K(D_1)\in S\right]\leqslant \exp(\varepsilon)\times \Pr\left[K(D_2)\in S\right] \quad (1)$$

其中，ε 为隐私预算，可以控制隐私保护水平。ε 越

小，两个数据集的查询结果的概率分布越相似，越不容易区分单个样本，隐私保护程度相应也越高，即较小的 ε 可以提供更强的隐私保证。$\exp(\varepsilon)$ 是指 ε 的指数函数，Pr 表示将算法 K 作用于数据集 D_1 或 D_2 得到输出集合 S 的概率。

定义 2　全局敏感度[17]

设有函数 f：$D \to R^d$，输入为数据集 D，输出为一个 d 维向量，对于任意相邻数据集 D_1 和 D_2，函数 f 的敏感度满足

$$\Delta f = \max_{D_1, D_2} \| f(D_1) - f(D_2) \| \tag{2}$$

其中，$\| f(D_1) - f(D_2) \|$ 表示 $f(D_1)$ 和 $f(D_2)$ 的 1-阶范数距离。全局敏感度只和函数本身有关，敏感度越小，需要添加的噪声也越少。

一般通过向函数 f 作用后的输出添加适量噪声来实现差分隐私机制。本文主要介绍 Laplace 噪声。

定义 3　Laplace 机制[18]

将均值为 0、尺度参数为 b 的 Laplace 分布表示为 Lap(b)，其概率密度函数为式(3)，则随机算法 $A(D) = f(D) + \mathrm{Lap}\left(\frac{\Delta f}{\varepsilon}\right)$ 满足 ε-差分隐私。

$$p(x) = \frac{1}{2b} \exp\left(-\frac{|x|}{b}\right) \tag{3}$$

对于隐私预算有两个重要性质，序列组合性质和并行组合性质，这里主要介绍用到的序列组合性质。

性质 1　序列组合性质

设算法 $K_1, K_2, \cdots, K_n$ 分别满足 ε_i-差分隐私（$1 \leqslant i \leqslant n$），对于数据集 D，算法 $\{K_1, K_2, \cdots, K_n\}$ 满足 $\sum_{i=1}^{n} \varepsilon_i$-差分隐私保护。根据该性质可看出，要达到一定隐私保护水平，每次应用该算法对所消耗的预算求和即可。

2.2　正则化

正则化主要解决如下两个问题。

1) 正则化主要在最小经验误差函数上加约束，该约束可以解释为具有引导作用的先验知识，优化误差函数时，在满足约束的条件下，倾向于选择梯度减少的方向，使最终的解更符合先验知识。

2) 正则化主要解决逆问题的不适定性，产生的解依赖于数据且是唯一的，这样噪声对不适定的影响就会较弱，解就不会过拟合，而且如果先验知识，即正则化项的值合适，解会更符合真实值，即更不会发生过拟合情况，同时也表明训练集中彼此不相关的样本数会很少。

神经网络的拟合过程中通常都倾向于让权值尽可能小，最后构造一个所有参数都比较小的模型。因为一般认为参数值小的模型比较简单，能适应不同的数据集，同时在一定程度上可以避免过拟合现象。显而易见，如果参数足够小，数据偏移得多一点对结果造成的影响也不会太大，其抗扰动能力较强。限制参数很小，从另一个角度实际上就是限制了多项式某些分量的影响很小，这样就相当于减少了参数个数，如式(4)。

$$J(\omega) = \frac{1}{2m}\left[\sum_{i=1}^{m}\left(y^i - h_w(x^i)\right)^2 + \lambda \sum_{j=1}^{n} \omega_j^2\right] \tag{4}$$

其中，m 为样本个数，n 为特征个数，λ 为任意超参数，$\sum_{i=1}^{m}\left(y^i - h_w(x^i)\right)^2$ 为原代价函数，$\sum_{j=1}^{n} \omega_j^2$ 为 L_2 范数，即正则化项。

2.3　神经网络

神经网络的训练过程是一个迭代的过程，最初随机获得权值，将样本输入神经元后进行加权求和，然后通过激活函数输出给后面连接的神经元，得到网络的输出。将输出值与目标值相比对，计算出损失函数，然后再通过损失函数反向调整神经网络各个层及各个神经元的权值。不断重复该迭代过程，直至收敛。一般情况下，神经网络的结构较复杂，所以一般用随机梯度下降[19]或其变体[20-21]对深度学习模型进行优化。

随机梯度下降根据初始化的权值，向着让损失函数变化最大的方向进行更新，如式(5)。

$$\omega_j = \omega_j - \alpha \frac{\partial}{\partial \omega_j} J(\omega) \tag{5}$$

其中，α 为步长，控制每次迭代时变化的幅度，损失函数 $J(\omega)$ 对权重向量 ω_j 的偏导数表示梯度变化最大的方向，由于求的是极小值，因此此处梯度方向取偏导数的反方向。

3　CNN 中的隐私预算分配方案

深度学习模型迭代过程中参数的更新是非线性、非均匀的，它会随损失函数的收敛过程缓慢减小，下面的方案将介绍如何在每轮迭代过程中分配不同的隐私预算，并使整体依然满足差分隐私的性质。这样可以保证在一定的隐私预算下，引入的噪声对模型的干扰最小，加快模型的收敛。同时，还

引入了正则项，该值不但能限制噪声的大小，还可以解决神经网络的过拟合现象。梯度自适应加噪步骤如图 1 所示。左边部分表示将数据输入神经网络模型进行训练，右边的部分表示在反向传播过程中对梯度信息进行差分隐私保护，使攻击者无法通过梯度反推出用户信息，不同迭代过程所添加的扰动不同，式(6)和式(7)分别表示随机加噪以及用正则化约束进行梯度更新的过程。

$$\omega_{t+1}=\omega_t-\eta\left(\nabla f(\omega_t)+\gamma\omega_t\right) \tag{6}$$

$$\omega_{t+1}=\omega_t-\eta\left(\nabla f(\omega_t)+\mathrm{Lap}\left(\frac{\Delta f}{\varepsilon_t}\right)\right) \tag{7}$$

3.1　隐私预算分配

对于传统的隐私保护方法，为每一轮迭代分配固定的隐私预算，即注入相同量的噪声。对比这些方法可以发现，在初始模型优化时，梯度值较大，所以初始阶段即使梯度值不准确，算法也可以很好地进行梯度更新。然而随着模型参数趋近于最优值，梯度开始减小，此时需要更准确地测量梯度，然而假如平均分配预算，该情况产生的噪声在模型即将收敛时会产生较大的影响，从而不能保证优化更好地进行。因此，在不同的迭代次数中本文考虑不同的隐私预算。

基于树状结构[22]的思想，在每轮迭代中，以固定值 d（$d\geqslant 0$）增加隐私预算，因此，第 t 轮迭代的隐私预算值为

$$\varepsilon_t=\varepsilon_1+(t-1)d,\quad 1\leqslant t\leqslant T \tag{8}$$

从第 1 轮到第 T 轮的总预算可以表示为

$$\varepsilon=\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_t \tag{9}$$

同理也可写成

$$\varepsilon=\varepsilon_t+\varepsilon_{t-1}+\cdots+\varepsilon_1 \tag{10}$$

将上边的式(9)和式(10)相加即得

$$2\varepsilon=(\varepsilon_1+\varepsilon_t)+(\varepsilon_2+\varepsilon_{t-1})+\cdots+(\varepsilon_t+\varepsilon_1) \tag{11}$$

所以 T 轮迭代后总的隐私预算进一步可写为

$$\varepsilon=T\varepsilon_1+\frac{T(T-1)d}{2} \tag{12}$$

根据等差数列的性质，需要单独考虑预算初值，即第 1 项的值，基于式(12)可得首项

$$\varepsilon_1=\frac{\varepsilon}{T}-\frac{T-1}{2}d \tag{13}$$

之后将式(13)代入式(8)的定义式中得到每轮迭代的隐私预算为

$$\varepsilon_t=\frac{\varepsilon}{T}+\left(\frac{T-1}{2}-t\right)d \tag{14}$$

且由于每轮的预算和增加值均需要大于或等于 0，因此，可得该值处在以下区间

$$0\leqslant d\leqslant\frac{2}{T(T-1)} \tag{15}$$

其中，T 为总的迭代次数。所以给定总的隐私预算，便可得到每一轮的预算值。

3.2　噪声值约束

以固定值递增的方式分配隐私预算，可能会存在预算过小导致噪声较大的情况，为了尽可能减少噪声带来的负面影响，将噪声的值限定在一定范围内。以前的工作也会考虑通过加噪防止神经网络的过拟合，基于该思想，本文引入正则化值对噪声值进行限制。

L2 正则化是正则化的一种，称为参数范数惩罚，该技术将一个额外项加入损失函数中，正则化项如下

$$\frac{\lambda}{2n}\sum_w\omega^2 \tag{16}$$

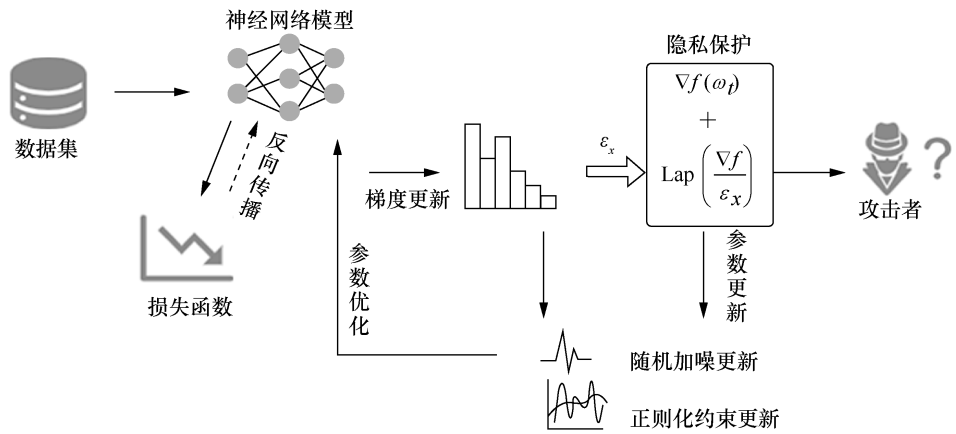


图 1　梯度自适应加噪步骤

其中，λ 是正则项系数，n 代表样本大小，ω 代表权重参数。

将 L2 正则化应用于损失函数，即

$$C = C_0 + \frac{\lambda}{2n}\sum_w \omega^2 \tag{17}$$

其中，C 是加入正则项后的正则化损失函数，C_0 是原损失函数。

本文主要对梯度做隐私保护，因此该项通过方程得到相应的梯度，对损失函数求偏导数得到

$$\frac{\partial C}{\partial \omega} = \frac{\partial C_0}{\partial \omega} + \frac{\lambda}{n}\omega \tag{18}$$

进行梯度更新时

$$\omega = \omega - \eta\left(\frac{\partial C_0}{\partial \omega} + \frac{\lambda}{n}\omega\right) \tag{19}$$

而对于梯度加噪的情况，梯度更新为

$$\omega = \omega - \eta\left(\frac{\partial C_0}{\partial \omega} + \mathrm{Lap}\left(\frac{\Delta f}{\varepsilon}\right)\right) \tag{20}$$

因此，本文将求导后的正则项与噪声项作对比，以此来限制噪声值的大小。假如噪声项的值小于正则项的值，证明没有引入过度的噪声，正常执行随机梯度下降过程；相反，则说明噪声引入相对较大，将噪声项替换为正则项，进行随机梯度下降过程，对梯度进行更精细的处理。同时可以看到，正则项值会使权重变小，即改变一些随机输入，网络的行为不会有太大变化，也就意味着正则化的网络很难学习数据中的局部噪声，而只会学习数据集经常看到的特征，即学习到了模型较重要的特征。如果是用正则项进行网络参数的迭代，则消耗的隐私预算会发生变化，所以需要重新更新剩余隐私预算值。

3.3　预算重分配

为了限制噪声值的大小，在每次迭代执行梯度下降的过程中，添加的噪声并不都是通过以 d 递增得到的隐私预算计算而来的。为了保证总的隐私预算值不变，需要知道该次迭代消耗了多少预算，以及还剩多少预算，这些预算该如何分配到后期的迭代过程中。

计算正则化项作为扰动项消耗的隐私预算的大小 ε_t'。

$$\frac{\lambda}{n}\omega == \mathrm{Lap}\left(\frac{\Delta f}{\varepsilon_t'}\right) \Rightarrow \varepsilon_t' \tag{21}$$

剩余隐私预算 ε' 即

$$\varepsilon' = \varepsilon - \varepsilon_t' - \sum_{t=1}^{t-1}\varepsilon_t \tag{22}$$

因此，下一轮迭代消耗的隐私预算大小即

$$\varepsilon_{t+1} = \frac{1}{T-t}\varepsilon' - \frac{(T-t-1)d}{2} \tag{23}$$

重复上述迭代过程，直到达到固定的迭代轮次数或模型收敛。

具体过程如算法 1 所示。

算法 1　CNN 中的隐私预算分配方案

输入：总隐私预算 ε，随机函数 f 的敏感度 Δf，隐私预算的增加值 d，正则项系数 γ。

输出：模型权重 ω

初始化模型权重 ω_t；

for　$t = 1, 2, \cdots, T$　do

$\varepsilon_t = \frac{\varepsilon}{T} + \left(\frac{T-1}{2}\right)d$；//消耗的隐私预算大小

$n = \mathrm{Lap}\left(\frac{\Delta f}{\varepsilon_t}\right)$；//噪声值大小

$r = \gamma\omega_t$；//正则化项值大小

if　$\mathrm{Lap}\left(\frac{\Delta f}{\varepsilon_t}\right) \leqslant \gamma\omega_t$

$\omega_{t+1} = \omega_t - \eta\left(\nabla f(\omega_t) + \mathrm{Lap}\left(\frac{\Delta f}{\varepsilon_t}\right)\right)$；

$\varepsilon_{t+1} = \varepsilon_t + d$；

else

$\omega_{t+1} = \omega_t - \eta\left(\nabla f(\omega_t) + \gamma\omega_t\right)$；// 为了限制噪声值大小，此处加入正则化项作为噪声量

令 $n == r$ 得到 $\varepsilon_t^{'}$；//此噪声值大小消耗的隐私预算量

$\varepsilon' = \varepsilon - \varepsilon_t' - \sum_{t=1}^{t-1}\varepsilon_t$；//计算剩余隐私预算

end for

4　理论分析

4.1　隐私性分析

在物联网场景下将差分隐私和深度学习进行结合，根据噪声的定义式可知隐私泄露风险和隐私预算直接相关。然而，以往工作一般都采用均匀的方式分配预算，但神经网络的训练是一个从随机到微调的过程，因此提出了本文的算法，在训练早期虽然引入相对较多的噪声，但由于初期权重参数其实也是随机化的，且有正则项值的约束，因此扰动是合理的，且在训练后期参数微调的过程中，扰动也逐渐变小，通过将隐私预算合理地分配在每次迭代过程中，较好地保证了模型的隐私。

在隐私预算的分配过程中，初始递增地分配预算过程是满足差分隐私保护的，后期引入正则项后可能打破了原有的预算分配，此时本文考虑引入该正则项大小的噪声需要消耗多少预算，之后计算剩余预算，再进行预算的重新分配，反复迭代，由于差分隐私是满足加性性质的，因此该方案的过程也满足差分隐私保护，证明过程如下。

由于该算法使用 Laplace 机制对敏感信息进行差分隐私随机梯度下降处理，因此算法的隐私性由 Laplace 机制保证。具体地，有如下定理。

定理 4.1.1 算法满足 ε-差分隐私

证明： 假设 $D_1 \to R^k$ 和 $D_2 \to R^k$ 是两个相邻数据集，且 $\| f(D_1)-f(D_2) \| \leqslant 1$，$x$ 是存在于数据集中的任意样本，$f(\bullet)$ 是一个满足 $f:D \to R^k$ 的函数，P_{D_1} 代表算法 $K_L(x_1,f,\varepsilon)$ 的概率密度函数，P_{D_2} 代表算法 $K_L(x_2,f,\varepsilon)$ 的概率密度函数。在任意点 x_1,x_2 处，算法所计算的输出相似度为：$z=f^{'}(x)=f(x)+Y$，由于 $Y \sim \mathrm{Lap}\left(\frac{\Delta f}{\varepsilon}\right)$，因此在同样的随机点 $z \in R^k$ 有

$$\frac{P_{D_1}(z)}{p_{D_2}(z)}=\prod_{i=1}^{k}\left(\frac{\exp\left(-\frac{\varepsilon \| f(x_1)_i-z_i \|}{\Delta f}\right)}{\exp\left(-\frac{\varepsilon \| f(x_2)_i-z_i \|}{\Delta f}\right)}\right)=$$

$$\prod_{i=1}^{k}\exp\left(\frac{\varepsilon\left(|| f(x_2)_i-z_i ||-|| f(x_1)_i-z_i ||\right)}{\Delta f}\right)\leqslant$$

$$\prod_{i=1}^{k}\exp\left(\frac{\varepsilon || f(x_1)_i-f(x_2)_i ||}{\Delta f}\right)=$$

$$\exp\left(\left(\frac{\varepsilon || f(x_1)-f(x_2) ||}{\Delta f}\right)\right)\leqslant \mathrm{e}^{\varepsilon} \tag{24}$$

最后两个不等式的成立可以由下面两个三角不等式得到，$\| f(x_2)_i-z_i \|-\| f(x_1)_i-z_i \| \leqslant \| (f(x_2)_i-z_i)-(f(x_1)_i-z_i) \|$，$\| f(x_1)-f(x_2) \| \leqslant \Delta f$，因此由上述定理的证明过程可知，该算法满足 ε−差分隐私。

定理 4.1.2 算法满足序列组合性质

证明： 假设一组差分隐私随机算法集合 $K=\{K_1,K_2,\cdots,K_n\}$ 在一组数据集上顺序执行，如果 K_i 满足 ε_i-差分隐私，且任意两个随机算法是独立的，那么随机算法 K 满足 $\sum_{i=1}^{n}\varepsilon_i$-差分隐私，证明过程如下。

$$\Pr[K(D_1)\in O]=\prod_{i=1}^{n}\Pr[K_i(D_1)\in O_i]\leqslant$$

$$\prod_{i=1}^{n}\left(\mathrm{e}^{\varepsilon_i}\times\Pr[K_i(D_2)\in O_i]\right)=$$

$$\exp\left(n\varepsilon_1+\frac{n\times(n-1)}{2}\times d\right)\times\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)=$$

$$\exp\left(\sum_{i=1}^{n}\varepsilon_1+(i-1)\times d\right)\times\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)=$$

$$\exp(\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_n)\times\prod_{i=1}^{n}(\Pr[K_i(D_2)\in O_i])=\exp\left(\sum_{i=1}^{n}\varepsilon_i\right)\times$$

$$\prod_{i=1}^{n}(\Pr[K_i(D_2)\in O_i])\leqslant\exp\left(\sum_{i=1}^{n}\varepsilon_i\right)\times\Pr[K(D_2)\in O] \tag{25}$$

以上是以 d 递增地分配隐私预算的过程，可知该过程满足 $\sum_{i=1}^{n}\varepsilon_i$ -差分隐私。

若更新过程中隐私预算的更新用到了正则思想，则算法整体依然满足差分隐私的序列组合性，其中 ς 是一个随机变量，服从 $\varsigma \sim UNI(0,1)$ 的均匀分布，Δf 是函数敏感度，且 $\Delta f=\left\| f(D_1)-f(D_2) \right\|$，sign 是一个用来获取参数正负的函数，abs 是一个用来获取绝对值的函数，n 是总的样本数，T 是总的迭代次数，t 表示当前迭代的次数，证明过程如下。

$$\Pr[K(D_1)\in O]=\prod_{i=1}^{n}\Pr[K(D_1)\in O]\leqslant$$

$$\prod_{i=1}^{n}\left(\mathrm{e}^{\varepsilon_i}\times\Pr[K_i(D_2)\in O_i]\right)=\exp(\varepsilon_1+\varepsilon_2+\cdots+\varepsilon_n)\times$$

$$\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)=\exp\left(\sum_{i=1}^{a}\varepsilon_1+(i-1)\times d\right)\times$$

$$\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)+$$

$$\exp\left(\sum_{i=a}^{a+1}\frac{\Delta f\times\mathrm{sign}(\varsigma)\times\ln(1-2|\varsigma|)\times n}{\lambda\omega}\right)\times$$

$$\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)+\mathrm{e}^{\sum_{i=a+2}^{n}\varepsilon_i}\times\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)=$$

$$\exp\left(a\varepsilon_1+\frac{a\times(a-1)}{2}\times d\right)\times\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)+$$

$$\exp\left(\frac{\Delta f\times\mathrm{sign}(\varsigma)\times\ln(1-2|\varsigma|)\times n}{\lambda\omega}\right)\times\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)+$$

$$\exp\left(\varepsilon-a\varepsilon_1+\frac{a\times(a-1)}{2}\times d-\frac{\Delta f\times\mathrm{sign}(\varsigma)\times\ln(1-2|\varsigma|)\times n}{\lambda\omega}\right)\times$$

$$\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)=$$

$$\exp\left(\sum_{i=1}^{t}\varepsilon_i\right)\times\prod_{i=1}^{n}\left(\Pr\left[K_i(D_2)\in O_i\right]\right)+$$
$$\exp\left(\frac{1}{T-t}\left(\varepsilon-a\varepsilon_1+\frac{a\times(a-1)}{2}\times d-\right.\right.$$
$$\left.\left.\frac{\Delta f\times\mathrm{sign}(\varsigma)\times\ln(1-2|\varsigma|)\times n}{\lambda\omega}\right)-\frac{T-t-1}{2}\times d\right)\times$$
$$\prod_{i=1}^{n}\left(\Pr\left[K_i(D_2)\in O_i\right]\right)+\mathrm{e}^{\sum_{i=t+2}^{n}\varepsilon_i}\times\prod_{i=1}^{n}\left(\Pr\left[K_i(D_2)\in O_i\right]\right)\Rightarrow$$
$$\exp\left(\sum_{i=1}^{n}\varepsilon_i\right)\times\prod_{i=1}^{n}\left(\Pr[K_i(D_2)\in O_i]\right)\leqslant\mathrm{e}^{\sum_{i=1}^{n}\varepsilon_i}\times\Pr\left[K(D_2)\in O\right] \tag{26}$$

由上述证明过程可看出，算法满足 $\sum_{i=1}^{n}\varepsilon_i$ -差分隐私。

在差分隐私算法中，序列组合是最普遍、最直接的分析隐私预算消耗的方式。当差分隐私用在深度学习中时，深度学习的迭代训练等于顺序地计算多个满足 ε -差分隐私的随机算法。因为在深度学习中训练次数比较多，因此造成隐私泄露的风险也比较高。本文提出更合理的隐私预算分配策略将预算分配到迭代过程中，从而减少隐私信息泄露的风险，增强数据的可用性，提供较强的隐私保证。

4.2　有效性分析

本文算法通过合理分配隐私预算，虽然向梯度中添加了噪声，但并不降低模型效用，且在迭代次数较少时增加了模型的泛化能力。

深度学习中，模型在早期训练时，权重一般是随机初始化的，可能与最优参数值相距较远。且初始梯度的值通常较大，此时即使向梯度添加较多噪声，随着梯度的更新，模型也会得到校正。且噪声可以防止过拟合的发生[23]，因此，合理扰动的添加对模型训练不会造成很大影响。随着训练次数的增加，当模型要收敛到最优值时，权重的微小变化对输出的影响较大，如果平均分配预算，可能每次的噪声都比较大，不利于模型收敛。如果根据这一特性进行噪声自适应的添加，既能保证预算的合理分配，又能加快模型的收敛，提高泛化能力，且不会降低模型的效用。因此，动态地分配隐私预算即合适量噪声的添加很好地保证了模型的隐私和效用。

该算法在递增分配隐私预算的过程中，会对扰动进行一定程度的限制。此处用估计量评价标准中最小方差性对有效性进行评估。该方法定理如下：设 $\hat{\theta}_1=\hat{\theta}_1(X_1,X_2,\cdots,X_n)$ 与 $\hat{\theta}_2=\hat{\theta}_2(X_1,X_2,\cdots,X_n)$ 都是 θ 的无偏估计量，如果 $D(\hat{\theta}_1)<D(\hat{\theta}_2)$，则称 $\hat{\theta}_1$ 比 $\hat{\theta}_2$ 有效。基于该思想，这里用输出的最小方差来对有效性进行衡量。具体地，有以下定理。

定理 4.2.1　算法有效性评估

已知：

$$\frac{\lambda}{2n}\omega<\mathrm{Lap}\left(\frac{\Delta f}{\varepsilon}\right) \tag{27}$$

求证：

$$\int\omega_{\mathrm{regularization}}\mathrm{d}\omega<\int\omega_{\mathrm{laplace}}\mathrm{d}\omega\Rightarrow$$
$$\int_{\omega}^{\omega-\Delta\omega}\left(\omega-\eta\left(\frac{\partial C_0}{\partial\omega}+\frac{\lambda}{n}\omega\right)\right)\mathrm{d}\omega<$$
$$\int_{\omega}^{\omega-\Delta\omega}\left(\omega-\eta\left(\frac{\partial C_0}{\partial\omega}+\mathrm{Lap}\left(\frac{\Delta f}{\varepsilon}\right)\right)\right)\mathrm{d}\omega \tag{28}$$

证明：首先，给出将正则项值和拉普拉斯函数值作为噪声求梯度的计算式。

$$\frac{\partial C_{\mathrm{regularization}}}{\partial\omega}=\frac{\partial C_0}{\partial\omega}+\frac{\lambda}{n}\omega \tag{29}$$

$$\frac{\partial C_{\mathrm{laplace}}}{\partial\omega}=\frac{\partial C_0}{\partial\omega}+\mathrm{Lap}\left(\frac{\Delta f}{\varepsilon}\right) \tag{30}$$

对于参数更新过程

$$\omega_{\mathrm{regularization}}=\omega-\eta\left(\frac{\partial C_0}{\partial\omega}+\frac{\lambda}{n}\omega\right) \tag{31}$$

$$\omega_{\mathrm{laplace}}=\omega-\eta\left(\frac{\partial C_0}{\partial\omega}+\mathrm{Lap}\left(\frac{\Delta f}{\varepsilon}\right)\right) \tag{32}$$

以相邻两轮梯度更新过程为例，计算迭代损失。

1) 对于正则项值作为噪声的情况：

$$\begin{aligned}&\int\omega_{\mathrm{regularization}}\mathrm{d}\omega=\\&\int_{\omega}^{\omega-\Delta\omega}\left(\omega-\eta\left(\frac{\partial C_0}{\partial\omega}+\frac{\lambda}{n}\omega\right)\right)\mathrm{d}\omega=\\&\int_{\omega}^{\omega-\Delta\omega}\left(\omega-\eta\frac{\partial C_0}{\partial\omega}-\eta\frac{\lambda}{n}\omega\right)\mathrm{d}\omega=\\&\frac{1}{2}\omega^2-\frac{\lambda\eta}{2n}\omega^2-\eta C_0\Big|_{\omega}^{\omega-\Delta\omega}=\\&\frac{1}{2}\Delta\omega^2-\omega\Delta\omega+\frac{\lambda\eta}{n}\omega\Delta\omega-\frac{\lambda\eta}{2n}\Delta\omega^2\end{aligned} \tag{33}$$

2) 对于递增增加隐私预算的加噪情况：

$$\int \omega_{\text{laplace}} \mathrm{d}\omega = \int_{\omega}^{\omega-\Delta\omega} \left(\omega - \eta \left(\frac{\partial C_0}{\partial \omega} + \text{Lap}\left(\frac{\Delta f}{\varepsilon} \right) \right) \right) \mathrm{d}\omega =$$

$$\int_{\omega}^{\omega-\Delta\omega} \left(\omega - \eta \frac{\partial C_0}{\partial \omega} - \eta \text{Lap}\left(\frac{\Delta f}{\varepsilon} \right) \right) \mathrm{d}\omega =$$

$$\frac{1}{2}\omega^2 - \eta \text{Lap}\pi\left(\frac{\Delta f}{\varepsilon} \right)\omega - \eta C_0 \Big|_{\omega}^{\omega-\Delta\omega} =$$

$$\frac{1}{2}\Delta\omega^2 - \omega\Delta\omega + \eta \text{Lap}\left(\frac{\Delta f}{\varepsilon} \right)\Delta\omega \tag{34}$$

若 $\frac{\lambda}{n}\omega > 0$， $\text{Lap}\left(\frac{\Delta f}{\varepsilon} \right) > 0$，

则有

$$\begin{cases} \frac{1}{2}\Delta\omega^2 - \omega\Delta\omega + \frac{\lambda\eta}{n}\omega\Delta\omega - \frac{\lambda\eta}{2n}\Delta\omega^2 < 0 \\ \frac{1}{2}\Delta\omega^2 - \omega\Delta\omega + \eta \text{Lap}\left(\frac{\Delta f}{\varepsilon} \right)\Delta\omega < 0 \end{cases}, \tag{35}$$

由此可得

$$\begin{cases} \omega > \frac{1}{2}\Delta\omega \\ \eta \text{Lap}\left(\frac{\Delta f}{\varepsilon} \right) < \omega - \frac{1}{2}\Delta\omega \end{cases} \tag{36}$$

不同情况添加噪声的差值为

$$\begin{aligned} &\int \omega_{\text{regularization}} \mathrm{d}\omega - \int \omega_{\text{laplace}} \mathrm{d}\omega = \\ &\int_{\omega}^{\omega-\Delta\omega} \left(\omega - \eta \left(\frac{\partial C_0}{\partial \omega} + \frac{\lambda}{n}\omega \right) \right) \mathrm{d}\omega - \\ &\int_{\omega}^{\omega-\Delta\omega} \left(\omega - \eta \left(\frac{\partial C_0}{\partial \omega} + \text{Lap}\left(\frac{\Delta f}{\varepsilon} \right) \right) \right) \mathrm{d}\omega = \\ &\eta\Delta\omega \left(\frac{\lambda\omega}{n} - \frac{\lambda}{2n}\Delta\omega - \text{Lap}\left(\frac{\Delta f}{\varepsilon} \right) \right) \end{aligned} \tag{37}$$

结合式(36)及 λ、η 等超参数远远小于样本数 n，因此可得

$$\eta\Delta\omega \left(\frac{\lambda\omega}{n} - \frac{\lambda}{2n}\Delta\omega - \text{Lap}\left(\frac{\Delta f}{\varepsilon} \right) \right) < 0 \tag{38}$$

所以有

$$\int \omega_{\text{regularization}} \mathrm{d}\omega - \int \omega_{\text{laplace}} \mathrm{d}\omega < 0 \tag{39}$$

即利用正则项对噪声进行限制后，一次迭代更新过程带来的误差要更小，因此对预算的再次调整进一步保证了算法的有效性。

5 实验与分析

5.1 实验设置

为了评估基于梯度加噪方案的有效性，实验使用CIFAR-10数据集和MNIST数据集进行实验验证。

CIFAR-10 数据集由 10 个类共 60 000 张 32 px×32 px 彩色图像组成，每个类有 6 000 张图像。CIFAR-10 数据集由 50 000 个训练图像和 10 000 个测试图像组成。其分为 5 个训练批次和一个测试批次，每个批次数量相等。

MNIST 数据集是机器学习领域中非常经典的一个数据集，包含 60 000 个训练样本和 10 000 个测试样本，每个样本图片均为 28 px×28 px 的灰度手写数字图片。

对于训练模型，本文选用具有通用性且在集中式训练上取得高效用的经典深度学习框架[24]，以此来测试深度模型迭代过程梯度参数变化特点和隐私预算的关系，并保证其适应物联网环境传感器节点资源受限的情况，算法中的超参数设置和 Abadi 等[15]实验中提到的相同，神经网络架构及参数如图 2 所示。

5.2 实验分析

在实验中，以模型损失作为评估指标。实验初期，在 CIFAR-10 数据集上利用上述提到的深度模

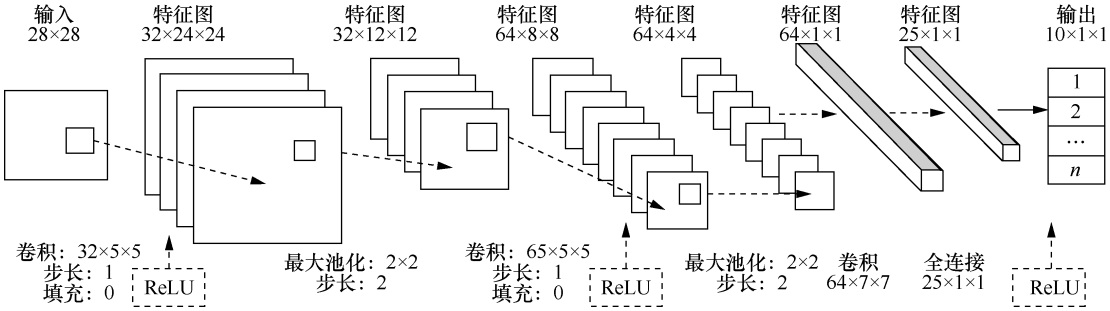


图 2 神经网络架构及参数

型进行训练，并在梯度参数上添加随机扰动，每 200 次迭代记录添加扰动前后模型的损失变化。由统计结果可以看出，适当添加扰动后的数据对于模型训练过程中损失函数的下降表现更好，即相较于原数据损失函数下降更快。实验结果表明，适当的扰动会提高模型的泛化能力，使得模型趋向于学习更重要的参数，降低模型损失。损失函数随迭代次数变化对比如图 3 所示。

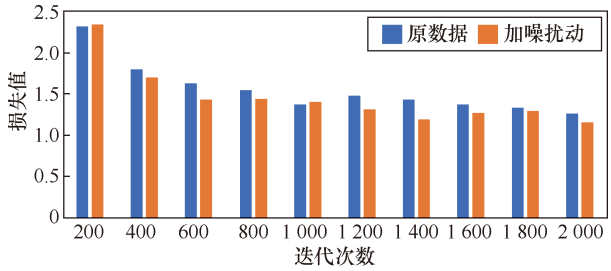


图 3　损失函数随迭代次数变化对比

基于本文提出的方法，在 MNIST 数据集上进行完整的验证过程，并与平均分配隐私预算策略和不具有隐私保护的方案进行对比。对于差分隐私随机梯度下降过程参数的选择属于超参数优化问题，超参数一般不能从学习中得到，但对模型性能有直接影响。在深度学习中，超参数并不存在通用优化方法，大部分都是依靠多次实验经验设置不同值，且不同参数之间可能会相互影响；其次，每次设置超参数都需要进行完整的迭代训练，会耗费大量的时间成本，复杂模型效率会更低。因此，这里参照以往实验设置超参数的值。

首先，测试固定隐私预算下，不同迭代次数准确率的变化。为保证较好的隐私性，使得预算值尽可能小，因此实验中设置隐私预算大小为 1，裁剪值为 0.002，正则项系数为 0.5，学习率为 1×10^{-2}。模型迭代 100、200、300、600、2 400、3 600 次准确率变化对比如图 4 所示，随着迭代次数的增加，模型预测效果变得越来越好。由图 4(a)～图 4(d)可以看出，当迭代次数较少时，本文方法明显要优于其他两种情况，因为适当噪声的添加相当于加入了一个正则化项，可以使模型趋向于选择更优的解；

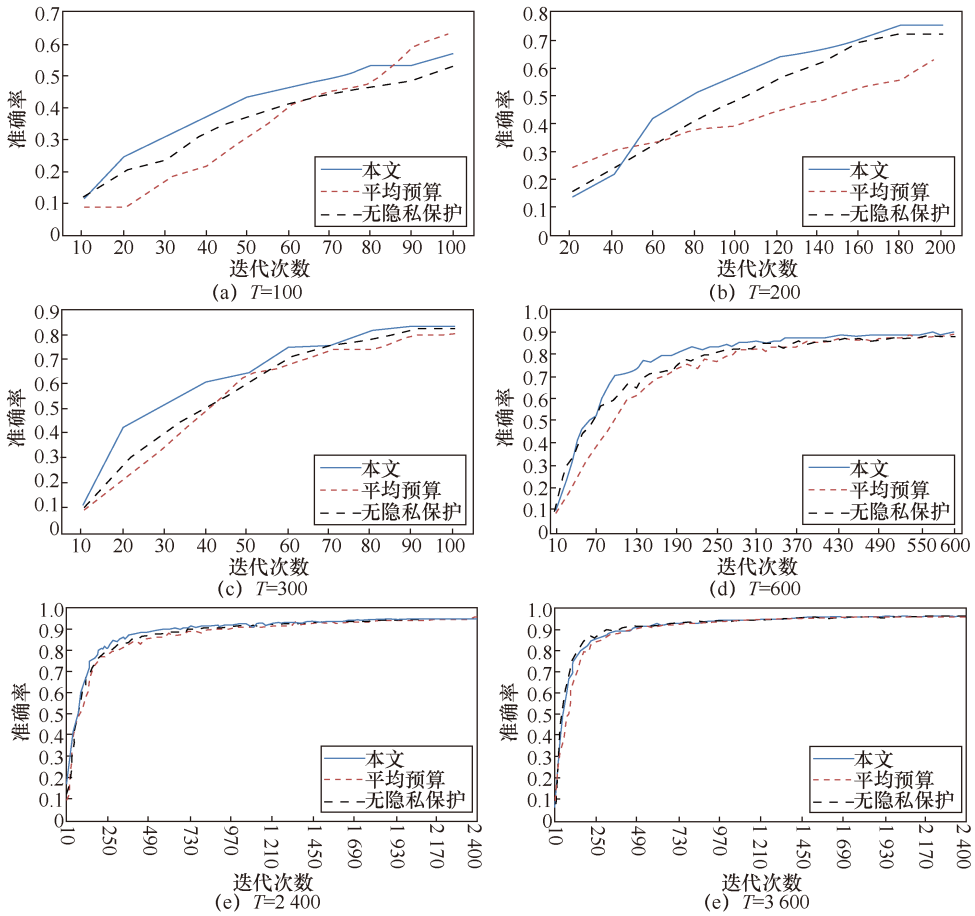


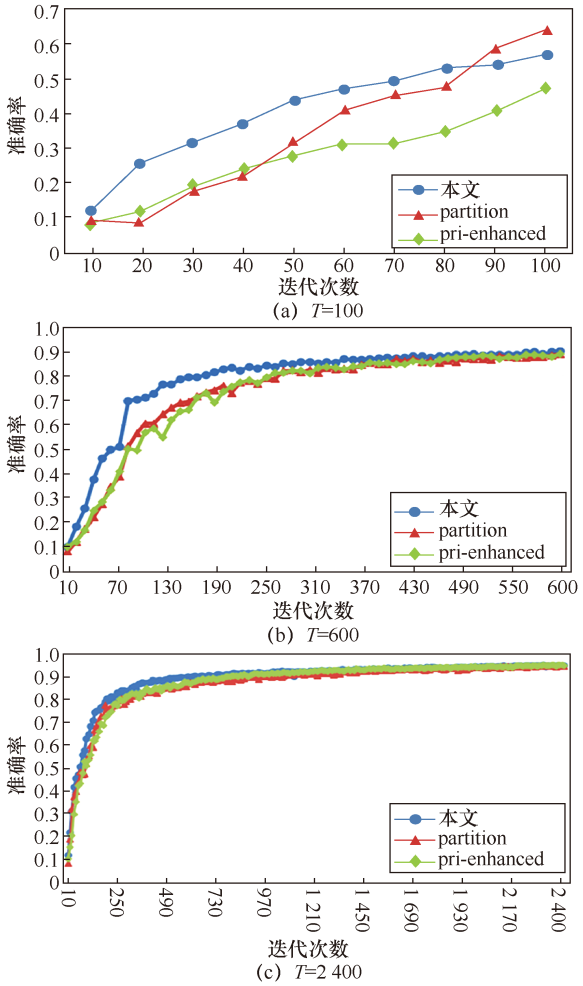
图 4　模型迭代 100、200、300、600、2 400、3 600 次准确率变化对比

由图 4(e)可以看出本文方法依然是最优的，且随着迭代次数的增加，后期加噪的准确率趋向于和原始数据相同；由图 4(f)可得，随着迭代次数的进一步增加，原始数据的效果最优，但本文方法依然优于平均分配预算的情况。因为随着迭代次数的增加，总预算不变，那么分配到每一轮的预算就会变小，相应引入的噪声会较大，隐私保护程度增强，但可用性并没有下降。同时，当迭代次数达到一定值时，模型趋向于稳定。

为了进一步验证模型的性能，本文将 Gong 等[24]提到的隐私增强策略的第一种策略，图例中标记为"pri-enhanced"以及 Wang[25]提到的隐私预算分配的均分策略，图例中标记为"partition"，作为基准模型进行对比。"pri-enhanced"策略首先设定最大和最小预算值以及迭代次数，每次以固定的步长进行增加，从最小值增加到最大值。"partition"策略首先给定迭代次数，然后在该迭代次数内进行预算的平均分配。实验中，将隐私预算设为定值，对比了不同迭代次数情况下模型准确率的变化以及将迭代次数设置为定值，对比了不同隐私预算情况下模型准确率的变化，其他参数的设置与上述实验均相同。

首先，测试固定隐私预算下，不同迭代次数对准确率的影响，如图 5 所示。图 5(a)～图 5(c)分别为隐私预算为 1，迭代次数为 100、600、2 400 次的情况下 3 种方法模型准确率的对比。图中结果表明，不同迭代次数下，本文结果表现更优，在迭代次数为 100，即迭代次数较少时，效果更显著。对于资源受限的物联网节点来说，可以利用较少的资源在更短时间内达到和其他算法相同的准确率。

其次，测试固定迭代次数的情况下，不同隐私预算对模型准确率的影响。设置迭代次数为 100，不同隐私预算对模型准确率的影响如图 6 所示，当隐私预算分别为 1、5、10 时，将本文提出的方法与 Gong[24]和 Wang[25]等提出的方法做对比，由图 6(a)～图 6(c)可以看出，在迭代次数较少时，本文方法优越性更明显，可以较快地实现较优的预测性能，对物联网环境更友好。由于在迭代次数为 600 时，模型的性能已相对较优，因此迭代次数固定为 600，不同隐私预算对模型准确率的影响如图 7 所示，测试隐私预算分别为 1、5、10 的情况下模型准确率变化，如图 7(a)～图 7(c)所示。可以看出，本文所提方法性能依然表现最优。当隐私



(a) T=100

(b) T=600

(c) T=2 400

图 5 固定隐私预算下，不同迭代次数对准确率的影响

预算较小时，本文方法明显优于其他两种方法，说明该方法在提供更强隐私保护的同时依然有较好的性能。随着隐私预算的增大，隐私保护程度相对减弱，但性能影响不大。

由实验结果分析可得，在迭代次数较少时，本文方法优于其他两种隐私预算分配策略及基准方法，表明适当的噪声会增加模型的泛化能力，使其更好地进行学习，权值变小使得网络不会因为一些简单的随机输入有太大的变化，从而学习到“噪声”数据特征的几率进一步变小，因此，在同等情况下，只需要更少的迭代次数便可达到和不加噪相同的精度，对于资源受限的物联网节点有很大的优势。但随着迭代次数的增加，分配到每轮迭代的隐私预算减小，引入的噪声会相对较大，优越性可能不是特别明显，但加噪后模型的精度依然会不断提升，即使引入了相对较多的噪声，也可以达到与不加噪几乎相同的准确率，很好地实现了隐私与可用性的平衡。

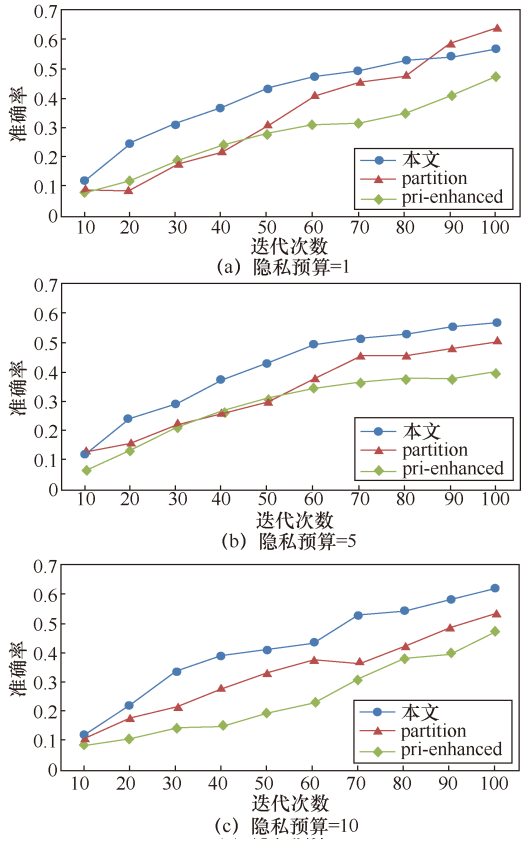


图 6　迭代次数为 100，不同隐私预算对模型准确率的影响

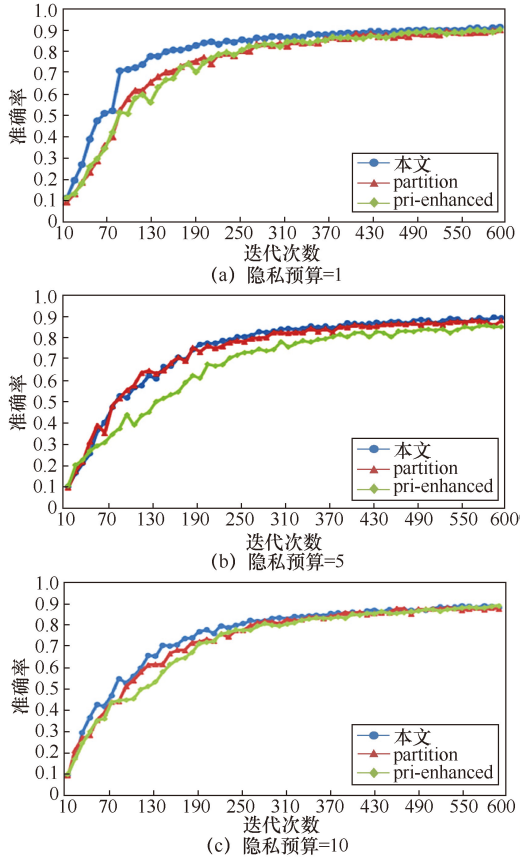


图 7　迭代次数为 600，不同隐私预算对模型准确率的影响

6　结束语

深度学习在物联网中的应用同时带来了机遇与挑战。为了防止用户隐私的泄露，本文引入差分隐私的方法，并合理分配隐私预算以适应模型参数更精细的变化。同时，为了限制噪声的大小，引入了正则化的方法，增强了模型的泛化能力，加快了模型的收敛。最后在数据集上进行实验验证，结果表明，本文方法表现更优，且随着迭代次数的增加，该方法实现了模型隐私和可用性的平衡。未来可以探索改进后的差分隐私算法在模型逆向攻击、成员推理攻击等场景中的防御性能。

参考文献：

[1] 杨毅宇, 周威, 赵尚儒, 等. 物联网安全研究综述：威胁、检测与防御[J]. 通信学报, 2021, 42(8): 188-205.
YANG Y Y, ZHOU W, ZHAO S R, et al. Survey of IoT security research: threats, detection and defense[J]. Journal on Communications, 2021, 42(8): 188-205.

[2] 吕建新, 郑伟, 马林, 等. 基于词向量语义扩展的网络文本特征选择方法研究[J]. 情报科学, 2019, 37(12): 47-51.
LV J X, ZHENG W, MA L, et al. Feature selection method of the network text based on semantic extension with word vector[J]. Information Science, 2019, 37(12): 47-51.

[3] 孟仕林, 赵蕴龙, 关东海, 等. 融合情感与语义信息的情感分析方法[J]. 计算机应用, 2019, 39(7): 1931-1935.
MENG S L, ZHAO Y L, GUAN D H, et al. Sentiment analysis method combining sentiment and semantic information[J]. Journal of Computer Applications, 2019, 39(7): 1931-1935.

[4] LI T, LI J, CHEN X F, et al. NPMML: a framework for non-interactive privacy-preserving multi-party machine learning[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(6): 2969-2982.

[5] ZHANG X L, FU A M, WANG H Q, et al. A privacy-preserving and verifiable federated learning scheme[C]//Proceedings of ICC 2020 - 2020 IEEE International Conference on Communications. Piscataway: IEEE Press, 2020: 1-6.

[6] SUH J, TANAKA T. Encrypted value iteration and temporal difference learning over leveled homomorphic encryption[C]//Proceedings of 2021 American Control Conference (ACC). Piscataway: IEEE Press, 2021.

[7] WANG Y C, LIANG X L, HEI X H, et al. Deep learning data privacy protection based on homomorphic encryption in AIoT[J]. Mobile Information Systems, 2021, 2021: 5510857.

[8] YE H, LIU J Q, WANG W, et al. Secure and efficient outsourcing differential privacy data release scheme in Cyber-physical system[J]. Future Generation Computer Systems, 2020, 108: 1314-1323.

[9] BU Z Q, WANG H, LONG Q, et al. On the convergence of deep learning with differential privacy[EB]. 2021.

[10] BU Z Q, GOPI S, KULKARNI J, et al. Fast and memory efficient differentially private-SGD via JL projections[EB]. 2021.

[11] CHEN X, WU S Z, HONG M. Understanding gradient clipping in

private SGD: A geometric perspective[J]. Advances in Neural Information Processing Systems, 2020, 33: 13773-13782.

[12] KOSKELA A, JALKO J, HONKELA A. Computing tight differential privacy guarantees using fft[C]//International Conference on Artificial Intelligence and Statistics. Online: PMLR, 2020: 2560-2569.

[13] GHAZI B, GOLOWICH N, KUMAR R, et al. On deep learning with label differential privacy[EB]. 2021.

[14] YUAN S, SHEN M, MIRONOV I, et al. Practical, label private deep learning training based on secure multiparty computation and differential privacy[EB]. 2021.

[15] ABADI M, CHU A, GOODFELLOW I, et al. Deep learning with differential privacy[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 308-318.

[16] DWORK C. Differential privacy[C]//Proceedings of 33th International Colloquium on Automata, Languages and Programming. Berlin: Springer, 2006: 1-12.

[17] DWORK C. Differential privacy: a survey of results[C]//Proceedings of the 5th International Conference on Theory and Applications of Models of Computation. Berlin: Springer-Verlag, 2008: 1-19.

[18] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating noise to sensitivity in private data analysis[C]//Theory of Cryptography. Berlin, Heidelberg: Springer, 2006: 265-284.

[19] ZINKEVICH M, WEIMER M, LI L, et al. Parallelized stochastic gradient descent[C]//Proceedings of Advances in neural information processing systems. Vancouver, Canada: NIPS, 2010: 2595 – 2603.

[20] CHANG D Q, LIN M, ZHANG C S. On the generalization ability of online gradient descent algorithm under the quadratic growth condition[J]. IEEE Transactions on Neural Networks and Learning Systems, 2018, 29(10): 5008-5019.

[21] BUKOVSKY I, HOMMA N. An approach to stable gradient-descent adaptation of higher order neural units[J]. IEEE Transactions on Neural Networks and Learning Systems, 2017, 28(9): 2022-2034.

[22] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition[J]. Proceedings of the IEEE, 1998, 86(11): 2278-2324.

[23] 汪小寒, 韩慧慧, 张泽培, 等. 树索引数据差分隐私预算分配方法[J]. 计算机应用, 2018, 38(7): 1960-1966.
WANG X H, HAN H H, ZHANG Z P, et al. Differential privacy budget allocation method for data of tree index[J]. Journal of Computer Applications, 2018, 38(7): 1960-1966.

[24] GONG M G, FENG J L, XIE Y. Privacy-enhanced multi-party deep learning[J]. Neural Networks, 2020, 121: 484-496.

[25] 王璇. 差分隐私保护中隐私预算的优化与应用[D]. 南京: 南京邮电大学, 2019.
WANG X. Optimization and application of privacy budget in differential privacy protection[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2019.

[作者简介]

罗丹（1997– ），女，华北电力大学硕士生，主要研究方向为隐私计算、信息安全。

徐茹枝（1966– ），女，博士，华北电力大学教授，主要研究方向为电力信息安全。

关志涛（1979– ），男，博士，华北电力大学副教授、博士生导师，主要研究方向为物联网安全、区块链技术、人工智能安全。