基于联邦学习的移动通信资源管理:方法、进展与展望

孙恩昌[1], 张 卉[1], 何若兰[1], 张冬英[2], 张延华[1,3]
(1. 北京工业大学信息学部, 北京 100124; 2. 北京工业大学信息化建设与管理中心, 北京 100124;
3. 先进信息网络北京实验室, 北京 100124)

摘 要: 由于联邦学习(federated learning, FL)具有在参与方不共享数据的情况下即可进行模型训练,在保护数据隐私的同时,实现有效的资源管理等特点,FL已成为移动通信资源管理领域的研究热点之一. 因此,对FL在移动通信资源管理中的方法、进展与展望进行综述与分析. 首先,在引入FL基本概念的基础上,重点对FL在分布式无线网络、移动边缘网络、车联网、雾无线接入网络和超密集网络场景中资源管理方法的性能进行讨论,并分析其优缺点;然后,结合FL在移动通信资源管理领域的研究进展,讨论FL面临的挑战并提出可行的解决方案;最后,展望FL在移动通信资源管理领域潜在的发展方向.

关键词: 联邦学习; 共享数据; 数据隐私; 移动通信; 资源管理; 机器学习
中图分类号: TN 915 **文献标志码**: A **文章编号**: 0254 - 0037(2022)07 - 0783 - 11
doi: 10.11936/bjutxb2021030017

Mobile Communication Resource Management Based on Federated Learning: Methods, Progress and Prospect

SUN Enchang[1], ZHANG Hui[1], HE Ruolan[1], ZHANG Dongying[2], ZHANG Yanhua[1,3]
(1. Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China;
2. Information Technology Support Center, Beijing University of Technology, Beijing 100124, China;
3. Beijing Laboratory of Advanced Information Networks, Beijing 100124, China)

Abstract: Federated learning (FL) has the characteristic of implementing model training without data sharing and operating effective resource management while protecting data privacy. Therefore, it has become one of the research hotspots in the field of mobile communication resource management. In this survey, the algorithms, progress and future trends of FL in mobile communication resource management were summarized and analyzed. First, the basic concept of FL was introduced. Then, the performance of FL resource management methods in distributed wireless network, mobile edge network, Internet of vehicles, fog radio access network, and ultra dense network scenarios were discussed, and their advantages and disadvantages were analyzed. Based on the progress of FL, the open issues of FL were analyzed, and the possible solutions were proposed. Finally, the potential development trends of FL in the field of mobile communication resource management were prospected.

Key words: federated learning (FL); shared data; data privacy; mobile communication; resource management; machine learning

---

收稿日期: 2021-03-22; 修回日期: 2021-05-24
基金项目: 国家自然科学基金资助项目(61671029); 中国国家留学基金资助项目(2018-10038); 北京市博士后工作经费资助项目(ZZ2019-73).
作者简介: 孙恩昌(1977—), 男, 副教授, 主要从事无线通信与网络、区块链、联邦学习、深度学习方面的研究, E-mail: ecsun@bjut.edu.cn

随着数字化进入高速发展时期,大数据和人工智能(artificial intelligence, AI)等技术迎来爆发式增长的同时移动网络也更加自主化、异构化和动态化,这使得网络资源的有效分配愈加复杂和困难. 因此,快捷且高效地分配和管理通信网络资源愈发迫切. 另外,加之人们信息保护意识的增强以及数据传输效率要求的提高,联邦学习(federated learning, FL)[1]成为解决上述问题的有效技术之一.

FL 于 2016 年由谷歌提出,已经成为 AI 研究与应用领域的焦点,有望成为下一代 AI 协作网络架构的基础[2]. 它作为一个较新的机器学习范例,一经推出便受到了广泛的关注. 与传统的机器学习相比,FL 能够提高学习效率,保护数据隐私,并且解决数据孤岛问题. 国内外 FL 的相关研究主要针对学习算法设计、激励机制设计与安全算法和计算与通信资源优化等. 目前,FL 在移动通信领域的研究进展主要侧重于在保护数据安全与隐私的同时对移动通信资源进行智能和有效的管理.

在移动通信中引入 FL,带来诸多便利的同时也面临着挑战,例如能量分配、功率控制、计算与通信开销的优化等. 与已有的 FL 资源管理方法综述不同,本文首先重点介绍了 FL 在不同网络场景,如分布式无线网络、移动边缘网络、车联网、雾无线接入网络(fog radio access network, F-RAN)和超密集网络等场景中的资源管理方法,纵向总结和横向比较各种方法的性能与不足;然后,给出了 FL 资源管理相关研究的主要挑战;最后,对 FL 资源管理未来潜在的研究方向进行了展望.

1 FL 基础知识

1.1 FL 概念

目前,对于 FL 概念有诸多描述,具有代表性的有:FL 是一种在不共享数据的情况下完成联合建模的技术[1];FL 是一种用加密机制完成数据传输从而在客户端建立高质量模型的框架[2];FL 是设备与中央服务器协作以进行分布式机器学习设置的方法[3];等等. 综上分析,本文认为 FL 是一种分布式机器学习方法,用于建立终端设备与服务器之间的共享模型,即各个参与者利用本地数据进行训练并将获得的模型训练参数上传至服务器,再由服务器进行聚合,更新得到总体参数,然后不断迭代直至达到给定精度的学习方法.

1.2 FL 分类

根据数据集分布情况的不同,FL 一般分为横向 FL(horizontal federated learning, HFL)、纵向 FL(vertical federated learning, VFL)和联邦迁移学习(federated transfer learning, FTL)[1].

1) HFL:在数据集间不同用户具有相同业务需求的情况下引入,将数据集按照横向(用户维度)划分(见图 1),取出具有相同业务需求的用户数据进行联合训练以扩大训练的样本空间. 由于数据集间具有相同业务需求的用户是不完全相同的,故数据集间用户相似度少,用户业务需求相似度多.

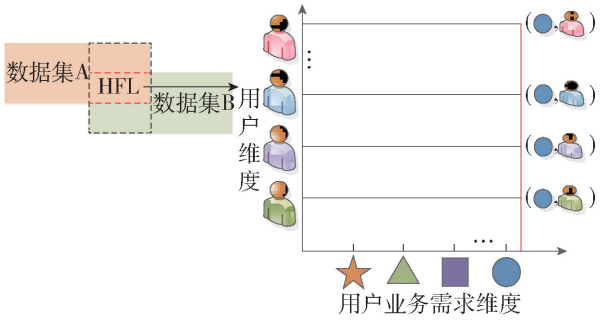

图 1 横向 FL[1]

Fig. 1 Horizontal federated learning[1]

2) VFL:在数据集间相同用户具有不同业务需求的情况下引入,将数据集按照纵向(用户业务需求维度)划分(见图 2),取出具有不同业务需求的用户数据进行联合训练以增强用户训练模型的效果. 由于数据集间相同用户分别有不完全相同的业务需求,故数据集间用户相似度多,用户业务需求相似度少.

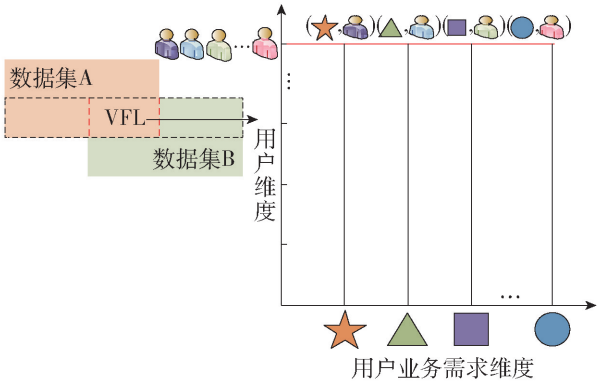

图 2 纵向联邦学习[1]

Fig. 2 Vertical federated learning[1]

3) FTL:在数据集间不同用户具有不同业务需求的情况下引入,不对数据集进行切分,如图 3 所示. 因数据集间不同用户具有不同的业务需求,故

数据集间用户和用户业务需求相似度都较少，利用迁移学习辅助 FL 训练以克服数据集间用户和用户业务需求相似度少引起的训练数据不足的问题[4].

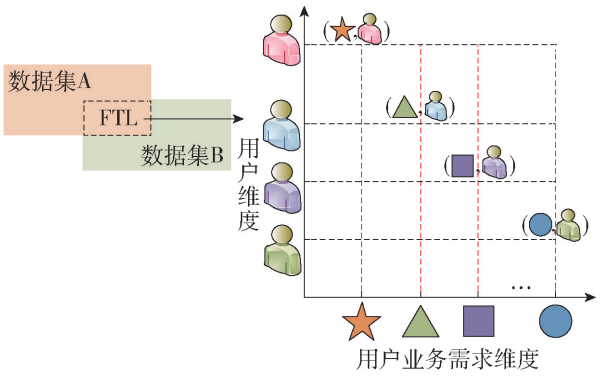

图 3　联邦迁移学习[1]

Fig. 3　Federated transfer learning[1]

本文对比了 3 类 FL 的主要特征，如表 1 所示. HFL、VFL 和 FTL 三者的本质区别在于不同数据集之间用户和用户业务需求的相似度.

表 1　3 类 FL 对比

Table 1　Comparison of three types of FL

类别	用户相似度	用户业务需求相似度	切分维度	应用场景
HFL	少	多	横向	用户不同需求相同
VFL	多	少	纵向	用户相同需求不同
FTL	少	少	无	用户不同需求不同

1.3　FL 主要特点

与其他机器学习相比，FL 主要具有如下特点：

1）保护用户隐私. 数据存储在本地，各个参与方数据不共享，保证了用户数据隐私[1].

2）参与方享有平等地位. 各参与方享有对等地位，实现共同繁荣[2].

3）保证训练出的模型效果无损. FL 模型训练过程中不会出现负迁移，保证联邦模型比独立模型效果好[5].

4）低延迟. 仅将模型更新参数上传至服务器进行全局聚合[6].

本文对 FL 与传统分布式机器学习[7]进行了对比，如表 2 所示. FL 相较于传统分布式机器学习最大的优点是 FL 在保护用户隐私的同时，还可以完成数据参数的高效传输.

表 2　FL 与传统分布式机器学习对比

Table 2　Comparison between FL and traditional distributed machine learning

类别	数据属性	控制权	数据存储方式	数据传输量	隐私保护性
FL	非独立同分布	本地或边缘节点	本地	少	强
分布式机器学习	独立同分布	中心服务器	中心服务器	多	弱

2　基于 FL 的通信资源管理方法

FL 主要包括 2 个核心过程（见图 4）：1）设备在本地训练完成后，将模型训练参数上传至服务器；2）服务器对各个设备的模型训练参数进行聚合和更新. 为了提高移动通信资源管理的效率，一些研究已经在相关领域场景中探索将 FL 与其他算法或技术相结合. 本节详细介绍 FL 在分布式无线网络、移动边缘网络、车联网、F-RAN 和超密集网络场景中资源管理方法的研究进展.

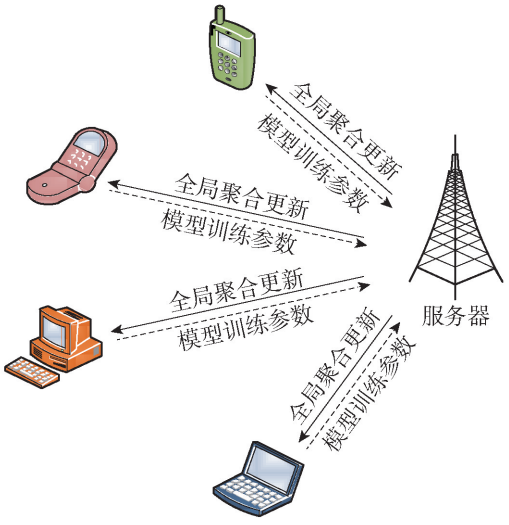

图 4　FL 工作过程

Fig. 4　Working process of FL

2.1　FL 与分布式无线网络

分布式无线网络是由分布在不同地点的终端节点互联而成的网状结构. 随着网络中新兴应用的增加，设备在进行数据处理时容易受到能量有限的制约. 为此，有学者利用 FL 以分布式方式训练模型的特点将上述问题优化为 FL 训练时间和设备能耗最小化问题[8-9]. 在能量有限情况下，文献[8]以 FL 模型训练时间最小化为目标，利用在线逐次凸逼近方法来解决 FL 训练时间与计算之间的随机非凸优

化问题. 在每次 FL 迭代过程中,利用网络接入点作为设备和中心服务器的中继点以提高系统更新参数的性能,根据设备能耗和信道估计不完全的实际条件与网络接入点和服务器之间实际能耗需求进行功率分配,在减少 FL 训练时间的同时,优化服务器聚合参数的频率. 受此启发,文献[9]提出低复杂度的迭代算法,利用 FL 低延迟的特点,在每一次迭代时实时推导出新的功率分配和带宽分配的封闭解,根据每一次迭代过程的封闭解调整和优化下一迭代过程中模型的参数,达到了消耗总能量少、资源利用率高的目标. 当参与设备较多时,能量利用率会急剧下降. 针对这一缺陷,文献[10]考虑到在无线网络中执行 FL 有时会受到能量限制,提出光波传输功率方案,每个设备通过红外光和可见光收集能量,利用所收集的能量执行计算和参数传输任务. 因为设备进行计算时比参数传输时消耗的能量多,所以 Tran 等[10]指出应尽可能地为计算过程分配更多的能量. 为了进一步优化传输功率,文献[11]提出度量参数更新时效性(age of update, AoU)算法,首先将需要向中心服务器发送的训练数据分离,使其保留在本地设备训练,然后将模型训练参数上传至服务器,服务器根据设备更新参数快慢进行功率分配,得到了在给定资源块约束下的最佳传输功率,但是该方法延迟较大. 对此不足,文献[12-13]做出改进. 与文献[11]相比,文献[12]同时考虑了资源块和设备能量的约束,提出一种启发式算法,利用 FL 支持服务器与设备共享模型参数的特点,研究了优化资源块分配和设备功率选择问题,相较于 AoU 算法,该算法有效降低了延迟. 文献[13]基于 FL 提出数字孪生(digital twin, DT)算法并将其应用于分布式无线网络,设备通过 DT 将局部模型参数直接映射到服务器,实现设备与服务器之间几乎实时的连接.

特别地,利用 FL 还可以实现分布式无线网络中带宽和功率的有效管理. 在带宽有限的条件下,文献[14]发现在不同的信噪比阈值下 FL 达到给定收敛域的速度不同,根据 FL 不同的收敛速度自适应调整用户设备的调度策略,然后利用最优化理论和随机几何推导分析得出用户设备数量和信道带宽之间的权衡. 进一步,文献[15]提出设备调度和带宽分配的具体策略,首先 FL 系统地协调服务器和设备上的模型训练以更快适应设备的计算能力和状态,从而保证设备的学习性能,然后根据上述状态优先调度计算能力或信道优先级高的用户设备,对于计算能力较差或信道较弱的设备,分配给其更多的带宽,这样可以在避免带宽浪费的同时降低能量消耗,但其受到延迟制约. 为了尽可能降低延迟,Shi 等[16]同样从用户设备调度和带宽分配问题出发进行研究,带宽分配同样采用文献[15]的策略,而设备调度则采用贪婪策略. 服务器根据各网络节点中分布的数据,快速地选择模型更新中消耗资源最少的用户设备执行任务,直到每轮学习效率和延迟之间取得较好的平衡. 与文献[14-16]所述不同的是,文献[17]提出自适应压缩 FL 共享参数算法,该算法在服务器获取各设备共享参数的基础之上,根据设备数量自适应调整 FL 共享参数信息的压缩率来适应动态带宽,但参数压缩率较低时,其在不可靠的网络条件下表现不佳. 针对此不足,文献[18]提出基于 FL 的动态缓存分配(federated learning-based dynamic cache allocation, FedCache)方案. FedCache 使用 FL 学习低通信开销的缓存分配,使边缘节点在本地学习以适应不同的网络条件并协作共享这些信息,服务器根据网络中设备的缓存效率,将带宽公平地分配给这些相互竞争的设备. 关于功率的有效分配,文献[19]提出基于支持向量机(support vector machine, SVM)的 FL,该方案使服务器和用户设备关联并建立全局 SVM 模型,服务器收集关联用户设备的相关任务信息,而 SVM 模型则用来分析未来关联设备与当前时隙中每个设备要处理的任务,然后结合梯度下降方法优化每个设备的功率和任务分配,使任务计算和参数传输时消耗能量最小. 文献[20]优先考虑设备服务质量(quality of service, QoS)要求,提出采用动作评价(actor-critic, AC)算法. FL 将 AC 模型作为局部训练模型,每个设备通过 FL 训练本地 AC 模型,将产生的梯度和权重上传到服务器聚合,实现边缘用户协作的同时获得功率分配策略. 相较于基于 FL 的 SVM 算法,该算法具有较好的收敛性、鲁棒性和更高的功率分配精度.

综上所述,基于 FL 的分布式无线网络资源管理方法,实现了能量、带宽和功率的有效管理. 其不需要将原始模型数据上传至服务器,仅将模型训练参数上传,为设备的训练过程提供了安全可靠的训练机制,有效地代替了传统分布式机器学习训练模型的方法,大大降低了系统的能耗,避免了资源浪费,提升了分布式无线网络的安全隐私性.

本文总结了基于 FL 的分布式无线网络资源管理方法,如表 3 所示. 上述方法在 FL 的辅助下,为分布式无线网络提供了动态的资源管理方案,使能

量管理、带宽分配和功率分配等的效率有所提升. 然而，如何利用 FL 的分布式架构在保证收敛性和低延迟的前提下解决更为复杂的分布式无线网络资源管理问题，同样值得深入研究.

表 3　基于 FL 的分布式无线网络资源管理方法

Table 3　Distributed wireless network resource management methods based on FL

场景	问题建模	解决策略	性能表现与创新	不足	文献
分布式无线网络	训练时间和设备能耗最小	FL + 在线逐次凸逼近算法	FL 训练时间较少；延迟小；功率分配精度准确	用户间的相互干扰较强	[8]
		FL + 迭代算法	消耗总能量少；资源利用率高	参与设备多时，能量利用率下降	[9]
	能量管理	FL + 光波功率传输方案	为设备提供充足能量以执行任务	算法计算量大；硬件需求高	[10]
	功率分配	FL + AoU 算法	在资源块约束下有最佳传输功率	受延迟制约较大	[11]
	资源块分配和频率选择	FL + 启发式算法	延迟低	不适于单个集群的多用户场景	[12]
	资源分配和延迟最小	FL + DT 算法	实现服务器与设备几乎实时连接	学习准确性低	[13]
	带宽分配	FL + 设备调度方案	得出设备数量和信道带宽之间的权衡	不同信噪比阈值条件下设备调度策略效率难以权衡	[14]
		FL + 设备调度 + 带宽分配策略	充分利用带宽；降低能量消耗	受延迟制约较大	[15]
		FL + 设备调度 + 贪婪策略	充分利用带宽；得到每轮学习效率和延迟之间的权衡；设备调度时间短	不适于异构场景	[16]
		FL + 自适应压缩算法	自适应调整带宽；训练速度快	模型压缩率低时，训练效果差	[17]
		FL + FedCache 算法	带宽分配公平；开销低；收敛快	缓存策略效率低	[18]
	功率分配	FL + SVM 算法	设备功率和任务分配得到优化；任务计算和传输时消耗能量少	算法复杂度高；计算量大	[19]
		FL + AC 算法	收敛性好；功率分配精度较高；鲁棒性高	受网络环境影响大；不适于密集用户场景	[20]

2.2　FL 与移动边缘网络

移动边缘网络是采用分布式移动边缘计算（mobile edge computing，MEC）[21] 的边缘接入网络，具有低延迟和高带宽等优势. 但是随着移动边缘网络复杂性的提高，当面临的数据量很大时，移动边缘网络的资源管理效率不佳. 为此，有学者基于 FL 研究了移动边缘网络计算和通信的联合优化问题[22-25]. Wang 等[22] 为了兼顾计算与通信开销之间的权衡提出“In-Edge AI”框架，该框架利用 FL 认知性、鲁棒性和灵活性的特点，在 FL 优化移动边缘网络计算和通信的同时，使设备和边缘节点协作来交换学习参数，智能部署资源，而当其业务种类较多时，业务处理效率下降. 针对这一不足，文献[23-24]以细粒度方式对业务进行精细划分. 文献[23]根据边缘网络上 FL 的非凸性，将移动边缘网络中的业务以细粒度方式分解为共享资源分配、局部模型精度调整和中央处理器（central processing unit，CPU）频率调整 3 个子业务来寻找最佳学习精度，然后 FL 系统将这些业务根据轻重缓急分时更新参数传输，提高了业务处理效率，实现了计算与通信开销之间的平衡. 文献[24]则根据 FL 处理数据的灵活性和精度可调的优势，利用李雅普诺夫理论设计了具有成本效益的跨边缘节点的 FL 框架，它可以灵活扩展，简化业务处理方式，实现在资源分配、模型精度调整、负载均衡等业务中做出接近最优的决策. 但上述研究都未考虑业务量和用户终端电池状态的关

联问题,对此文献[25]将 FL 和 MEC 联合构成移动边缘系统,该系统一方面使服务器从相关边缘设备收集模型参数,降低延迟,另一方面用以缓解边缘用户设备的电池消耗和计算资源异构问题,然后根据设备的业务量、通信质量和剩余电池电量选择系统要处理的业务,提高了业务的处理效率和用户设备之间的公平性.

FL 还可以实现移动边缘网络中设备频率的有效管理[26-29]. 文献[26]提出自适应同步算法,使每个参与设备同时进入 FL 迭代过程执行局部模型更新,服务器定期对设备迭代过程快慢进行评估,为速度慢的设备增加通信频率,使整个 FL 系统趋近于平衡. 但是,同步算法中快速完成训练的设备必须等待其他速度较慢的设备完成训练后才能进入下一迭代过程,这会增加迭代过程的时间,引起资源浪费. 针对这一不足,文献[27]基于 FL 提出了异步频率聚合算法,在初期 FL 进行局部模型训练获得共享参数信息,服务器根据共享参数信息推断出设备的训练速度,然后根据不同的训练速度为设备分配不同的频率以实现异步聚合,在减少 FL 迭代过程收敛时间的同时,保护了各个用户设备的隐私. 但文献[26-27]都未考虑全局聚合频率的适应性,文献[28]提出确定全局聚合频率的算法,通过服务器在不同的边缘节点获得模型参数,从而确定 FL 训练过程局部更新参数和全局参数聚合之间的最佳折中,实时动态自适应设备全局聚合的频率以最大程度地减少固定资源下的学习损失预算,不幸的是其在异构场景中效果较差. 针对这一缺陷,Zhan 等[29]从实际出发考虑了移动设备和网络连接的异构性提出基于深度强化学习(deep reinforcement learning, DRL)的经验驱动算法,使其更适于异构场景. 该方法采用 AC 训练 DRL 代理,然后代理根据设备的工作状态为其分配合适的 CPU 频率. 此外,DRL 代理通过适当降低参与设备中数据处理速度快的设备的 CPU 频率来提高系统的能量利用率.

Mills 等[30]、Sattler 等[31]对移动边缘网络的链路参数传输进行了研究. 文献[30]提出高效联邦聚合算法(communication-efficient federated averaging, CE-FedAvg). 该算法由分布式优化和上传模型压缩算法两部分构成:分布式优化算法可以使 FL 以较少的迭代过程达到学习精度,降低通信开销;上传模型压缩算法通过适当压缩 FL 系统中设备的模型参数减少上行链路参数传输的大小. 文献[31]指出仅对上行链路参数传输进行调整存在着一定的局限性,针对此不足,提出稀疏三进制压缩(sparse ternary compression, STC)算法. STC 算法扩展了 Top-k 梯度稀疏化,通过分散分层的方法压缩上行链路和下行链路共享模型参数以及权重更新,实现向高频低带宽通信模式的转变. 与 CE-FedAvg 算法相比,该算法更适用于带宽受限的环境,同时以更少的迭代次数达到 FL 的学习精度.

综上所述,基于 FL 的移动边缘网络资源管理方法,实现了移动边缘网络中资源管理的优化,使 FL 成为移动边缘网络资源管理的使能技术. 因为它不仅可以实现机器学习模型的协同训练,也可以利用边缘邻近的中心服务器进行全局参数聚合更新,减轻远程云服务器的负担.

本文总结了基于 FL 的移动边缘网络资源管理方法,如表 4 所示. FL 与移动边缘网络资源管理的相关研究进展主要集中于计算与通信开销联合优化、频率管理和链路资源管理. 虽然 FL 的快速发展与广泛运用为移动边缘网络的资源管理提供了新思路,但是如何在移动边缘网络中深度融合 FL 来实现高稳定性、低成本的保障隐私安全的资源管理方案,仍然是值得思考的问题.

2.3 FL 与其他新兴网络

FL 不仅可以在分布式无线网络和移动边缘网络中进行高效的资源管理,它还广泛应用于各类动态且复杂的网络场景. 本节以 FL 在车联网、F-RAN 和超密集网络中资源管理方法的研究进展为例进行介绍.

在车联网中,文献[32]将联合功率控制和资源分配表述为全网功率最小化问题,结合 FL 和极限值理论,提出基于李雅普诺夫的车辆用户分布式发射功率和资源分配算法. FL 不依赖于车载用户之间实际队列长度样本的信息同步,便可学习网络范围队列的统计信息,而李雅普诺夫优化算法利用统计信息得出车辆用户的队列长度,然后根据队列长度进行合理的功率和资源分配. 与集中式解决方案相比,该方案能耗低、效率高,但是该方案无法适应具有多种潜在车辆用户的场景. 为了弥补文献[32]的不足,文献[33]提出车联网 MEC 方案,该方案自适应地将车辆用户和路边单元作为代理,利用 FL 优化参数集成来提高数据处理效率和降低延迟,使其适用于复杂的车辆用户场景,但是当车辆用户较多时,代理可信度骤降. 文献[34]提出异步 FL,将 FL 与 DRL 相结合,利用 DRL 对可信度高的代理进行选择. 同时,为了保证车辆用户间共享数据的可

表 4　基于 FL 的移动边缘网络资源管理方法

Table 4　Mobile edge network resource management methods based on FL

问题建模	解决策略	性能表现与创新	不足	文献
计算与通信开销联合优化	FL + In-Edge AI 框架	优化边缘缓存和通信；训练模型效率高	不适于异构场景	[22]
	FL	精细划分业务种类；适于异构场景	计算和通信延迟与系统学习时间的关系尚不明确	[23]
	FL + 李雅普诺夫理论	简化业务处理；做出最优决策	算法稳定性差；隐私保护性的成本较高	[24]
	FL + MEC	业务处理效率高；保护用户间的公平性	存在过拟合问题	[25]
频率管理	FL + 自适应同步算法	保证 FL 系统的稳定性	迭代过程时间长；稳定性差	[26]
	FL + 异步频率聚合算法	有效降低延迟；保护用户隐私	服务器更新频率效果差	[27]
	FL + 全局聚合频率算法	减少损失预算	不适于异构场景	[28]
	FL + DRL + 经验驱动算法	能源利用率高；适于异构场景	通信成本较高	[29]
链路资源管理	FL + CE-FedAvg 算法	资源传输效率高；通信迭代较少；可靠性强	非独立同分布数据优化效果差	[30]
	FL + STC 算法	实现向高频低带宽的转变	算法复杂	[31]

靠性，又提出将 FL 与区块链集成到车联网中，开发了混合区块链算法，FL 用于保护车辆用户的隐私，区块链为不可信车辆用户提供有保证的协作方案，从而实现信息的高效、安全、共享.

在 F-RAN 中，文献[35]基于 FL 提出交替方向算法(alternative direction algorithm, ALTD)，研究了设备的 CPU 频率和无线传输功率控制问题，将控制问题联合优化为非线性规划问题来平衡 F-RAN 中设备能耗与 FL 计算和通信延迟之间的权衡. 在该研究中利用 FL 在物联网设备中进行局部模型训练，仅在 F-RAN 节点中共享模型参数信息，以减少网络流量的使用，而 ALTD 算法则根据网络带宽适当调整设备无线传输功率，通过动态电压控制 CPU 工作频率，实现 FL 在时间约束下设备能耗最小的目标. 文献[36-37]均采用自适应智能联合算法来提高资源利用率. 具体来讲，文献[36]基于 FL 提出上下文感知流行度预测策略，运用 FL 分布式训练模型的特点来构建全局预测模型以降低计算复杂度，节省传输本地数据参数的带宽. 预测模型的输入是集群用户内容的平均受欢迎程度参数，该参数通过用户偏好学习和自适应上下文空间划分进行预处理，准确地预测内容(受欢迎程度)可以有效地降低通信开销. 为了进一步提高用户 QoS，文献[37]基于 FL 提出采用遗传算法来解决由于本地过载而导致的 QoS 下降的问题，该方法允许 FL 在共享资源的多个雾程序之间分配负载，使设备用户享受无延迟体验的同时，FL 保证了用户的隐私安全.

此外，在超密集网络中，Yu 等[38]联合 FL 和 DRL 提出两时标 DRL 算法，实现了低开销的资源分配. 该研究包括 2 个过程，分别是快速时间尺度和慢速时间尺度学习过程，参与这 2 个过程的设备都进行 FL 训练，以保护边缘用户的敏感服务请求信息. 其中：快速时间过程用来处理对延迟敏感的任务，如计算卸载和资源分配策略；慢速时间过程用来处理对延迟不敏感的任务，即服务缓存. 通过 2 个过程的联合来最小化总卸载延迟和节省网络资源.

综上所述，FL 在车联网、F-RAN 和超密集网络中的资源管理方案，大都以 FL 分布式训练模型的特点为出发点展开研究，也即 FL 机器学习模型分布在不同的本地设备进行训练，将模型参数上传至中心服务器进行共享，然后聚合生成鲁棒性强的学习模型参数，达到一方面降低中心服务器的压力，提高数据处理效率，另一方面保证通信效率和数据隐私性.

本文总结了基于 FL 的其他新兴网络场景中的

资源管理方法,如表 5 所示. FL 与 MEC、DRL 和区块链等方法进行融合,获得了可靠性高、延迟小的车联网信息共享方案. 此外,基于 FL 的 F-RAN 资源管理方案在能耗低、收敛快等方面取得创新性进展,基于 FL 的超密集网络资源管理方案在开销低和可靠性高方面表现优异,这些成果均体现了 FL 的可扩展性与灵活性. 同时将 FL 与区块链等技术进行协作与配合实现更为完备与可靠的资源管理方案,可能成为未来通信网络的重要发展方向.

综上,FL 凭借其自适应性和可靠性,实现了分布式无线网络、移动边缘网络、车联网和 F-RAN 等场景中有效的资源管理,同时也存在着不足,如鲁棒性差,存在过拟合等问题. 因此,如何在网络环境中自适应地调整不同资源管理方法的学习结构和网络参数来优化 FL 的网络架构与训练过程,进而提高算法在复杂度与计算量方面的性能,使其更适于多用户和异构网络场景是解决高维且动态资源管理问题的关键任务,因此,还需进一步研究,从而为上述网络场景提供性能最优的资源管理方案.

表 5 基于 FL 的其他新兴网络资源管理方法

Table 5 Other emerging network resource management methods based on FL

场景	问题建模	解决策略	性能表现与创新	不足	文献
车联网	信息共享	FL + 极限值理论	可靠性高;设备能耗低	无法适应具有多种潜在车辆用户的场景	[32]
		FL + MEC	低延迟;数据处理效率高	车辆用户较多时,代理可信度骤降	[33]
		FL + DRL + 区块链	共享数据可靠性高;有效保护用户隐私	参数多,计算量大;对硬件要求较高	[34]
F-RAN	资源分配	FL + ALTD 算法	能耗低;泛化能力强	鲁棒性差;不适于多用户场景	[35]
		FL + 上下文感知流行度预测策略	收敛快;算法复杂度低;通信开销低	不适于高维预测;存在过拟合问题	[36]
		FL + 遗传算法	提高用户 QoS;低延迟	计算量大;可扩展性差	[37]
超密集网络	资源分配	FL + DRL + 两时标 DRL 算法	资源分配开销低;可靠性高;收敛快	不适于异构边缘网络	[38]

3 挑战与展望

下面对基于 FL 的移动通信资源管理方法存在的挑战以及可行的解决方案进行探讨,并进一步展望 FL 与移动通信资源管理的未来研究方向.

3.1 挑战

基于 FL 的资源管理方法虽有其独特优势,但是仍然存在如下问题:

1) 多个性能指标协同优化效率低的问题. 当前基于 FL 移动通信资源管理的研究,只针对能量、带宽、功率和频率等其中一个性能指标进行优化,以分布式无线网络中的迭代算法与 AoU 算法、移动边缘网络中的自适应同步算法与 STC 算法、车联网中基于 FL 和极值理论的资源分配算法和 F-RAN 中的 ALTD 算法为例,上述算法只针对能量、带宽、功率和频率等其中一个指标进行优化时效率较高,而当同时兼顾这其中多个性能指标时,很难确定算法的最优解.

针对不同系统性能提出的解决方案可以相互结合,实现多个系统性能协同优化的目标,如多任务学习便运用了该思想. 具体来讲,可以在系统的预训练过程中,同时训练多个学习任务. 例如,在上述任一网络场景中,同时进行能量、带宽、功率和频率分配的训练学习. 在同一个训练过程中,多个任务间共享的模型结构和参数信息是相同的,通过共同训练实现参数信息共享,与分别优化单个性能指标相比,这不仅可以加速模型收敛速度、减少模型训练次数,还可以实现对能量、带宽、功率和频率进行同步管理,有效提升算法性能.

2) 设备的有效连接问题. FL 参与的网络场景由大量的设备互联而成,它们需要占用一定的带宽频繁地与中心服务器交互以在网络环境中保持最佳工作状态. 由于设备的电源电量有限以及网络连接等不稳定性因素,会使设备从 FL 系统中脱离,这在

一定程度上会减弱 FL 算法的泛化能力、降低系统训练模型的精度等. 以车联网为例，由于车辆高度动态、电源电量有限及网络连接不稳定等因素，车辆可能会从 FL 系统脱离，导致 FL 系统处理数据能力下降、增加系统模型训练时间.

因此，在未来研究中可考虑采用 AI 算法辅助的有源设备采样技术[39]或提高现有基于 FL 研究算法的鲁棒性，保障部分设备退出时，FL 系统仍能维持其原有精度和收敛能力. 用 AI 算法辅助有源设备采样可以通过 AI 算法使设备与环境不断交互，例如，将电量充足和网络连接状态好的设备选择出来，以供 FL 系统进行有效训练.

3）安全与隐私问题. 当前多数相关文献的研究假设 FL 的参与者和服务器是安全和可信任的，然而在实际应用中，由于场景的复杂性和动态性，存在着将训练过程中获得具有用户敏感的模型参数信息暴露给服务器或第三方的可能，而且恶意的参与者可以从共享的参数中推断出其他参与方的敏感信息，这会造成隐私泄露，降低 FL 系统的安全性.

关于安全与隐私问题可以考虑采用安全聚合算法或合适的检测机制来改善. 安全聚合算法一方面在参数聚合前先加密单个设备的参数信息，这有效降低了数据隐私泄露的风险；另一方面还可以防止不明身份的参与者访问服务器. 同时，未来研究中需要一种合适的检测机制来检测 FL 系统中恶意窃取敏感信息的参与者. 例如，采用区块链、智能合约和差分隐私相结合的技术，由区块链构建可靠平台提供安全的环境，在智能合约中加入准确度检测算法来识别恶意和不可靠的参与者，以防范投毒攻击[40]，而差分隐私技术则用来防止参与者推理攻击[41].

3.2　展望

鉴于此，本文根据 FL 与移动通信资源管理方法的进展，对未来 FL 与移动通信资源管理潜在的研究方向进行展望.

1）边缘智能技术. 边缘智能技术与 FL 架构类似，都是计算资源与服务的下沉和分散化. 然而，FL 系统需要不断地进行迭代训练以达到给定的模型训练精度，这可能会导致训练时间增加. 边缘智能技术通过融合计算和存储，使边缘设备执行智能算法，从而为系统提供智能服务并满足时延率低、能耗量小、精确度高和安全可靠的要求[42]. 融合 AI 算法的边缘智能技术可以快速分析和训练网络边缘产生的大量数据. 若将边缘智能技术融合至 FL，能够做到对数据实时训练和控制，快速完成给定精度下的迭代训练，使整个系统具有较高的泛化能力. 因此，将边缘智能技术应用于 FL 是移动通信资源管理领域极具前景的研究方向.

2）FL 与区块链协同. 数据隐私性的保证是 FL 的关键理念之一. 区块链是一种分散的、分布式的和公共的数字分类账本，用于在各个节点中保存事务，具有安全性、公开透明性和不可篡改性等优点. FL 与区块链具有天然契合的优势，通过 FL 与区块链的融合，可以提供安全可靠的资源管理方案. 例如，设备在本地完成训练后借助区块链中的智能合约执行 FL 更新步骤，通过共识验证分批次地将参数信息保存在区块链中，保证所有上链的模型参数都有据可查，从而构建高效智慧的移动通信资源管理方案.

3）FL 赋能第 6 代移动通信网络（6th generation mobile networks，6G）. 随着无线通信技术的迅速发展，6G 等未来通信网络技术被相继提出. 6G 旨在实现空天地海一体化和全球无缝覆盖连接[43]，其应用场景的多样性及网络的开放性，使用户的敏感隐私信息从相对封闭安全的平台转移到开放的平台，这可能会造成隐私泄露. 因此，需要 FL 这样的技术对与用户行为相关的数据进行加密处理，FL 基于对数据进行分布式存储和训练，仅将模型训练参数上传至中心服务器的特点，可以很大程度上减少隐私泄露的风险. 若将 FL 独特的数据处理方式应用于 6G 及未来通信网络，一方面可以为 6G 及未来通信网络提供安全可靠的数据处理方式，另一方面可以加强 6G 及未来通信网络的安全性和可信度，为基于 FL 的移动通信资源管理研究的发展带来新机遇.

参考文献：

[1] YANG Q，LIU Y，CHEN T，et al. Federated machine learning：concept and applications [J]. ACM Transactions on Intelligent Systems and Technology，2019，10(2)：1-19.

[2] 王亚珅. 面向数据共享交换的联邦学习技术发展综述[J]. 无人系统技术，2019，2(6)：58-62.
WANG Y S. A survey on federated learning for data sharing and exchange [J]. Unmanned Systems Technology，2019，2(6)：58-62.（in Chinese）

[3] LI L，FAN Y X，MIKE T，et al. A review of applications in federated learning [J]. Computers & Industrial Engineering，2020，149：1-15.

[4] 杨强. AI 与数据隐私保护：联邦学习的破解之道[J]. 信息安全研究，2019，5(11)：961-965.

YANG Q. AI and data privacy protection: the way to federated learning [J]. Journal of Information Security Research, 2019, 5(11): 961-965. (in Chinese)

[5] 周俊, 方国英, 吴楠. 联邦学习安全与隐私保护研究综述 [J]. 西华大学学报, 2020, 39(4): 9-17.
ZHOU J, FANG G Y, WU N. Survey on security and privacy-preserving federated learning [J]. Journal of Xihua University, 2020, 39(4): 9-17. (in Chinese)

[6] LIM W Y B, LUONG N C, HOANG D T, et al. Federated learning in mobile edge networks: a comprehensive survey [J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 2031-2063.

[7] QIRONG H, CIPAR J, CUI H, et al. More effective distributed ML via a stale synchronous parallel parameter server [J]. Advances in Neural Information Processing Systems, 2013: 1223-1231.

[8] VU T T, NGO D T, TRAN N H, et al. Cell-free massive MIMO for wireless federated learning [J]. IEEE Transactions on Wireless Communications, 2020, 19(10): 6377-6392.

[9] YANG Z, CHEN M, SAAD W, et al. Energy efficient federated learning over wireless communication networks [J]. IEEE Transactions on Wireless Communications, 2021, 20(3): 1395-1949.

[10] TRAN H, KADDOUM G, ELGALA H, et al. Lightwave power transfer for federated learning-based wireless networks [J]. IEEE Communications Letters, 2020, 24(7): 1472-1476.

[11] YANG H H, ARAF A, QUEK T, et al. Age-based scheduling policy for federated learning in mobile edge networks [C]// 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Piscataway: IEEE, 2020: 8743-8747.

[12] KHAN L U, ALSENWI M, HAN Z, et al. Self organizing federated learning over wireless networks: a socially aware clustering approach [C] // 2020 International Conference on Information Networking (ICOIN). Piscataway: IEEE, 2020: 453-458.

[13] LU Y, HUANG X, ZHANG K, et al. Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks [J]. IEEE Transactions on Industrial Informatics, 2021, 17(7): 5098-5107.

[14] YANG H H, LIU Z, QUEK T Q S, et al. Scheduling policies for federated learning in wireless networks [J]. IEEE Transactions on Communications, 2020, 68(1): 317-333.

[15] ZENG Q, DU Y, HUANG K, et al. Energy-efficient radio resource allocation for federated edge learning [C]// 2020 IEEE International Conference on Communications Workshops (ICC Workshops). Piscataway: IEEE, 2020: 1-6.

[16] SHI W, ZHOU S, NIU Z. Device scheduling with fast convergence for wireless federated learning [C]// 2020 IEEE International Conference on Communications (ICC). Piscataway: IEEE, 2020: 1-6.

[17] ZHANG X T, ZHU X M, WANG J, et al. Federated learning with adaptive communication compression under dynamic bandwidth and unreliable networks [J]. Information Sciences, 2020, 540: 242-262.

[18] CHILYKURI S, PESCH D. Achieving optimal cache utility in constrained wireless networks through federated learning [C]// 2020 IEEE 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). Piscataway: IEEE, 2020: 254-263.

[19] WANG S, CHEN M, SAAD W, et al. Federated learning for energy-efficient task computing in wireless networks [C] // 2020 IEEE International Conference on Communications (ICC). Piscataway: IEEE, 2020: 1-6.

[20] YAN M, CHEN B, FENG G, et al. Federated cooperation and augmentation for power allocation in decentralized wireless networks [J]. IEEE Access, 2020, 8: 48088- 48100.

[21] 田辉, 范绍帅, 吕昕晨, 等. 面向 5G 需求的移动边缘计算 [J]. 北京邮电大学学报, 2017, 40(2): 1-10.
TIAN H, FAN S S, LÜ X C, et al. Mobile edge computing for 5G requirements [J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(2): 1-10. (in Chinese)

[22] WANG X, HAN Y, WANG C, et al. In-edge AI: intelligentizing mobile edge computing, caching and communication by federated learning [J]. IEEE Network, 2019, 33(5): 156-165.

[23] TRAN N H, BAO W, ZOMAYA A, et al. Federated learning over wireless networks: optimization model design and analysis [C] // 2019 IEEE Conference on Computer Communications (ICC). Piscataway: IEEE, 2019: 1387-1395.

[24] ZHOU Z, YANG S, PU L, et al. CEFL: online admission control, data scheduling and accuracy tuning for cost-efficient federated learning across edge nodes [J]. IEEE Internet of Things Journal, 2020, 7(10): 9341-9356.

[25] JENO J, PARK S, CHOI M K, et al. Optimal user selection for high-performance and stabilized energy-efficient federated learning platforms [J]. Electronics,

2020，9(9)：1-17.

[26] WANG J，JOSHI G. Adaptive communication strategies to achieve the best error-runtime trade-off in local-update SGD [EB/OL]. [2021-03-05]. https://arxiv.org/abs/1810.08313.

[27] DIWANGKARA S S，KISTIJANTORO A I. Study of data imbalance and asynchronous aggregation algorithm on federated learning system [C] // 2020 International Conference on Information Technology Systems and Innovation (ICITSI). Piscataway：IEEE，2020：276-281.

[28] WANG S Q，TUOR T，SALONIDIS T，et al. Adaptive federated learning in resource constrained edge computing systems [J]. IEEE Journal on Selected Areas in Communications，2019，37(6)：1205-1221.

[29] ZHAN Y，LI P，GUO S. Experience-driven computational resource allocation of federated learning by deep reinforcement learning [C] // 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS). Piscataway：IEEE，2020：234-243.

[30] MILLS J，HU J，MIN G. Communication-efficient federated learning for wireless edge intelligence in IoT [J]. IEEE Internet of Things Journal，2020，7(7)：5986-5994.

[31] SATTLER F，WIEDEMAANN S，MULLER K R，et al. Robust and communication-efficient federated learning from non-i. i. d data [J]. IEEE Transactions on Neural Networks and Learning Systems，2019，31(9)：3400-3413.

[32] SAMARAKOON S，BENNIS M，SAADW W，et al. Federated learning for ultra-reliable low-latency V2V communications [C] // 2018 IEEE Global Communications Conference (GLOBECOM). Piscataway：IEEE，2018：1-7.

[33] CAO J，ZHANG K，WU F，et al. Learning cooperation schemes for mobile edge computing empowered Internet of vehicles [C] // 2020 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway：IEEE，2020：1-6.

[34] LU Y，HUANG X，ZHANG K，et al. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of vehicles [J]. IEEE Transactions on Vehicular Technology，2020，69(4)：4298-4311.

[35] YAO J，AASARI N. Enhancing federated learning in fog-aided IoT by CPU frequency and wireless power control [J]. IEEE Internet of Things Journal，2021，8(5)：3438-3445.

[36] WU Y，JIANG Y，BENNIS M，et al. Content popularity prediction in fog radio access networks：a federated learning based approach [C] // 2020 IEEE International Conference on Communications (ICC). Piscataway：IEEE，2020：1-6.

[37] SHAMSEDDINE H，NIZAM J，HAMMOUD A，et al. A novel federated fog architecture embedding intelligent formation [J]. IEEE Network，2021，35(3)：198-204.

[38] YU S，CHEN X，ZHOU Z，et al. When deep reinforcement learning meets federated learning：intelligent multi-timescale resource management for multi-access edge computing in 5G ultra dense network [J]. IEEE Internet of Things Journal，2021，8(4)：2238-2251.

[39] LI T，SAHU A K，TALWALKAR A，et al. Federated learning：challenges，and future directions [J]. IEEE Signal Processing Magazine，2020，37(3)：50-60.

[40] ALFELD S，ZHU X J，BARFORD P. Data poisoning attacks against autoregressive models [C] // Proc of the 30th AAAI Conf on Atifical Intelligence. New York：ACM，2016：1452-1458.

[41] 李欣姣，吴国伟，姚琳，等. 机器学习安全攻击与防御机制研究进展和未来挑战 [J]. 软件学报，2021，32(2)：406-423.
LI X J，WU G W，YAO L，et al. Progress and future and challenges of security attacks and defense mechanisms in machine learning [J]. Journal of Sorftware，2021，32(2)：406-423. (in Chinese)

[42] DENG S，ZHAO H，FANG W，et al. Edge intelligence：the confluence of edge computing and artificial intelligence [J]. IEEE Internet of Things Journal，2020，7(8)：7457-7469.

[43] LIU G Y，HUANG Y H，LI N，et al. Vision，requirements and network architecture of 6G mobile network beyond 2030 [J]. China Communications，2020，17(9)：92-104.

(责任编辑　梁　洁)