

doi: 10.12052/gdutxb.210114

面向6G网络的联邦学习资源协作激励机制设计

蒋 丽¹, 谢胜利¹, 张 彦²

(1. 广东工业大学 自动化学院, 广东 广州 510006; 2. 挪威奥斯陆大学 信息学院, 奥斯陆 0316)

摘要: 第6代(6G)移动通信在满足人类智能通信需求的同时,也给用户数据的安全与隐私保护带来了极大挑战。为此,基于联邦学习的分布式机器学习架构应运而生。然而,在联邦的模型训练过程中,移动设备会产生大量计算和通信开销。自私的移动设备不愿意参与模型训练,这将降低联邦学习性能。本文基于迭代双边拍卖设计了一种有效的联邦学习资源协作激励机制,任务计算终端作为卖方,任务请求终端作为买方,本地接入点根据买卖双方的出价做出模型训练时延和相应定价决策,在买卖双方信息非对称情况下最大化联邦学习市场总效用。仿真实验表明,所提机制具有良好的收敛性,可显著提高联邦学习的准确率,同时降低训练损失。

关键词: 6G网络; 安全与隐私保护; 联邦学习; 资源协作; 迭代双边拍卖

中图分类号: TN929.5 文献标志码: A 文章编号: 1007-7162(2021)06-0047-06

Incentivizing Resource Cooperation for Federated Learning in 6G Networks

Jiang Li¹, Xie Sheng-li¹, Zhang Yan²

(1. School of Automation, Guangdong University of Technology, Guangzhou 510006, China;
2. Department of Informatics, University of Oslo, Oslo 0316, Norway)

Abstract: Recent advances in 6th Generation (6G) mobile networks can meet the needs of deeper intelligent communication. Meanwhile, it also brings great challenges to the security and privacy preservation of user data. Federated learning is emerging as a distributed learning method to preserve privacy by enabling users to train machine learning models locally and requiring the users to upload only model parameters instead of sending original data to the server. However, the users with mobile devices may be unwilling to participate in federated learning tasks due to considerable overhead for computation and communication, which degrades performance and hinders the application of federated learning. In this study, an iterative double auction is designed based on resource cooperation scheme to incentivize the mobile devices to contribute their resources in federated learning tasks, where model trainers act as sellers and task requesters as buyers. Access point determines optimal training time cost and payment according to the prices offered by the sellers and the buyers. The goal of our incentivizing resource cooperation scheme is to maximize the total utility of federated learning market under information asymmetry. Numerical results show that the proposed scheme can converge to the optimal solution, and also can significantly improve model accuracy and degrade model loss value.

Key words: 6G mobile networks; security and privacy preservation; federated learning; resource cooperation; iterative double auction

为了应对未来海量数据、新兴的服务和动态应用场景的通信需求,学术界、工业界以及政府已启动第6代(6G)移动通信研究计划,通过采用太赫兹和可

见光新频谱技术、全新信道编码、超大规模天线、全自由度双工、空天地海一体化通信等,提供每秒太比特速率、支撑平均每人1 000+无线节点连接,并提供

收稿日期: 2021-07-14

基金项目: 国家重点研发计划项目(2020YFB1807801); 移动通信教育部工程研究中心开放研究项目(cqupt-mct-202003)

作者简介: 蒋丽(1986-),女,特聘副教授,主要研究方向为6G网络和网络内生安全等,E-mail: jiangli@gdut.edu.cn

通信作者: 张彦(1977-),男,教授,博士,欧洲科学院院士,主要研究方向为6G网络和绿色通信等,E-mail: yanzhang@ieee.org

随时随地即时全息连接。随着立体覆盖、极致性能、深度连接、泛在连接、全息连接等6G愿景达成共识,智能终端和网元节点激增、个性化服务定制、多场景多业务动态叠加等问题给网络优化和管理带来严峻挑战。传统以规则式算法为核心的运行机理已无法应对规模和复杂性空前的6G网络。在此背景下,引入人工智能,借鉴其解决复杂非线性系统问题的能力,以及强大的预测和决策能力,能够促进网络智能化升级,突破无线网络发展瓶颈^[1-3]。

近年,人工智能和大数据挖掘技术的快速发展,为应对6G复杂挑战提供了有效助力。通过在网络终端、网元节点与网络架构、网络承载业务等多个层次嵌入智能,同时将人工智能的逻辑嵌入到网络结构中,使网络组件能够自主连接和控制,并能自动进行网络配置、自主分析和决策、主动优化网络故障,最终实现网络的自主发展,构建智慧内生的6G网络。有关无线网络智能化的研究和标准化工作已成为业界的研究热点。2020年11月中兴通讯发布首份无线网络智能化白皮书,通过在无线网络的规划、建设、维护、优化以及运营等各阶段全面引入人工智能,并基于网络分析、控制和管理三大能力,保障网络连接和性能承诺,实现无线网络的单域自治闭环。然而,人工智能在提高无线网络的效能、灵活性和自治能力的同时,也存在新的安全挑战。在大多数情况下,人工智能任务是在数据中心进行计算和部署的,其中的学习机制需要大量的网络数据训练模型。而这些网络数据除了机密文件、隐私信息,还包含人的生物特征识别信息、家庭电器控制信息、车辆的自动驾驶控制信息等敏感信息。一旦恶意用户攻击数据中心,将会导致这些信息的泄露,进而对用户的财产甚至生命造成威胁^[4]。

联邦学习是一种新兴的分布式机器学习架构^[5]。在联邦学习中,大规模移动设备使用本地存储的数据执行训练任务,并将训练的本地模型参数上传到数据中心聚合。与传统基于数据中心的集中式训练方式相比,联邦学习只需要上传训练好的模型参数,能有效减少数据传输开销,提升对用户隐私数据的保护。目前,谷歌已在谷歌输入法Gboard上测试联邦学习^[6]。当联邦学习应用到未来无线网络中,仍面临着一些严峻的挑战。移动设备有限的资源以及复杂多变的无线传输环境将导致信号严重失真以及模型聚合误差,进而使联邦学习的收敛速率和预测准确率下降。Chen等^[7]研究了无线网络中的联邦学习训练过程,提出联合移动设备选择和无线资源分配的优

化方案,以实现最小化联邦学习损失函数的目标。Ni等^[8]提出使用智能反射面辅助本地模型参数传输,通过优化移动设备的发送功率和智能反射面的相移,以实现最小化联邦学习聚合模型平均均方误差的目标。Lu等^[9]将联邦学习应用到车联网中,通过选择训练精度高和训练速度快的移动车辆完成模型聚合,提高全局模型的预测准确率。但上述研究均忽略了移动设备参与模型聚合的意愿问题。在联邦的模型训练过程中,移动设备会产生大量计算和通信开销。自私的移动设备不愿意无偿参与模型训练,这将使模型聚合样本减少,进而导致全局模型聚合性能下降。针对联邦学习资源协作激励机制的研究相对较少。Le等^[10]提出使用组合拍卖博弈,基站作为买方向移动设备发布训练任务,移动设备作为卖方根据训练任务需要的资源、本地训练准确率以及相应能量开销,向基站提交出价。基站确定竞拍成功者并支付相应报酬。Sun等^[11]研究了联邦学习在无人机网络中的应用,提出使用斯塔克伯格博弈激励地面移动设备参与模型训练。但在实际无线网络中,买卖双方存在信息非对称性,即考虑隐私信息的保护,移动设备作为卖方不愿意向买方揭露自身真实信息,例如可用资源、本地模型训练准确率、模型训练能量开销等。因此,买方难以制定相应报酬。

为了解决以上问题,本文主要研究工作如下。

(1) 在6G无线网络中,构建基于联邦学习的终端到终端(Device to Device, D2D)数据共享框架。本地接入点采集移动终端的任务请求,并将采集的任务请求发布给模型训练终端。模型训练终端根据自身存储的数据训练本地模型,并把训练好的本地模型上传给本地接入点聚合。本地接入点和模型训练终端迭代地训练全局模型,然后将训练好的全局模型反馈给任务请求终端。最后,任务请求终端向模型训练终端支付相应报酬,以补偿模型训练过程中的资源消耗。

(2) 考虑任务请求终端和模型聚合终端之间的信息非对称性,提出基于迭代双边拍卖的资源协作激励机制。模型训练方作为卖方,任务请求方作为买方。本地接入点充当拍卖师,引导买卖双方根据各自联邦学习性能需求以及可用资源出价,并根据买卖双方的出价进行最优模型训练资源分配和定价,以实现最大化联邦学习市场的总效用。

(3) 根据真实数据集,对提出的资源协作激励机制进行仿真实验验证。结果表明,本文提出的基于双边拍卖的联邦学习资源协作激励机制可以提高联邦

学习模型的准确率,并且减少模型训练损失。同时,在买卖双方信息非对称性情况下,最大化联邦学习市场效用。

1 系统模型

本文构建的系统模型如图1所示。考虑6G网络中的D2D通信场景,其中,本地接入点配有边缘计算服务器,具有较强的计算和存储功能。同时,本地接入点部署有人工智能模块,可通过感知、预测、挖掘、推理对多维网络信息进行认知和分析,并做出相应决策。在本地接入点的覆盖范围内,分布有多个智能终端,智能终端之间以D2D通信的方式共享数据。此处的数据共享是指根据本地存储的数据进行联邦的任务计算,并将计算结果反馈给请求方,例如,流行音乐、电影、游戏等多媒体内容的推荐。本地接入点协助建立智能终端用户之间的D2D通信链路。考虑当前有 Q 个任务请求终端,表示为 $Q \triangleq \{1, 2, \dots, Q\}$,任务请求终端 q , $q \in Q$,发送共享数据请求 Req_q 。本地接入点采集共享数据请求,并将采集的共享数据请求发布给 R 个任务计算终端,表示为 $R \triangleq \{1, 2, \dots, R\}$ 。每个任务计算终端存储有任务请求终端需要的数据,存储关于共享数据请求 Req_q 的数据表示为 $\mathcal{D}_q = \{\mathcal{D}_{1q}, \mathcal{D}_{2q}, \dots, \mathcal{D}_{Rq}\}$, $q \in Q$, $\mathcal{D}_{rq} = \{(x_{rq,1}, y_{rq,1}), (x_{rq,2}, y_{rq,2}), \dots, (x_{rq,D_{rq}}, y_{rq,D_{rq}})\}$ 。任务计算终端采用联邦学习完成计算任务。在联邦学习中,任务计算终端根据本地存储的数据 $\mathcal{D}_q$,执行本地模型训练,并将训练好的本地模型参数上传到本地接入点聚合。任务计算终端和本地接入点迭代地交互训练模型,直到获得训练模型 $\mathcal{M}_q$ 和模型参数 w_q ,以实现最小化损失函数 $f(w_q)$ 的目标。具体优化问题构造如下:

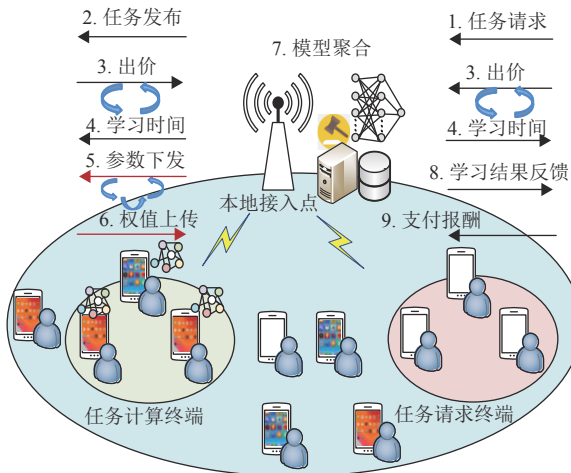


图1 基于迭代双边拍卖的联邦学习框架

Fig.1 Iterative double auction-based federated learning

$$\min_{w_q} \frac{1}{R} \sum_{r=1}^R \frac{1}{\mathcal{D}_{rq}} \sum_{i=1}^{\mathcal{D}_{rq}} f_i(w_q, x_{rq,i}, y_{rq,i}) \quad (1)$$

其中: $f_i(w_q, x_{rq,i}, y_{rq,i})$ 是关于数据样本 $(x_{rq,i}, y_{rq,i})$ 和参数 w_q 的损失函数。

在本地训练过程中,任务计算终端 r , $r \in R$ 根据本地存储的数据 $\mathcal{D}_{rq}$ 使用梯度下降法寻找模型参数 w_{rq} ,以最小化本地训练模型的损失函数。在第 t 次本地训练迭代中,任务计算终端 r 根据模型参数 $w_{rq}(t-1)$ 和本地梯度下降 $\nabla F_{rq}(w_{rq}(t-1))$,训练本地模型参数 $w_{rq}(t)$ 。

$$w_{rq}(t) = w_{rq}(t-1) - \gamma \cdot \nabla F_{rq}(w_{rq}(t-1)), \quad \forall r \in R, q \in Q \quad (2)$$

其中: γ 表示梯度下降的学习速率。任务计算终端 r 发送本地模型参数到本地接入点聚合,以更新全局模型。本地接入点的聚合模型表示为

$$\mathcal{M}_q = \frac{1}{R} \sum_{r=1}^R \mathcal{D}_{rq} w_{rq}, \quad \forall r \in R, q \in Q \quad (3)$$

1.1 联邦学习的计算模型

任务计算终端 r 根据本地存储的数据 $\mathcal{D}_{rq}$ 训练本地模型参数时,贡献的计算资源表示为 f_{rq}^C ,即CPU周期频率。训练一个数据样本需要的CPU周期表示为 c_r 。因此,在本地训练过程中,任务计算终端 r 一次本地迭代的计算时延表示为

$$T_{rq}^{\text{cmp}} = \frac{b_r \mathcal{D}_{rq} c_r}{f_{rq}^C}, \quad \forall r \in R, q \in Q \quad (4)$$

其中: b_r 表示训练数据 $\mathcal{D}_{rq}$ 的批量大小。用 ϑ_r 表示任务终端 r 本地训练的准确率,任务终端 r 本地训练的迭代次数表示为 $\lg\left(\frac{1}{\vartheta_r}\right)^{[12]}$ 。因此,任务终端 r 本地训练的总时延表示为

$$T_{rq}^C = \lg\left(\frac{1}{\vartheta_r}\right) T_{rq}^{\text{cmp}} \quad (5)$$

1.2 联邦学习的通信模型

每个任务计算终端使用正交频分多址接入技术(Orthogonal Frequency Division Multiple Access, OFDMA)将训练的本地模型参数发送到本地接入点聚合。任务终端 r 分配到的子信道表示为 W_{rq} ,每个子信道的带宽均为 W_0 。从任务计算终端 r 到本地接入点的数据速率表示为

$$R_{rq} = \sum_{s=1}^{W_{rq}} W_0 \log_2 \left(1 + \frac{P_{rq}^s |h_{rq}^s|^2}{\sum_{r' \in R \setminus \{r\}} P_{r'q}^s |h_{r'q}^s|^2 + N_0} \right) \quad (6)$$

其中, P_{rq}^s 表示任务计算终端 r 在子信道 s 上的发送功率, $s \in W_{rq}$; $|h_{rq}^s|^2$ 表示任务计算终端 r 到本地接入点子信道 s 的信道增益; $\sum_{r' \in \mathcal{R} \setminus \{r\}} P_{r'q}^s |h_{r'q}^s|^2$ 表示任务终端 r' 共用子信道 s 产生的干扰; N_0 表示噪声功率。任务终端 r 发送本地训练模型参数的时延表示为

$$T_{rq}^{\text{trans}} = \frac{|w_{rq}|}{R_{rq}} \quad (7)$$

其中: $|w_{rq}|$ 表示本地训练模型参数的大小。根据式(5)和式(7),任务计算终端 r 参与联邦学习一次全局迭代的时延表示为

$$T_{rq}^{\text{gt}} = T_{rq}^{\text{C}} + T_{rq}^{\text{trans}} \quad (8)$$

基于以上分析,如果任务计算终端在本地训练过程中贡献更多计算资源,同时在本地图模型参数传输过程中分配更多通信资源,例如分配更多发送功率和子信道等,式(2)中本地模型训练和式(3)中全局模型训练的收敛速率会加快。然而,任务计算终端资源有限,而且其处理自身数据业务也需要消耗资源。因此,为了激励任务终端贡献资源参与联邦学习,有必要设计合适的资源协作激励机制,以补偿任务终端的资源消耗。

2 基于迭代双边拍卖的联邦学习资源协作激励机制

本文提出基于迭代双边拍卖的联邦学习资源协作激励机制,以激励任务计算终端贡献自身资源参与联邦学习的模型训练。迭代双边拍卖广泛用于经济学中,解决信息非对称性情况下的买卖双方交易问题。拍卖师设计合适的价格机制引导买卖双方真实地出价,以揭露买卖双方隐藏的信息,最终实现交易均衡的目标。已有研究^[13]证明迭代双边拍卖具有个体理性、弱预算均衡和高经济效率等特征,适用于具有多个买卖双方的交易场景。

在设计的基于迭代双边拍卖的联邦学习资源协作激励机制中,本地接入点充当拍卖师,任务发布终端和任务计算终端分别充当买方和卖方。考虑任务发布终端 q , $q \in \mathcal{Q}$, 需要任务计算终端 r , $r \in \mathcal{R}$ 在一次全局迭代计算时延为 $T_{qr}^{\text{gt}(-1)}$ 。定义任务请求终端 q , $q \in \mathcal{Q}$ 的请求时延向量为 $\mathbf{T}_{qr}^{\text{gt}(-1)} \triangleq (T_{qr}^{\text{gt}(-1)}; \forall r \in \mathcal{R})$, 任务请求终端 q 的效用函数表示为 $F_q(\mathbf{T}_{qr}^{\text{gt}(-1)})$, $q \in \mathcal{Q}$, 此处的效用函数是指任务请求终端在请求时延范围内收到联邦学习结果获的效用。 Q 个任务请求终端的总效用函数表示为 $\sum_{q=1}^Q F_q(\mathbf{T}_{qr}^{\text{gt}(-1)})$, 其中, 效用函数 $F_q(\cdot)$ 是

关于请求时延向量 $\mathbf{T}_{qr}^{\text{gt}(-1)}$ 的递增且严格凹的函数。每个任务计算终端根据每个任务请求终端的请求 Req_q 做出相应响应 Req_r , 而且给出在一次全局迭代的接受时延 $\Gamma_{rq}^{\text{gt}(-1)}$ 。定义任务计算终端 r ($r \in \mathcal{R}$) 的接受时延向量为 $\mathbf{\Gamma}_{rq}^{\text{gt}(-1)} \triangleq (\Gamma_{rq}^{\text{gt}(-1)}; \forall r \in \mathcal{R})$, 任务计算终端 r 的成本函数表示为 $C_r(\mathbf{\Gamma}_{rq}^{\text{gt}(-1)})$, $r \in \mathcal{R}$, 此处的成本函数是指任务计算终端在接受时延范围内参与联邦学习模型训练产生等资源开销。 R 个任务计算终端的总效用函数表示为 $\sum_{r=1}^R C_r(\mathbf{\Gamma}_{rq}^{\text{gt}(-1)})$, 其中, 效用函数 $C_r(\cdot)$ 是关于接受时延向量 $\mathbf{\Gamma}_{rq}^{\text{gt}(-1)}$ 的递增且严格凹的函数。

2.1 问题构造

可以看出,任务计算终端和任务请求终端的效用函数是相互矛盾的,如果独立地对请求时延和接受时延做决策,难以使双方达成共识。为了解决此困难,本地接入点充当拍卖师,通过构建最大化联邦学习市场总效用的优化问题,求解最优时延向量 $(\mathbf{T}_{qr}^{\text{gt}(-1)}, \mathbf{\Gamma}_{rq}^{\text{gt}(-1)})$ 。具体优化问题构造如下

$$\begin{cases} \max_{\mathbf{T}_{qr}^{\text{gt}(-1)}, \mathbf{\Gamma}_{rq}^{\text{gt}(-1)}} \sum_{q=1}^Q F_q(\mathbf{T}_{qr}^{\text{gt}(-1)}) + \sum_{r=1}^R C_r(\mathbf{\Gamma}_{rq}^{\text{gt}(-1)}) \\ \text{s.t. } \text{C1: } T_{qr}^{\text{gt}(-1)} \geq T_q^{\text{gt}, \max(-1)}, \forall q \in \mathcal{Q}, r \in \mathcal{R}, \\ \text{C2: } \Gamma_{rq}^{\text{gt}(-1)} \leq \Gamma_r^{\text{gt}, \min(-1)}, \forall q \in \mathcal{Q}, r \in \mathcal{R}, \\ \text{C3: } T_{qr}^{\text{gt}(-1)} = \Gamma_{rq}^{\text{gt}(-1)}, \forall q \in \mathcal{Q}, r \in \mathcal{R}, \\ \text{C4: } T_{qr}^{\text{gt}(-1)} \geq 0, \Gamma_{rq}^{\text{gt}(-1)} \geq 0, \forall q \in \mathcal{Q}, r \in \mathcal{R} \end{cases} \quad (9)$$

其中: C1 表示每个任务请求终端的请求时延应满足其能容忍的最大时延 $T_q^{\text{gt}, \max(-1)}$ 。C2 表示每个任务计算终端的接受时延不能超过其最小学习时延 $\Gamma_r^{\text{gt}, \min(-1)}$ 。C3 表示每个任务请求终端的请求时延应和每个任务计算终端的接受时延相等。C4 表示每个任务请求终端的请求时延和每个任务计算终端的接受时延均应大于或等于零。

2.2 问题求解

优化问题式(9)的目标函数是严格凹的函数,限制条件 C1~C4 在可行域范围内是严格凸的^[14]。因此,优化问题有唯一的最优解 $(\mathbf{T}_{qr}^{\text{gt}(-1)\circ}, \mathbf{\Gamma}_{rq}^{\text{gt}(-1)\circ})$ 。优化问题式(9)的 Karush-Kuhn-Tucker (KKT) 条件推导如下。

$$\frac{\partial F_q(\mathbf{T}_{qr}^{\text{gt}(-1)\circ})}{\partial T_{qr}^{\text{gt}(-1)}} = \lambda_{qr} + \tau_{qr} \quad (10a)$$

$$\frac{\partial C_r(\mathbf{\Gamma}_{rq}^{\text{gt}(-1)\circ})}{\partial \Gamma_{rq}^{\text{gt}(-1)}} = \tau_{qr} - \sigma_{rq} \quad (10b)$$

式中: λ_{qr} , τ_{qr} 和 σ_{rq} 表示拉格朗日乘子。由于任务请求

终端和任务计算终端不会向本地接入点揭露各自的效用函数 $F_q(\cdot)$ 和 $C_r(\cdot)$,本地接入点无法通过KKT条件求解最优解。因此,本地接入点需要设计合理的价格策略以引导任务请求终端和任务计算终端出价,以揭露各自的隐藏信息。

定义任务请求终端 q , $q \in \mathcal{Q}$ 的出价向量为 $\mathbf{X}_{qr}^{gt} \triangleq (x_{qr}^{gt}; \forall r \in \mathcal{R})$,每个任务计算终端 r , $r \in \mathcal{R}$ 的出价向量为 $\mathbf{Y} \triangleq (y_{rq}^{gt}; \forall r \in \mathcal{R})$ 。这些出价表征了任务请求终端的需求,以及任务计算终端的服务成本。本地接入点根据双方的出价,构造如下新的优化问题,确定最优联邦学习时延。具体优化问题构造如下

$$\begin{cases} \max_{\mathbf{T}_{qr}^{gt(-1)}, \mathbf{Y}_{rq}^{gt(-1)}} \sum_{q=1}^Q \sum_{r=1}^R \left(x_{qr}^{gt} \log_2 T_{qr}^{gt(-1)} - \frac{y_{rq}^{gt}}{2} (\Gamma_{rq}^{gt(-1)})^2 \right) \\ \text{s.t. C1: } T_{qr}^{gt(-1)} \geq T_q^{gt, \max(-1)}, \forall q \in \mathcal{Q}, r \in \mathcal{R}, \\ \text{C2: } \Gamma_{rq}^{gt(-1)} \leq \Gamma_r^{gt, \min(-1)}, \forall q \in \mathcal{Q}, r \in \mathcal{R}, \\ \text{C3: } T_{qr}^{gt(-1)} = \Gamma_{rq}^{gt(-1)}, \forall q \in \mathcal{Q}, r \in \mathcal{R}, \\ \text{C4: } T_{qr}^{gt(-1)} \geq 0, \Gamma_{rq}^{gt(-1)} \geq 0, \forall q \in \mathcal{Q}, r \in \mathcal{R} \end{cases} \quad (11)$$

可以看出,优化问题式(11)和(9)有相同的限制条件,但是优化目标各不相同。根据KKT条件,可推导出以下等式。

$$T_{qr}^{gt(-1)*} = \frac{x_{qr}^{gt}}{\lambda_{qr} + \tau_{qr}} \quad (12a)$$

$$\Gamma_{rq}^{gt(-1)*} = \frac{\tau_{qr} - \sigma_{rq}}{y_{rq}^{gt}} \quad (12b)$$

可以看出,式(12a)~(12b)和式(10a)~(10b)不相同,如果任务请求终端和任务计算终端按照式(13)出价。

$$x_{qr}^{gt} = T_{qr}^{gt(-1)*} \frac{\partial F_q(\mathbf{T}_{qr}^{gt(-1)*})}{\partial T_{qr}^{gt(-1)}} \quad (13a)$$

$$y_{rq}^{gt} = \frac{1}{\Gamma_{rq}^{gt(-1)*}} \frac{\partial C_r(\mathbf{\Gamma}_{rq}^{gt(-1)*})}{\partial \Gamma_{rq}^{gt(-1)}} \quad (13b)$$

优化问题式(11)的最优解和优化问题式(9)的最优解相等,即 $\mathbf{T}_{qr}^{gt(-1)*} \triangleq \mathbf{T}_{qr}^{gt(-1)\circ}$, $\mathbf{\Gamma}_{rq}^{gt(-1)*} \triangleq \mathbf{\Gamma}_{rq}^{gt(-1)\circ}$ 。因此,需要设计合适的价格策略,引导任务请求终端和任务计算终端按照式(13)出价。

定义任务请求终端 q , $q \in \mathcal{Q}$ 的支付函数为 $Z_q(\mathbf{T}_{qr}^{gt(-1)})$,任务请求终端通过求解如下效益函数最大化问题,获得最优出价 x_{qr}^{gt*} 。

$$\begin{cases} \max_{x_{qr}^{gt}} F_q(\mathbf{T}_{qr}^{gt(-1)}) - Z_q(\mathbf{T}_{qr}^{gt(-1)}) \\ \text{s.t. } x_{qr}^{gt} \geq 0, \forall q \in \mathcal{Q}, r \in \mathcal{R} \end{cases} \quad (14)$$

优化问题式(14)的解应满足式(15)条件

$$\frac{\partial F_q(\mathbf{T}_{qr}^{gt(-1)\circ})}{\partial T_{qr}^{gt(-1)}} = \frac{\partial Z_q(\mathbf{T}_{qr}^{gt(-1)\circ})}{\partial x_{qr}^{gt}} = \lambda_{qr} + \tau_{qr} \quad (15)$$

类似地,定义任务计算终端 r , $r \in \mathcal{R}$ 的补偿函数为 $H_r(\mathbf{\Gamma}_{rq}^{gt(-1)})$,任务计算终端通过求解式(16)的效益函数最大化问题,获得最优出价 y_{rq}^{gt*} 。

$$\begin{cases} \max_{y_{rq}^{gt}} H_r(\mathbf{\Gamma}_{rq}^{gt(-1)}) - C_r(\mathbf{\Gamma}_{rq}^{gt(-1)}) \\ \text{s.t. } y_{rq}^{gt} \geq 0, \forall q \in \mathcal{Q}, r \in \mathcal{R} \end{cases} \quad (16)$$

优化问题式(16)的解应满足式(17)条件。

$$\frac{\partial C_r(\mathbf{\Gamma}_{rq}^{gt(-1)})}{\partial \Gamma_{rq}^{gt(-1)}} = \frac{\partial H_r(\mathbf{\Gamma}_{rq}^{gt(-1)})}{\partial y_{rq}^{gt}} = \frac{(y_{rq}^{gt})^2}{\tau_{qr} - \sigma_{rq}} \quad (17)$$

为了引导任务请求终端和任务计算终端按照式(13)出价,相应的价格规则定义为

$$Z_q(x_{qr}^{gt}) = \sum_{q=1}^Q \sum_{r=1}^R x_{qr}^{gt} \quad (18)$$

$$H_r(y_{rq}^{gt}) = \sum_{q=1}^Q \sum_{r=1}^R \frac{(\tau_{qr} - \sigma_{rq})^2}{y_{rq}^{gt}} \quad (19)$$

优化问题式(11)和价格规则式(18)~(19)求出的最优请求时延和最优接受时延,可保证优化问题式(9)实现最大化联邦学习市场效用的目标。可以看出,最优请求时延 $T_{qr}^{gt(-1)*}$ 和最优接受时延 $\Gamma_{rq}^{gt(-1)*}$ 与优化问题式(14)和式(16)的出价有关。因此,优化问题式(11)、(14)和(16)需要迭代地求解。本地接入点初始化请求时延 $T_{qr}^{gt(-1)}$ 、接受时延 $\Gamma_{rq}^{gt(-1)}$ 以及拉格朗日乘子,并广播初始值。每个任务请求终端和任务计算终端根据初始值求解问题式(14)和(16),计算最优出价,并将最优出价发送给本地接入点。然后,本地接入点根据接收的出价更新请求时延 $T_{qr}^{gt(-1)}$ 、接受时延 $\Gamma_{rq}^{gt(-1)}$ 以及拉格朗日乘子。本地接入点、任务请求终端和任务计算终端迭代地求解问题式(11)、(14)和(16),直到请求时延和接受时延收敛。

3 仿真结果

本节通过实验验证提出的基于迭代双边拍卖的联邦学习资源协作激励机制的性能。考虑任务请求终端个数 Q 为5,任务计算终端个数 R 为10。所有终端随机地分布在本地接入点覆盖范围内。采用真实数据集CIFAR10^[15]进行联邦学习实验仿真。任务请求终端最大容忍学习时延 $T_q^{gt, \max(-1)}$ 的取值范围为[200, 300] s,任务计算终端最小接受学习时延 $\Gamma_r^{gt, \min(-1)}$ 的取值范围为[60, 200] s。为了与提出方案对比,设计基于固定价格的资源协作激励机制,即任务请求终端根

据固定单位价格向任务计算终端支付报酬。

图2对比了两种方案的模型训练损失。从图中可以看出,随着全局训练次数增加,两种方案的损失先降低,然后收敛到固定值。提出方案的损失对比方案的损失低,因为提出方案可激励所有任务计算终端贡献资源参与联邦学习。对比方案中,任务计算终端不能获得最大效益,因此,部分任务计算终端不愿意参与联邦学习,上传的本地模型参数减少,导致聚合模型损失增加。

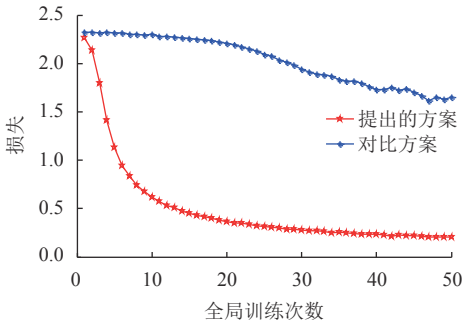


图2 模型训练损失对比

Fig.2 Comparison of training loss of two schemes

图3对比了两种方案的模型准确率。从图中可以看出,随着全局训练次数增加,两种方案的模型准确率先增加,然后收敛到固定值。提出方案的准确率高,因为,提出方案可保证任务计算终端的效益函数最大化,从而激励任务计算终端提供高质量的本地模型参数。对比方案中,任务计算终端不能获得最大的效益,因此,任务计算终端可能提供低质量的本地模型参数,导致聚合模型准确率降低。

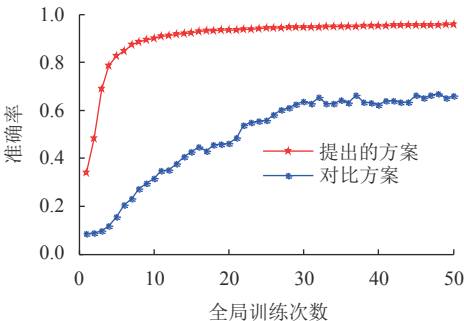


图3 模型准确率对比

Fig.3 Comparison of accuracy of two schemes

图4展示了任务请求终端 q 的请求时延 T_{qr}^{gt} 以及任务计算终端 r 的接受时延 Γ_{rq}^{gt} 。以 $q=1, q=2$ 和 $r=1, r=2$ 为例。从图中可以看出,请求时延与接受时延相等,证明了提出方案的有效性,即 $T_{qr}^{gt} = \Gamma_{rq}^{gt}$ 。此外,在迭代

13次之后,请求时延和接受时延均收敛到最优解。因此,提出方案可以有效引导任务计算终端和任务请求终端真实地出价,以揭露双方的隐藏信息(即双方的效用函数),最终获得最大化联邦学习市场总效用的最优请求时延和接受时延。

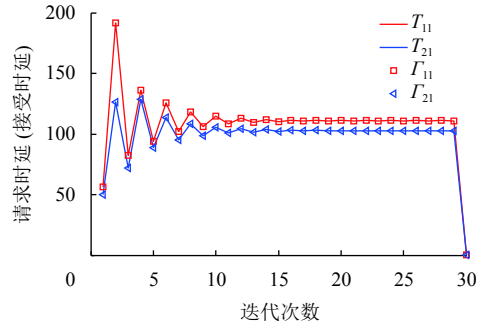


图4 请求时延 T_{qr}^{gt} (接受时延 Γ_{rq}^{gt})

Fig.4 The required learning time T_{qr}^{gt} (The admitted learning time Γ_{rq}^{gt})

4 结论

本文提出了6G网络D2D通信的联邦学习框架。移动终端通过联邦学习实现数据共享。针对自私的移动设备不愿意参与模型训练问题,提出基于迭代双边拍卖的资源协作机制。其中,任务计算终端作为卖方,任务请求终端作为买方,本地接入点根据买卖双方的出价对模型训练时延和定价做出决策,在买卖双方信息非对称情况下最大化联邦学习市场总效用。仿真实验表明,提出的机制可以显著提高联邦学习的准确率,降低训练损失,而且具有良好的收敛性。

参考文献:

[1] 索士强, 王映民. 未来6G网络内生智能的探讨与分析[J]. 移动通信, 2020, 44(6): 126-30.
SUO S Q, WANG Y M. Discussion and analysis on the native intelligence for the future 6G network [J]. Mobile Communications, 2020, 44(6): 126-30.

[2] 孙耀华, 王则予, 袁硕, 等. 智能内生6G网络: 架构、用例和挑战[J]. 电子技术应用, 2021, 47(3): 8-13.
SUN Y H, WANG Z Y, YUAN S, et al. The sixth-generation mobile communication network with endogenous intelligence architectures, use cases and challenges [J]. Application of Electronic Technique, 2021, 47(3): 8-13.

[3] 郑思远, 崔苗, 张广驰. 基于强化学习的无人机安全通信轨迹在线优化策略[J]. 广东工业大学学报, 2021, 38(4): 60-64.
ZHENG S Y, CUI M, ZHANG G C. Reinforcement learning-based online trajectory optimization for secure UAV communications [J]. Journal of Guangdong University of Technology, 2021, 38(4): 60-64.