面向无线边缘网络的分层Stackelberg博弈群体激励方法

康海燕,冀珊珊
(北京信息科技大学信息管理学院,北京 100192)

摘 要: 现有分布式机器学习模型的相关激励机制大多基于单层服务器架构,难以适应当前异构无线计算场景,同时存在计算资源分配不平衡、通信成本高昂等问题. 针对上述问题,创新地提出一种面向无线边缘网络的分层Stackelberg博弈群体激励方法(Hierarchical Stackelberg game Swarm Learning Incentive method for wireless edge network, HSISL),创新地将Stackelberg博弈机制引入群体学习模型中,依据各参与方性能差异,云端聚合平台、边缘簇节点、边缘计算节点三方进行动态博弈,通过双定价公平激励过程,共同制定个性化分层资源分配策略,得到模型训练的最优纳什解,有效引导边缘计算模型进行正向加速. 通过理论与实验分析,HSISL能够有效提升模型公平性与训练效率,其在MNIST数据集上的准确率可达96.06%.

关键词: 数据共享;群体学习;Stackelberg博弈;动态博弈;无线网络通信;激励机制
基金项目: 国家社科基金(No.21BTQ079);教育部人文社科基金(No.20YJAZH046);国家自然科学基金(No.61370139)
中图分类号: TP391.9;TN929.52 **文献标识码:** A **文章编号:** 0372-2112(2024)07-2382-11
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20231158

Hierarchical Stackelberg Game Swarm Learning Incentive Method for Wireless Edge Network

KANG Hai-yan, JI Shan-shan
(*School of Information Management, Beijing Information Science and Technology University, Beijing* 100192, *China*)

Abstract: In today's rapidly evolving landscape of distributed machine learning, conventional data incentive solutions often fall short due to their reliance on simplistic single-server architectures, in addition, as computing environments become increasingly complex, particularly within the context of heterogeneous wireless networks, these traditional approaches struggle to meet the dynamic computational demands such as unbalanced resource allocation and exorbitant communication costs. In response to the above dilemma, this paper innovatively proposes a hierarchical Stackelberg game swarm learning incentive method for wireless edge network (HSISL). This paper innovatively introduces the Stackelberg game mechanism into the swarm learning. Based on the performance differences of each computing terminal, the cloud aggregation platform, edge cluster nodes, and edge computing nodes conduct dynamic games and jointly formulate personalized hierarchical resource allocation strategies through the fair incentive process of dual pricing, which can effectively guide the edge computing model to accelerate forward. Through theoretical and experimental analysis, the HSISL method can obtain the optimal incentive Nash equilibrium solution for model training. Compared with other incentive methods, the HSISL method can effectively improve the fairness of the model. With training efficiency, its accuracy on the MNIST data set can reach 96.06%.

Key words: data sharing; swarm learning; Stackelberg game; dynamic games; wireless network communication; incentives
Foundation Item(s): National Social Science Foundation of China (No.21BTQ079); Humanities and Social Sciences of the Ministry of Education (No.20YJAZH046); National Natural Science Foundation of China (No.61370139)

收稿日期:2023-12-12;修回日期:2024-04-08;责任编辑:覃怀银

1 引言

人工智能驱动型生产模式的兴起,数据隐私威胁也逐渐显现,随着隐私法规的完善与用户隐私意识的觉醒,近年来,数据安全协作领域相关研究数量呈爆炸性增长,群体学习(Swarm Learning,SL)[1]与联邦学习(Fedreated Learning,FL)应运而生,并且已取得了一些技术进展[2~10],但现有相关方案仍面临计算资源贡献不足等问题,特别是在无线边缘网络等复杂计算环境下,计算终端通常在接近数据源的位置执行计算任务,这需要更低的传输延迟与网络负载,否则会严重影响协作效率.

为提升边缘计算场景下的数据协作效率,典型的思路有梯度压缩、异步聚合、激励机制的改进等,首先,梯度压缩会产生巨大的额外开销,并且会对模型精度有负面影响;其次,异步聚合相关方案中,大多基于静态聚合路径选择思路,因此其与边缘计算场景的适配度较低,无法实现智能化数据处理,另外,当前激励机制的相关研究工作中,很多都是通过额外的复杂计算过程来实现模型的加权聚合,也会带来许多不必要的计算开销,因此为实现多维度公平评估[11],有必要探索更高效的模型激励优化方案[12],这正好与Stackelberg博弈理论非常契合,Stackelberg博弈是一种可解释性强的信息动态博弈过程,博弈双方都会根据对方策略来判断自身行动,以保证利益最大化,其能够达到有效合成价值指标、激励训练的目的.

现有基于Stackelberg的相关数据协作方案[13~21]中,往往存在训练效率低、自适应能力弱、中央服务器决策能力过强、隐私威胁应对能力弱等主要问题. 其中,文献[13]提出一种引入声誉策略的两周期的动态契约以吸引移动用户参与模型训练,但如果遇到局部区域训练时间不同的情况,固定时间内未完成的训练任务会被错误丢弃,影响模型效率;文献[14]提出一种基于多领导者多追随者Stackelberg博弈的FL模型,但其中增加的罗宾汉机制会带来额外的参数调整,增加实施复杂性并影响收敛速度;文献[15]虽然创新改进了基于异构无人机协作的三阶段Stackelberg博弈激励模型,但其中一对多的分布式结构考虑不周全,这会降低模型可扩展性,并且中央服务器极容易受到单点攻击威胁,不利于数据安全,且其中对于参与者参与训练的假设过于理想,并不能完全考虑整体的训练情况.

综上所述,为提升数据协作效率与公平性、增强模型自适应能力、提升模型隐私防御能力,以深入研究SL与Stackelberg博弈的综合应用为导向,多维度、多阶段评判计算节点贡献度,本文创新提出一种面向无线边缘网络的分层Stackelberg博弈群体激励方法(Hierarchical Stackelberg game Swarm Learning Incentive method for wireless edge network,HSISL),其中创新设计一种基于组内、组间双定价的三阶段动态博弈分层激励算法,并将其引入SL这一新兴机器学习框架中,大大提升无线边缘计算场景下的激励效率、模型安全性与自适应能力.

2 HSISL方法设计与分析

2.1 HSISL方法设计

针对无线边缘计算场景下的模型效率与公平性、隐私威胁与计算资源浪费等问题,提出HSISL方法,整体框架如图1所示. 其中,任务发布层的云端聚合平台负责全局聚合与激励奖励下发;边缘簇聚合层的边缘簇节点管理组内聚合;本地训练层的计算节点执行本地训练,图1左侧展示模型聚合过程,右侧为激励奖励的最优纳什均衡解求取过程.

HSISL可描述为以下三个阶段:

(1)初始阶段

云端聚合平台广播训练请求,初始化全局模型及结构、激励奖励,对应图1中步骤①.

(2)群体学习训练阶段

在每轮次的训练中,参与方依次执行以下步骤. 首先计算节点更新本地模型,执行本地训练,上传模型参数,对应步骤②;边缘簇节点负责簇内局部聚合,对应步骤③;云端聚合平台收集所有参数,进行全局聚合,对应步骤④;随后进行步骤⑤,云端聚合平台计算双定价阶段的纳什均衡解,返回最优支付策略,对应步骤⑥,最后,云端聚合平台根据实际情况重新聚类确认最新模型结构,重新发布下轮次任务及激励,直至收敛.

(3)双定价阶段

对应图1右侧激励策略选择模块,我们设计了基于Stackelberg博弈的双定价分层激励方法,效用及博弈过程分析详见第2.2~2.4节,具体定价激励算法过程详见第2.5节.

模型聚合中的参数说明如表1所示.

第t轮中,用户n根据$\Delta w_n^k(t+1)$更新本地模型,然后进行本地训练,其更新方式为

$$w_n^k(t+1)=w_n^k(t)-l\cdot\Delta w_n^k(t+1) \tag{1}$$

随后,边缘簇节点k聚合本地梯度,根据组内定价策略进行局部模型更新,其更新方式为

$$w_k(t+1)=w_k(t)-l\cdot\sum_{n=1}^{N_k}\frac{q_n^k}{\sum_{n=1}^{N_k}q_n^k}\cdot w_n^k(t+1) \tag{2}$$

所有簇节点上传本轮次更新后,根据组内定价策略计算全局梯度加权平均值$\Delta w(t+1)$,其计算如式(3)所示,随后进行全局更新,更新方式如式(4)所示.

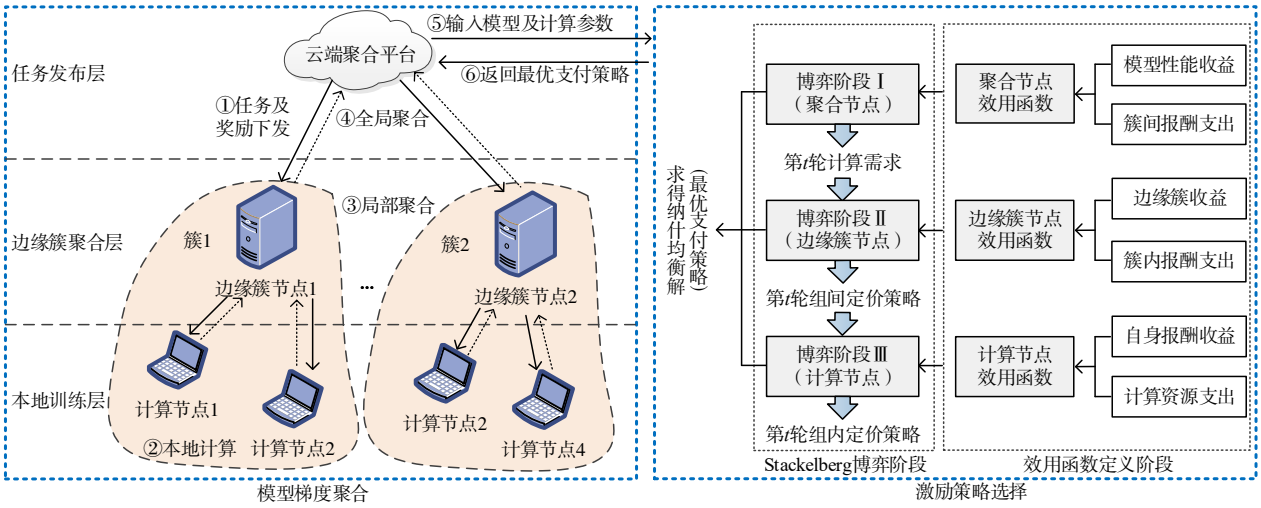


图1 面向无线边缘网络的分层Stackelberg博弈群体激励方法

表1 模型训练参数说明

符号	说明
K	所有边缘簇节点集合
N_k	边缘簇节点k管理的计算节点数量
n	边缘簇节点k管理的第n个计算节点
l	学习率
$w_n(0)$	用户n的初始模型
$w_n^k(t)$	第t轮用户n的本地模型
$w_k(t)$	第t轮边缘簇节点k的局部模型
$w(t)$	第t轮全局模型
q_n^k	用户n的组内定价
p_n^k	用户n的组间定价

$$\Delta w(t+1)=\sum_{k=1}^{K}\frac{\sum_{n=1}^{N_K}p_n^k}{\sum_{k=1}^{K}\sum_{n=1}^{N_K}p_n^k}\cdot w_k(t+1) \tag{3}$$

$$w(t+1)=w(t)-l\cdot\Delta w(t+1) \tag{4}$$

当模型精度满足要求或达到模型训练的最大迭代次数时，停止训练，综上所述，HSISL的具体执行步骤如算法1所示.

2.2 模型开销分析

我们将整个HSISL系统的效用优化目标分解为若干子问题以便求解，创新增加边缘簇节点参与中间数据处理环节，以减轻云端聚合平台计算压力. 在整个学习过程中，计算节点、边缘簇节点与云端聚合平台在学习过程中的开销及效用分析如下.

2.2.1 计算节点端

每个计算节点的效用函数等于其收到的模型奖励$p_n^k f_n^k$减去参与训练的开销，其中训练开销部分我们重点考虑了通信传输开销$e_n^{k,\,\mathrm{comm}}$、训练计算开销$e_n^{k,\,\mathrm{comp}}$与数据采集开销$e_n^{k,\,\mathrm{coll}}$.

(1)通信传输开销

假设边缘簇节点k共拥有M个子信道，且各子信道的带宽是W. 规定在首次迭代中，边缘簇节点主动均分信道资源至下属节点. 第t轮次中，计算节点n的子信道数量为M_n. h_n为传输信道增益，p_n为数据传输功率，N_0为传输噪声功率. 则计算节点n的数据传输速率可表示为

$$r_n^k=WM_n\log_2\left(1+\frac{h_n p_n}{N_0}\right) \tag{5}$$

规定$c_n^{k,\,\mathrm{comm}}$为单位时间内计算节点n的无线传输开销，w为单次模型参数传输大小，则计算节点n的通信开销可表示为

$$e_n^{k,\,\mathrm{comm}}=\frac{c_n^{k,\,\mathrm{comm}}w}{r_n^k}=\frac{c_n^{k,\,\mathrm{comm}}w}{WM_n\log_2\left(1+\frac{h_n p_n}{N_0}\right)} \tag{6}$$

(2)本地计算开销

规定$D=\{D_1,\cdots,D_n,\cdots,D_N\}$为边缘簇节点$k$下属所有计算节点的数据集组成的集合，$c_n^{k,\,\mathrm{comp}}$为计算节点$n$的单位计算成本，$f_n$为计算节点$n$的参与训练的计算需求，计算节点$n$的计算开销为

$$e_n^{k,\,\mathrm{comp}}=c_n^{k,\,\mathrm{comp}}D_n f_n^k \tag{7}$$

(3)数据采集开销

规定$c_n^{k,\,\mathrm{coll}}$为单位数据采集开销，则计算节点n的数据采集开销为

$$e_n^{k,\,\mathrm{coll}}=c_n^{k,\,\mathrm{coll}}D_n f_n^k \tag{8}$$

(4)总开销

规定计算节点n的组内单价为p_n^k. 则计算节点n的总开销成本为

算法1　HSISL算法

输入:训练节点数量M,簇个数K,最大训练轮次T,最大聚合等待时间max _wait_time,学习率l等训练参数

输出:全局模型参数$w(t)$

1.初始化$t=0$;

2.初始化簇结构,指定初始簇节点集合$K=\{1,2,\cdots,k\}$,初始计算节点集合$N_k=\{1,2,\cdots,n\}$,$\sum_{k=1}^{K}N_k=M$

3.初始化$w(0)$为常数或随机值,$w_n^k(0)=w_k(0)=w(0)$;模型激励策略I_0

4.FOR $t<T$ DO:

5.　云端聚合平台进行全局聚合:

6.　　接收局部梯度更新$w_k(t)$

7.　　根据式(4)更新全局梯度$w(t+1)$,下发第$t+1$轮各计算节点梯度更新$\Delta w_n^k(t+1)$

8.　　IF 云端聚合平台接收到新的簇节点注册标识sign_n^k THEN

9.　　重新定义簇结构

10.　　更新并广播当前簇节点及对应计算节点列表

11.　　根据算法2计算并广播第$t+1$轮最优激励策略I_{t+1}

12.　　边缘簇节点进行局部聚合:

13.　　接收组内所有计算节点本地更新进行局部聚合,根据式(2)更新$w_k(t+1)$并上传至云端聚合平台

14.　　根据I_{t+1}下发激励奖励至组内所有计算节点

15.　　IF 边缘簇节点k接收到簇结构更新 THEN

16.　　根据广播内容更新簇结构

17.　　计算节点进行本地聚合:

18.　　接收模型更新$\Delta w_n^k(t+1)$与激励I_{t+1}

19.　　根据式(1)计算第$t+1$轮的本地模型更新并进行本地训练得到$w_n^k(t+1)$,上传至所属边缘簇节点k

20.　　IF 计算节点n接收到簇节点注册请求 THEN

21.　　发送簇节点注册标识sign_n^k至云端聚合平台

22.　　根据广播内容更新簇结构

23.RETURN 全局模型参数$w(t)$

$$\begin{aligned}U_n^k&=p_n^kf_n^k-e_n^{k,\,\mathrm{comm}}-e_n^{k,\,\mathrm{comp}}-e_n^{k,\,\mathrm{coll}}\\&=p_n^kf_n^k-\frac{c_n^{k,\,\mathrm{comm}}w}{WM_n\log_2\left(1+\dfrac{h_np_n}{N_0}\right)}\\&\quad-c_n^{k,\,\mathrm{comp}}D_nf_n^k-c_n^{k,\,\mathrm{coll}}D_nf_n^k\end{aligned}\tag{9}$$

2.2.2　边缘簇节点端

边缘簇节点k的效用等于奖励$\sum_{n=1}^{N_k}q_n^kf_n^k$减去组内奖励成本与自身开销,此处开销考虑计算开销$e_k^{\mathrm{comp}}$与传输开销$e_k^{\mathrm{comm}}$.

(1)计算开销

规定c_k^{comp}为k的单位计算成本,N_k为k的计算数据量,则边缘簇节点k的计算开销为

$$e_k^{\mathrm{comp}}=c_k^{\mathrm{comp}}N_kw\tag{10}$$

(2)传输开销

规定边缘簇节点k的数据传输速率为r_k,c_k^{comm}为边缘簇节点k的单位传输成本,w为单次传输参数大小,则边缘簇节点k的通信开销为

$$e_k^{\mathrm{comm}}=\frac{c_k^{\mathrm{comm}}w}{r_k}\tag{11}$$

(3)边缘簇节点开销

规定计算节点n的计算资源单价为q_n^k,则边缘簇节点k的总开销成本为

$$\begin{aligned}e_k&=\sum_{n=1}^{N_k}q_n^kf_n^k-\sum_{n=1}^{N_k}p_n^kf_n^k-e_k^{\mathrm{comp}}-e_k^{\mathrm{comm}}\\&=\sum_{n=1}^{N_k}(q_n^k-p_n^k)f_n^k-c_k^{\mathrm{comp}}N_kw-\frac{c_k^{\mathrm{comm}}w}{r_k}\end{aligned}\tag{12}$$

2.2.3　云端聚合平台端

(1)总奖励分析

规定本轮次所有奖励为

$$\mathrm{Expense}=\sum_{k=1}^{K}\sum_{n=1}^{N_k}\beta A_n^kQ\tag{13}$$

其中,k为单位精度利润,A_n^k为测试精度,随计算资源需求增加而产生的边际效益递减Q为

$$Q=\ln(1+\alpha f_n^k)\tag{14}$$

在边际效用递减定理中,收益函数应是导数递减的增函数. 函数Q的导数需>0且二阶导数需<0. 则α的取值范围为$(0,+\infty)$.

(2)云端聚合平台开销

云端聚合平台的总开销等于本轮次规定的所有奖励减去参与模型训练的开销,可表示为

$$\begin{aligned}e_c&=\mathrm{Expense}-\sum_{k=1}^{K}\sum_{n=1}^{N_k}p_n^kf_n^k\\&=\sum_{k=1}^{K}\sum_{n=1}^{N_k}\beta A_n^kQ_{f_n^k}-\sum_{k=1}^{K}\sum_{n=1}^{N_k}q_n^kf_n^k\\&=\sum_{k=1}^{K}\sum_{n=1}^{N_k}\beta A_n^k\ln(1+\alpha f_n^k)-q_n^kf_n^k\end{aligned}\tag{15}$$

2.3　Stackelberg博弈分析

结合2.2节的计算,可将整个Stackelberg博弈问题可分为三阶段.

(1)博弈阶段Ⅰ

迭代开始时,云端聚合平台作为上层博弈领导者发起博弈,其效用函数可定义为

$$\begin{aligned}&\max_{f_n^k}U_c=\sum_{k=1}^{K}\sum_{n=1}^{N_k}(\beta A_n^k\ln(1+\alpha f_n^k)-q_n^kf_n^k)\\&\text{s.t. }0\leqslant f_n^k\leqslant f_n^{k,\max}\end{aligned}\tag{16}$$

(2)博弈阶段Ⅱ

根据云端聚合平台的最优组间定价q_n^k,边缘簇节点k最大化自身效用,其效用函数可定义为

$$\max_{q_n^k} U_k = \sum_{n=1}^{N_k}(q_n^k - p_n^k)f_n^k - c_k^{\text{comp}}N_k w - \frac{c_k^{\text{comm}}w}{r_k} \quad (17)$$
$$\text{s.t. } 0 \leqslant q_n^k \leqslant q_n^{k\max}$$

(3)博弈阶段Ⅲ

每个计算节点根据边缘簇节点k制定的组内定价定价p_n^k,最大化自身效用,其效用问题可定义为

$$\max_{p_n^k} U_n^k = p_n^k f_n^k - \frac{c_n^{k,\text{comm}}w}{WM_n\log_2\left(1+\frac{h_n p_n}{N_0}\right)} - c_n^{k,\text{comp}}D_n f_n^k - c_n^{k,\text{coll}}D_n f_n^k \quad (18)$$
$$\text{s.t. } 0 \leqslant p_n^k \leqslant p_n^{\max}$$

上述三阶段的待解决问题相互影响,分析如下:

首先,云端聚合平台的组间资源分配策略影响边缘簇节点的组间定价策略及计算节点的计算资源付出水平;其次,边缘簇节点求解最优组间定价策略阶段,计算节点的参与影响了边缘簇节点能量消耗,组间定价策略也影响了式(16)和式(18)的计算;最后,博弈阶段Ⅲ中每个计算节点的计算资源贡献由博弈阶段Ⅰ决定,并影响自身组内定价策略制定,同时间接影响了博弈阶段Ⅱ的计算.

综上所述,以上三个子博弈问题互相影响,构成了一个完整的多阶段Stackelberg博弈,必须综合考虑以共同商讨博弈解.

2.4 Stackelberg博弈问题分析

基于上述最佳动态响应函数求解,本节讨论唯一的Stackelberg均衡解的存在性.

2.4.1 上层博弈问题求解

为找到上层子博弈的均衡解,首先需要求解U_c的1阶导数为

$$\frac{\partial U_c}{\partial f_n^k} = \frac{\alpha\beta A_n^k}{1+\alpha f_n^k} - q_n^k \quad (19)$$

为证明效用函数U_n^k为凸函数,继续求解U_n^k的2阶导数为

$$\frac{\partial^2 U_n^k}{\partial (f_n^k)^2} = \frac{-\alpha^2\beta A_n^k}{(1+\alpha f_n^k)^2} < 0 \quad (20)$$

故U_n^k严格凹,证明U_n^k满足得到唯一纳什均衡解的全部条件,由上述内容可知,U_n^k的最优纳什均衡解为

$$f_n^*(q_n^k) = \max\left\{\frac{\beta A_n^k}{q_n^k} - \frac{1}{\alpha},\ f_n^{\max}\right\} \quad (21)$$

根据上述公式,可知当$q_n^k = \frac{\alpha\beta A_n^k}{\alpha f_n^{\max}+1}$时,$f_n^* = f_n^{\max}$,证明其足够让计算节点以最优贡献上传参数,也就是说,$q_n^k > \frac{\alpha\beta A_n^k}{\alpha f_n^{\max}+1}$时浪费资源. 因此有

$$f_n^*(q_n^k) = \frac{\beta A_n^k}{q_n^k} - \frac{1}{\alpha} \quad (22)$$

2.4.2 中层博弈问题求解

同样地,继续求解基于上层子博弈最优解的中层博弈问题最优解.

首先,将式(22)代入U_k得

$$U_k{}^* = \sum_{n=1}^{N_k}(q_n^k - p_n^k)\left(\frac{\beta A_n^k}{q_n^k} - \frac{1}{\alpha}\right) - c_k^{\text{comp}}N_k w - \frac{c_k^{\text{comm}}w}{r_k} \quad (23)$$

$U_k{}^*$的最优均衡解求取问题可抽象为一个多元函数的极值求解过程,因此首先求解式(23)的黑塞矩阵$\boldsymbol{G}$为

$$\boldsymbol{G} = \begin{pmatrix} \frac{\partial^2 U_k{}^*}{\partial (q_1^k)^2} & \cdots & \frac{\partial^2 U_k{}^*}{\partial q_1^k \partial q_n^k} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 U_k{}^*}{\partial q_n^k \partial q_1^k} & \cdots & \frac{\partial^2 U_k{}^*}{\partial (q_n^k)^2} \end{pmatrix} \quad (24)$$

求得

$$\frac{\partial U_k{}^*}{\partial q_n^k} = \frac{\beta A_n^k p_n^k}{(q_n^k)^2} - \frac{1}{\alpha} \quad (25)$$

$$\frac{\partial^2 U_k{}^*}{\partial q_m^k \partial q_n^k} = 0 \quad (26)$$

$$\frac{\partial^2 U_k{}^*}{\partial q_n^{k\,2}} = \frac{-2\beta A_n^k p_n^k}{(q_n^k)^3} \quad (27)$$

则式(24)可化简为

$$\boldsymbol{G} = \begin{pmatrix} \frac{-2bA_1^k p_1^k}{(q_1^k)^2} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{-2bA_n^k p_n^k}{(q_n^k)^2} \end{pmatrix} \quad (28)$$

由上述计算可知,矩阵$\boldsymbol{G}$的特征值均≤0,则矩阵$\boldsymbol{G}$负定,因此U_n^{k*}为凸函数. 证明U_n^k存在且唯一的纳什均衡解:

$$q_n^{k*}(p_n^k) = \sqrt{\alpha\beta A_n^k p_n^k} \quad (29)$$

2.4.3 下层博弈问题求解

将得到的计算需求f_n^{k*}和边缘簇节点组内定价p_n^{k*}最优解代入计算节点的效用函数中:

$$U_n^{k*} = p_n^k\left(\frac{\beta A_n^k}{\sqrt{\alpha\beta A_n^k p_n^k}} - \frac{1}{\alpha}\right) - \frac{c_n^{k,\text{comm}}w}{WM_n\log_2\left(1+\frac{h_n p_n}{N_0}\right)} - c_n^{k,\text{comp}}D_n\left(\frac{\beta A_n^k}{\sqrt{\alpha\beta A_n^k p_n^k}} - \frac{1}{\alpha}\right) - c_n^{k,\text{coll}}D_n\left(\frac{\beta A_n^k}{\sqrt{\alpha\beta A_n^k p_n^k}} - \frac{1}{\alpha}\right) \quad (30)$$

同样地,首先求解U_n^{k*}的1阶导数为

$$\frac{\partial U_n^{k*}}{\partial p_n^k}=-\frac{1}{\alpha}+\frac{\sqrt{\beta A_n^k}}{2\sqrt{\alpha}}p_n^{k-\frac{1}{2}}+\frac{c_n^{k,\,\mathrm{comp}}D_n\sqrt{\beta A_n^k}+c_n^{k,\,\mathrm{coll}}D_n\sqrt{\beta A_n^k}}{2\sqrt{\alpha}}p_n^{k-\frac{3}{2}} \tag{31}$$

继续求解U_n^{k*}的二阶导数为

$$\frac{\partial^2 U_n^{k*}}{\partial (p_n^k)^2}=\frac{-\sqrt{\beta A_n^k}}{4\sqrt{\alpha}}p_n^{k-\frac{3}{2}}+\frac{-3(c_n^{k,\,\mathrm{comp}}D_n\sqrt{\beta A_n^k}+c_n^{k,\,\mathrm{coll}}D_n\sqrt{\beta A_n^k})}{4\sqrt{\alpha}}p_n^{k-\frac{5}{2}} \tag{32}$$

已知$p_n^k>0$,可知$\frac{\partial^2 U_n^{k*}}{\partial (p_n^k)^2}<0$,证明$U_n^{k*}$存在唯一纳什均衡解,当$p_n^{k*}=p_n^{k\max}$时,$U_n^{k*}$达到最优,当$p_n^{k*}=p_n^{k\max}$时,$U_n^{k*}$达到最优,在边缘簇节点$k$的效用值为0,有$p_n^{k\max}=\dfrac{c_k^{\mathrm{comp}}N_k w+\dfrac{c_k^{\mathrm{comm}}w}{r_k}}{N_k f_n^k}$.

2.5 基于Stackelberg博弈的双定价分层激励算法设计

基于第2.2~2.4节的博弈过程分析,对HSISL方法中基于Stackelberg博弈的双定价分层激励算法描述如下:

(1)初始化阶段

初始化平均分配所有计算节点的组内定价、组间定价与各计算节点计算需求.

(2)计算需求确定阶段

在第t次迭代中,首先根据第$t-1$次迭代中的组间定价策略q^{t-1},根据式(16)计算本轮次计算需求f^t.

(3)组间定价阶段

根据上述阶段求得的f^t与第$t-1$次迭代中的组内定价策略p^{t-1},根据式(17)确定本轮次组间定价策略q^t,激励计算较慢的计算节点增加算力,从而增加自己的效用值.

(4)组内定价阶段

根据上述阶段所得f^t与q^t,根据式(18)计算本轮次组内定价策略p^t.

(5)动态平衡阶段

云端聚合平台得到重新分配的组内单价后,重复阶段(2)~(4),直至三方效用函数及各定价参数全部保持稳定,达到纳什均衡,获得最优定价策略.

上述定价激励步骤如算法2所示.

算法2　基于Stackelberg博弈的双定价分层激励算法

输入:参与训练的边缘簇节点集合$K=\{1,2,\cdots,k\}$,边缘簇节点k下属SL计算节点集合$N_k=\{1,2,\cdots,n\}$,纳什均衡的迭代轮次t与纳什均衡阈值ε

输出:最优定价激励$I=\{q_n^{k*},p_n^{k*},f_n^{k*}\},k\in K,n\in N_k$

1. 初始化q^0,p^0,f^0
2. WHILE 第t轮开始 DO
3. 边缘簇节点k→云端聚合平台:第$t-1$轮的组间定价策略q^{t-1}
4. 云端聚合平台根据f^{t-1}与q^{t-1}计算$\max U_c^t$得到f^t
5. 云端聚合平台→边缘簇节点k:第t轮各计算节点的计算需求f^t
6. 边缘簇节点k计算$\max U_k^t$得到第t轮的定价策略q^t
7. 边缘簇节点k→计算节点n:第t轮的定价策略q^t
8. 计算节点n计算$\max U_n^{k,t}$得到组内定价策略p^t
9. $t=t+1$
10. UNTIL $\left\|U_c^t-U_c^{t-1}\right\|\leqslant\varepsilon$
11. RETURN $I=\{q_n^{k*},p_n^{k*},f_n^{k*}\},k\in K,n\in N_k$

3 实验与分析

3.1 实验设置

本节设计对比实验评估HSISL的可行性. 实验平台操作系统为Ubuntu 20.04,硬件配置为Intel(R)Core(TM) i7-11800H CPU 2.3 GHz RTX 3050 GPU 32 GB RAM,实验使用Python 3.9、Pytorch 1.7.1实现模型训练,测试数据集采用MNIST数据集、Fashion-MNIST数据集与CIFAR-10数据集. 对比实验分别从收敛性、稳定性、模型性能三方面进行分析.

3.2 对比实验与分析

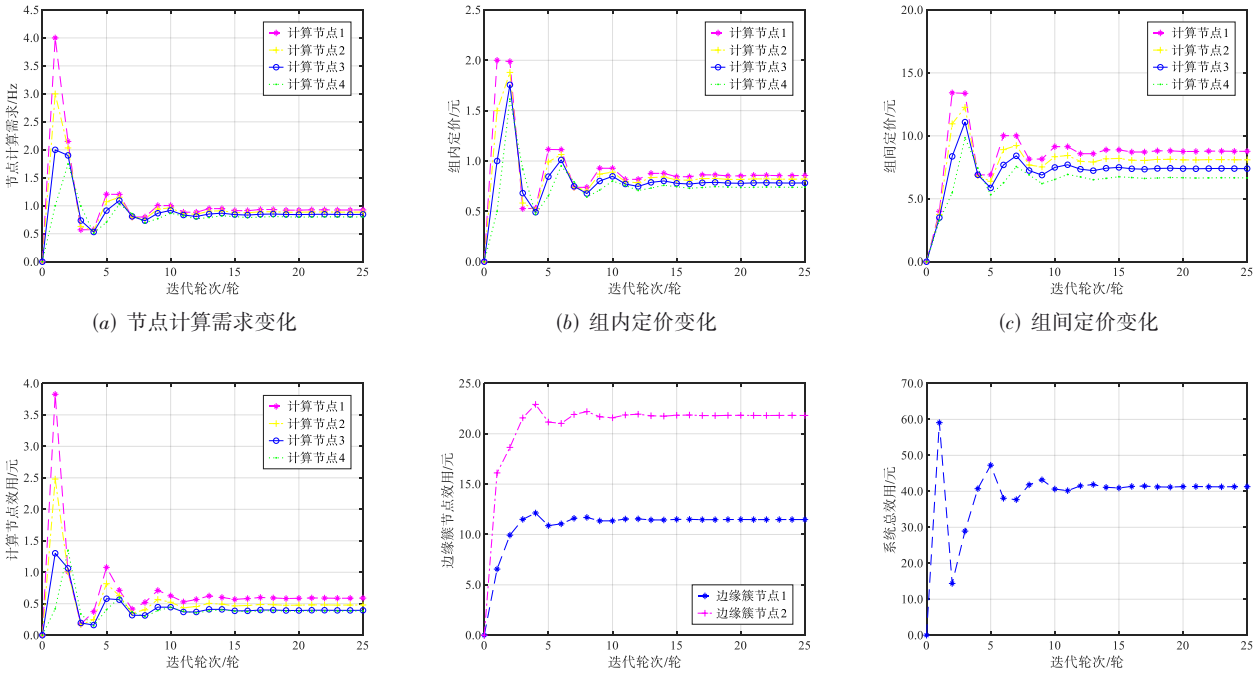
3.2.1 收敛性分析

规定最大迭代轮次为25,计算节点数量为4,边缘簇节点数量为2,边际效益参数α与β均为10,边缘簇节点计算单位开销c_k^{comp}与通信单位开销c_k^{comm}均为0.8,传输率r_k为0.9,h_n为10 mW,噪声功率N_0为10^{-8} W,W为20,w为0.8,各计算节点的通信开销成本$c_n^{k,\,\mathrm{comm}}$与计算开销成本$c_n^{k,\,\mathrm{comp}}$均为$\{0.2,0.4,0.6,0.8\}$,计算节点的数据收集开销$c_n^{k,\,\mathrm{coll}}$为0.000 1. 激励过程中的相关参数与效用值变化如图2所示.

由图2可知以下结论:

(1)激励资源有限时,计算能力强的节点会承担更多计算任务,且HSISL中的各参与方都能够逐渐适应各自偏好,直至整体收敛,系统总效用并不会随迭代进程推进持续增加,继续追加超需求的计算资源是一种资源浪费行为,因此为节省系统成本并不会继续加价.

(2)定价策略与计算节点状态相关. 图中最初的15次迭代中波动较大,各方效用取值都不稳定,因此定价策略也受到了消极影响,原因在于我们将组内定价定义



(a) 节点计算需求变化 (b) 组内定价变化 (c) 组间定价变化

(d) 计算节点效用变化 (e) 边缘簇节点效用变化 (f) 系统总效用变化

图2 收敛性分析

为 $p_n^{k*}=\dfrac{c_k^{\mathrm{comp}}N_k w+\dfrac{c_k^{\mathrm{comm}}w}{r_k}}{N_k f_n^k}$，因此 p_n^k 会随 f_n^k 稳定；同样地，组间定价 $q_n^{k*}=\sqrt{\alpha k A_n^k p_n^k}$，$q_n^k$ 也会随 p_n^k 稳定在 6～9 之间.

3.2.2 稳定性分析

(1)效用稳定性分析

激励参数设置不变，将 HSISL 与随机定价[22]、主从博弈定价[23]、ThreeStage-SFL[15]进行对比，其中整个系统的社会公共福利为所有节点效用之和：

$$\text{social_welfare}=U_C+\sum_{k=1}^{K}U_k+\sum_{k=1}^{K}\sum_{n=1}^{N_k}U_n^k \tag{33}$$

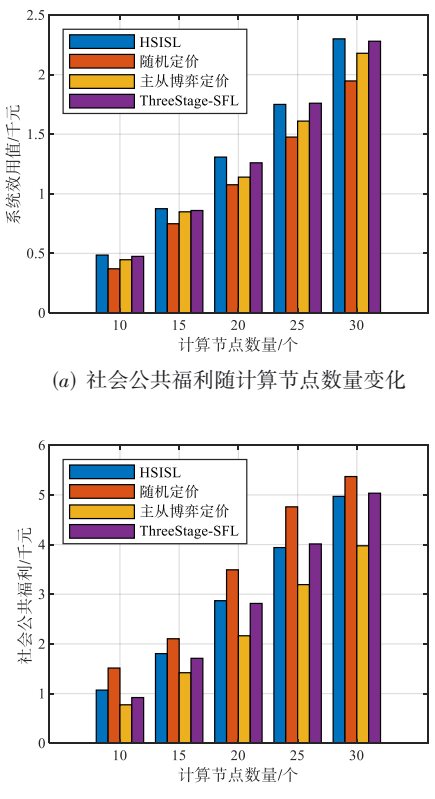
计算节点数量分别设置为{10,15,20,25,30}，各方法的社会公共福利及系统效用值变化如图3所示.

由图3可知以下结论：

图3中各曲线都呈增长趋势，系统投入的成本随节点数量增加而上涨，故效用与社会公共福利也随之增加. 同等情况下，HSISL 需要提供的社会公共福利最低，且整体系统效用最高，增速最快，因此 HSISL 更适用于无线边缘计算等复杂计算环境中，能够承担更加复杂的计算任务，更快地适应不断变化的环境条件.

(2)参数稳定性分析

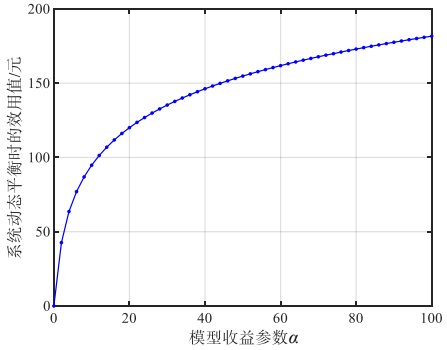
系统效用随收益参数变化如图4所示.



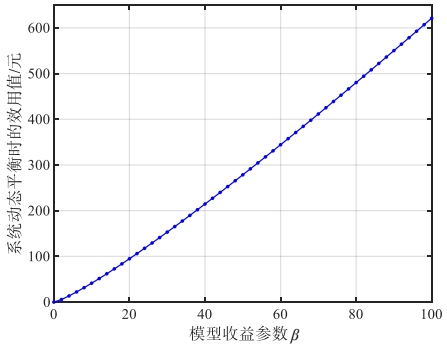
(a) 社会公共福利随计算节点数量变化

(b) 系统效用值随计算节点数量变化

图3 效用稳定性分析



(a) 模型收益参数α对效用值的影响



(b) 模型收益参数β对效用值的影响

图4　参数稳定性分析

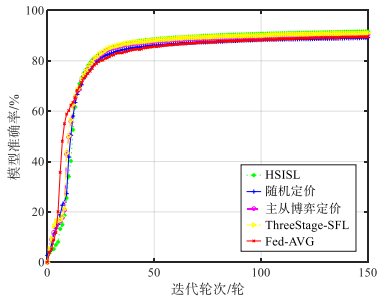
由图4可知,最优服务器效用与模型收益参数成正比,由于边缘簇节点效用增加,云端聚合平台付出增加,节点训练成本会逐渐贴近βA_n^k;HSISL的参数稳定性较好. 收益参数变化仅影响效用最值,不影响效用值变化趋势.

3.2.3　模型性能分析

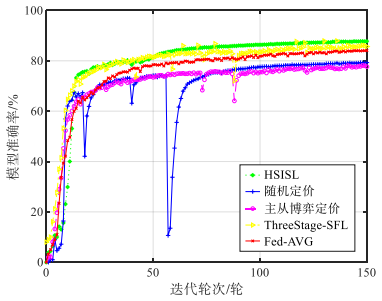
本节分别在MNIST数据集、Fashion-MNIST数据集、CIFAR-10数据集三种不同数据集上对HSISL方法进行了模型性能对比实验. 对于MNIST数据集,网络模型由1个输入层及两个全连接层组成,隐藏层神经元个数为32,激活函数为ReLU;对于Fashion-MNIST数据集,网络模型由两个卷积层及三个全连接层组成,卷积核大小为3×3,激活函数为ReLU;对于CIFAR-10数据集,网络模型为ResNet-20. 本地梯度下降函数分别为SGD、Adam、SGD,学习率均为0.01. 其余激励相关参数默认与3.2.1节的参数设置相同. 对比方法分别选择基于主从博弈的FL方法、基于随机定价的FL方法、ThreeStage-SFL方法、基于所提双定价分层激励机制的Fed-AVG方法.

(1)模型准确性与收敛性分析

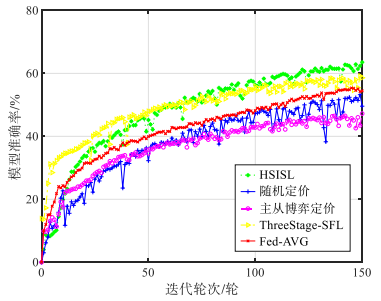
规定最大迭代次数为150,计算节点数量为4. 上述几种方法在三种不同数据集上的模型准确率与损失函数变化如图5所示.



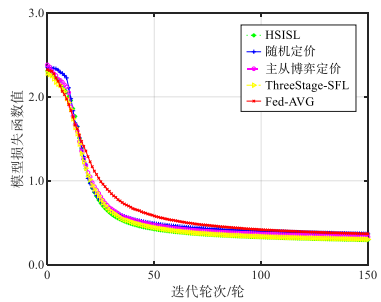
(a) 基于MNIST的模型准确率对比



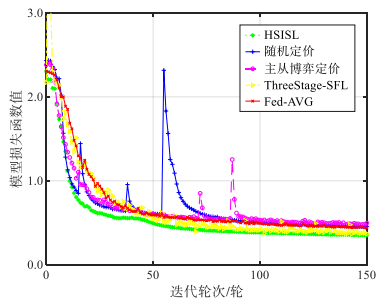
(b) 基于Fashion-MNIST的模型准确率对比



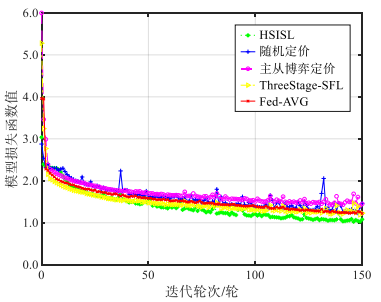
(c) 基于CIFAR-10的模型准确率对比



(d) 基于MNIST的模型损失对比



(e) 基于Fashion-MNIST的模型损失对比



(f) 基于CIFAR-10的模型损失对比

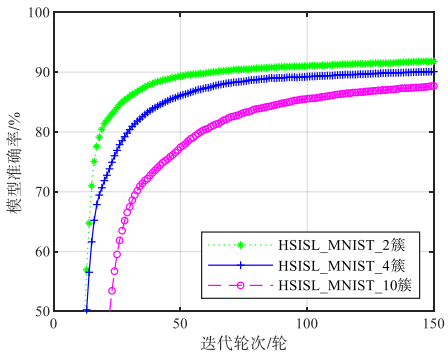
图5　不同数据集下的模型测试准确率与损失函数值对比

由图5(*a*)~(*f*)可知以下结论：

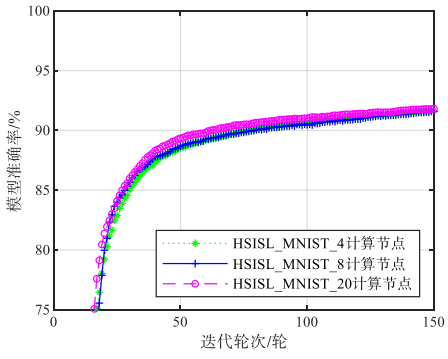
首先，HSISL的精度更高，处理复杂数据时更有优势．基于三种数据集的HSISL的最高准确率分别为92.06%、88.29%、65.49%，均高于其他方法；其次，HSISL的激励效果更好．开始阶段，ThreeStage-SFL的模型准确率增加速度虽然较高，但最后收敛时的准确率低于HSISL，且曲线较为动荡，其他方法也明显逊于HSISL；最后，HSISL的可用性较好．HSISL的收敛轮次分别约为80、110、150，均较快于其他方法．

(2)模型参数稳定性分析

为探究HSISL的参数稳定性，本节分别测试其在不同簇数量与计算节点数量设置下的模型训练情况．首先，规定学习率l为0.01，计算节点数量为20，训练数据集为MNIST数据集，其他参数设置不变，对比其在簇个数分别为{2，4，10}下的模型准确率，实验结果如图6(*a*)所示；其次，规定簇个数为2，训练数据集仍为MNIST数据集，其他参数不变，对比其在计算节点数量分别为{4，8，20}下的模型准确率，实验结果如图6(*b*)所示．



(*a*) 模型准确率随簇个数变化



(*b*) 模型准确率随计算节点数量变化

图6 基于不同计算节点数量与簇数量的HSISL准确率

由图6可知以下结论：

计算节点数量固定时，模型准确率及收敛速度随簇个数增加而降低，这可能与局部优化难度增加有关，簇数量增加时，簇内训练量减少，可能导致陷入局部最优解，或与通信开销增加有关，导致更多的网络延迟与通信开销，降低整体训练效率，因此在实际应用时，要根据具体情况合理定义模型结构，否则可能影响实际应用效率．簇个数固定时，模型准确率及收敛速度随计算节点增加而增加，随着计算节点数量增加，数据特征多样性也随之增加，模型能够吸收更多不同数据源的信息，这使得模型泛化能力增加，因此最终的模型准确率会有所提升．

规定计算节点数量为4，其余参数不变，不同学习率下的准确率变化如图7所示．

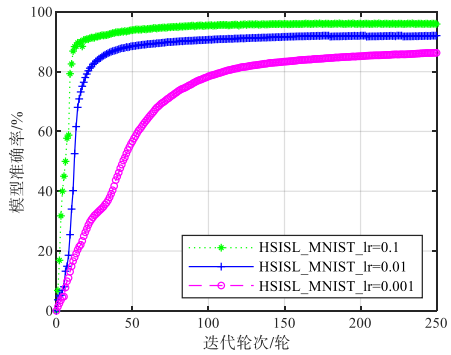


图7 模型准确率随学习率变化

由图7可知，同等情况下，模型准确率及收敛速度随学习率增加而增加，较高的学习率可帮助模型更有效地梯度下降优化，但过高学习率可能导致模型动荡无法收敛．

综上所述，在群体学习中，Stackelberg博弈可用于确定云端聚合平台与追随节点之间的角色分配与协作策略，领导者可以在综合考虑整体训练情况后制定合理的协作策略．HSISL能够有效激励计算节点积极参与训练，提升整体训练效率．

4 总结与展望

Stackelberg博弈为群体学习等分布式学习架构提供了一种强大的博弈论框架，用于管理和优化模型管理者与计算节点之间的协作关系，通过实验分析，HSISL确实能够提升模型训练效率，与基于传统Stackelberg博弈的FL相关方案相比，所提HSISL方法的激励效果更明显，并且最终的模型准确率更小，收敛速度更快．因此，本文所提HSISL方法设计的双定价激励策略效应更优，可以作为边缘数据协作模型性能提升的有用参考，但该方法没有考虑模型隐私性的影响，且目前相关研究方向仍处于起步阶段，后续可以针对激励模型的隐私性展开深入研究．

参考文献

[1] WARNAT-HERRESTHAL S, SCHULTZE H, SHASTRY K L, et al. Swarm learning for decentralized and confidential clinical machine learning[J]. Nature, 2021, 594(7862): 265-270.

[2] KALRA S, WEN J F, CRESSWELL J C, et al. Decentralized federated learning through proxy model sharing[J]. Nature Communications, 2023, 14(2899): 1-10.

[3] BO Z H, GUO Y C, LYU J H, et al. Relay learning: A physically secure framework for clinical multi-site deep learning[J]. NPJ Digital Medicine, 2023, 6(204): 1-11.

[4] LI W T, KIM M, ZHANG K, et al. COLLAGENE enables privacy-aware federated and collaborative genomic data analysis[J]. Genome Biology, 2023, 24(204): 1-38.

[5] WANG Z, LI X H, WU T H, et al. A credibility-aware swarm-federated deep learning framework in Internet of vehicles[J]. Digital Communications and Networks, 2024, 10(1): 150-157.

[6] LIU Y B, HUO L J, WU J, et al. Swarm learning-based dynamic optimal management for traffic congestion in 6G-driven intelligent transportation system[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(7): 7831-7846.

[7] SALDANHA O L, QUIRKE P, WEST N P, et al. Swarm learning for decentralized artificial intelligence in cancer histopathology[J]. Nature Medicine, 2022, 28(6): 1232-1239.

[8] DONG X S, SARKER S, QIAN L J. Integrating human-in-the-loop into swarm learning for decentralized fake news detection[C]//2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA). Piscataway: IEEE, 2022: 46-53.

[9] SALDANHA O L, MUTI H S, GRABSCH H I, et al. Direct prediction of genetic aberrations from pathology images in gastric cancer with swarm learning[J]. Gastric Cancer, 2023, 26(2): 264-274.

[10] KANG H Y, JI Y R, ZHANG S X. Enhanced privacy preserving for social networks relational data based on personalized differential privacy[J]. Chinese Journal of Electronics, 2022, 31(4): 741-751.

[11] 陈颢瑜, 李浥东, 张洪磊, 等. 面向可信联邦学习公平性的研究综述[J]. 电子学报, 2023, 51(10): 2985-3010.
CHEN H Y, LI Y D, ZHANG H L, et al. Fairness in trustworthy federated learning: A survey[J]. Acta Electronica Sinica, 2023, 51(10): 2985-3010. (in Chinese)

[12] 王勇, 李国良, 李开宇. 联邦学习贡献评估综述[J]. 软件学报, 2023, 34(3): 1168-1192.
WANG Y, LI G L, LI K Y. Survey on contribution evaluation for federated learning[J]. Journal of Software, 2023, 34(3): 1168-1192. (in Chinese)

[13] ZHAO N, WAN Q X, CHEN J L, et al. Dynamic incentive mechanism in mobile crowdsourcing networks by combining reputation and contract theory[J]. International Journal of Distributed Sensor Networks, 2022, 18(6): 1-14.

[14] LU J F, LIU H B, JIA R H, et al. Toward personalized federated learning via group collaboration in IIoT[J]. IEEE Transactions on Industrial Informatics, 2023, 19(8): 8923-8932.

[15] HE W J, YAO H P, MAI T L, et al. Three-stage stackelberg game enabled clustered federated learning in heterogeneous UAV swarms[J]. IEEE Transactions on Vehicular Technology, 2023, 72(7): 9366-9380.

[16] 贾云健, 黄宇, 梁靓, 等. 基于主从博弈的分层联邦学习激励机制研究[J]. 电子与信息学报, 2023, 45(4): 1366-1373.
JIA Y J, HUANG Y, LIANG L, et al. Research on hierarchical federated learning incentive mechanism based on master-slave game[J]. Journal of Electronics & Information Technology, 2023, 45(4): 1366-1373. (in Chinese)

[17] 周赞, 张笑燕, 杨树杰, 等. 面向联邦算力网络的隐私计算自适激励机制[J]. 计算机学报, 2023, 46(12): 2705-2725.
ZHOU Z, ZHANG X Y, YANG S J, et al. Adaptive incentive mechanism for privacy computing in federated compute first networks[J]. Chinese Journal of Computers, 2023, 46(12): 2705-2725. (in Chinese)

[18] LI C L, SONG M Y, LUO Y L. Federated learning based on Stackelberg game in unmanned-aerial-vehicle-enabled mobile edge computing[J]. Expert Systems with Applications, 2024, 235(121023): 1-15.

[19] CHEN Y L, ZHOU H, LI T, et al. Multifactor incentive mechanism for federated learning in IoT: A stackelberg game approach[J]. IEEE Internet of Things Journal, 2023, 10(24): 21595-21606.

[20] HUANG Z H. Incentive mechanism design for joint resource allocation in post-quantum blockchain-based federated learning[C]//2023 International Conference on Electronics and Devices, Computational Science (ICEDCS). Piscataway: IEEE, 2023: 447-451.

[21] LIU Y, LIU P, JING W P, et al. PD2S: A privacy-preserving differentiated data sharing scheme based on blockchain and federated learning[J]. IEEE Internet of Things

Journal, 2023, 10(24): 21489-21501.
[22] FREDRIKSON M, JHA S, RISTENPART T. Model inversion attacks that exploit confidence information and basic countermeasures[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2015: 1322-1333.
[23] 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.

作者简介

康海燕 男,1971年生,河北石家庄人,博士,教授,北京信息科技大学信息管理学院副院长,主要研究方向为网络安全、隐私计算等.
E-mail: kanghaiyan@126.com

冀珊珊 女,1999年生,河北保定人,北京信息科技大学网络空间安全专业在读硕士研究生,主要研究方向为网络安全与隐私保护等.
E-mail: jishanshan022@126.com