

基于在线双边拍卖的分层联邦学习激励机制

杜辉^{1,2} 李卓^{1,2} 陈昕²

1 网络文化与数字传播北京市重点实验室(北京信息科技大学) 北京 100101

2 北京信息科技大学计算机学院 北京 100101

(duhui199801@163.com)

摘要 在分层联邦学习中,能量受限的移动设备参与模型训练会消耗自身资源。为了降低移动设备的能耗,文中在不超过分层联邦学习的最大容忍时间下,提出了移动设备能耗之和最小化问题。不同训练轮次的边缘服务器能够选择不同的移动设备,移动设备也能够为不同的边缘服务器并发训练模型,因此文中基于在线双边拍卖机制提出了 ODAM-DS 算法。基于最优停止理论,支持边缘服务器在合适的时刻选择移动设备,使得移动设备的平均能耗最小,然后对提出的在线双边拍卖机制进行理论分析,证明其满足激励相容性、个体理性、弱预算均衡约束等特性。模拟实验的结果证明,ODAM-DS 算法产生的能耗比已有的 HFEL 算法平均降低了 19.04%。

关键词: 分层联邦学习;能耗最小化;在线双边拍卖;最优停止理论;激励机制设计

中图法分类号 TP393

Incentive Mechanism for Hierarchical Federated Learning Based on Online Double Auction

DU Hui^{1,2}, LI Zhuo^{1,2} and CHEN Xin²

1 Beijing Key Laboratory of Internet Culture and Digital Dissemination Research (Beijing Information Science & Technology University), Beijing 100101, China

2 School of Computer Science, Beijing Information Science & Technology University, Beijing 100101, China

Abstract In hierarchical federated learning, energy constrained mobile devices will consume their own resources for participating in model training. In order to reduce the energy consumption of mobile devices, this paper proposes the problem of minimizing the sum of energy consumption of mobile devices without exceeding the maximum tolerance time of hierarchical federated learning. Different training rounds of edge server can select different mobile devices, and mobile devices can also train models under different edge servers concurrently. Therefore, this paper proposes ODAM-DS algorithm based on an online double auction mechanism. Based on the optimal stopping theory, the edge server is supported to select the mobile device at the best time, so as to minimize the average energy consumption of the mobile device. Then, the theoretical analysis of the proposed online double auction mechanism proves that it meets the characteristics of incentive compatibility, individual rationality and weak budget equilibrium constraints. Simulation results show that the energy consumption of ODAM-DS algorithm is 19.04% lower than that of the existing HFEL algorithm.

Keywords Hierarchical federated learning, Minimization of energy consumption, Online double auction, Optimal stopping theory, Incentive mechanism design

1 引言

随着人工智能应用的飞速发展及物联网设备的普及,数十亿台移动设备和物联网设备连接到互联网,在网络边缘生成了数十亿字节的数据^[1]。而在传统的机器学习中,为了更有效地学习,通常将用户数据上传至云服务器。但是,这将会导致用户隐私泄露,并随着产生的数据越来越多,将其上传至

云服务器会产生较大的时延和能耗。

面对这些挑战,2016年,谷歌提出了联邦学习^[2]。在联邦学习中,模型训练仅仅在移动设备上进行,只需要将训练的本地模型上传至云服务器进行聚合,从而生成全局模型。在上传过程中只需要上传模型参数,这使得上传的数据规模大幅降低,导致能耗减少与传输时延缩短,并且不需要将原始数据上传至云端,从而使用户的隐私得到保护。

到稿日期:2021-08-05 返修日期:2021-10-19

基金项目:国家自然科学基金(61872044);北京市青年拔尖人才项目;网络与文化传播北京市重点实验室开放课题

This work was supported by the National Natural Science Foundation of China(61872044), Beijing Municipal Program for Top Talent and Open Program of Beijing Key Laboratory of Internet Culture and Digital Dissemination Research.

通信作者:李卓(lizhuo@bistu.edu.cn)

根据参数服务器位置的不同,联邦学习分为基于云的联邦学习和基于边缘的联邦学习^[3]。然而,基于云的联邦学习中,移动设备的规模达到数百万台,与云服务器的通信速度慢且不可预测,导致模型上传时模型训练效率低下^[4]。基于边缘的联邦学习中,计算的延迟相当于与边缘服务器通信的延迟,当边缘服务器下的移动设备数量有限时,模型训练的效率低^[5]。因此,Liu等^[6]提出了基于云-边缘-移动设备的分层联邦学习,既解决了基于云联邦学习传输距离远和移动设备规模大的问题,又解决了基于边缘联邦学习的移动设备数量少的问题。

在分层联邦学习中,由于移动设备的电源受限,参与模型训练会消耗自身资源,为了激励移动设备参与模型训练,需要设计有效的激励机制。由于分层联邦学习中多个边缘服务器之间相互竞争选择移动设备参与模型训练,因此本文基于在线双边拍卖设计了 ODAM-DS 算法。为了不产生过多能耗,在不超过分层联邦学习的最大容忍时间下,最小化移动设备的能耗。因此,本文提出移动设备能耗之和最小化问题,将移动设备建模为卖家,将边缘服务器建模为买家。在传统的双边拍卖机制中,由于参与者自身资源随时间的改变,其身份会发生变化,即从卖家变为买家,或者相反。而在分层联邦学习中,边缘服务器和移动设备作为参与者,其身份是固定的。与传统的基于云的联邦学习或基于边缘的联邦学习不同,在 ODAM-DS 算法中,不仅移动设备之间相互竞争来参与模型训练,多个边缘服务器之间也会相互竞争来选择移动设备。

在 ODAM-DS 算法中,移动设备可以并发训练来自多个边缘服务器的局部模型,每一个边缘服务器的局部模型由多个移动设备参与训练。首先根据每个移动设备的自身资源,在一定时延约束下最小化能耗,可计算出训练模型所需的成本,提交其类型,其类型包括移动设备的到达时间、离开时间、报价、供应量或需求量。对于移动设备来说,供应量指其同时并发训练边缘服务器的局部模型的最大数量;对于边缘服务器来说,需求量指其参与模型训练的移动设备的最大数量。为了使能耗最小化,基于最优停止理论,边缘服务器在其预算和时延约束下,在移动设备平均能耗最小的时刻选择移动设备参与模型训练,并支付相应的费用。最后证明了该机制的激励相容性、个体理性和满足弱预算均衡约束的特性。

本文第 2 节介绍了相关工作;第 3 节介绍了分层联邦学习系统模型,并定义了能耗最小化的问题;第 4 节介绍了在线双边拍卖机制及理论分析;第 5 节进行了实验分析;最后总结全文。

2 相关工作

在分层联邦学习的现有工作中,Luo等^[7]提出了分层联邦边缘学习 HFEL。HFEL 在选择移动设备时有助于通过边缘模型聚合来减小设备用户和云之间通过广域网传输的显著通信开销。此外,通过相邻边缘服务器之间的协调,可以实现设备用户之间更高效的通信和计算资源分配,以有效地缩短训练时间和减小能量开销。由于参与模型训练需要消耗自身资源,但 Luo 等并未提出有效的激励机制来激励移动设备参与模型训练。

在无线通信领域激励机制设计的现有工作中,将激励

机制分为离线激励机制^[8-13]与在线激励机制^[14-15]。在离线激励机制中,Khan等^[8]提出了基于 Stackleberg 博弈的激励机制,其中基站作为领导者,以激励移动设备参与模型训练。Chai等^[9]提出了基于车辆-路边设备-基站的分层联邦学习,并且在车辆和路边设备之间设计多领导者多玩家的 Stackleberg 博弈,路边单元作为领导者为训练结果定价,车辆充当参与者,根据所有领导者设定的价格来确定所收集数据的最佳大小。Zhan等^[10]提出了基于深度强化学习的激励机制,可以自动学习最优定价策略。Tang^[11]在 Ad Hoc 网络中基于贝叶斯博弈激励自私阶段参与数据转发。Zhou等^[12]在群智感知中提出基于显性时空关联和隐性时空关联的用户激励算法。在离线激励机制中,需要保证每一个移动设备从始至终都要联邦学习模型训练。然而,在现实中,移动设备会在不同时间到达或离开,因此需要提出在线激励机制,用于激励移动设备参与模型训练。Zeng等^[13]针对联邦学习,提出了一个多维激励框架 FMore。FMore 使用博弈论为边缘参与者推导最优策略,并利用期望效用理论指导聚合者有效地获得所需资源。在在线激励机制中,Zhang等^[14]在移动群智感知中提出了基于在线逆向拍卖的在线激励机制,该激励机制能够让用户报告他们的真实到达时间和离开时间以及感知成本。但在此场景中,该激励机制是一个任务发布者和多个参与者之间的激励,而在本文中是多个边缘服务器与多个移动设备之间的激励。因此,该激励机制无法应用到分层联邦学习中。Li等^[15]利用在线双边拍卖机制研究了智能电网中车对车技术的微电网需求响应问题,并考虑了车联网支持下的位置隐私保护。然而,在该在线双边拍卖机制中的不同时期,车根据对电力的需求,会改变在拍卖场景中的角色,例如卖家变为买家,该激励机制无法应用到分层联邦学习中。因此,本文基于在线双边拍卖机制提出了 ODAM-DS 算法,边缘服务器作为买家,移动设备作为卖家,并且基于最优停止理论,边缘服务器在最佳的时间选择移动设备,使得移动设备的平均能耗最小化。

3 系统模型与问题定义

本节将对分层联邦学习训练模型和能耗最小化的问题进行建模。本文常用的数学符号如表 1 所列。

表 1 常用符号

Table 1 Key notations

Symbols	Definitions
$t_j^{(comp)}$	Delay of mobile device j for a round of local training
$e_j^{(comp)}$	Energy consumption of mobile device j for a round of local training
$t_{ij}^{(com)}$	Delay when mobile device j communication to edge server i
$e_{ij}^{(com)}$	Energy consumption when mobile device j communication to edge server i
ω_i	Type of participant i
b_i	Participant i 's valuation of model training in period $t \in [a_i, d_i]$
$x_i^t(\omega^t)$	Allocation of participant i
$p_i^t(\omega^t)$	Payment of participant i
q_i	Supply/demand for participant i
t_{max}	Maximum tolerance time in hierarchical federated learning
t_{max}^t	Maximum waiting time of each round of training in hierarchical Federation learning

3.1 分层联邦学习训练模型

分层联邦学习的训练由云服务器向边缘服务器发送初始模型框架,边缘服务器再将模型框架发送到可以参与模型训练的移动设备。然后,移动设备进行模型训练,将模型参数上传至边缘服务器,再由边缘服务器进行本区域内参数的聚合。最后,边缘服务器将聚合后的参数上传至云服务器进行全局模型的聚合,如此往复,直到联邦学习模型达到令人满意的精确度。分层联邦学习的框架如图1所示。

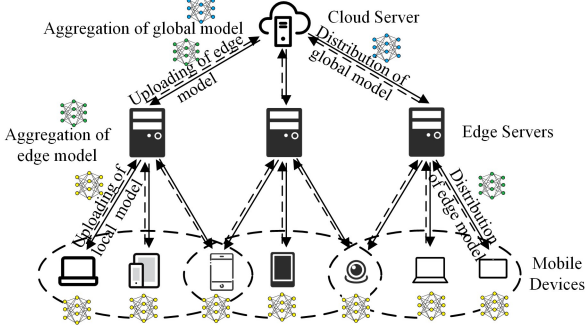


图1 分层联邦学习的框架

Fig. 1 Framework of hierarchical federated learning

在本文提出的分层联邦学习训练过程中,移动设备会将模型参数上传至多个边缘服务器,而多个边缘服务器会将多个更新后的参数发送至多个移动设备。在离散的时间周期 $T = \{1, 2, \dots, t, \dots\}$ 上,假设边缘服务器的集合为 $E = \{e_1, \dots, e_i, \dots, e_n\}$, 移动设备的集合为 $M = \{m_1, \dots, m_i, \dots, m_l\}$, $M_i \subset M$ 表示与边缘服务器 i 通信的参与模型训练的移动设备集,并将边缘服务器和移动设备作为在线双边拍卖机制的参与者,记为 $E \cup M$ 。每一个移动设备 j 的本地数据样本集为 $D_j = \{(x_k, y_k)\}_{k=1}^{|D_j|}$, 其中, x_k 表示第 k 个输入样本, y_k 是 x_k 的样本标签。

在本地模型训练中,对于移动设备 j , 利用自身数据样本集 D_j 进行模型训练,得到模型参数 θ , $f_j(x_k, y_k, \theta)$ 表示损失函数。设备 j 上的损失函数定义为:

$$F_j(\theta) = \frac{1}{|D_j|} \sum_{k=1}^{|D_j|} f_j(x_k, y_k, \theta) \quad (1)$$

边缘服务器 i 与移动设备所产生的模型参数聚合,边缘服务器 j 聚合后的损失函数为:

$$F_i(\theta) = \sum_{j=1}^m \frac{|D_j|}{|D_i|} F_j(\theta) \quad (2)$$

其中, $D_i = \bigcup_{j \in M_i} D_j$ 。

在云服务器聚合所有边缘服务器,得到全局模型的损失函数为:

$$F(\theta) = \sum_{i=1}^n \frac{|D_i|}{|D|} F_i(\theta) \quad (3)$$

其中, $D = \bigcup_{i \in E} D_i$ 。

对分层联邦学习模型进行训练的目标是使损失函数最小化,即:

$$\theta^* = \arg \min_{\theta} F(\theta) = \sum_{i=1}^n \frac{|D_i|}{|D|} F_i(\theta) \quad (4)$$

3.2 分层联邦学习计算与通信模型

通过在线双边拍卖机制,边缘服务器选择移动设备后

模型训练的计算与通信模型的流程如下^[7]。

在移动设备上进行本地模型训练时,为了达到令人满意的精确度 α , 移动设备 j 在本地迭代的次数^[16] 为 $l(\alpha) = \log \frac{1}{\alpha}$ 。本地模型在设备 j 上的第 k 次迭代为:

$$\theta_j^k = \theta_j^{k-1} - \eta \nabla F_j(\theta_j^{k-1}) \quad (5)$$

直到满足 $\|\nabla F_j(\theta_j^k)\| \leq \alpha \|\nabla F_j(\theta_j^{k-1})\|$, 其中 η 为学习率。

由此能够得到移动设备 m_j 在一次本地训练的时延和能耗。假设移动设备 j 处理一个数据样本的 CPU 周期数为 τ_j , 则进行一轮本地训练所需的 CPU 周期数为 $\tau_j |C_j|$; 假设移动设备 j 给模型训练分配的 CPU 频率为 f_j , 则进行 $l(\alpha)$ 次迭代的时延为:

$$t_j^{(cmp)} = \frac{l(\alpha) \tau_j |D_j|}{f_j} \quad (6)$$

能耗为:

$$e_j^{(cmp)} = l(\alpha) \frac{\alpha_j}{2} f_j^2 \tau_j |D_j| \quad (7)$$

其中, $\frac{\alpha_j}{2}$ 表示移动设备 j 计算芯片组的有效电容系数。

移动设备 j 将模型参数上传至边缘服务器 i 时,模型参数的数据规模为 S , 传输速率为 $r_j = B \ln \left(1 + \frac{h_j p_j}{N_0} \right)$, 则移动设备 j 向边缘服务器 m_i 传递参数时的传输时延为 $t_{ij}^{(com)} = \frac{S}{r_j}$ 。

移动设备 j 的传输功率定义为 p_j , 则移动设备 m_j 向边缘服务器 i 传递参数过程中的能耗为 $e_{ij}^{(com)} = \frac{s \cdot p_j}{r_j}$ 。

因此,本地模型向边缘服务器传输时,移动设备 m_i 的总时延和总能耗分别为:

$$t_j = \max_{i \in E} \{t_{ij}^{(com)} + t_j^{(cmp)}\} \quad (8)$$

$$e_j = \sum_{i \in E} \{e_{ij}^{(com)} + e_j^{(cmp)}\} \quad (9)$$

3.3 问题定义

参与者 i 的类型表示为 $\omega_i = (a_i, d_i, b_i)$, 其中 a_i 表示参与者 i 的到达时间, d_i 表示参与者 i 的离开时间, b_i 表示参与者 i 在 $t \in [a_i, d_i]$ 时期区间对模型训练的估值。到达时间为参与者初次愿意参与模型的时间,离开时间为参与者最后愿意参与模型的时间。若 $b_i < 0$, 则表明该参与者为移动设备; 若 $b_i > 0$, 则表明该参与者为边缘服务器。定义 q_i 为参与者 i 的供应量或需求量。对于移动设备来说, q_i 指其同时并发训练 q_i 个边缘服务器下发的局部模型; 对于边缘服务器来说, q_i 指其最多有 q_i 个移动设备参与模型训练。

假设 Ω_i 表示参与者 i 所有可能类型的集合。 ω_i 为参与者 i 的私人信息。记 $\Omega = \bigcup_{i \in E \cup M} \Omega_i$, $\Omega_{-i} = \bigcup_{j \neq i, j \in E \cup M} \Omega_j$, $\omega = (\omega_1, \omega_2, \dots, \omega_l, \dots)$, $\omega_{-i} = (\omega_1, \omega_2, \dots, \omega_{i-1}, \omega_{i+1}, \dots)$, ω'_i 为到达时间在第 $t \in T$ 时期及之前的所有参与者类型, ω'_{-i} 为除参与者 i 以外到达时间在第 $t \in T$ 时期及之前的所有参与者类型。

由于类型为私人信息,为了自身利益,理性的参与者可能报告虚假的类型。由于到达时间为参与者首次愿意参与模型训练的时间,因此参与者不可能在 a_i 之前参与模型训练,

参与者 $i \in E \cup M$ 可能报告的类型集合为:

$$A(\omega_i) = \{ \hat{\omega}_i = (\hat{a}_i, \hat{d}_i, \hat{b}_i) \mid i \in E \cup M, \hat{a}_i \leq \underline{a}_i \leq \hat{d}_i, \hat{b}_i \in (\underline{b}_i, \bar{b}_i) \} \subseteq \Omega_i \quad (10)$$

定义在线双边拍卖机制的分配规则为:

$$X = \{ x_i^t(\omega') \mid t \in T, i \in E \cup M \} \quad (11)$$

支付规则为:

$$P = \{ p_i^t(\omega') \mid t \in T, i \in E \cup M \} \quad (12)$$

其中,当参与者 i 是边缘服务器时, $x_i^t(\omega')$ 表示第 t 时期参与模型训练的移动设备数;当参与者 i 是移动设备时, $x_i^t(\omega')$ 表示第 t 时期参与模型训练的次数。若 $p_i^t(\omega') < 0$, $-p_i^t(\omega')$ 表示移动设备 i 在第 t 时期模型训练所得到的回报;若 $p_i^t(\omega') > 0$, $p_i^t(\omega')$ 表示边缘服务器 i 为移动设备在第 t 时期参与模型训练所支付的价格。

记 $x_i(\omega) = \sum_{t \in [a_i, d_i]} x_i^t(\omega')$ 为整个 T 时期参与者 i 的所有模型训练的次数, $p_i(\omega) = \sum_{t \in [a_i, d_i]} p_i^t(\omega')$ 为参与者 i 的支付价格。假设参与者的效用是拟线性的,当参与者报告真实类型 ω_i 时,其效用为:

$$u_i(\omega) = x_i(\omega_i, \omega'_{-i})(b_i - p_i(\omega_i, \omega'_{-i})) \quad (13)$$

在实际情况下,由于参与者报告虚假类型会导致拍卖机制不可行,因此,为了保证机制的可行性,需要设计一种满足激励相容性的机制,使参与者报告真实类型。当拍卖机制运作时,不论其余参与者如何报价,参与者均可以通过真实报告到达时间、离开时间以及估值来获得最大效用。

定义 1(激励相容性) 若对于所有的参与者 $i \in E \cup M$, $\omega_i \in \Omega_i$, $\hat{\omega}_i \in A(\omega_i)$, $\omega'_{-i} \in A(\omega_{-i})$, 有:

$$x_i(\omega_i, \omega'_{-i})(b_i - p_i(\omega_i, \omega'_{-i})) \geq x_i(\hat{\omega}_i, \omega'_{-i})(b_i - p_i(\hat{\omega}_i, \omega'_{-i})) \quad (14)$$

则称在线双边拍卖机制中对于参与者 i 是满足激励相容的。

为了吸引参与者参与拍卖,要求对参与者的效用非负,即所设计的机制满足个体理性。

定义 2(个体理性) 若对于所有的参与者 $i \in E \cup M$, $t \in T$, $\omega \in \Omega$, 有:

$$x_i(\omega_i, \omega'_{-i})(b_i - p_i(\omega_i, \omega'_{-i})) \geq 0 \quad (15)$$

则称在线双边拍卖机制对于参与者是满足个体理性的。

为了使每个时期的参与者获得收益,即对于边缘服务器来说,需要得到更好的训练结果,对于移动设备来说,需要得到更多的回报,因此所设计的机制需要满足弱预算平衡约束,即在每个时期参与者的收益之和非负。

定义 3(弱预算平衡约束) 若对于所有的 $\forall t \in T, \forall \omega \in \Omega$, 有:

$$\sum_{i: a_i \leq t \leq d_i} x_i^t(\omega') p_i^t(\omega') \geq 0 \quad (16)$$

则称该在线双边拍卖机制是满足弱预算平衡约束的。

根据计算与通信模型中能耗的分析,若需要使全局迭代的能耗最小化,则需要使所有移动设备的能耗之和最小化。因此,定义如下优化问题:

$$\min \sum_{t \in T} \sum_{i \in E} \sum_{j \in M_t} e_{ij} x_{ij}^t$$

$$\text{s. t. C1: } \sum_{i \in E} \sum_{j \in M_t} \omega_{ij}^k x_{ij}^t \leq q_k, k \in M, t \in T$$

$$\text{C2: } \sum_{j \in M_t} x_{ij}^t = 1, i \in E, t \in T$$

$$\text{C3: } t_j \leq t_{\max}$$

$$\text{C4: } x_{ij}^t \in \{0, 1\}, i \in E, j \in M_t, t \in T$$

$$\text{C5: } x_i^t(\omega') = \sum_{i \in E} x_{ij}^t, j \in M, t \in T$$

$$\text{C6: } x_i(\omega_i, \omega'_{-i})(b_i - p_i(\omega_i, \omega'_{-i})) \geq$$

$$x_i(\hat{\omega}_i, \omega'_{-i})(b_i - p_i(\hat{\omega}_i, \omega'_{-i})), i \in E \cup M$$

$$\text{C7: } x_i(\omega_i, \omega'_{-i})(b_i - p_i(\omega_i, \omega'_{-i})) \geq 0, i \in E \cup M$$

$$\text{C8: } \sum_{i: a_i \leq t \leq d_i} x_i^t(\omega') p_i^t(\omega') \geq 0, t \in T \quad (17)$$

其中, e_{ij} 表示分配到边缘服务器 i 下移动设备 j 的能耗; $x_{ij} = 1$ 表示移动设备 j 分配到边缘服务器 i 下, $x_{ij} = 0$ 表示移动设备 j 没有分配到边缘服务器 i 下; ω_{ij}^k 表示移动设备 k 是否在 M_t 中,当 $k \in M_t$ 时, $\omega_{ij}^k = 1$, 当 $k \notin M_t$ 时, $\omega_{ij}^k = 0$; C1 表示对于每一个移动设备 k 所能并发训练的模型数不能超过其最大值 q_k ; C2 表示分配到边缘服务器 i 下的移动设备 j 不能相同; C3 表示模型训练时间不能超过联邦学习的最大容忍时间。

4 在线双边拍卖机制设计

为了使所有移动设备能耗之和最小化,设计了有效的在线双边拍卖机制。在本文设计的在线拍卖机制中,移动设备计算本地训练的时延和能耗,从而确定模型的训练成本,得到移动设备的类型。移动设备将自身的类型上传至邻近的多个边缘服务器,边缘服务器选择合适的移动设备,并定义分配规则和支付规则。

4.1 在线双边拍卖机制设计

4.1.1 移动设备的报价

移动设备在向边缘服务器发送本地模型更新时,需考虑分层联邦学习的最大容忍时间。本文提出在一定时延约束下,对移动设备 j 的能耗进行最小化。优化问题的定义如下:

$$\text{P1: } \min e_{ij}$$

$$\text{s. t. C1: } t_j \leq t_{\max}$$

$$\text{C2: } f_j \in [f_j^{\min}, f_j^{\max}]$$

$$\text{C3: } p_{ij} \leq p_{ij}^{\max} \quad (18)$$

其中, C1 指模型的本地训练时间不能超过最大容忍时间; C3 指传输功率不能超过最大值。

优化问题 P1 是一个易求解优化问题^[17],通过求解该问题,可以得到移动设备 j 在一定时延约束下的最小能耗 e_{ij}^* ,从而可以计算移动设备 j 的报价 $b_i = \gamma e_{ij}^*$,其中 γ 为常数。边缘服务器 i 的报价,即边缘服务器 i 对其训练局部模型的移动设备给出的预算。

4.1.2 移动设备选择时间的确定

对于每一个边缘服务器 i ,为了使参与其局部模型训练的移动设备的平均能耗最小化,需要在最佳的时刻选择一定数量的移动设备。因此,为了选择最佳的时刻,需要利用最优停止理论^[18]。定义 t_i^k 为边缘服务器 i 从开始选择移动设备到本轮模型训练结束时的耗时,其中 k 为轮次。因此,提出以下优化问题:

$$\begin{aligned} \text{P2: } \min & \frac{1}{|M_i^k|} \sum_{j \in M_i^k} e_j & (19) \\ \text{s. t. } \text{C1: } & t_i^k - t_{M_i^k}^{(\text{edge})} \leq t'_{\max} \\ & \text{C2: } \cup M_i^k = M_i \end{aligned}$$

其中, C1 表示边缘服务器在选择移动设备时的等待时间不能超过最大等待时间 t'_{\max} ; M_i^k 表示边缘服务器 i 第 k 轮参与模型训练的所有移动设备的集合。

在优化问题 P2 中, 由于 t_i^k 无法提前确定, 因此可利用最优停止理论求解该问题。在最大等待时间 t'_{\max} 的约束下, 边缘服务器需要选择已到达的移动设备参与模型训练。为了最小化模型全局训练的能耗, 使已到达移动设备的平均能耗达到最小。在最优停止理论中, 放过 k 个应聘者后见优则录的秘书问题能够实现这一问题。当 $k = \lfloor \sqrt{N} \rfloor - 1$, 遇到比前 k 个移动设备能耗更小的移动设备时, 已到达移动设备的平均能耗最小^[19]。而本文中, 在最大等待时间 t'_{\max} 下, 仍没有遇到比前 k 个移动设备能耗更小的移动设备, 因此在最大等待时间 t'_{\max} 下的所有移动设备中进行选择。

4.1.3 边缘服务器与移动设备的选择

现在引入基于有效价格的边缘服务器与移动设备的选择规则, 根据到达时间、出发时间和报价来决定参与模型训练的移动设备及其支付规则。

定义 4(有效价格) 有效价格表示边缘服务器对选择参与模型训练的移动设备的支付价格, 与移动设备的类型无关。参与者 i 在 $t \in T$ 时期的有效价格为 $v_i^t(\omega^t)$ 。

定义 5(活跃状态) 若 $t \in [a_i, d_i]$, $q_i > \sum_{\tau \in [a_i, t-1]} x_i^\tau(\omega^\tau)$ 且 $b_i > \max_{\tau \in \{\max(d_i - \lambda, 0), \dots, t-1\}} v_i^\tau(\omega^\tau)$, 则称参与者 i 在 $t \in T$ 时期处于活跃状态。

在参与者 i 的类型 ω_i 中, 当参与者 i 为移动设备时, b_i 为移动设备训练一个模型所需的成本; 当参与者 i 为边缘服务器时, b_i 为训练局部模型对移动设备的预算。

在单个时间周期 t 内的拍卖过程为:

步骤 1 对于每一个参与者 i 满足 $t \in [a_i, d_i]$, $q_i > \sum_{\tau \in [a_i, t-1]} x_i^\tau(\omega^\tau)$ 且 $b_i > \max_{\tau \in \{\max(d_i - \lambda, 0), \dots, t-1\}} v_i^\tau(\omega^\tau)$, 将其放入活跃状态集 C' 。当 $t=0$ 时, 活跃状态集为 $C' = \{i | i \in E \cup M, a_i = 0\}$ 。对于所有处于活跃状态的参与者 i , 初始化 $x_i^t(\omega^t) = 0$, 参与模型训练的移动设备集初始化为 $M' = \emptyset$ 。

步骤 2 当处于活跃状态的移动设备 j 将其类型 ω_j 上传至多个边缘服务器后, 边缘服务器 i 在所有与其通信的移动设备集 M_i' 中, 将移动设备报价 $b_j^{(m)}$ 的绝对值按降序排列。根据移动设备 j 的报价 $b_j^{(m)}$ 与边缘服务器 i 对移动设备 j 的预算 $b_i^{(e)}$ 之间的关系, 分为如下两种情况:

(1) 当移动设备 j 的报价大于边缘服务器 i 的预算, 即 $-b_j^{(m)} > b_i^{(e)}$ 时, 找到满足以下条件的移动设备 k 和边缘服务器 r :

$$b_r^{(e)} \geq -b_k^{(m)} \geq b_{r+1}^{(e)}, \sum_{o=1}^{k-1} q_o^{(m)} \leq \sum_{n=1}^r q_n^{(e)} \leq \sum_{o=1}^k q_o^{(m)} \quad (20)$$

或

$$-b_{k+1}^{(m)} \geq b_r^{(e)} \geq -b_k^{(m)}, \sum_{n=1}^{r-1} q_n^{(e)} \leq \sum_{o=1}^k q_o^{(m)} \leq \sum_{n=1}^r q_n^{(e)} \quad (21)$$

此时, 在 t 时期有效价格如下:

$$v_i^t(\omega^t) = \begin{cases} b_k^{(m)}, & i \in M \\ b_r^{(e)}, & i \in E \end{cases} \quad (22)$$

(2) 当移动设备 j 的报价小于边缘服务器 i 的预算, 即 $-b_j^{(m)} < b_i^{(e)}$ 时, 在 t 时期有效价格如下:

$$v_i^t(\omega^t) = \begin{cases} b_i^{(e)}, & i \in M \\ b_i^{(e)}, & i \in E \end{cases} \quad (23)$$

步骤 3 在 t 时期, 当处于活跃状态的移动设备 j 的报价 $b_j^{(m)} > v_j^t(\omega^t)$, 边缘服务器 i 的预算 $b_i^{(e)} > v_i^t(\omega^t)$ 时, 移动设备 j 将参与边缘服务器 i 的局部模型训练, 并且定义参与模型训练的移动设备集 $M' = M' \cup \{j\}$ 。移动设备 j 和边缘服务器 i 将得到分配, 即 $x_j^t(\omega^t) = x_j^t(\omega^t) + 1$, $x_i^t(\omega^t) = x_i^t(\omega^t) + 1$ 。

步骤 4 对于参与局部模型训练的移动设备, 边缘服务器对其的支付价格为:

$$p_i^t(\omega^t) = \max_{\gamma \in \{\max(d_i - \lambda, 0), \dots, t\}} v_i^\gamma(\omega^\gamma) \quad (24)$$

根据支付价格的定义, 对于边缘服务器来说, 参与模型训练的移动设备的支付价格低于其预算; 对于移动设备来说, 需要付出的成本低于其报价。

边缘服务器与移动设备的具体选择流程如算法 1 所示。

算法 1 基于在线双边拍卖机制的移动设备与边缘服务器选择算法(ODAM-DS)

输入: 参与者 i 的类型, 其供应量或需求量 q_i

输出: 分配规则 $x_i^t(\omega^t)$, 支付规则 $p_i^t(\omega^t)$

1. for $t \in T$ do
2. for $i \in E \cup M$
3. 计算有效价格 $v_i^t(\omega^t)$
4. $x_i^t(\omega^t) = 0$
5. if $t \in [a_i, d_i]$ and $q_i > \sum_{\tau \in [a_i, t-1]} x_i^\tau(\omega^\tau)$ and $b_i > \max_{\tau \in \{\max(d_i - \lambda, 0), \dots, t-1\}} v_i^\tau(\omega^\tau)$ then
6. $C' \leftarrow i$
7. end if
8. if $b_i > v_i^t(\omega^t)$ then
9. $x_i^t(\omega^t) = x_i^t(\omega^t) + 1$
10. $p_i^t(\omega^t) = \max_{\gamma \in \{\max(d_i - \lambda, 0), \dots, t\}} v_i^\gamma(\omega^\gamma)$
11. end if
12. end for
13. end for
14. return $x_i^t(\omega^t), p_i^t(\omega^t)$

算法 1 中, 边缘服务器和移动设备共同作为参与者进行在线双边拍卖, 基于有效价格实现边缘服务器和移动设备的选择。

4.2 在线双边拍卖机制的理论分析

本节通过理论分析证明了所提出的 O DAM-DS 算法满足激励相容性、个体理性、弱预算平衡约束的特性, 并对其时间复杂度进行了分析。

定理 1 对于所有的参与者, O DAM-DS 算法满足激励相容性。

证明: 当参与者满足激励相容性, 即当参与者报告真实

类型时,所产生的效用最大,而参与者报告虚假类型时,会出现以下两种情况。

(1)参与者 i 会报告虚假的报价 b_i' 。

当 $b_i' \geq v_i(\omega')$ 时,根据分配规则和支付规则,参与者 i 得到的分配和支付价格与真实报价时得到的相同。因此,参与者 i 的效用不变。当 $b_i' < v_i(\omega')$ 时,参与者 i 将无法参与模型训练,从而使效用为 0。

(2)参与者 i 会报告虚假的到达时间或离开时间。

当参与者报告虚假的到达时间 a_i' 或离开时间 d_i' 时,根据本文提出的在线拍卖机制,有 $a_i' > a_i$ 或 $d_i' < d_i$ 。这样会使得参与者 i 参与模型训练的时间比报告真实类型的时间短,从而导致效用更低。

综上所述,ODAM-DS 算法对于所有的参与者满足激励相容性。

定理 2 对于所有的参与者,ODAM-DS 算法满足个体理性。

证明:对于参与模型训练的参与者 i ,其报价 $b_i > \max_{\gamma \in \{\max(d_i - \lambda, 0), \dots, t-1\}} v_i^\gamma(\omega^\gamma)$ 。由分配规则,该参与者 i 将得到分配 $x_i^t(\omega') \geq 0$ 。由支付规则,参与者 i 的支付价格 $p_i^t(\omega') > b_i$ 。因此,在 t 时期,参与者 i 的效用为 $u_i^t(\omega') = (b_i - p_i^t(\omega')) x_i^t(\omega') \geq 0$ 。

对于未参与模型训练的参与者 i ,参与者 i 将得到分配 $x_i^t(\omega') = 0$,支付价格为 $p_i^t(\omega') = 0$ 。因此,参与者 i 的效用为 $u_i^t(\omega') = 0$ 。

综上所述,在 t 时期,所有的参与者 i 的效用为 $u^t(\omega') \geq 0$ 。因此,对于所有的参与者,ODAM-DS 算法满足个体理性。

定理 3 O DAM-DS 算法满足弱预算平衡约束。

证明:根据本文提出的在线拍卖机制,在 t 时期,对于边缘服务器 i 的有效价格 $v_i^t(\omega') = b_i^{(e)}$ 和移动设备 j 的有效价格 $v_j^t(\omega') = b_j^{(m)}$ 。根据有效价格的定义可知,无论在何种情况下,都有 $b_i^{(e)} \geq b_j^{(m)}$,因此可得 $b_i^{(e)} + b_j^{(m)} \geq 0$ 。

根据支付规则, t 时期对于每一个参与者 i 的支付价格 $p_i^t(\omega') = \max_{\gamma \in \{\max(d_i - \lambda, 0), \dots, t\}} v_i^\gamma(\omega^\gamma)$ 。由此可知, t 时期总支付 $\sum_{i \in MUE} p_i^t(\omega') \geq 0$ 。又根据分配规则,有 $\sum_{i \in E} x_i^t(\omega') = \sum_{j \in M'} x_j^t(\omega')$ 。因此,对于参与模型训练的参与者,有 $\sum_{i \in E} x_i^t(\omega') p_i^t(\omega') + \sum_{j \in M'} x_j^t(\omega') p_j^t(\omega') \geq 0$ 。

对于没有参与模型训练的移动设备 j ,有 $p_j^t(\omega') = 0$, $x_j^t(\omega') = 0$ 。

因此,在所有的时期,有:

$$\sum_{t \in T} \sum_{i \in EUM} x_i^t(\omega') p_i^t(\omega') \geq 0 \quad (25)$$

综上所述,ODAM-DS 算法满足弱预算平衡约束。

定理 4 O DAM-DS 算法的时间复杂度为 $O(|T| \times (n+l))$ 。

证明:根据 O DAM-DSO($|T| \times (n+l)$)算法,在 $|T|$ 个时间周期内有 $n+l$ 个参与者,其中包括 n 个边缘服务器和 l 个移动设备。这一过程通过两次嵌套循环实现。在内层循环中循环 $n+l$ 次,在外层循环中循环 $|T|$ 次,因此 O DAM-DS

算法的时间复杂度为 $O(|T| \times (n+l))$ 。

5 实验分析

基于仿真实验,对基于在线拍卖机制提出的 O DAM-DS 算法进行分析。考虑在 60 个移动设备、10 个边缘服务器和 1 个云服务器下的分层联邦学习。假设每个移动设备最多并行训练 2 个模型,每个边缘服务器最多需要 10 个移动设备,移动设备随机到达和离开, $\gamma=3$,边缘服务器对每个移动设备的预算和成本分别服从 $[1,8]$ 和 $[1,5]$ 上的均匀分布。假设每个移动设备的训练样本的数据量相同,每个模型训练任务为在标准数据集 MNIST 上的图像分类任务,并将所有的移动设备与边缘服务器随机分布在 $100\text{m} \times 100\text{m}$ 的区域内。

移动设备与边缘服务器之间参数传递时的信道带宽为 $B=10\text{MHz}$,噪声功率为 10^{-8}W ,信道增益为 10^{-8} 。每个移动设备的传输功率为 200mW ,CPU 频率范围为 $1 \sim 10\text{GHz}$,执行一个样本的 CPU 周期数为 $30 \sim 100\text{cycle/bit}$,每个移动设备计算芯片组的有效电容系数为 2×10^{-8} 。

为了验证最优停止理论能够降低边缘服务器下移动设备的平均能耗,对有无基于最优停止理论的能耗进行比较。在无须等待的条件下以及基于最优停止理论后,每个边缘服务器下移动设备平均能耗的比较结果如图 2 所示。由图 2 可知,基于最优停止理论的每个边缘服务器下移动设备的平均能耗低于在无须等待的条件下的平均能耗,且平均降低了 12.29%。是否采用最优停止理论随着训练轮次增加的能耗变化比较结果如图 3 所示。

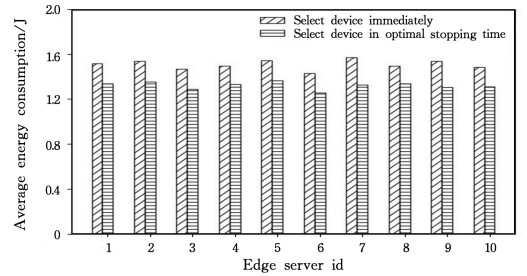


图 2 有无基于最优停止理论的能耗比较

Fig. 2 Comparison of energy consumption with and without optimal stopping theory

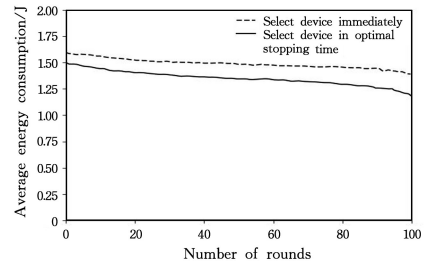


图 3 有无基于最优停止理论的能耗变化比较

Fig. 3 Comparison of energy consumption with and without optimal stopping theory with the increase of rounds

由图 3 可知,随着训练轮次的增加,与无须等待的条件下移动设备的平均能耗最大的边缘服务器的能耗相比,在基于最优停止理论后,移动设备能耗最小的边缘服务器的能耗

更低,平均降低了 9.22%。这是由于等待一段时间后,能耗更低的移动设备到达系统,边缘服务器将选择能耗更低的移动设备参与模型训练,并且随着迭代次数的增加,平均能耗逐渐降低。这是由于随着越来越多的移动设备参与模型训练,其中包含能耗更低的移动设备,因此平均能耗逐渐降低。

为了验证采用 ODAM-DS 算法能够降低所有移动设备能耗之和,将 HFEL 算法^[7]和 FMore 算法^[11]作为对比算法。其中,HFEL 是没有采用激励机制的分层联邦学习优化算法。有无在线双边拍卖机制的能耗比较结果如图 4 与图 5 所示。由图 4 可知,本文提出的 ODAM-DS 算法在每个边缘服务器上的能耗比 HFEL 算法更低,平均降低了 19.04%。由图 5 可知,随着模型轮次的增加,与 HFEL 算法和 FMore 算法中能耗最小的边缘服务器的能耗相比,ODAM-DS 算法中能耗最大的边缘服务器的能耗更低,分别平均降低了 13.09%和 10.13%。在图 5 中,在训练刚开始时,ODAM-DS 算法的能耗明显低于 HFEL 算法和 FMore 算法,这是由于 ODAM-DS 算法在训练开始时边缘服务器选择最优移动设备参与模型训练,而在 HFEL 算法中,移动设备选择其邻近的边缘服务器,因此 ODAM-DS 算法的能耗明显低于 HFEL 算法。在 HFEL 中,首先移动设备选择其邻近的边缘服务器,得到每个边缘服务器最优的资源分配,然后调整边缘服务器与移动设备的关联来降低能耗。而在本文引入的在线双边拍卖机制中,不仅移动设备之间相互竞争参与模型训练,边缘服务器之间也相互竞争选择低能耗的移动设备。FMore 算法是,在基于云联邦学习的场景下,云服务器直接通过激励机制选择低能耗的移动设备参与模型训练,此时大量的移动设备将与云服务器进行通信,这将产生大量的能耗。因此,本文提出的 ODAM-DS 算法的性能优于 HFEL 算法和 FMore 算法。

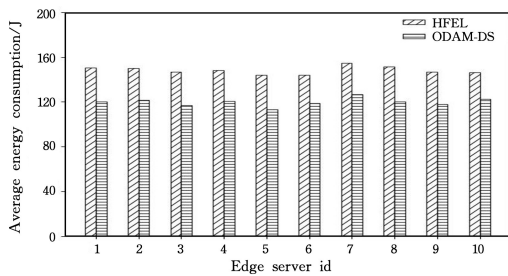


图 4 有无在线双边拍卖机制的能耗比较

Fig. 4 Energy consumption comparison between online double auction mechanism and HFEL

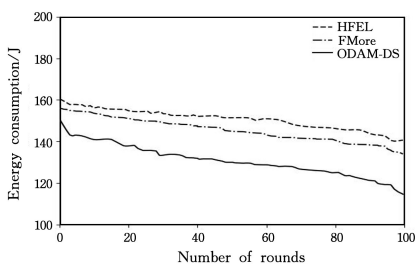


图 5 有无在线双边拍卖机制的能耗变化比较

Fig. 5 Energy consumption comparison between online double auction mechanism and HFEL with the increase of rounds

结束语 在分层联邦学习中,电源受限的移动设备参与模型训练会消耗自身资源。为了降低移动设备的能耗,本文在不超过分层联邦学习的最大容忍时间下,提出了移动设备能耗之和最小化问题。不同训练轮次的边缘服务器能够选择不同的移动设备,移动设备也能够为不同的边缘服务器并发训练模型,因此本文基于在线双边拍卖机制提出了 ODAM-DS 算法。基于最优停止理论,支持边缘服务器在合适的时刻选择移动设备,使得移动设备的能耗最小。通过仿真实验,边缘服务器在基于最优停止理论选择移动设备时产生的能耗比边缘服务器直接选择移动设备时产生的能耗平均降低了 12.29%。本文提出的 ODAM-DS 算法与现有的 HFEL 算法和 FMore 算法相比,能耗分别平均降低了 19.04%和 13.09%。在未来的工作中,移动设备在模型训练时不但会相互竞争,还会相互协作,从而达到更低的能耗。

参考文献

- [1] ZHOU Z, CHEN X, LI E, et al. Edge intelligence: paving the last mile of artificial intelligence with edge computing[J]. Proceedings of the IEEE, 2019, 107(8): 1738-1762.
- [2] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv:1602.05629v2, 2016.
- [3] LIM W Y B, LUONG N C, HOANG D H, et al. Federated learning in mobile edge networks: A comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 2031-2063.
- [4] BONAWITZ K, EICHNER H, GRIESKAM P, et al. Towards federated learning at scale: System design[J]. arXiv:1902.01046, 2019.
- [5] WANG S Q, TOUR T, SALONIDIS T et al. Adaptive federated learning in resource constrained edge computing systems[J]. IEEE Journal on Selected Areas in Communications (JSAC), 2019, 37(6): 1205-1221.
- [6] LIU L, ZHANG J, SONG S H, et al. Client-edge-cloud hierarchical federated learning[J]. arXiv:1095.06641v1, 2019.
- [7] LUO S, CHEN X, WU Q, et al. HFEL: Joint edge association and resource allocation for cost-efficient hierarchical federated edge learning[J]. arXiv:2002.11343, 2020.
- [8] KHAN L U, PANDEY S R, TRAN N H, et al. Federated learning for edge networks: Resource optimization and incentive mechanism[J]. IEEE Communications Magazine, 2020, 58(10): 88-93.
- [9] CHAI H, LENG S, CHEN Y, et al. A Hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(7): 3975-3986.
- [10] ZHAN Y, ZHANG J. An incentive mechanism design for efficient edge learning by deep reinforcement learning approach[C]//IEEE INFOCOM: 2020 IEEE Conference on Computer Communications. Toronto, ON, Canada: IEEE, 2020: 1-10.

- [11] TANG J. Nodes incentive strategy based on bayesian game in Ad Hoc networks[J]. Computer Engineering, 2019, 45(8): 152-158, 164.
- [12] ZHOU Q, LI P, NIE L. User incentive mechanism based on spatial-temporal correlation for crowd sensing[J]. Computer Engineering, 2021, 47(3): 227-236.
- [13] ZENG R, ZHANG S, WANG J, et al. FMore: An Incentive Scheme of Multi-dimensional Auction for Federated Learning in MEC[C] // 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS 2020). Singapore, IEEE, 2020: 278-288.
- [14] ZHANG X, YANG Z, ZHOU Z, et al. Free market of crowd-sourcing: incentive mechanism design for mobile sensing[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(12): 3190-3200.
- [15] LI D, YANG Q, AN D, et al. On location privacy-preserving online double auction for electric vehicles in microgrids[J]. IEEE Internet of Things Journal, 2019, 6(4): 5902-5915.
- [16] ZHAN Y, LI P, QU Z, et al. A learning-based incentive mechanism for federated learning[J]. IEEE Internet of Things Journal, 2020, 7(7): 6360-6368.
- [17] LE T H T, TRAN N H, TUN Y K, et al. Auction based incentive design for efficient federated learning in cellular wireless networks[C] // WCNC: 2020 IEEE Wireless Communications and Networking Conference. Seoul, Korea (South): IEEE, 2020: 1-6.
- [18] PENG Y, WANG G C, HUANG S Q, et al. An energy consumption optimization strategy for data transmission based on optimal stopping theory in mobile network[J]. Chinese Journal of Computers, 2016, 39(6): 1162-1175.
- [19] WANG F S, WANG G C. Study on energy minimization data transmission strategy in mobile cloud computing[C] // SmartWorld/SCALCOM/UIC/ATC/CBDCCom/IOP/SCI: 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation. Guangzhou, China: IEEE, 2018: 1211-1218.



DU Hui, born in 1998, postgraduate. His main research interests include edge computing and so on.



LI Zhuo, born in 1983, Ph.D, associate professor, is a member of China Computer Federation. His main research interests include mobile wireless network and distributed computing.

(责任编辑:柯颖)