计算机科学
COMPUTER SCIENCE

跨机构联邦学习的激励机制综述

王鑫，黄伟口，孙凌云

引用本文

王鑫，黄伟口，孙凌云. 跨机构联邦学习的激励机制综述[J]. 计算机科学，2024，51(3)：20-29.

WANG Xin, HUANG Weikou, SUN Lingyun. Survey of Incentive Mechanism for Cross-silo Federated Learning [J]. Computer Science, 2024, 51(3): 20-29.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230700194

跨机构联邦学习的激励机制综述

王　鑫[1,2]　黄伟口[1]　孙凌云[2]
1 浙江工业大学计算机科学与技术学院　杭州 310023
2 浙江大学计算机科学与技术学院　杭州 310058

摘　要　联邦学习作为一种分布式机器学习,有效地解决了大数据时代的数据共享难题。其中,跨机构联邦学习是机构之间互相合作的一种联邦学习类型。如何在跨机构合作的过程中设计合理的激励机制十分重要。文中从跨机构合作的角度,对现有的跨机构联邦学习的激励机制研究进行了综述。首先介绍跨机构合作过程中的3个基本问题,即高隐私性、数据异质性、公平性,然后分析了以全局模型为中心和以参与者为中心这两种不同的跨机构合作模式下的激励机制设计方法,最后总结了影响跨机构合作稳定发展的几个影响因素,即参与者的数据演变、参与者合作关系变动和参与者的负面行为,并展望了跨机构联邦合作的未来方向。

关键词:跨机构联邦学习;激励机制;跨机构合作;分布式机器学习;隐私计算
中图分类号　TP181;TP309

Survey of Incentive Mechanism for Cross-silo Federated Learning

WANG Xin[1,2],HUANG Weikou[1] and SUN Lingyun[2]
1 College of Computer Science and Technology,Zhejiang University of Technology,Hangzhou 310023,China
2 College of Computer Science and Technology,Zhejiang University,Hangzhou 310058,China

Abstract　As a kind of distributed machine learning,federated learning effectively solves the problem of data sharing in big data era. Among them,cross-silo federated learning,as a type of federated learning in which institutions cooperate with each other,is obviously very important to design a reasonable incentive mechanism in the process of cross-silo cooperation. Based on the perspective of cross-silo cooperation,this paper makes a comprehensive analysis of the existing incentive mechanism of cross-silo federated learning. Firstly,this paper introduces three basic problems in the process of cross-silo cooperation:high privacy,data heterogeneity,and fairness. Then,it analyzes the incentive mechanism design methods under two different cross-silo cooperation models centered on the global model and centered on participants. Finally,it summarizes the several factors that affect the stable development of cross-silo cooperation:data evolution of participants,changes in the cooperative relationship of participants,and negative behaviors of participants,and looks forward to the future direction of cross-silo federal cooperation.

Keywords　Cross-silo federated learning,Incentive mechanism,Cross-silo cooperation,Distributed machine learning,Privacy computing

1　引言

随着社会数字化程度不断加深,数字经济也成为高速增长的国民经济支柱,其所产生的数据更是呈爆发式增长,成为个人、组织机构、行业乃至国家的新型资产。大数据的出现使人们对数据的价值有了新的认知,从而对数据的隐私保护有了更多的要求,而这也使得数据共享变得愈发困难。这对于传统的机器学习的冲击是巨大的,传统的机器学习需要将所有的训练数据传输到一台高算力的服务器中,然后进行模型训练,但对数据的隐私保护的法律法规阻止了这种行为。

为了解决数据共享的问题,谷歌首次提出了联邦学习的概念[1]。联邦学习是一种分布式机器学习,其中数据所有方在中央服务器的协调下共同训练全局模型,数据所有方使用本地的私有数据进行本地模型训练,然后只需将模型更新上传至参数服务器,由参数服务器聚合局部模型参数成为全局模型即可。因此,联邦学习不需要上传原始数据,这保证了参与者的数据隐私,同时降低了计算和通信资源的消耗,一定程度上解决了数据共享的难题。根据参与者的数量和训练规模,联邦学习可以分为跨设备联邦学习和跨机构联邦学习。跨设备联邦学习的参与者数量多,个体数据规模小,通常是由

到稿日期:2023-07-25　返修日期:2023-12-10
基金项目:国家重点研发计划(2020YFB0906000,2020YFB0906004);浙江工业大学科技项目(KYY-HX-20220288,KYY-HX-20180649)
This work was supported by the National Key R&D Program of China(2020YFB0906000,2020YFB0906004) and Zhejiang University of Technology Science and Technology Project(KYY-HX-20220288,KYY-HX-20180649).
通信作者:王鑫(xinw@zjut.edu.cn)

大量的移动设备或物联网节点来共同训练的。跨机构的联邦学习的参与者数量较少，但个体持有的数据规模较大，通常是多个企业或机构之间进行共同训练。

跨机构联邦学习被广泛地应用于各个领域，例如在医疗保健行业[2]中，多家医疗企业或医院联合训练疾病预测模型，或者在金融行业中，不同的金融机构共同训练经济预测模型等。跨机构联邦学习有效促进了不同机构或企业之间的合作与发展。因此，提高跨机构联邦学习的训练效率和模型效用成为了当前研究的重点。

为了提高跨机构联邦学习的效果，研究者们在聚合算法、数据收集、模型训练效率等方面提出了许多的研究成果。然而，很多研究成果是在假设参与者自愿贡献其所拥有的数据资源来参与联邦学习的前提下提出的，这种理想化的情况在真实的环境中显然是不可能的。对此，研究者们开始探索如何激励更多的机构参与联邦学习并且积极贡献高质量数据，激励机制的设计由此成为了联邦学习研究的核心子问题。早期的激励机制设计大都是关于跨设备的联邦学习的激励机制，从提高通信和计算效率或者筛选高质量设备的角度来设计的。但是，随着近几年跨机构联邦学习的兴起，这些激励机制已不适用。机构不同于终端/边缘设备，机构本身持有大量的数据，并且拥有相对稳定的计算和通信资源，若是没有足够的激励是无法令机构积极参与跨机构联邦学习的。同时，机构之间的信任度、合作的公平性、数据共享的高隐私性以及数据异质性等方面都是跨机构联邦学习的激励机制设计过程中需要关注和解决的问题，这使得激励机制的设计变得愈发复杂且困难。

目前，联邦学习虽然在激励机制方面有着许多的研究综述，但在跨机构联邦学习的激励机制方面尚未看到相关研究。Zhan 等[3]从客户贡献、声誉和资源分配驱动的角度来研究分析联邦学习的激励机制，但是对于高隐私性需求和数据异质性的问题却没有提及。Zeng 等[4]则将激励机制分为 3 个组成部分，分别从贡献衡量、节点选择和支付分配 3 个方面来对激励机制进行归类，但同样没有提及高隐私性的需求。与文献[4]类似，Liang 等[5]从贡献测量、客户选择、支付分配子问题出发对激励机制进行综述，但同样很少讨论高隐私性和数据异质性的问题。文献[6]则仅对基于经济学和博弈论的激励机制进行综合分析。另外，这些激励机制文献均为对跨设备的联邦学习进行综合分析，是基于大量的不稳定互联网设备参与联邦学习的情况，对于机构合作之间的公平性问题没有一个完整的讨论，不适用于参与者较少且通信稳定的跨机构联邦学习。除此之外，Leon 等[7]对去中心化的激励机制和联邦学习框架进行了综述，并提出了系统文献综述方法，对数据异质性、奖励机制等问题均有涉及，但是对于以全局模型为中心的跨机构联邦学习的激励机制却没有更多的讨论。Yang 等[8]对纵向联邦学习的概念和算法以及当前在有效性、效率和隐私等方面的进展和挑战进行了综述，对于跨机构联邦学习的激励机制仅部分提及。Yan 等[9]则对个性化的联邦学习的激励机制进行综述。这 3 篇综述虽然未对跨机构联邦学习的激励机制进行全面的综合分析，但对于本文的分析研究有着一定的启发作用。

综上所述，结合 Huang 等[10]对目前跨机构联邦学习面对的主要挑战的综述，本文从跨机构合作的角度，对机构之间合作过程中的关键问题进行整理分析，从跨机构合作的基本问题、合作模式、稳定发展的影响因素 3 个方面对现有的跨机构联邦学习的激励机制进行全面的综合分析。图 1 是本文叙述的跨机构合作的关键问题及相关激励机制设计的框架图。最后，本文对跨机构联邦合作的未来方向进行了展望。

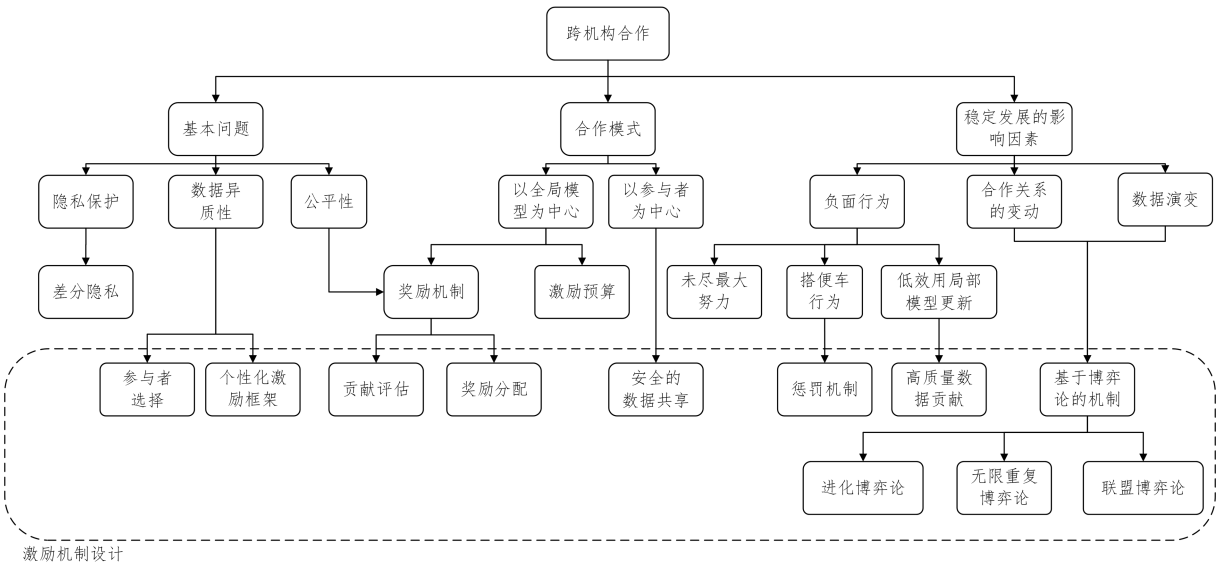

图 1　跨机构合作的关键问题及相关激励机制设计

Fig. 1　Key issues of cross-silo cooperation and design of related incentive mechanism

2　背景知识

2.1　跨机构联邦学习概述

联邦学习是一种新式的分布式机器学习，主要分为参数服务器和参与者。与传统的机器学习不同，联邦学习不需要将数据集中在一个服务器中，参数服务器只需收集参与者本地模型更新后的局部模型参数或梯度等，对其进行聚合更新后重新下发到参与者本地，如此往复。其中，跨机构的联邦学习的

参与者多为机构或企业，它们持有大量的本地数据和稳定的计算通信资源。

图 2 给出了跨机构联邦学习的训练过程，可以分为以下 4 个步骤。

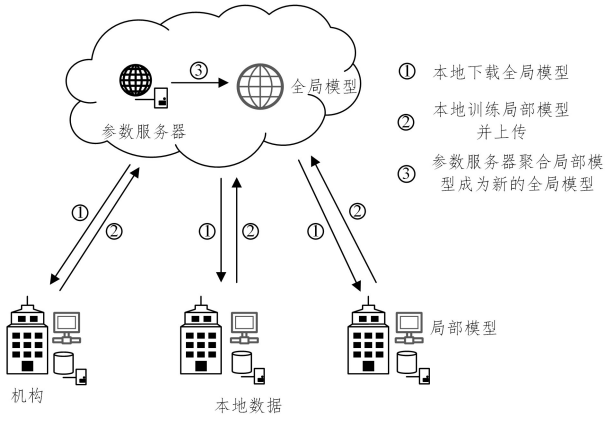

图 2 跨机构联邦学习的训练过程

Fig. 2 Training process of cross-silo federated learning

1)初始化：参数服务器首先决定全局模型的初始架构，根据训练任务对全局模型进行初始化。

2)本地下载全局模型：参与机构从参数服务器上下载全局模型。

3)本地模型训练：参与机构运用本地的私有数据及全局模型进行本地的局部模型训练，然后将更新后的局部模型参数或者模型更新上传到参数服务器。

4)全局模型聚合：参数服务器将接收到的局部模型参数进行聚合更新，使其成为新的全局模型。

重复步骤 2)－步骤 4)，直到全局模型收敛或达到预设的时间。

2.2 激励机制概述

激励机制是通过特定的方法来激励参与者以最大的努力和承诺完成工作。在联邦学习中，参与者进行本地模型训练需要消耗本地的计算资源和通信资源，若是没有合理的激励机制，参与者有可能出现不参与、消极参与、中途退出等不好的现象。这种现象在跨机构的联邦学习中尤为明显，因为参与的机构需要投入本地持有数据和计算通信资源来进行本地模型训练，若是没有合理的收益，则会造成参与机构不愿意投入。因此，跨机构联邦学习的激励机制设计时需要解决跨机构合作过程中将会出现的各种情况。在跨机构联邦学习中，首先需要考虑跨机构合作的基本问题，例如机构对于高隐私性的联邦学习的要求、由于机构之间的数据异质性带来的数据差异问题，以及公平的跨机构联邦学习环境。表 1 列出了跨机构联邦学习的激励机制设计在基本问题方面与跨设备联邦学习的不同之处。其次需要考虑跨机构合作的合作模式，不同合作模式的激励机制设计的重心也会有所不同。最后需要考虑跨机构合作稳定发展过程中的影响因素，跨机构联邦学习是各机构长期合作的过程，在这个合作过程中会出现许多的突发情况影响机构之间的合作，例如部分恶意参与者可能会破坏训练过程。因此，需要设计相应的激励机制保持跨机构合作的稳定性和持续性。

表 1 跨机构联邦学习与跨设备联邦学习在激励机制方面的不同

Table 1 Difference in incentive mechanism between cross-silo federated learning and cross-device federated learning

	跨机构联邦学习激励机制	跨设备联邦学习激励机制
参与者规模	参与者数量较少，多为企业或机构	参与者数量巨大，多为移动设备或物联网节点
数据数量与质量	参与者持有数据量较多且质量较高	参与者持有数据较少且数据质量参差不齐
稳定性	有稳定的通信和计算资源	缺乏稳定的通信和计算资源
隐私性	对隐私保护级别有着极高的要求	对隐私保护级别的要求不高
数据异质性	因参与者的数量较少，对于数据异质性问题的解决需求较高	因参与者数量极多并且通常持有同类型数据，可以通过多次筛选规避数据异质性问题
公平性	有极高的需求	部分设备运营商可能有较高的需求

3 跨机构合作的基本问题

在跨机构联邦学习中，跨机构合作需要解决 3 个基本问题：高隐私性、数据异质性、公平性。

3.1 高隐私性

联邦学习的初衷是保护参与者的数据隐私，并且在跨设备联邦学习方面已经取得了不错的效果。然而，随着技术的发展，通过联邦学习获取参与者数据信息的隐私攻击也逐渐出现，例如推理和重建攻击。相比跨设备联邦学习，跨机构联邦学习有更多需要被保护的数据类型，机构数据对隐私保护的级别往往也更高，毕竟跨设备联邦中经常是个人数据。因此，那些拥有大量数据资源的机构不会容忍这种潜在的隐私安全风险存在于合作中，提升隐私保护级别成为跨机构联邦学习的首要任务。目前，主流的隐私强化技术包括对上传更新添加噪声的差分隐私技术和对数据进行加密计算的同态加密技术。

差分隐私[11]是目前广泛采用的隐私保护技术，其基本思想是在个人敏感属性中添加噪声以保护隐私。差分隐私技术的应用较为复杂，需要对噪声化的数据进行重建才能继续进行后续的运算。Wang 等[12]提出了一个三层框架，将联邦学习的数据上传过程分为 3 层，在这个框架中，参与者先将数据上传到边缘服务器中，在上传之前先应用本地隐私差分对用户数据添加噪声，在边缘服务器中根据数据重构算法重建数据，之后边缘服务器与云服务器之间转化为传统的联邦学习模式，这有效保护了客户的数据隐私，但也提高了计算和通信的复杂度。在将差分隐私运用于激励机制以提高参与者的隐私保护级别方面，研究者们主要通过在激励机制的数据交互步骤对参与者的数据隐私信息添加噪声，之后以重构的方式来达成高隐私性的目的。Ren[13]提出了将差分隐私与基于拍卖的激励机制相结合的差分私人拍卖激励机制。与传统的

基于拍卖的激励机制不同,该机制不再假设参与者数据分布的可访问性,改为在竞价时,向客户的数据分布信息中应用差分隐私添加一些随机噪声。Zhang 等[14]开发设计了一个私人奖励游戏,将差分隐私与博弈论结合,该游戏引入了"隐私货币"的概念,允许客户通过评估隐私数据泄露导致的损失,选择参数服务器添加噪声的集中式差分隐私模型或者是本地添加噪声的本地隐私模型,并对使用集中式差分隐私模型的客户给出一定的补偿。Wang 等[15]提出将差分隐私与基于多维反向拍卖的激励机制相结合的激励机制,应用差分隐私在参与者的投标中添加数据扰动,在保护参与者的真实成本和本地模型参数隐私的情况下,激励参与者提供高质量数据。差分隐私技术虽然在隐私保护方面有着卓越的效果,但是对数据信息添加的噪声也对全局模型训练造成了一定影响,这种干扰会降低模型收敛的速度,甚至会降低全局模型的准确性和泛用性。Li 等[16]也揭示了差分隐私对模型更新的扰动越大,全局模型的质量就会越低。在这方面也有研究者提出了解决方案,例如 Liu 等[17]提出了更加细致的样本级差分隐私,他们将数据主体视为隐私对象而不是机构本身,在这种更加严格的隐私要求下,激励参与者更多的互相联合,以减小差分隐私造成的影响。

相比添加噪声可能扭曲数据的差分隐私方法,有着充足的计算和通信资源的机构更加喜欢对数据进行加密计算的同态加密技术,因为数据计算的精确性更高。但是如何不断降低同态加密的高昂计算成本仍然是研究热点。Zheng 等[18]提出了一种双服务器协议,在避免了同态加密的高额计算消耗的同时,取得了不错的隐私保护效果。Luo 等[19]使用掩蔽技术取代了同态加密的繁琐操作,提出了一种支持安全梯度聚合和验证的联邦学习协议。Tran 等[20]提出了一种双层加密方案,在保护参与者隐私的同时允许参与者训练过程中的退出和重新加入,有利于吸引对此好奇的其他机构参与联邦学习。

高隐私性的要求使得激励机制的设计变得更加复杂,目前的高隐私性的激励机制研究基本是在数据交互步骤中使用隐私强化技术,通过对参与者的私人数据进行加密或添加噪声来保护其数据隐私,例如部分激励机制可能需要参与者的私人信息,这种激励机制显然不会被机构接受并且参加跨机构联邦学习。更大可能性是通过对参与者上传的数据信息进行加密和重构,来提高激励机制的隐私保护级别,从而激励其他机构参与跨机构联邦学习。然而,这些隐私强化技术对于真实数据信息的隐藏也会使得最终的结果出现部分偏差,甚至出现南辕北辙的情况。并且这些隐私强化技术较高的计算成本也影响了跨机构联邦学习性能的提升,而跨机构联邦学习又对性能要求较高,这样就形成了一个矛盾。

综上所述,目前的高隐私保护的强化方法仍然有继续提升的空间,差分隐私技术、同态加密技术等与激励机制相结合的方法还有减小计算开销、解决差分隐私技术中的噪声问题等难点待攻破。

3.2　数据异质性

跨机构联邦学习中的数据异质性指不同机构之间的数据具有不同的特征分布、数据类型、数据规模或数据质量等方面的差异。这种数据异质性是由于不同机构的业务需求、数据收集方式、数据源等因素的差异而引起的。数据异质性普遍存在于一些拥有规模小且碎片化的数据的机构之间,促使这些机构更加容易合作,充分提高了碎片化数据的利用率[21]。数据异质性虽然有激励小机构互相合作的作用,但更多的是对跨机构合作过程和模型训练的负面影响。首先,数据异质性会导致全局模型的收敛速度减慢,这是由不同机构的局部模型的收敛速度不同造成的。其次,机构之间的特征分布不同会导致全局模型在特征选择和权重调整方面更加困难。最后,机构之间的数据分布不同会导致数据的非独立同分布情况的出现。在跨机构联邦学习中,非独立同分布指不同机构参与合作的数据在概率分布上不完全相同或独立同分布的情况。数据的非独立同分布会导致全局模型的泛化能力受限,同时可能导致全局模型在某些机构的训练数据上过拟合,而在其他机构上欠拟合。数据异质性对跨机构合作构成了一定的阻碍,解决机构之间的数据异质性问题成为了跨机构合作的基本问题。

对于数据异质性带来的诸多负面影响,一个直接的解决方法是选择近似数据分布和相近规模的机构加入联邦学习,这样不仅可以使得参与者的局部模型收敛速度相近,也可以规避不同数据分布和特征分布带来的数据差异问题。其中,Ren[13]提出了基于拍卖机制的激励机制,对参与者在拍卖时提交的数据信息进行数据评估,选择数据分布与预期数据分布相似的参与者。Zhang 等[22]提出了一种应用动态融合方法的激励机制,根据本地模型性能动态决定参与者,通过本地模型的性能优化来减小数据异质性带来的影响。Li 等[23]建立了基于契约理论的激励机制,根据联邦学习的异质性,将参与者按训练能力水平进行区分,训练能力由数据规模、数据质量、计算能力构成,通过选择具有相近的高训练能力水平的客户参与全局模型训练。除了选择近似参与者的方法外,还有研究者提出了一些个性化的激励机制框架[24-26],用于解决数据异质性。解决数据异质性的激励机制方法还有数据贡献加权的方法[27],根据机构的数据贡献对其权重进行加权,减小数据样本不均衡带来的不平衡性。还可以通过奖励机制[28]激励参与者贡献高质量数据,鼓励参与者积极进行数据交换和共享。

机构之间的数据异质性问题使得激励机制的设计需要考虑这种数据差异带来的不契合或不公平问题,例如通过激励机制选择参与者时,不仅要考虑参与者的数据数量和质量,还要考虑其数据分布是否适合当前的项目或者是否能与其他参与者的数据进行配合,从而加快训练进程,或者通过激励机制分配贡献奖励时也要考虑小型机构与大型机构之间存在的天然的数据贡献的差异,从而避免部分参与者因这种天然限制而退出跨机构联邦学习。另外,数据异质性问题使得参与者对全局模型的需求也可能不同,激励机制的设计需要考虑这种差异,从而激励更多的机构参与联邦学习,丰富模型训练的数据多样性。数据异质性问题是机构合作的一道天然的屏障,解决机构之间的数据异质性问题是促使更多机构参与合作的基本要求之一。

3.3 公平性

公平是机构合作的基本要素，跨机构联邦学习的公平性问题是激励机制研究的重点方向。跨机构联邦学习的公平性[29]主要有3个方面：首先是不同参与者对模型的贡献不同，需要设计能公平反映每个参与者的贡献的奖惩机制；其次是无论参与方接收到的全局模型的用途是什么，最终其使用的模型在预测性或精确度上应该具有公平性；最后是需要统筹多种公平性之间的平衡性，不至于顾此失彼。公平性问题是跨机构合作的基本问题，不满足公平性要求的激励机制会降低参与者贡献数据的积极性[30]，造成参与者消极参与甚至中途退出等现象。对此，Zhuan 等[31]提出了公平意识激励机制，该机制通过设计一种新颖的模型梯度聚合方法来过滤低质量的局部模型梯度，以达到聚合公平的目的，同时采用 Shapley 值与声誉机制相结合的方法来确定分配给每个参与者的全局模型的性能水平，以达到奖励公平。Chu 等[32]提出了一种联邦估计方法，可以在不需要参与者的隐私信息的情况下准确估计模型的公平性。或者可以通过合理的奖励机制，针对企业的收益分配机制[33]，合理分配模型收益，以达到社会效益最大化。这里的社会效益指参与者均能在跨机构联邦学习中获得满意的收益。满足公平性要求的激励机制可以充分调动参与者的积极性，同时可以吸引更多的机构参与联邦学习。

3.4 基本问题之间的关联性和制约关系

基本问题之间不是独立存在的，尤其是数据异质性的存在影响着高隐私和公平的激励机制设计，一方面对于数据异质性的解决方案通常需要参与者的部分数据信息，以便筛选近似数据分布的参与者，但这显然侵犯了参与者的隐私，因此激励机制的设计需要考虑在不侵犯参与者数据隐私的情况下解决数据异质性问题；另一方面，由于数据异质性的问题，参与者之间的数据资源、计算资源等存在着明显的差异，这种差异使得低数据资源的参与者的数据贡献天然存在着限制，因此激励机制的设计需要考虑这种由于数据异质性带来的不公平问题。除此之外，高隐私性和公平性之间也存在着一些冲突，目前的高隐私性的激励机制通常是对上传的数据信息进行加密或者噪声化处理，这虽然提高了跨机构联邦学习的隐私保护级别，为公平的合作环境提供了基础，但也可能使得最终的贡献评估出现部分偏差，而精确的贡献评估是公平的激励机制的基本要求，这两者之间的平衡也是目前的激励机制设计要考虑的内容。数据异质性为高隐私性和公平性带来了更大的挑战，高隐私性为公平性提供了基础环境的同时也与其产生了部分冲突。

因此，由于3个基本问题之间的关联和制约，目前能同时解决3个基本问题的跨机构联邦学习的激励机制较少。如表2所列，目前大部分跨机构联邦学习的激励机制仅能解决1个或2个基本问题，可以同时解决3个基本问题的仅有1篇。这说明目前的跨机构联邦学习的激励机制设计仍然有提升的空间。可以预见，若能同时解决3个基本问题，那么无论是竞争性机构还是互补性机构都会愿意参加跨机构联邦学习并且积极贡献高质量数据。

表2 跨机构合作的基本问题

Table 2 Basic issues of cross-silo cooperation

文献	高隐私性	数据异质性	公平性
[12]	√	√	
[13]	√		√
[14]	√		
[15]	√	√	
[22]		√	
[30]			√
[31]	√		√
[32]			√
[34]	√		√
[35]	√	√	√
[36]	√		√
[37]			√
[38]	√		√

4 跨机构合作的合作模式

在跨机构联邦学习中，根据数据和模型的位置与管理方式，可以将跨机构合作分为以全局模型为中心的合作模式和以参与者为中心的合作模式。

4.1 以全局模型为中心的合作模式

以全局模型为中心的合作模式指所有参与者将其本地数据用于训练局部模型，将更新后的局部模型参数发送到参数服务器，参数服务器负责聚合所有参与者的模型参数，然后更新全局模型，并将更新后的模型参数再次分发给参与者。这种模式下，模型的训练和参数聚合都集中在全局模型上。在这种合作模式下，激励机制主要包括设计奖励机制来充分调动参与者贡献数据的积极性以及合理分配激励预算来保证全局模型训练的效率。

4.1.1 奖励机制

奖励机制指根据参与者的数据贡献以及对全局模型的有效影响来分配“奖励”，以激励机构积极参与数据共享和模型训练。常见的奖励机制包括数据贡献奖励、模型贡献奖励、模型性能奖励等。奖励机制通常由两个部分组成：贡献评估和奖励分配。

在奖励机制中，准确评估参与者在全局模型训练中的有效贡献是分配奖励的前提。在跨设备联邦学习中，有着许多贡献评估的研究综述[39]，其中 Shapley 值就是一种被广泛提到的贡献评估技术，但此前针对终端/边缘设备而设计的基于 Shapley 值的贡献测量方法并不适用于以机构作为参与者的跨机构联邦学习。因此，研究者们对 Shapley 值的应用进行了诸多的改进和研究[27,40-41]，使其更加适配跨机构联邦学习。Yang 等[40]提出了一种改进的贡献评估方法，通过为不必要的计算提出加权截断来改进 Shapley 值算法，并进一步使用动态规划，降低构建与参与者联盟对应的子模型并评估其准确性的计算成本，更高效率地对参与者进行贡献衡量。

奖励机制的另一重要组成部分就是“奖励”的设计与分配。全局模型对本地数据的适应性就是一种隐性的奖励，参与者贡献的优质数据越多，全局模型对本地数据集的适应性就越好，但这种奖励机制缺乏公平性，容易造成大型机构对小型机构的排挤。因此，有研究者设计了虚拟代币作为一种“奖励”。Tang 等[42]提出了一个跨机构联邦学习的激励

机制,该机制可以预测参与者训练本地模型的支出,对参与者的本地支出给予一定的代币补偿。通过这种方法使跨机构联邦学习达到社会效益最大化的目的,通过代币补偿的方式弥补参与者的损失,使参与者不会因为参与全局模型训练而变得更加糟糕。Han 等[34]提出了一种新颖的代币化激励机制,其中代币是为参与者提供相关服务和基础训练设施的支付费用,代币可以由可信任的第三方组织进行发放,以实现无延迟的代币奖励。该机制会对提供高质量数据的参与者和长期频繁参与全局模型训练的参与者给予一定的代币奖励,激励高质量数据持有者长期参与全局模型训练,同时若模型更新后的效用没有较大的提高,则该机制将基于参与者的损失给予一定的代币补偿。除了使用虚拟代币作为奖励之外,还有研究者提出可以用物质收益作为一种奖励。Huang 等[28]提出将全局模型中获得的市场收益作为奖励适当地分配给参与者,以此激励拥有高质量数据的参与者贡献更多的数据。

目前的奖励机制主要还是以虚拟代币或者全局模型的适用性作为奖励,其中虚拟代币可以转化为相应的物质收益,并设计相应的贡献评估机制(如 Shapley 值)作为分配机制,对高贡献的参与者给予相应的奖励,以此激励其贡献更多的数据。研究者们可以在贡献评估的准确性和"奖励"形式的多样性上进行深入研究,同时也需要考虑奖励分配的公平性和可持续性。

4.1.2　激励预算

激励预算指为促使机构参与联邦学习并贡献其数据和资源所需的成本。在一次跨机构合作中,激励预算是有限的,合理分配每个训练轮次的激励资源,可以有效地提高全局模型的训练效率并减少资源的过度消耗。Yang 等[43]提出了一种名为反向拍卖预算分配的激励预算分配算法,该算法通过建立高斯模型来分析奖励预算分配与全局模型的效用之间的关系,设计联邦学习过程中每个训练轮次的奖励预算分配,从而最大化全局模型的效用。Liu 等[44]为了最小化激励预算,通过定义两种私有类型的参与者,提出了一种基于二维契约理论的激励机制以及一种基于合约的聚合器,在最大化经济效益的同时提高全局模型的泛化精度。Yang 等和 Liu 等提出的方法的激励预算均由模型所有者提供。

目前在激励预算方面的激励机制研究较少,但其是机构合作的关键要点之一,机构不会在得到相对较少回报的情况下,在激励方面投入大量的资源。因此,如何降低激励成本预算并合理分配激励资源将成为一个值得深入讨论的研究方向。

4.2　以参与者为中心的合作模式

以参与者为中心的合作模式指每个参与机构都保留其本地数据,并在本地进行模型训练。训练后的模型参数通常不会离开参与者的设备,只有模型的更新版本(例如梯度)被聚合或共享给其他参与者。如图 3 所示,模式一由参与者轮流作为聚合中心的聚合更新梯度,模式二则是所有参与者均为聚合中心,参与者之间共享更新梯度。这种模式下,数据和模型都分布在各个参与者之间,没有一个中心化的全局模型。由于参与者之间的个体差异,不同机构的数据资源、模型需求等不尽相同,因此需要一种个性化的联邦学习[9]方法来满足其个性化的需求。以参与者为中心的合作模式就是一种个性化的联邦学习,相应的激励机制设计也更加偏向参与者而非全局模型。Cao 等[35]提出了一种新颖的联邦学习方法,基于未标记数据的伪标记,通过称为协同训练的过程,参与者可以学习其他参与者的数据的有效部分,用于训练自身的个性化模型。目前以参与者为中心的合作模式的研究较少,原因有两点:1)因为这种模型更新共享的模式可能会涉及到敏感数据和隐私信息,很多机构可能不愿意共享数据或让数据离开自己的环境;2)这种模式要建立合作伙伴之间的信任关系和有效的合作管理机制,这涉及到合作方的信誉、合作意愿、合作规则和机制的制定等,对于机构之间存在竞争关系或信任度不高的情况,会限制以参与者为中心的合作模式的实施。但是随着隐私保护技术的发展和合作伙伴关系之间信任的进一步建立,这种模式的应用可能会逐渐增多。

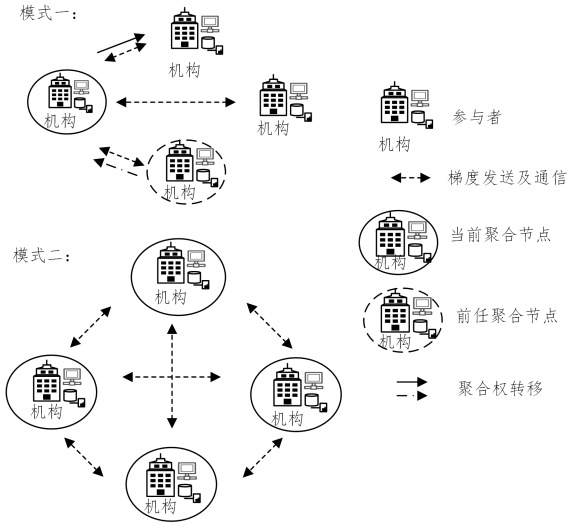

图 3　以参与者为中心的合作模式

Fig. 3　Cooperation model centered on participants

5　跨机构合作稳定发展的影响因素

在跨机构联邦学习中,跨机构合作过程中的稳定性和持续性受到以下几个关键因素的影响。

5.1　参与者的数据演变

数据演变指在跨机构合作中,参与者所持有的数据随着时间的推移和合作进展发生变化的现象。这种数据演变可能涉及新的数据样本的加入、数据标签的更新或更正,以及数据特征的变化。随着时间的推移,参与者可能新增、删除或修改其数据,这可能导致模型的性能变化、数据不一致性或概念漂移等问题,进而影响跨机构合作发展的稳定性。

对于如何解决参与者的数据演变问题,有研究者提出应用进化博弈论来设计激励机制的方法,以动态调整全局模型的训练过程。进化博弈论将数据演变问题转化为参与者的决策变动问题,从而不断调整行动策略来保持机构长期合作的稳定性。Luo 等[45]基于进化博弈论的视角,分析了 8 种不同的场景下联邦学习系统的进化稳定状态以及参数服务器和参与者的行动策略。Chen 等[46]提出了基于进化博弈论的动态

激励模型 DIM-DS,对参与者在数据共享中的博弈过程进行建模,分析参与者参与全局模型训练的决策,将生物进化与博弈中的参与者在做出决策的过程中不断调整策略以实现博弈平衡的思想相结合,允许参与者根据他们的当前信息调整自身的决策。DIM-DS 可以使参与者更加快速地参与全局模型训练并保持联邦学习的稳定性,以此激励更多的客户参与联邦学习,从而提高全局模型的性能。除了进化博弈论,还有研究者提出利用无限重复博弈论[47]来解决数据演变的问题,将数据变动的过程视为无限重复参与联邦学习的过程。Li 等[48]提出了一种基于无限重复博弈的激励机制 VARF,在这个博弈中客户由于数据的变动会多次重复地参与联邦学习,而 VARF 通过解决基于服务器和客户的无限重复博弈的效率最大化问题来优化参与者的长期收益,以保持合作的稳定性。

综上所述,通过应用进化博弈论和无限重复博弈论等激励机制,可以有效解决参与者数据演变问题,促进跨机构合作的稳定发展,并提高全局模型的性能。这些方法为解决合作过程中的数据不一致性、概念漂移等问题提供了一种理论和实践的指导,有助于构建更可靠和可持续的机构合作模式。

5.2 参与者合作关系的变动

参与者之间的合作关系会因为机构的业务需求、合作协议调整或者组织结构变化等原因而发生变动。这种合作关系的变动会影响跨机构合作发展的稳定性和持续性,例如业务需求的冲突会导致参与者可能不愿意贡献高质量的数据,合作协议的调整可能使参与者中途退出跨机构联邦学习等。在面对这种合作关系的变动方面,Jiang 等[36]提出了基于联盟博弈论的联邦学习框架,将不稳定的多方组织转化为由不相交的稳定联盟组成的结构化网络,并提出了一种成本分摊机制,将个人效用与其联盟的效用保持一致,以此促进组织之间稳定、长期的合作。Yuan 等[49]则提出了一种基于收益再分配的自适应激励机制,从历史潜在博弈中学习接近最优的数据贡献策略,而无需任何其他组织的私人信息,以在真实的动态训练环境中最大化其长期收益,通过这种长期的有效收益来保持整体合作的稳定。

目前,维持参与者合作关系的稳定方法包括:将不稳定的整体联盟架构调整为多个稳定的小联盟组成的结构化网络,以及将长期的有效收益作为机构之间互相合作的粘合剂。

5.3 参与者的负面行为

参与者的负面行为也是影响跨机构合作稳定发展的重要因素,本节主要对当前主要的参与者负面行为及其解决办法进行总结分析。

5.3.1 未尽最大努力

在跨机构联邦学习中,会出现参与者未尽最大努力参与模型训练的情况。Lu 等[50]开发了一个真实激励机制 TEA,通过设计一个转移支付规则将参与者的收益和全局模型的效用绑定,使参与者如实报告个人信息成为纳什均衡,从而激励参与者提供高质量数据参与模型训练。Xiong 等[51]通过多重信誉机制来评估客户的真实性和可靠性,并引入反向拍卖来选择最优参与者。除了参与者存在不尽最大努力参与模型训练外,第三方参数服务器也有可能出现不尽最大努力聚合模型的情况。Xu 等[52]提出了参与者与参数服务器双方均存在不尽最大努力参与模型训练的情况,并推导出了一种最优的多阶段契约理论激励机制来最大限度地降低这种风险。不尽最大努力参与模型训练在真实的联邦学习环境中是一种常见的负面行为,一个合理的激励机制就是最好的解决方法。

5.3.2 搭便车行为

搭便车指某些机构在参与联邦学习的过程中,试图从其他参与机构的贡献中获益,而不主动分享自己的数据或模型更新。这种不劳而获的行为严重破坏了跨机构合作发展的稳定性。对于搭便车行为,研究者首先提出了检测搭便车者的识别机制。Lin 等[53]提出了一种高维异常检测方法,通过检测异常的梯度更新来识别搭便车者。Huang 等[54]设计了一种名为梯度审计的保护机制来检测和惩罚搭便车行为。Fraboni 等[57]通过研究分析搭便车者的行为模式,得出应将检查客户端的分布作为检测搭便车行为的常规方法。但仅仅只是检测出搭便车者并不能满足跨机构合作稳定发展的需求,研究者们提出通过收益调整和惩罚机制来遏制搭便车行为。Zhang 等[55]在无限重复博弈中,推导出了一个子博弈完美纳什均衡,即通过惩罚机制强制执行的参与者合作方案,该方案可以将部分搭便车者转变为数据贡献者,有效减少搭便车者的数量,并且增加本地模型的训练数据量。Chen 等[56]将跨机构联邦学习中各组织之间的互动建模为公共物品博弈,使用多人多动作零决定因素策略来最大化跨机构联邦学习中的社会效益,以此遏制搭便车行为的出现。这些方法基于博弈论设计跨机构联邦学习的激励机制,使贡献数据成为纳什均衡的条件,旨在促进跨机构联邦学习的稳定发展和公平合作,确保每个机构都积极参与并做出贡献,而不是只从其他机构中获益而不付出努力。通过综合运用这些方法,可以更好地应对搭便车行为,推动跨机构联邦学习的可持续发展。

5.3.3 低效用的局部模型更新

在跨机构联邦学习中,无论是无意的还是有意的,总会有一些参与者的局部模型的本地训练效果较差,导致其模型更新的质量较低。这种低质量的局部模型更新会降低全局模型的收敛速度,同时造成资源的浪费。对此,一种显而易见的解决方法就是筛选并过滤低质量的局部模型更新,从而保证聚合的模型更新参数是较高质量的。Ranathunga 等[38]就采用了一种新颖的聚合器分层网络,用于检测低质量模型的更新。另一种解决方法则是激励参与者使用高质量数据训练本地模型,以提高模型更新质量。Qi 等[57]提出了一种用于高质量模型聚合的信誉机制,通过透明化的、公平的联邦学习进程,激励参与者贡献高质量的数据来训练本地模型,以此提高模型更新的质量。低效用的局部模型训练是对资源的一种浪费,这对于跨机构合作的持续性有着一定的影响。通过激励和过滤的方式可以有效地减少这种现象的出现,有利于跨机构联邦学习的可持续发展。

6 跨机构联邦学习激励机制的比较

本节对目前的跨机构联邦学习的激励机制研究的性能特性进行了对比分析,从个体理性、激励相容性、帕累托效率、预算平衡、鲁棒性和计算成本 6 个方面进行了比较。

以下是部分特性的说明。

1）个体理性：只有当所有参与者都有非负利润时，激励机制才是个体理性的，即当跨机构联邦学习的收益低于其成本时，机构会犹豫是否参加跨机构联邦学习。

2）激励相容性：当所有参与者如实声明其贡献和成本类型是最优时，激励机制具有激励相容的特性，伪造信息不会给恶意参与者带来收益。

3）帕累托效率：当社会剩余最大化时，激励机制具有帕累托效率，即跨机构联邦学习的整体收益最大化。

4）预算平衡：当且仅当参与者的支付总额不超过模型所有者或参与者服务器给出的激励预算时，激励机制才是预算平衡的。

5）鲁棒性：当跨机构联邦学习进程在突发情况下仍能正常进行并且能得到及时解决时，其激励机制具有稳定性。

表3列出了跨机构联邦学习的激励机制的性能特性。现有工作在帕累托效率方面较为欠缺，说明目前的参与者可能对于个体利益的关注大于整体利益；在鲁棒性方面现有工作的重视度不高，然而这是跨机构合作长期发展的重要影响因素，需要增加重视度。另外，部分激励机制通过与其他强化技术相结合来提升跨机构联邦学习的整体效用，虽然带来了较好的效果，但是额外的计算成本也成为了性能提升的阻碍。

表3　跨机构联邦学习的激励机制的性能特性对比表

Table 3　Performance characteristic comparison of incentive mechanism of cross-silo federated learning

问题	文献	关键技术	个体理性	激励相容性	帕累托效率	预算平衡	鲁棒性	计算成本
3.1	[13]	拍卖理论，差分隐私	√	√				高
	[14]	博弈论，差分隐私	√	√	√			高
	[15]	反向拍卖理论，差分隐私	√	√	√			低
3.2	[30]	契约理论	√			√	√	
3.3	[31]	公平意识激励机制	√	√			√	高
4.1.1	[28]	博弈论	√					
	[35]	Shapley 值						低
	[37]	博弈论	√	√	√	√		
	[34]	代币机制	√			√	√	
4.1.2	[43]	拍卖理论，贝叶斯优化	√			√		
	[44]	二维契约理论	√	√		√		高
5.1	[46]	进化博弈论	√	√		√	√	高
	[48]	无限重复博弈，质量感知，信誉感知	√	√	√		√	高
5.2	[36]	联盟博弈论			√	√	√	
	[49]	多智能体强化学习	√	√	√		√	
5.3.1	[50]	博弈论	√	√	√	√	√	
	[51]	拍卖理论，信誉机制	√	√	√	√	√	
	[52]	契约理论	√				√	
5.3.2	[55]	无限重复博弈	√	√	√		√	高
5.3.3	[57]	信誉机制	√	√			√	

7　跨机构合作的未来研究方向

随着时间的推移，跨机构联邦学习的激励机制在许多领域取得了大量的研究成果，涉及隐私安全、公平性和数据异质性等方面。然而，仍然存在一些领域未能得到充分的开发和深入研究。

1）联邦学习框架的异构性：随着联邦学习的发展，不同机构很可能拥有各自独特的联邦学习框架，具有不同的模型聚合方法、数据收集方法和激励机制等，这种差异是联邦学习框架的异构性。未来的跨机构联邦学习可能是由多个不同联邦学习框架组成的复合跨机构联邦学习。对于这种复合跨机构联邦学习，如何设计合理的激励机制来处理不同联邦学习框架之间的异构性将成为未来新兴的研究方向。

2）联邦学习全局模型的准确性：现有的跨机构联邦学习的激励机制大多着重于全局模型训练的效率、公平性、隐私安全等方面，较少关注全局模型的准确性。对于一些普通行业而言，模型准确性可能并不是特别重要，然而，在某些特殊领域，如医疗领域，模型的准确性至关重要。例如，在准确预测疾病方面[58]，模型准确性显然比模型的泛用性更加重要，因为没有患者愿意得到错误的病情判断。因此，未来或许可以在牺牲全局模型的训练效率的情况下，采用更加复杂但精确的聚合算法来增加全局模型的预测准确性。

3）联邦学习大模型的计算效率：联邦学习大模型是近年来提出的一个新颖概念，旨在利用联邦学习来训练像 ChatGPT 这样的大型数据模型。然而，这类大模型的一轮训练涉及到巨量的训练数据，即使采用联邦学习这种分布式计算方式，对计算和通信资源的消耗也只是杯水车薪。因此，未来跨机构联邦学习大模型的激励机制的设计目标是，如何激励这些拥有巨量数据的大企业参与大模型的训练，同时减少计算开销和通信资源的消耗。

结束语　随着大数据时代的发展，机构之间的数据共享变得愈发困难。跨机构联邦学习的出现有效解决了隐私数据共享的难题，但同时也出现了新的问题，那就是如何激励更多的机构参加跨机构联邦学习并且积极贡献高质量数据。本文从跨机构合作的角度，针对跨机构合作过程中不同效用的激励机制设计，从跨机构合作的基本问题、合作模式、稳定发展的影响因素3个方面对现有跨机构联邦学习的激励机制研究进行综述，并对跨机构联邦合作的未来方向进行展望。

参 考 文 献

[1] MCMAHAN B，MOORE E，RAMAGE D，et al. Communication-efficient learning of deep networks from decentralized data

[C]// Artificial Intelligence and Statistics. PMLR, 2017: 1273-1282.
[2] NIE W, XIN L, LI Z. Study on the Application of Federated Learning in Medical Informatization[J]. Journal of Medical Informatics, 2022, 43(10): 12-13.
[3] ZHAN Y, ZHANG J, HONG Z, et al. A survey of incentive mechanism design for federated learning[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 10(2): 1035-1044.
[4] ZENG R, ZENG C, WANG X, et al. Incentive Mechanisms in Federated Learning and A Game-Theoretical Approach [J]. IEEE Network, 2022, 36(6): 229-235.
[5] LIANG W, LIU B, LIN W, et al. Survey of Incentive Mechanism for Federated Learning [J]. Computer Science, 2022, 49(12): 46-52.
[6] TU X, ZHU K, LUONG N, et al. Incentive mechanisms for federated learning: From economic and game theoretic perspective [J]. IEEE Transactions on Cognitive Communications and Networking, 2022, 8(3): 1566-1593.
[7] WITT L, HEYER M, TOYODA K, et al. Decentral and Incentivized Federated Learning Frameworks: A Systematic Literature Review [J]. IEEE Internet of Things Journal, 2023, 10(4): 3642-3663.
[8] LIU Y, KANG Y, ZOU T, et al. Vertical federated learning [J]. arXiv: 2211. 12814, 2022.
[9] YAN Y, LIGETI P. A Survey of Personalized and Incentive Mechanisms for Federated Learning [C]// 2022 IEEE 2nd Conference on Information Technology and Data Science. IEEE, 2022: 324-329.
[10] HUANG C, HUANG J, LIU X. Cross-silo federated learning: Challenges and opportunities [J]. arXiv: 2206. 12949, 2022.
[11] DWORK C. Differential privacy [C]// International Colloquium on Automata, Languages, and Programming. Berlin, Heidelberg: Springer, 2006: 1-12.
[12] WANG C, WU X, LIU G, et al. Safeguarding cross-silo federated learning with local differential privacy [J]. Digital Communications and Networks, 2022, 8(4): 446-454.
[13] REN K. Differentially Private Auction for Federated Learning with Non-IID Data [C] // 2022 International Conference on Service Science. IEEE, 2022: 305-312.
[14] ZHANG L, ZHU T, XIONG P, et al. A Game-theoretic Federated Learning Framework for Data Quality Improvement [J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(11): 10952-10966.
[15] WANG D, REN J, WANG Z, et al. PrivAim: A Dual-Privacy Preserving and Quality-Aware Incentive Mechanism for Federated Learning [J]. IEEE Transactions on Computers, 2023, 72(7): 1913-1927.
[16] WEI K, LI J, DING M, et al. Federated learning with differential privacy: Algorithms and performance analysis[J]. IEEE Transactions on Information Forensics and Security, 2020(15): 3454-3469.
[17] LIU K, HU S, WU S Z, et al. On privacy and personalization in cross-silo federated learning [J]. Advances in Neural Information Processing Systems, 2022, 35: 5925-5940.
[18] ZHENG S, CAO Y, YOSHIKAWA M. Secure shapley value for cross-silo federated learning [J]. arXiv: 2209. 04856, 2022.
[19] LUO F, AL-KUWARI S, DING Y. SVFL: Efficient Secure Aggregation and Verification for Cross-Silo Federated Learning [J]. IEEE Transactions on Mobile Computing, 2022(1): 1-14.
[20] TRAN H Y, HU J, YIN X, et al. An Efficient Privacy-Enhancing Cross-Silo Federated Learning and Applications for False Data Injection Attack Detection in Smart Grids [J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2538-2552.
[21] LI Q, WEN Z, WU Z, et al. A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection [J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(4): 3347-3366.
[22] ZHANG W, ZHOU T, LU Q, et al. Dynamic-fusion-based federated learning for COVID-19 detection [J]. IEEE Internet of Things Journal, 2021, 8(21): 15884-15891.
[23] LI L, YU X, CAI X, et al. Contract-Theory-Based Incentive Mechanism for Federated Learning in Health CrowdSensing [J]. IEEE Internet of Things Journal, 2022, 10(5): 4475-4489.
[24] LI B, SHI Y, GUO Y, et al. Incentive and Knowledge Distillation Based Federated Learning for Cross-Silo Applications [C] // IEEE INFOCOM 2022 — IEEE Conference on Computer Communications Workshops. IEEE, 2022: 1-6.
[25] TRAN V T, PHAM H H, WONG K S. Personalized privacy-preserving framework for cross-silo federated learning [J]. arXiv: 2302. 12020, 2023.
[26] LUO J, WU S. Adapt to Adaptation: Learning Personalization for Cross-Silo Federated Learning [C]// IJCAI: Proceedings of the Conference. 2022.
[27] YANG X, TAN W, PENG C, et al. Federated learning incentive mechanism design via enhanced Shapley value method [J]. Wireless Communications and Mobile Computing, 2022, 22: 1-11.
[28] HUANG C, KE S, KAMHOUA C, et al. Incentivizing data contribution in cross-silo federated learning[J]. arXiv: 2203. 03885, 2022.
[29] GU T, LI L, CHANG L, et al. Fair federated machine learning and its design: A comprehensive survey [J]. Chinese Journal of Conputers, 2020, 46(9): 1991-2024.
[30] TRAVADI Y, PENG L, BI X, et al. Welfare and Fairness Dynamics in Federated Learning: A Client Selection Perspective [J]. arXiv: 2302. 08976, 2023.
[31] SHI Z, ZHANG L, YAO Z, et al. FedFAIM: A Model Performance-based Fair Incentive Mechanism for Federated Learning [J]. IEEE Transactions on Big Data, 2022(1): 1-13.
[32] CHU L, WANG L, DONG Y, et al. Fedfair: Training fair models in cross-silo federated learning [J]. arXiv: 2109. 05662, 2021.
[33] ZHANG X, DOU Y, ZHANG C, et al. Reserch on the Profit-sharing Mechanism for Federated Learning [J]. Frontiers of Science and Technology of Engineering Management, 2023, 42(2): 8-15.
[34] HAN J, KHAN A F, ZAWAD S, et al. Tiff: Tokenized incentive for federated learning [C]// 2022 IEEE 15th International Conference on Cloud Computing. IEEE, 2022: 407-416.

[35] CAO X,LI Z,SUN G,et al. Cross-Silo Heterogeneous Model Federated Multitask Learning [J]. arXiv:2202.08603,2022.

[36] JIANG S,WU J. Coalition Formation Game in the Cross-Silo Federated Learning System [C]// 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems. IEEE,2022:49-57.

[37] FRABONI Y,VIDAL R,LORENZI M. Free-rider attacks on model aggregation in federated learning [C] // International Conference on Artificial Intelligence and Statistics. PMLR,2021:1846-1854.

[38] RANATHUNGA T,MCGIBNEY A,REA S,et al. Blockchain-Based Decentralized Model Aggregation for Cross-Silo Federated Learning in Industry 4.0 [J]. IEEE Internet of Things Journal,2022,10(5):4449-4461.

[39] WANG Y,LIG,LI K. Survey on Contribution Evaluation for Federated Learning [J]. Journal of Software,2023,34(3):1168-1192.

[40] YANG C,LIU J,SUN H,et al. WTDP-Shapley:Efficient and Effective Incentive Mechanism in Federated Learning for Intelligent Safety Inspection [J]. IEEE Transactions on Big Data,2022(1):1-10.

[41] WANG Z,YAN B,DONG A. Blockchain Empowered Federated Learning for Data Sharing Incentive Mechanism [J]. Procedia Computer Science,2022,202:348-353.

[42] TANG M,WONG V. An incentive mechanism for cross - silo federated learning:A public goods perspective [C]// IEEE INFOCOM 2021 — IEEE Conference on Computer Communications. IEEE,2021:1-10.

[43] YANG Y,ZHOU Y,HU M,et al. BARA:Efficient Incentive Mechanism with Online Reward Budget Allocation in Cross-Silo Federated Learning[J]. arXiv:2305.05221,2023.

[44] LIU Y,TIAN M,CHEN Y,et al. A contract theory based incentive mechanism for federated learning [M] // Federated and Transfer Learning. Cham: Springer International Publishing,2022:117-137.

[45] LUO X,ZHANG Z,HE J,et al. Strategic Analysis of the Parameter Servers and Participants in Federated Learning:An Evolutionary Game Perspective [J]. IEEE Transactions on Computational Social Systems,2024,11(1):132-143.

[46] CHEN Y,ZHANG Y,WANG S,et al. Dim-ds:Dynamic incentive model for data sharing in federated learning based on smart contracts and evolutionary game theory [J]. IEEE Internet of Things Journal,2022,9(23):24572-24584.

[47] WANG W. Research on Incentive Mechanism of Federated Learning Based on Repeated Game [D]. Xi'an:Xidian University,2022.

[48] LI Y,WANG X,ZENG R,et al. VARF:An Incentive Mechanism of Cross-silo Federated Learning in MEC [J]. IEEE Internet of Things Journal,2023,10(17):15115-15132.

[49] YUAN S,LIU H,LV H,et al. Adaptive incentive for cross-silo federated learning: A multi-agent reinforcement learning approach [J]. arXiv:2302.07493,2023.

[50] LU J,PAN B,SEID A,et al. Truthful incentive mechanism design via internalizing externalities and lp relaxation for vertical federated learning [J]. IEEE Transactions on Computational Social Systems,2023,10(6):2909-2923.

[51] XIONG A,CHEN Y,CHEN H,et al. A Truthful and Reliable Incentive Mechanism for Federated Learning Based on Reputation Mechanism and Reverse Auction [J]. Electronics,2023,12(3):517-540.

[52] XU H,NANDA P,LIANG J,et al. The Force of Compensation,a Multi-stage Incentive Mechanism Model for Federated Learning[C]// International Conference on Network and System Security. Cham:Springer Nature Switzerland,2022:357-373.

[53] LIN J,DU M,LIU J. Free-riders in federated learning:Attacks and defenses [J]. arXiv:1911.12560,2019.

[54] HUANG J,TALBI R,ZHAO Z,et al. An exploratory analysis on users' contributions in federated learning [C]// 2020 Second IEEE International Conference on Trust,Privacy and Security in Intelligent Systems and Applications. IEEE,2020:20-29.

[55] ZHANG N,MA Q,CHEN X. Enabling Long-Term Cooperation in Cross-Silo Federated Learning:A Repeated Game Perspective [J]. IEEE Transactions on Mobile Computing,2023,22(7):3910-3924.

[56] CHEN J,HU Q,JIANG H. Social welfare maximization in cross-silo federated learning [C] // 2022 IEEE International Conference on Acoustics,Speech and Signal Processing(ICASSP 2022). IEEE,2022:4258-4262.

[57] QI J,LIN F,CHEN Z,et al. High-quality model aggregation for blockchain-based federated learning via reputation-motivated task participation [J]. IEEE Internet of Things Journal,2022,9(19):18378-18391.

[58] PANDL K,LEISER F,THIEBES S,et al. Reward Systems for Trustworthy Medical Federated Learning [J]. arXiv: 2205.00470,2022.

WANG Xin, born in 1984, Ph.D, associate professor, master supervisor, is a member of CCF(No. 11687M). His main research interests include machine learning, big data analysis and federated learning.

(责任编辑:喻藜)