联邦元学习综述

张传尧[1,2]，司世景[1]，王健宗[1]，肖京[1]
1. 平安科技（深圳）有限公司，广东 深圳 518063；
2. 中国科学技术大学，安徽 合肥 230026

摘要
随着移动设备的普及，海量的数据在不断产生。数据隐私政策不断细化，数据的流动和使用受到严格监管。联邦学习可以打破数据壁垒，联合利用不同客户端数据进行建模。由于用户使用习惯不同，不同客户端数据之间存在很大差异。如何解决数据不平衡带来的统计挑战，是联邦学习研究的一个重要课题。利用元学习的快速学习能力，为不同数据节点训练不同的个性化模型来解决联邦学习中的数据不平衡问题成为一种重要方式。从联邦学习背景出发，系统介绍了联邦学习的问题定义、分类方式及联邦学习面临的主要问题。主要问题包括：隐私保护、数据异构、通信受限。从联邦元学习的背景出发，系统介绍了联邦元学习在解决联邦学习数据异构、通信受限问题及提高恶意攻击下鲁棒性方面的研究工作，对联邦元学习的工作进行了总结展望。

关键词
联邦学习；元学习；数据异构；联邦元学习；隐私保护

中图分类号：TP181 文献标志码：A doi: 10.11959/j.issn.2096-0271.2022051

Federated meta learning: a review

ZHANG Chuanyao[1,2], SI Shijing[1], WANG Jianzong[1], XIAO Jing[1]
1. Ping An Technology (Shenzhen) Co., Ltd., Shenzhen 518063, China
2. University of Science and Technology of China, Hefei 230026, China

Abstract
With the popularity of mobile devices, massive amounts of data are constantly produced. The data privacy policies are becoming more and more specified, the flow and use of data are strictly regulated. Federated learning can break data barriers and use client data for modeling. Because users have different habits, there are significant differences between different client data. How to solve the statistical challenge caused by the data imbalance becomes an important topic in federated learning research. Using the fast learning ability of meta learning, it becomes an important way to train different personalized models for different clients to solve the problem of data imbalance in federated learning. The definition and classification of federated learning, as well as the main problems of federated learning were introduced systematically based on the background of federated learning. The main problems included privacy protection, data heterogeneity and limited communication. The research work of federated metalearning in solving the heterogeneous data, the limited communication environment, and improving the robustness against malicious attacks were introduced systematically

starting from the background of federated meta learning. Finally, the summary and prospect of federated meta learning were proposed.

Key words
federated learning, meta learning, heterogeneous data, federated meta learning, privacy protection

0 引言

随着移动设备的普及，海量的数据在不断产生，合理有效地利用这些数据成为重点研究方向。由于隐私政策的保护，很多数据不能被轻易地获取，数据间相互隔离，形成了一个个数据“孤岛”。如何建立数据“孤岛”间沟通的桥梁，打破数据之间的界限，成为一个热点问题。联邦学习为解决该问题提供了一个新的方向。

联邦学习在满足数据隐私要求、保护数据安全、遵守政府法规的前提下，进行数据的使用和建模，即通过只在各节点间传递模型参数，而不分享节点间数据的方式训练一个共享的数据模型[1]。许多早期的研究旨在在数据不公开的情况下分析和利用分布在不同所有者手中的数据。早在20世纪80年代，对加密数据进行计算的研究就已经展开，直到2016年，谷歌研究院[2]正式提出联邦学习这一术语，对分布式数据的隐私保护研究才开始归于一类。联邦学习成为解决数据隐私保护问题的一个有力工具。

在传统的机器学习中，通常需要大量的数据样本进行训练，才能获得一个较好的模型。例如在神经网络中，需要大量的标签数据进行模型训练，才能使模型具有良好的分类效果，并且一个训练好的神经网络模型往往只能解决某一类问题。在某些情况下，数据本身是稀缺的，大量的有标签数据是不容易获得的，往往只有少量的样本能够进行数据训练。人类可以通过少量的某一类动物的图片学习到这种动物的概念，再见到这种动物时能够很快地识别出来。这种通过少量样本图片快速学习到新概念的能力，对应机器学习中元学习的概念。元学习的训练目标是训练一个模型，这个模型只需要通过少量的数据和迭代训练就可以快速适应新的任务，即训练一个具有很强适应能力的模型[3]。元学习能够很好地解决训练数据不足的问题。元学习算法由两个部分构成：基础学习者和元学习者[2]。基础学习者在单个任务的水平上工作，其特征在于只有一小组标记的训练图像可用。元学习者从几个这样的情节中学习，目的是提高基础学习者在不同情节中的表现。一般认为元学习系统应当具有以下3个特征：拥有一个基础学习子系统；具有能够利用先前的经验获取知识的能力；能够动态地选择学习偏差。

元学习的早期研究工作主要集中在教育科学相关的领域，主要研究并控制自身的学习状态。随着机器学习的发展，元学习开始进入机器学习领域。元学习的第一个例子出现在20世纪80年代[2]，参考文献[4]提出了一个描述何时可以动态调整学习算法归纳偏差，从而隐式地改变其假设空间元素顺序的框架。参考文献[5]提出具有两个“嵌套学习层”的元学习方法。元学习可以跨越多个问题进行经验的积累，以适应基础假设空间[3]。

考虑联邦学习在解决异构数据训练方面的需求和元学习在多任务模型上的良好表现，利用元学习训练一个个性化的联

邦学习算法成为一种选择。现有的联邦学习[6]主要是利用不同的数据节点联合训练一个统一的全局模型，这种统一的全局模型不利于解决数据的非独立同分布问题。联邦元学习为不同的数据节点训练单独的数据模型，这种多模型的训练方式可以直接捕捉客户端间的数据不平衡关系，使它们很适合解决联邦学习的数据不平衡问题。

1 联邦学习简介

1.1 问题定义

联邦学习在满足数据隐私要求、保护数据安全、遵守政府法规的前提下，进行数据的使用和建模，即通过只在各节点间传递模型参数，而不分享节点间数据的方式训练一个共享的数据模型[1]。联邦学习不需要交换各数据节点间的数据，各节点间仅交换共享数据模型的参数，以保护用户的隐私安全。

定义 n 个数据拥有者 $\{f_1,f_2,\cdots,f_n\}$，不同数据拥有者 f_i 的本地目标用 $F_i(\omega)$ 表示，它们各自拥有自己的数据 $\{D_1,D_2,\cdots,D_n\}$，并希望利用这些数据训练机器学习模型。传统的机器学习方法是利用数据 $D=D_1\cup D_2\cup\cdots\cup D_n$ 训练一个机器学习模型 ω_{sum}。在联邦学习中，服务器端使用聚合函数 $G(\cdot)$ 聚合来自不同数据拥有者的模型参数。数据拥有者在保护自身数据安全、互相不交换本地数据的情况下共同训练一个模型 ω_{fed}。联邦学习的全局目标定义如式（1）所示：

$$\min_{\omega_{\text{fed}}} G(F_1(\omega_{\text{fed}}),\cdots,F_n(\omega_{\text{fed}})) \qquad (1)$$

模型 ω_{fed} 的精度 v_{fed} 应当非常接近模型 ω_{sum} 的精度 v_{sum}。如果存在非负实数 δ 使得式（2）成立：

$$|v_{\text{fed}}-v_{\text{sum}}|<\delta \qquad (2)$$

则称联邦学习算法具有δ精度损失。

1.2 联邦学习的训练过程

随着联邦学习研究的开展，各种各样的联邦学习框架被开发出来。例如微众银行的FATE已经覆盖了3种联邦学习：横向联邦学习、纵向联邦学习、联邦迁移学习[7]。谷歌开源的Tensor/IO已经可以较好地支持横向联邦学习。尽管不同的算法框架（例如PySyft、FFL-ERL、CrypTen、LEAF、TFF）[8]对联邦学习的支持不同，但是联邦学习的主要训练过程均可以分为以下4步。①中心服务器将最新的模型分发给各数据节点；②各数据节点利用本地数据更新模型；③各训练节点将更新的模型参数加密传送给中心服务器，中心服务器聚合各节点的参数，得到新的模型参数；④中心服务器将更新后的模型参数发送给各节点，节点更新本地模型参数，并进行下一轮训练。联邦学习训练过程如**图1**所示。

1.3 联邦学习特点

联邦学习与传统机器学习存在很大不同，具体见**表1**。联邦学习的分布式环境设置导致不同数据节点的地理位置可能不同，用户的使用习惯存在差异，从而影响数据的分布。不同数据节点间是非独立同分布的，任何一个数据节点都不能代表整个数据集的分布。设备环境是否稳定也是影响联邦学习的一个重要因素，有限的网络通信速率要求找到一种合适的方式提高设备间的通信效率，同时还要避免因环境不

稳定导致的设备随机加入与退出。隐私保护是联邦学习最基本的属性要求，当中间结果与数据结构一起暴露时，可能造成数据的泄露。因此如何解决数据非独立同分布问题，提高通信效率，如何进行隐私保护成为联邦学习的关键。

1.3.1 数据隐私保护

隐私性是联邦学习的基本属性，如果不能做到对数据的隐私进行有效保护，联邦学习将失去可靠性，不同的数据“孤岛”也不会将自己的数据贡献出来用于数据训练[9]。联邦学习在参数更新过程中，交换了工作的中间结果，因此不同数据方更容易受到推理攻击，敌对的参与方可以推断出训练数据子集的相关属性[7]。在数据交换时，隐私保护的方式有很多种，例如在机器学习期间通过加密机制下的参数交换来保护用户数据隐私[7]，或者使用差分隐私的方式保护数据[10-13]。安全多方计算、安全聚合[14]也是常用的隐私保护手段。其中，使用差分隐私方式保护数据隐私的方法通过向数据加入噪声的方式掩盖真实的数据，但是加入的噪声可能会影响最终结果的准确度。如何确定加入的噪声量是一个值得研究的问题，加入的噪声太多会导致计算结果失去准确性，加入的噪声不足则导致隐私保护效果不好。

1.3.2 数据非独立同分布

身份、性格、环境的差异导致由用户产生的数据集可能存在很大的差异，训练样本并不是均匀随机地分布在不同的数据节点间的[15-17]。不平衡的数据分布可能导致模型在不同设备上的表现出现较大偏差。因此在进行联邦学习前，如何选取有效的数据集进行数据处理是一个重要的问题。

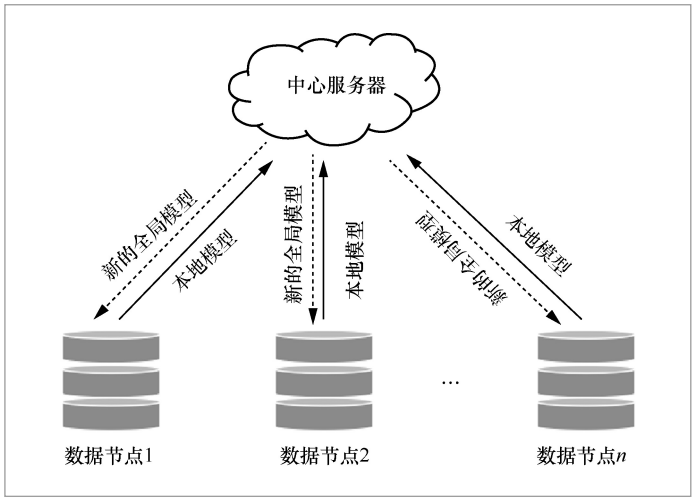

图1 联邦学习训练过程

表1 联邦学习与传统机器学习比较

比较项	联邦学习	传统机器学习
数据隐私	强调数据隐私	无数据保护要求
通信环境	通信受限	通信连接良好
数据分布	分布式存储	数据集中

要解决联邦学习中的数据非独立同分布问题，主要的思路有两种，一种是通过优化模型聚合的方法降低数据不平衡带来的影响，另一种是通过优化本地模型的更新过程解决联邦学习的统计挑战问题。参考文献[18]提出了一种基于迭代模型平均的深层网络联合学习方法，该方法对于不平衡和非独立同分布是稳健的。参考文献[15]提出通过每个设备上的类别分布和人口分布之间的地球移动者距离来量化数据集间的差异，并创建一个在所有边缘设备之间全局共享的数据子集来改进对非独立同分布数据的训练。

1.3.3 通信环境受限

在联邦学习中，中心服务器与计算节点间的物理距离很远，通信成本较高[14]，且由于计算节点环境的不稳定性，可能随

时存在计算节点加入和退出的情况，因此联邦学习一般应选取网络环境稳定免费且计算节点空闲时进行。通信成本成为制约联邦训练的主要因素，因此如何对设备间的通信进行压缩是一个值得研究的问题，可以通过减小客户端传送到服务器的对象的大小、减小从服务器向客户端广播的模型大小、客户端从全局模型开始培训本地模型等方法降低对通信链路的要求[19]。参考文献[20]中给出两种降低上行链路通信成本的方法：结构化更新和草图更新。结构化更新直接从使用较少数量的变量（如低秩或随机掩码）的受限空间中学习更新；草图更新先模型更新，然后在发送到服务器之前，使用量化、随机旋转和二次采样的组合对其进行压缩。

1.4 联邦学习算法

联邦学习的更新过程主要分为服务器端更新和客户端更新两部分，按照算法对联邦学习改进的阶段，可以将联邦学习算法分为两类：基于服务器端聚合方法优化的算法和基于客户端优化的算法。

1.4.1 基于服务器端聚合方法优化的算法

联邦学习算法通过聚合不同客户端参数共同训练一个全局模型，由于不同客户端数据是非独立同分布的，更新的模型参数可能存在很大不同，同时由于隐私保护的要求，服务器不能直接访问客户端数据，容易受到恶意攻击的影响，例如将使用错误标签更新的模型参数发送给服务器以误导模型更新方向。如何聚合来自不同客户端的数据以降低恶意攻击带来的影响，并提供一个针对不同客户端表现良好的全局模型是一个重要问题。联邦平均算法（federated averaging algorithm，FedAvg）[1]使用一种简单直白的权重聚合方法，将客户端内数据量与全体客户端总数据量的比值作为权重聚合不同客户端发送的参数。相较于联邦随机梯度下降算法（federated stochastic gradient descent algorithm，FedSGD）[1]每次使用客户端所有数据进行一轮梯度下降的方式，其采用的本地多轮更新的方式加快了模型收敛速度。联邦平均算法因为其简单有效的思想很快流行起来，但是其简单的加权聚合方式难以解决数据异构、易受攻击的问题。基于服务器动量的联邦平均算法（federated averaging with server momentum algorithm，FedAvgM）[21]通过引入动量的方法缓解数据异构对联邦平均算法的影响。参考文献[22]借鉴非联邦环境下的自适应优化器（自适应梯度（adaptive gradient，AdaGrad）[23]、自适应矩估计（adaptive moment estimation，Adam）[24]和YOGI[25]）提出了联邦学习版本的自适应优化器（联邦自适应梯度（federatedadaptive gradient,FEDADAGRAD）算法[22]、联邦化YOGI[22]和联邦自适应矩估计（federated adaptive moment estimation，FEDADAM[22]）算法），通过自适应优化器显著提高了模型在数据异构情况下的收敛速度。简单的聚合难以应对不同客户端的个性化需求，参考文献[26]和[27]提出两种分层聚合的方式，其中参考文献[27]提出了共享基础层加个性化层的个性化联邦学习模型算法（personalized federated training algorithm，FedPER），其中基础层由不同客户端共同训练，个性化层由本地数据训练，这种带有个性化层的方法可以有效减少数据异构带来的模型在不同客户端上表现差异的问题。参考文献[26]提出了联邦匹配平均算法（federated matched averaging algorithm，

FedMA），该算法以分层方式构建共享全局模型。

1.4.2 基于客户端优化的算法

由于不同客户端上的数据是非独立同分布的，且不同节点间互相不能交换数据，客户端在本地数据进行模型训练时，无法得知其他客户端的信息，模型的更新方向可能会受到本地数据分布的影响，导致各个客户端模型更新方向出现较大差异。利用全局模型的信息约束本地模型的更新，可以在增加模型个性化的同时避免模型间出现较大偏差。参考文献[28]进一步扩展联邦平均算法，提出了一种新的算法FedProx，它规定客户端有局部损失函数，进一步使用基于前一步权重的二次惩罚进行正则化，在数据异构的环境中显示出联邦平均算法的进步性，该方法受到连续迁移学习早期工作的影响，还具有很大的改进空间。参考文献[15]提出基于地球移动距离的联邦算法（federated earth mover' distance，Fed-EMD），该算法将部分客户端生成的参数或服务器生成的模型共享给整个客户端，并通过创建一个在所有数据节点间共享的数据子集，减少数据不平衡的影响。但是这些解决方案需要很高的通信成本，且难以满足联邦学习的隐私保护要求。以往的目标是通过网络训练一个统一的全局模型[29]，这种方法难以解决联邦学习中的统计问题。参考文献[30]提出了一种自适应个性化联邦学习算法（adaptive personalized federated learning algorithm，APFL），其通过推导全局模型和局部模型的一般边界找出最优混合参数，并提出了一种高效的通信方法，帮助客户端高效地学习个性化模型。联邦平均算法虽然简单、通信成本低，但是其受到数据不平衡的影响很大，且不同客户端在进行本地更新时无法了解到其他客户端的更新信息，可能会由于本地数据的异构性导致其更新方向与其他客户端产生漂移，利用正则化项可以很好地约束本地模型的更新方向。参考文献[31]提出了一种随机控制平均算法（stochastic controlled averaging algorithm，SCAFFOLD），其使用控制变量（方差减少）来纠正本地更新中的“客户端漂移问题”，还可以利用客户间的相似性，进一步降低所需的沟通成本。同样的，在参考文献[32]中，Ditto算法在不同客户端损失函数中引入正则化项，并通过正则化项前系数控制模型在个性化和鲁棒性间的平衡。参考文献[33]借鉴对比学习的思想提出模型对比联邦学习（model contrastive federated learning， MOON）算法，其不同于Ditto算法将本地模型与全局模型的欧氏距离作为正则化项以鼓励个性化模型向全局最优模型靠近，MOON算法利用模型表示之间的相似性纠正各个客户端的局部学习，将全局模型与本地模型表示间的对比损失作为正则化项约束本地模型的更新。

联邦学习算法分类见**表2**。

2 元学习介绍

2.1 元学习定义

很难给出元学习的确切形式化定义[34]。一般来说元学习就是学会去学习，希望训练一个通用的学习算法，该算法可以很好地适应新的任务，元学习研究系统如何通过经验提高效率，目标是了解学习本身如何根据学习领域灵活变动[35-36]，元学习往往以小样本学习和对任务的快速适应作为切入点[37]。

表 2 联邦学习算法分类

分类	联邦学习算法	特点
基于服务器端聚合方法优化的算法	FedSGD	每次使用客户端所有数据进行一轮梯度下降，收敛速度慢
	FedAvg	以客户端数据量与总数据量的比值作为权重，聚合不同客户端发送的参数，客户端使用多轮更新的方式加快模型收敛速度
	FedAvgM	通过引入动量更新缓解数据异构对联邦平均算法的影响
	FEDADAGRED FEDYOGI FEDADAM	借鉴非联邦环境下的自适应优化器(ADAGRAD、ADAM和YOGI)提出了联邦学习版本的自适应优化器，通过自适应优化器显著提高了模型在数据异构情况下的收敛速度
	FedPER	通过共享基础层加个性化层的个性化模型提高模型公平性
	FedMA	以分层方式构建共享全局模型
基于客户端优化的算法	FedProx	客户端局部损失函数使用基于前一步权重的二次惩罚进行正则化，减少数据异构对模型的影响
	Fed-EMD	通过创建一个在所有数据节点间共享的数据子集，来减少数据不平衡的影响。需要很高的通信成本，降低隐私安全性
	APFL	通过推导全局模型和局部模型的一般边界找出最优混合参数
	SCAFFOLD	使用控制变量纠正本地更新中的“客户端漂移”问题
	Ditto	使用本地模型与全局模型的欧氏距离作为正则化项以鼓励个性化模型向全局最优模型靠近
	MOON	利用模型表示之间的相似性来纠正各个客户端的局部学习

人类可以通过几张动物的照片快速地学习到该动物的概念，这对应元学习的少镜头学习（few-shot learning，FSL）情景。人类甚至可以在没有图像的情况下，仅仅凭借描述就能认识到新的类别，这对应元学习的零镜头学习情景。元学习按照支持集每类样本的数量可以分为3类：单镜头学习（one-shot）、k镜头学习（k-shot）、零镜头学习（zero-shot）。

元学习一般训练过程如图2所示。首先在训练集上采样构建不同的任务 T_i^{train}（由支持集S_i和查询集Q_i组成），模型在支持集S_i上进行参数优化，得到对应该任务 T_i^{train} 的中间参数模型 φ_i，然后在查询集Q_i上使用模型 φ_i 计算损失函数L_i，并最小化不同任务上损失函数值的和训练一个基础模型 φ。然后在测试集中，通过任务 T_i^{val} 的支持集数据进行简单的几步梯度下降就可以得到新的模型 φ'，以适应新的任务。最后在测试集中，利用任务 T_i^{val} 中查询集测试模型 φ' 的表现。培养机器利用先前经验快速适应新任务的能力，就是让机器学会学习。

2.2 元学习分类

传统的机器学习目的在于让机器学会理解事物的异同以区分不同的事物，而不是学会识别没见过的事物。元学习的目的是教会机器如何利用先验知识快速学习新知识，快速掌握识别新物体的能力。根据训练数据有无标签，可以将元学习分为监督元学习和无监督元学习两种，如图3所示。

2.2.1 无监督元学习方法

当训练数据没有标签时，无监督元学习[38-39]常采用一种显式的方式自动构建数据集，通过构建虚标签的方式，将无监

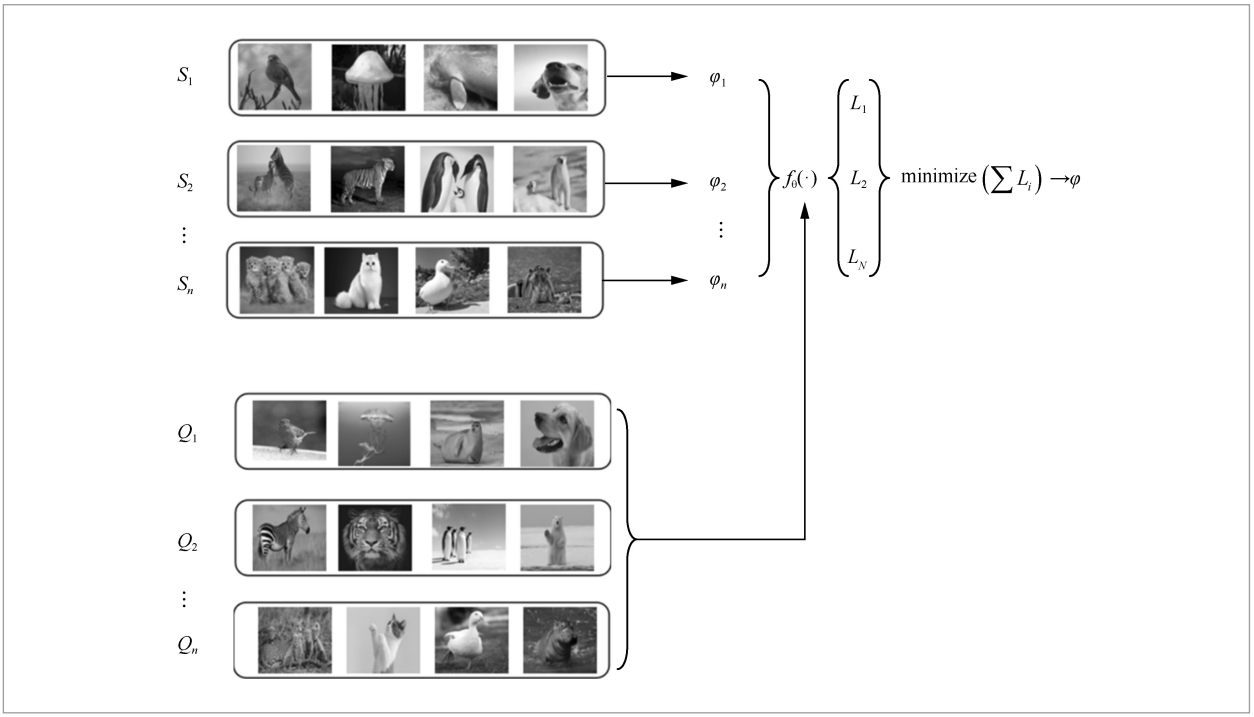

图 2 元学习一般训练过程

督学习转换为监督学习。参考文献[38]为了解决训练数据无标签问题，提出了一个分阶段训练集群自动构造任务（clustering to automatically construct tasks，CACTUs）算法，其先在无标签训练数据上使用无监督训练方法学习一个特征表示器，然后通过聚类的方式在无标签数据上进行聚类划分，并生成伪标签。其通过伪标签构建元学习任务，在元学习任务上训练常规的监督元学习模型，如模型不可知元学习算法（model-agnostic meta-learning，MAML）[5]、原型网络算法（prototypical networks，ProtoNet）[40]等。与CACTUs算法分阶段训练的过程不同，参考文献[39]提出一种端到端的无监督元学习（unsupervised meta-learning with tasks constructed by random sampling and augmentation，UMTRA）算法，其通过数据增强的方式为每个图片生成一个增强数据，并将原数据作为支撑集，将增强图片作为查询集，构建N类单镜头（N-way-1-shot）任务。UMTRA在无标签数据上的分类准确度已经非常接近有标签数据集上MAML模型的分类准确度。

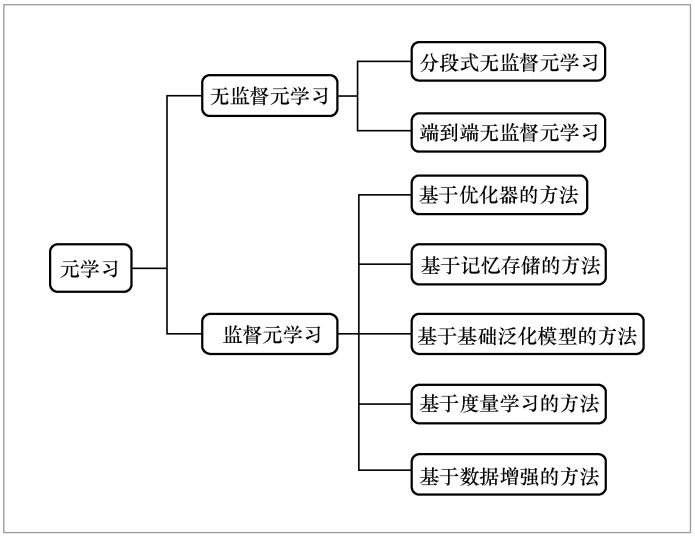

图 3 元学习分类

2.2.2 监督元学习方法

监督元学习旨在根据有限的数据信息，快速学习适应新任务的能力，根据算法分类，可以将监督元学习的方法分为以下5种：基于优化器的方法、基于记忆存储的方法、基于基础泛化模型的方法、基于度量学习的方法、基于数据增强的方法。

（1）基于优化器的方法

基于优化器的方法旨在通过学习一个更好的优化器加快学习过程。参考文献[41]中提出使用一个基于长短期记忆网络（long short term memory，LSTM）的元学习者来学习一个更新规则，这个更新规则可以被看成一种新的类似于但不同于梯度下降的优化算法。在参考文献[42]中RL^2（fast reinforcement learning via slow reinforcement learning）利用一个慢速调整的强化学习方法去训练一个快速调整的强化学习，达到学会学习的目标，即用一个强化学习去学习一个强化学习算法。参考文献[43]中提出了一种加快神经网络训练速度的方法LTL（learning to learn by gradient descent by gradient descent）以实现快速学习，通过以往的神经网络学习的任务预测梯度，文章通过为梯度下降算法训练一个学习器以加快梯度下降算法的收敛速度。

（2）基于记忆存储的方法

先验知识对于后续任务具有重要作用，合理利用先验知识可以帮助模型快速适应新的任务。参考文献[44]提出了一种带有记忆增强神经网络的元学习（memory-augmented neural network，MANN）算法，该算法利用外部存储器进行样本特征的保存，使用元学习算法改进单元的读取和写入方式，并采用错位匹配的方式避免在训练过程中记住样本的相应位置。权重的缓慢更新实现了网络的长期记忆功能，并利用外部存储实现短期记忆，最终实现元学习的快速训练。在参考文献[45]中，作者引入时间卷积网络访问之前的特征信息提出了一种元学习模型简单神经注意力学习器（simple neural attentive learning，SNAIL），使其可以在某个固定的时间内使用更加灵活的计算。通过时间卷积网络和注意力机制的结合，网络可以更加准确地在先前的信息中进行选择。

（3）基于基础泛化模型的方法

基于基础泛化模型的方法旨在学习一个可以快速适应新任务的基础模型，当面对新任务时，仅仅通过简单的几步梯度下降就能获得快速适应新任务的模型。参考文献[5]提出一种模型无关（MAML）的算法。MAML算法的关键在于训练一个良好的模型初始化参数，当遇到一个新的任务时，只需要使用很少的样本，进行几次简单的梯度下降，就能获得一个能适应新的任务的模型，MAML算法训练过程如**图4**所示。原始的MAML算法包含二阶求导，这就需要对内循环的高阶导数进行计算和保存。隐式模型不可知元学习算法（implicit model-agnostic meta-learning，iMAML[46]）通过推导出外循环的梯度解析式，解决了MAML算法多步梯度消失、内循环存储和高阶求导的问题。参考文献[47]将进化策略（evolutionary strategies，ES）[48]应用于MAML算法，从而避免内层循环的二阶导数计算。基于评估策略的模型不可知元学习（evolutionary strategies model-agnostic meta-learning，ES-MAML）算法使用确定性的策略避免了很多在随机策略情况下反向传播引起的问题。Reptile算法[49]将MAML算法的两次求导过程简化为一次，直接使用参数差值方向决定外循环更新方向。潜在的嵌入优化算法（latent embedding optimization，LEO）[50]利用编码器和关系

网络将样本数据投影到一个低维空间，在内循环中对低维特征向量直接更新，并将特征向量通过解码器获得一个条件概率分布，通过随机采样获得参数。

（4）基于度量学习的方法

基于度量学习的方法旨在获得一个强大的特征提取器，通过在特征空间中不同样本间的距离进行分类。参考文献[51]设计了一个元评价（meta-critic）网络，该网络由核心价值网络（meta value network）和任务行为编码器（task-actor encoder）组成。使用任务编码通过批评网络驱动对目标网络的监督，而不是合成其权重。匹配网络[52]通过对比数据间的相似度来判断数据类别。原型网络[53]示意如**图5**所示，对每个数据进行提取特征，并将每个类别的特征均值作为该类别的原型，通过判断样本特征到不同类别的原型的距离来判断样本的类别。匹配网络[52]、原型网络[53]、孪生网络[54]都是通过计算特征向量间的距离判断样本类别的。而关系网络[55]提出使用神经网络计算样本间的匹配程度，首先对查询集与支持集中的样本进行特征提取，然后进行拼接，将拼接后的特征输入神经网络计算出关系得分。

（5）基于数据增强的方法

元学习在解决小样本分类问题时，面临的最大挑战来源于训练数据不足，通过不同的数据增强方式[56-60]扩展训练数据集成为一种选择。参考文献[60]提出了一种分离光照网络（separating-illumination network，Sill-Net），该网络可以针对图片分离光照特征，并通过在特征空间使用该网络分离光线的影响来增强训练样本。参考文献[61]提出了一个统一的元数据增强框架并在此框架下解释了现有的增强策略。参考文献[62]通过将样本数据增强策略作为样本重加权问题来学习一个具有样本感知能力的元数据增强策略(sample-aware data augmentation policy，MetaAugment)，该策略网络通过捕捉样本间的不同性来评估不同样本增强策略的有效性。参考文献[63]为少镜头学习提出了一个简单通用的算法——基于对抗性方法的少镜头学习（anadversarial approach to few-shot learning，MetaGAN）算法，其引入了一个以任务为条件的对抗生成器，其目标是生成与从特定任务中采集的真实数据无法区分的样本。参考文献[64]结合小样本文本分类问题介绍了一种新的框架——数据增强元学习（meta-learning with data augmentation，MEDA），该框架引入一个球生成器用于生成新的数据样本，首先通过生成器计算支持集样本的最

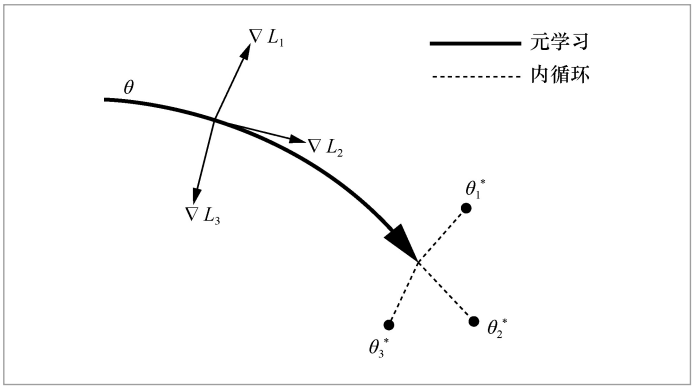

图 4 MAML 算法训练过程

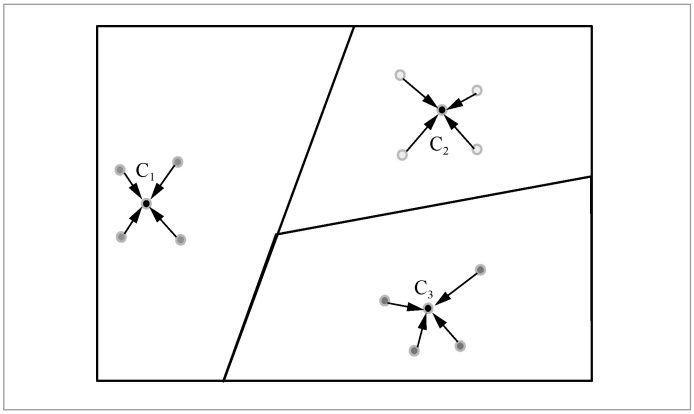

图 5 原型网络示意图

小球形封闭边界，然后在边界内合成新的数据样本。

监督元学习分类见**表3**。

3 联邦元学习介绍

3.1 联邦元学习定义

在联邦学习中，通过元学习算法，为每个客户端训练个性化的模型，降低模型在不同客户端上表现的差异，提高模型公平性，就称为联邦元学习算法[65]。元学习旨在学习和提取先前任务内部可转移的知识，训练一个良好的初始化模型，以快速适应新的任务。其防止过拟合并快速适应新任务的能力特别适合解决联邦学习中不同客户端数据分布不一致的问题，联邦元学习将每个客户端视作一个任务，训练一个良好的初始化模型，其可以在客户端上通过几步简单的梯度下降快速适应新的任务。元学习因其快速适应新任务的能力，表现出在解决联邦设置的系统和统计挑战问题的巨大潜力[65]。联邦元学习算法与元学习方法不同，联邦元学习算法运行在分布式数据集上，数据不再是集中分布的，同时不同客户端与服务器的连接并不稳定，客户端的本地更新通过简单的平均聚合可能会导致元模型产生梯度偏差。

3.2 联邦元学习算法分类

联邦学习旨在利用不同客户端的数据联合训练一个全局模型，同时保护各个客户端隐私。相较于只使用本地数据进行模型训练，联合利用多个客户端的数据可以提高模型的表现，但是在联邦学习环境中，由于不同客户端所处地理位置不同，个人用户可能受到不同的地域环境、风俗文化的影响，导致其本地数据间存在很大差异，数据是非独立同分布的。因此一个单一的全局模型无法满足所有用户的需求，具体问题如下。

①如何为不同用户提供不同的个性化模型是一个重要问题。在联邦学习中对客户端隐私进行保护，服务器不能随意检查客户端发送的数据，这使得联邦学习更加容易受到恶意攻击的影响。②如何提高联邦学习面对恶意攻击时的鲁棒性，加强联邦学习对于隐私数据的保护同样是一个重要问题。不同于集中式中心化训练，联邦学习中不同客户端距离分散，设备间性能差异巨大，服务器与客户端间的通信信道带宽有限，客户端的计算资源、设备电量、参与计算时间都十分有限。③如何为联邦

表 3 监督元学习分类

分类	方法	参考文献
基于优化器的方法	Meta-Learner, LSTM, RL^2, LTL	[42-44]
基于记忆存储的方法	MANN, SNAIL	[45-46]
基于基础泛化模型的方法	MAML, iMAML, ESMAML、Reptile, LEO	[5, 47-48] [50-51]
基于度量学习的方法	Meta-critic Network, Matching Network、Prototy Network, Siamses Network、Relation Network	[52-56]
基于数据增强的方法	Sill-Net, MetaAugment, MetaGAN, MED	[61, 63-65]

学习制订一套合理的资源分配策略，以提高设备公平性、提高通信效率、加快收敛速度也是一个重要问题。联邦元学习算法分类如**图6**所示。

本节我们从以下3个问题出发，介绍近年来联邦元学习为解决这些问题所做的工作：①如何通过联邦元学习为不同用户提供个性化模型，解决联邦学习中的数据异构问题；②如何利用联邦元学习进行合理资源分配，提高联邦学习的通信效率，加快收敛速度；③如何利用元学习算法增强联邦学习面对恶意攻击的鲁棒性，保护数据隐私。

3.2.1 面向数据异构的联邦元学习算法

(1) FedMeta算法

联邦学习的统计挑战和系统挑战已经成为制约联邦学习发展的关键瓶颈，参考文献[65]指出元学习因为其快速适应新任务的能力和良好的泛化能力特别适合联邦学习设置，文中提出了一个联邦元学习算法FedMeta(federated meta-learning)。FedMeta框架将每个客户端视为一个任务，目标是训练一个初始化良好的全局模型，而不是训练一个全局最优模型。FedMeta框架使用一个共享的元学习者取代联邦学习中共享的全局模型，可以很好地使不同的元学习算法适应联邦学习系统。文中将元学习者的参数初始化以及更新工作设置在中心服务器上。在每个节点上采样形成一个支持集及一个查询集。在每个节点的支持集上利用元学习者训练一个个性化模型 f_θ，并在查询集上验证meta-learner的训练能力。该框架允许以更灵活的方式共享参数化算法，同时保护客户端隐私，不将数据收集到服务器上。

(2) FedAvg-Reptile算法

同样是与经典元学习算法相结合，与FedMeta在各个客户端上利用MAML算法不同，参考文献[66]提出如果简化联邦学习的约束条件并且假设所有客户端上的数据量相同，联邦平均聚合各个客户端参数时权重相同，那么联邦平均算法其实和Reptile算法变成了同一种元学习算法。为了使联邦学习能够更加满足实践需求，参考文献[66]提出联邦学习应当同时解决3个问题：①由于大多数客户端数据的异构性，应当提供一个个性化的模型以提高在不同数据集上的表现；②部分客户端可

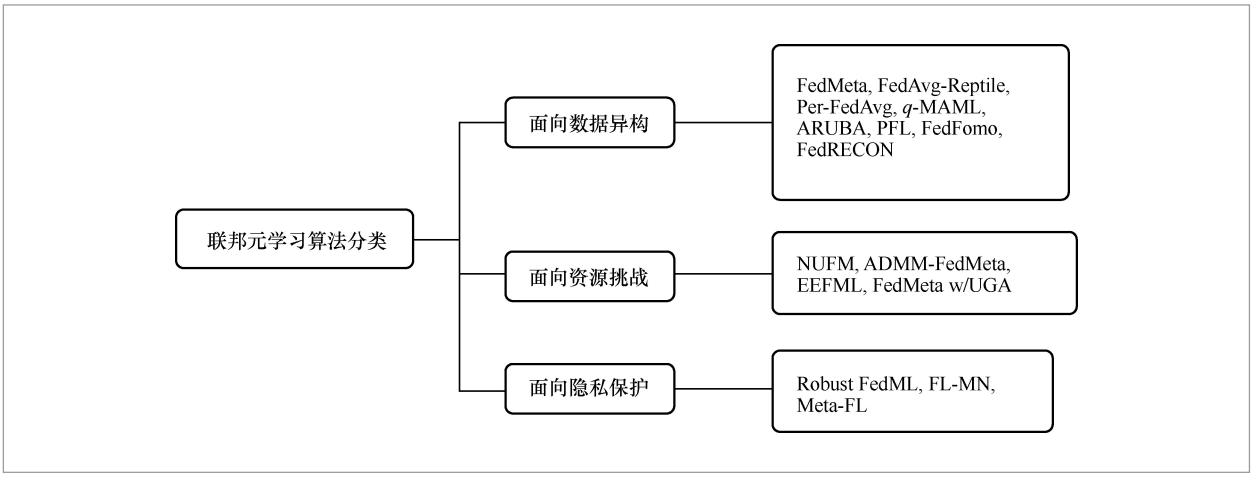

图 6 联邦元学习算法分类

能只拥有很少的数据甚至没有数据用于个性化微调，因此应当提供一个可靠的初始化模型，使其在缺少数据的客户端上也能拥有可靠的表现；③由于联邦学习通信环境受限，模型应当能够实现快速收敛。同时指出通过选择动量随机梯度下降（momentum stochastic gradient descent，Momentum SGD）算法作为服务器优化器，FedAvg算法可以提供个性化模型，即解决问题①。通过减少本地学习率和训练轮次可以加快收敛，即解决问题③。针对问题②，为了提供一个可靠的初始化模型，文中提出了在联邦平均算法阶段后插入元学习微调阶段的方案，通过仔细地微调全局模型使得全局模型精度更高，更易于个性化。该方案分为训练和微调两个阶段：首先运行联邦平均算法，将其作为服务器优化器；然后切换到Reptile[49]算法将其作为服务器优化器来微调初始模型以提供一个稳定的个性化初始模型，同时也能保持一个稳定的个性化模型；最后使用相同的客户端优化器进行个性化优化。实验结果表明，相比于其他优化器，Reptile产生了更好的结果。该方法与其他联邦元学习算法最大的不同在于该方法将元学习作为一个微调阶段放置在联邦学习之后，而不是将元学习算法作为联邦学习算法的一部分引入联邦学习的全过程。

（3）Per-FedAvg算法

参考文献[67]提出了一个联邦平均算法的个性化变体方法：个性化联邦平均算法（personalized federated avgrage learning，Per-FedAvg），其利用元学习算法寻找一个能够快速适应不同客户端的共享全局模型，该模型在每个客户端上仅需几步迭代就能获得良好的表现。与同样利用元学习方法的FedMeta算法不同，该方法聚焦MAML算法在联邦学习情景下的收敛性分析，提供了一个可证明收敛的方法解决函数为非凸的情况。传统的联邦学习中，我们将 $f_i:\mathbb{R}^d\to\mathbb{R}$ 作为不同用户i的损失函数。则联邦学习的目标如式（3）所示：

$$\min_{w\in\mathbb{R}^d} f(w):=\frac{1}{n}\sum_{i=1}^{n} f_i(w) \quad (3)$$

参考文献[67]借鉴MAML算法，考虑为每个用户取相同的初始点，并希望使用自身的损失函数的几个梯度下降来优化初始点。将问题③转化为如式（4）所示：

$$\min_{w\in\mathbb{R}^d} F(w):=\frac{1}{n}\sum_{i=1}^{n} f_i(w-\alpha\nabla f_i(w)) \quad (4)$$

借鉴联邦平均算法最优化的过程，Per-FedAvg算法求解式（4）的过程类似，每一轮训练服务器随机选择一部分用户，并将当前模型发送给用户，用户根据自身的损失函数f_i通过随机梯度下降更新参数，然后将更新的参数返回给服务器，服务器通过计算使用这些选定用户接收模型的平均值来更新全局模型，然后进行下一轮。参考文献[67]考虑了异构情况下的联合学习问题，其目标是为用户找到一个合适的初始化模型。其假设为每个用户取初始点，并使用自身损失函数的梯度下降步骤更新，利用联邦平均算法聚合该模型，不仅保持了联邦学习的优势，还捕获了用户间的差异，在训练阶段后快速适应每个用户的本地数据。该模型是MAML算法的一种。

（4）q-MAML算法

公平性对于机器学习模型来说是一个重要问题，在传统的机器学习中，可以通过衡量准确度差异来表示公平性，但是当联邦学习中存在大量设备时，准确得到每个设备上的测试准确度会异常困难，且将耗费巨大的计算资源与通信资源。参考文献[68]通过引入异类误分类，确保模型对任何设备的适应都不会以牺牲其他设备为代价。但是这种方法仅仅优化性能最差组的设备，且只在小型网络上进行了测试。针

对上述不足，参考文献[69]借鉴无线网络公平资源分配工作的思想，提出了q-公平联邦学习（q-fair federated learning，q-FFL）算法，其通过最小化一个聚合的加权损失函数，使损失函数值较高的设备在目标优化函数中具有较高的相对权重，从而促进模型在各个设备间的表现更加公平。通过改变参数q可以权衡模型的准确度和公平性，使得模型在保持较高准确度的同时在不同设备上的表现更加公平。作者进一步将q-FFL算法与流行的元学习算法MAML相结合，提出了一个在不同任务上表现更加公平的新算法q-MAML。与传统的MAML算法求解过程不同，其使用了q-FFL中的目标函数和权重更新全局参数。虽然文中的q-MAML算法是在元学习设置下进行的测试，但是由于联邦学习的多客户端特性与元学习多任务特性的情景相似，q-MAML算法可以很好地推广到联邦学习情景中。

（5）ARUBA算法

参考文献[70]将在线凸优化和序列预测算法相结合，提出了一个新的理论框架平均后悔上限分析（average regret-upper-bound analysis，ARUBA）算法，该算法将元学习视为在线学习一系列损失。ARUBA通过学习一个在线镜像下降的正则化项来确定参数空间中哪些方向需要更新。其提供了一个动态调整学习率的方法，该方法是一种简单的无须步长调整的方法，可以显著提升联邦学习的个性化特性。

（6）PFL算法

参考文献[71]提出利用梯度矫正方法为每个边缘设备定制个性化模型，其提出了一种新的基于元学习的联邦训练方法，将每个客户端与不同的任务相关联，在不同任务上学习一个元模型，并在每轮训练过程中动态地修改设备损失函数以消除元模型对不同用户的偏见，该模型通过简单的微调就能快速适应新的任务。

（7）FedFomo算法

一个单一的全局模型不可能适应所有客户端的模型，参考文献[72]不再只学习一个单一的平均模型，而是根据客户端间的模型联系，计算不同客户端间的相互影响，得到最佳的模型组合。其通过n个服务器元模型，向不同客户端组发送不同的元模型。

（8）FedRECON算法

由于隐私和通信约束，客户端可能无法与服务器传递全部的模型参数，例如模型中特定于用户的嵌入模块（例如用于协同过滤的矩阵分解模型），如果直接将用户嵌入参数发送给服务器，将会暴露个人敏感偏好。同时在大规模训练中，训练一个单一的全局模型对于不同用户将存在巨大差异。为了解决上述问题，参考文献[73]提出了一种模型无关的局部联邦重构（federated reconstruction，FedRECON）算法。训练过程中，模型参数被划分为全局参数和敏感的本地参数，本地参数在训练过程中不会离开客户端，从而保护客户端的数据隐私。其利用元学习训练一个可以快速重构局部参数的全局参数，并在客户端上使用全局参数进行局部参数重构。

3.2.2 面向资源挑战的联邦元学习算法

（1）NUFM算法

由于联邦学习各个数据节点间的通信限制，联邦元学习模型很容易受到通信链路的影响，导致通信效率低下、收敛速度慢等问题。同时在无线网络中部署联邦元学习算法时如何分配可用的通信频谱和有限的设备电源能量也是一个重要的问题。现有的方法在设备选择和资源分配方面往往采用均匀选择的方式，导致模型的收敛速度很慢。一些非均匀的设备选择方案由于联邦元学习算法中的随机梯度的偏置与高阶信息不能直接应用于联邦元学习算法

中。为了解决上述挑战，参考文献[74]提出了一种非均匀的联邦元学习设备选择方案NUFM（non-uniform device selection scheme federated meta learning）来促进模型收敛速度提高，并提出了一种用户资源分配策略URAL（user selection and resource allocation），该策略通过权衡模型收敛性、时钟时间和能源消耗问题给出了一种设备选择和资源分配策略。

（2）ADMM-FedMeta算法

联邦学习中，不同数据节点的数据量不同，节点间的计算资源也不相同，有限的数据资源和计算能力对联邦学习提出了重大挑战。为了克服这一困难，参考文献[75]提出通过边缘节点利用先前任务的知识转移协作学习一个元模型。其将先前任务的有价值的知识提取为正则化项，并设计了一种基于交替方向乘子法（alternating direction method of multipliers，ADMM）的联邦元学习算法ADMM-FedMeta（ADMM based federated meta-learning algorithm）。其中ADMM提供了一种自然的机制，将原始问题分解为许多子问题，可以跨边缘节点和平台并行解决；此外，还采用了一种非精确化ADMM方法的变体，通过线性近似和海森估计将计算复杂度降为$O(n)$。

（3）EEFML算法

模型不可知元学习算法（MAML）有良好的收敛性和快速适应新任务的能力，但是在其模型优化过程中需要计算二阶导数进行反向传播，计算高阶导数会带来很高的计算成本，并可能产生梯度消失的问题。当在联邦环境下使用这些算法时，客户端可能无法满足计算资源需求。使用一阶近视优化算法（一阶MAML（first-order MAML，FOMAML）算法、Reptile算法）虽然不需要计算二阶导数，但是它们都没有考虑元模型对任务模型的影响。参考文献[76]提出了一种节能联邦元学习（energy-efficient federated meta-learning，EEFML）算法，其可以以较低的计算资源和通信成本学习一个元模型，该模型使用投影随机梯度上升（projected stochastic gradient ascent，P-SGA）反向查找元模型，证明了在元学习的双层循环（外部更新和内部更新）中，内部更新可以由一个简单封闭的表达式解决，通过一个SGD步骤和投影步骤，使得内部更新不需要计算二阶导数（海森矩阵），大大降低了计算成本，提高了通信效率。

（4）FedMeta w/UGA算法

传统的联邦学习算法由服务器随机选择部分客户端加入训练，并将全局模型发送给客户端进行本地更新，参考文献[77]提出在客户端的多步骤更新可能会对模型聚合带来梯度偏差，随机选择客户端将导致每轮的优化目标与真正的目标不一致。这两个问题都是在联邦学习分布式环境下自然产生的，并提出了一种无偏梯度聚集（unbiased gradient aggregation，UGA）算法。该算法使用保持追踪梯度下降和梯度评估策略减少本地更新造成的梯度偏差，并引入一个元更新过程，通过一个可控的元训练集来促进优化目标向目标分布靠近。

3.2.3 面向隐私保护的联邦元学习算法

（1）Robust FedML算法

联邦学习中除了要考虑数据的异构性，还要考虑环境中训练节点的边缘性。由于其计算资源和本地数据有限，单独的边缘设备难以实现实时的边缘智能，同时元学习算法更容易受到对抗性攻击[78-79]，扰动的数据输入可能导致目标处的局部快速适应模型的性能出现显著下降。为了应对有限的计算资源和本地数据带来的挑战，同时增强联邦元学习面对对

抗性攻击的鲁棒性，参考文献[80]提出一个建立在分布式鲁棒优化上的联邦元学习框架（federated meta-learning algorithm based on distributionally robust optimization，Robust FedML），其中模型首先通过联合元学习在一组边缘节点上进行训练，然后仅仅使用几个样本就可以快速适应在目标节点上学习新任务。作者指出基于分布式鲁棒优化的最新进展，可以通过解决以下问题来实现联邦元学习算法面对数据扰动时的鲁棒性，如式（5）所示：

$$\min_{\theta}\{L_t(\phi_t)+\max_{P:D(P,P_t)\leqslant\pi}E_P[l(\phi_t,(x,y))]\} \quad (5)$$

其中，$D(P,P_t)$ 是概率分布空间上的距离度量。作者采用Wasserstein距离作为概率分布空间上的距离度量。文中使用了一个对抗式数据生成过程，即在迭代过程中，每个边缘节点使用梯度上升构造对抗数据样本，并将其添加到自己的对抗数据集中。每个节点首先使用训练数据集更新θ_t，然后使用测试数据集和构建的敌对数据集本地更新θ_t。当本地更新完成后，将更新好的参数传递给中心服务器，通过构造对抗数据的方式实现算法的鲁棒性。

（2）FL-MN

相对于只使用本地数据进行更新，联邦学习虽然可以提高模型的准确性，但是很容易受到后门攻击，参与训练的客户端可能会向服务器发送使用恶意数据生成的模型参数，而且恶意后门攻击很难在实践中被检验到。元学习可以为联邦学习训练一个快速适应新任务的模型，但是后门攻击对联邦元学习的影响却少有研究，后门攻击在客户端微调初始共享模型后还能否继续是一个值得研究的问题。参考文献[81]首次研究了这个问题，并通过实验证明，即使在遭受后门攻击后使用良性数据进行长时间的元训练，或者使用良性数据进行微调，后门攻击的效果仍然是持续的。为了降低后门攻击对于联邦元学习的影响，受到匹配网络的启发，提出了一种防御机制基于匹配网络的联邦学习算法（federated learning with matching network，FL-MN），其中用户使用匹配网络的分类机制，根据输入样本特征与支持集中样本特征的距离进行分类。通过这种本地分类机制，可以在几轮更新后有效降低后门更新的成功率。这种本地防御机制虽然降低了后门攻击的成功率、增加了联邦元学习面对后门攻击的鲁棒性，但是也会导致在一些任务上准确度的降低。匹配网络是一种基于度量的元学习方法，自然地，可以进一步研究使用其他基于度量的元学习方法作为本地防御机制，以消除匹配网络带来的在一些任务上准确度降低的问题。

（3）Meta-FL

联邦学习由于其分布式设置和对隐私的保护，易受到后门攻击，现有的联邦学习要发现后门攻击[82]大多需要检查每个客户端发送的更新。而在联邦学习安全聚合的要求下，检查用户更新往往是不可接受的，那么能否在不检查用户更新的方式下进行后门攻击的防御。参考文献[83]提出了一个新的联邦元学习框架Meta-FL（meta federated learning），该框架旨在不检查各客户端的情况下防御后门攻击，其主要思想是将防御检查点从用户端级别移动到聚合级别，以有效缓解后门攻击带来的影响。Meta-FL算法将不同客户端进行分组，将传统的联邦聚合从一个阶段的全局聚合变为两个阶段的多层次聚合，首先根据客户端分组，在组内进行安全聚合[84]，每个组获得一个组内全局模型，然后中央服务器使用聚合规则聚合不

同组的组内全局模型以获得一个全体客户端共享的模型。通过组内聚合，安全聚合算法保证服务器可以聚合客户端提交的更新，但不能得知提交的具体值。通过聚合不同组的组内全局模型进行安全检查以防御攻击，虽然组间聚合时仍然可能泄露组内全局模型的信息，但是泄露的信息不再与单个用户相关，从而在保护单个用户数据安全的情况下进行后门攻击的防御。

联邦元学习算法分类见**表4**。

3.3 联邦元学习应用

相较于传统的联邦学习算法，联邦元学习因为其收敛快速、个性化能力强等优点被广泛应用到不同的领域，以下为现有的工作中联邦元学习算法的一些应用。

(1) 信用卡欺诈检测

信用卡诈骗每年给银行带来数十亿美元的损失。然而由于对用户数据安全和隐私保护的需求，各个银行间无法共享数据集。面对不同银行间数据流动的限制，传统的利用集中数据训练的模型很难检测到信用欺诈的存在。因为仅约2%的交易活动存在欺诈可能，所以数据集往往是不平衡的。人类可以利用以往的经验很快地识别出信用卡欺诈行为（对应元学习的快速学习能力）。参考文献[85]利用联邦元学习技术进行信用卡欺诈检测，该方法可以在不共享数据的情况下，通过使用联邦元学习算法聚合不同银行的信用卡欺诈检测模型的参数，构建一个共享的全局模型，

表 4 联邦元学习算法分类

分类	方法	特点
面向数据异构	FedMeta	使用一个共享的元学习者取代联邦学习中共享的全局模型，以更灵活的方式共享参数化算法
	Fedavg-Reptile	在联邦平均算法阶段后插入一个元学习微调阶段以提供一个可靠的初始化模型
	PerFedAvg	聚焦MAML算法在联邦学习情景下的收敛性分析，并提供了一个可证明收敛的方法解决函数为非凸的情况
	q-MAML	通过最小化一个聚合的加权损失函数，使得损失函数值较高的设备在目标优化函数中具有较高的相对权重从而促进模型在各个设备间的表现更加公平
	ARUBA	将在线凸优化和序列预测算法相结合，将元学习视为在线学习一系列损失
	PFL	在每轮训练过程中动态地修改设备损失函数以消除元模型对不同用户的偏见
	FedFomo	不再只学习一个单一的平均模型，通过n个服务器元模型，向不同客户端组发送不同的元模型
	FedRECON	利用元学习训练一个可以快速重构局部参数的全局参数，并在客户端上使用全局参数进行局部参数重构
面向资源挑战	NUFM	使用非均匀的设备选择方案NUFM促进模型收敛速度提高
	ADMM-FedMeta	将原始问题分解为许多子问题，可以跨边缘节点和平台并行解决，通过线性近似和海森估计将计算复杂度降为$O(n)$
	EEFML	该模型使用投影随机梯度上升（P-SGA）来反向查找元模型，大大降低了计算成本、提高了通信效率
	FedMeta w/UGA	提出了一种无偏梯度聚集算法（UGA）并引入一个元更新过程，通过一个可控的元训练集来促进优化目标向目标分布靠近
面向隐私保护	RobustFedML	通过构造对抗数据的方式实现算法的鲁棒性
	FL-MN	使用匹配网络的分类机制有效降低后门攻击的成功率，但是也会导致在一些任务上准确度降低
	Meta-FL	将防御检查点从用户端级别移动到聚合级别，有效缓解后门攻击带来的影响

从而保护不同用户的隐私信息，同时，文中提出了一种新的基于元学习的分类器以改进三重态度量学习（triplet-like metric learning），该分类器可以同时与K个负样本进行比较。相比于其他最先进的信用卡欺诈检测模型FlowScope[86]、新型信用卡欺诈检测策略（a realistic modeling and a novel learning strategy，RMNLS）[87]，该方法在检测准确度方面得了明显的提升。

（2）分布式通信设备数据处理

第6代通信技术旨在实现全球互联，通信需求也从太空扩展到大气、地面和海洋。水下通信的要求也越来越高，水下声音通信是最有效的水下信息传输方式。深度学习在解决水下声音信号恢复问题上取得了很好的效果，然而依然存在两个问题：设备是分布式的；在单个节点上的数据可能不足。参考文献[88]提出一种基于声学无线电合作增强的联邦元学习算法以解决数据水下通信设备分布式连接和数据不足的问题，其只需要在本地数据集上通过几步梯度下降进行简单微调就能快速适应新任务的特性。ARC/FML算法可以从边缘节点快速更新网络，传递网络参数而不是发送节点数据的方式大大提高了分布式节点间的通信效率，并通过元学习算法提高机器学习在通信领域的鲁棒性。

（3）个性化联邦元学习推荐系统

相较于数据集中的传统推荐系统而言，联邦推荐系统在保护数据隐私、整合利用数据方面具有很大优势。然而以往的联邦推荐系统没有考虑到设备在计算资源、通信带宽方面的限制，提出的推荐模型过于庞大，很难在移动设备上运行。同时，一个统一的全局推荐模型很难利用用户间的协同过滤信息。为了解决上述问题，参考文献[89]引入一个联邦矩阵分解算法元矩阵分解（meta matrix factorization，MetaMF），该方法在服务器上使用元推荐模型生成私用项嵌入和评级预测模型以更好地利用联邦推荐系统中的协同过滤信息，同时该方法可以在不损失性能的情况下减少模型参数。

参考文献[90]借鉴Reptile算法提出了一种简单有效的联邦元学习推荐系统。其采用循环训练的方式，每个循环中包含一个全局训练阶段和一个本地训练阶段。在全局训练过程中，客户端在经过几步随机梯度下降更新后，将本地模型发送给服务器；服务器聚合模型参数后，将全局模型发送给不同的客户端；在进行指定数目的全局训练更新后，客户端保存本地模型参数，并进入本地训练过程。在本地训练过程中，模型经过指定数目的本地模型更新后，客户端加载之前保存的本地模型参数，并进入下一轮更新中。该算法与Reptile算法有很大的相似之处，客户端从随机初始化的参数开始，采用边缘设备模型参数与初始模型参数的差值更新模型向量。参考文献[91]开发了一款基于客户端服务器架构的联邦元学习（federated meta-learning，FMLearn）模型，该模型允许上传机器学习模型的参数和数据集用于元学习算法的选择和配置，可以更快地为输入数据选择最优的模型和参数，极大地降低了为数据集训练模型的时间。

4 总结和展望

本文从联邦学习的背景出发，分别详细介绍了联邦学习、元学习、联邦元学习的相关概念。文章首先介绍了联邦学习的定义、训练过程、分类、特点以及联邦学习所面临的3个问题（数据异构、隐私保护、通信受限）并介绍了现有的应对方法。同时，从联邦学习客户端优化方面和服务器端优化方面对常见的联邦学习算法进行了

分类。第2节从元学习的基本概念出发，介绍了元学习的一般训练过程，并对元学习算法进行了分类总结。第3节详细介绍了联邦元学习算法在联邦学习个性化、合理分配资源、增强面对恶意攻击鲁棒性这3个方面所做的工作。元学习由于其快速适应新任务的能力，可以为联邦学习数据异构问题提供很好的解决方案，通过为每个客户端训练一个个性化模型解决联邦学习数据异构问题。同时联邦学习由于其分布式、重隐私的特性，很容易受到恶意攻击。联邦学习环境下，通信带宽有限、客户端上计算资源的限制等都是制约其发展的重要因素，通过引入元学习增强联邦学习面对恶意攻击的鲁棒性、合理分配资源都已经得到了广泛的研究。最后介绍了联邦元学习在不同领域的应用，详细介绍了联邦元学习在信用卡欺诈检测、分布式通信设备数据处理、个性化联邦学习推荐系统3个方面的研究实例。

随着人们对数据隐私保护重视程度的提高，机器学习中数据使用的安全性要求将越来越高。联邦学习作为数据隐私保护的重要方式，必将受到更多的重视。现有的关于联邦学习的研究只能应用于个别的机器学习模型，虽然对某个特定模型设计单独的算法可以使模型效果更好，但是一个通用、高效的联邦学习框架更加被需要，如何为不同节点训练不同模型成为一个重要课题。现有联邦学习算法的研究主要针对集中式的联邦学习架构，需要一个中心服务器，对于分布式联邦学习算法的研究还有待深入。

未来的研究难点在于如何解决联邦学习所面临的数据异构、隐私保护、通信环境不稳定的问题。元学习在联邦学习数据异构方面将起到更加重要的作用。如何将元学习与联邦学习更好地结合，使元学习适应联邦学习面临的复杂环境仍然是一个重要的课题。现有的联邦元学习主要研究如何为不同客户端训练一个良好的初始化模型，但是这种从不同客户端学习可转移知识的方法在面临恶意客户端攻击[92]时，相较于传统联邦学习算法可能会受到更大的影响，同时客户端的本地更新可能会使聚合的元模型产生梯度偏移。在隐私保护方面，利用基于度量的元学习算法增强元学习面对恶意攻击时的鲁棒性[81]是一个引人注目的方向，但是向服务器发送度量模型参数可能会产生用户敏感信息的泄露。目前一些元学习算法受益于特定的模型结构，如何将元学习中与模型耦合度较高的元学习算法与模型解耦以更好地应用于联邦学习中仍然值得研究。元学习算法是参数敏感的，在联邦学习环境中，客户端的突然加入与退出、通信的突然中断都可能会对元模型造成不利影响。如何提高联邦元学习算法面对通信受限环境的鲁棒性也是一个重要的研究方向。同时元学习本身也有很多研究难点，如何使基础模型更好更快地适应新的学习任务，甚至适应跨领域的任务，以及在元学习的进化性、可解释性、连续性、可扩展性方面都还有很多工作需要进行。

参考文献:

[1] 王健宗，孔令炜，黄章成，等. 联邦学习算法综述[J]. 大数据，2020，6(6)：64-82.
WANG J Z，KONG L W，HUANG Z C，et al. Research review of federated learning algorithms[J]. Big Data Research，2020，6(6)：64-82.

[2] BERTINETTO L，HENRIQUES J F，TORR P H S，et al. Meta-learning with differentiable closed-form solvers[J]. arXiv preprint，2018，arXiv:1805.08136.

[3] VILALTA R，DRISSI Y. A perspective

view and survey of meta-learning[J]. Artificial Intelligence Review, 2002, 18(2): 77-95.

[4] MITCHELL R, MICHALSKI J, CARBONELL T. An artificial intelligence approach[M]. Machine Learning. Heidelberg: Springer, 2013.

[5] FINN C, ABBEEL P, LEVINE S. Model-agnostic meta-learning for fast adaptation of deep networks[C]//Proceedings of the 34th International Conference on Machine Learning. New York: ACM Press, 2017: 1126-1135.

[6] YANG Q, LIU Y, CHENG Y, et al. Federated learning[J]. Synthesis Lectures on Artificial Intelligence and Machine Learning, 2019, 13(3): 1-207.

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

[8] ALEDHARI M, RAZZAK R, PARIZI R M, et al. Federated learning: a survey on enabling technologies, protocols, and applications[J]. IEEE Access: Practical Innovations, Open Solutions, 2020, 8: 140699-140725.

[9] 王健宗, 孔令炜, 黄章成, 等. 联邦学习隐私保护研究进展[J]. 大数据, 2021, 7(3): 130-149. WANG J Z, KONG L W, HUANG Z C, et al. Research advances on privacy protection of federated learning[J]. Big Data Research, 2021, 7(3): 130-149.

[10] 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.

[11] DWORK C. Differential Privacy: a survey of results[C]//Proceedings of International Conference on Theory and Applications of Models of Computation. Heidelberg: Springer, 2008: 1-19.

[12] DWORK C, ROTH A. The algorithmic foundations of differential privacy[J]. Foundations and Trends® in Theoretical Computer Science, 2013, 9(3/4): 211-407.

[13] 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.

[14] SATTLER F, WIEDEMANN 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, 2020, 31(9): 3400-3413.

[15] ZHAO Y, LI M, LAI L Z, et al. Federated learning with non-IID data[J]. arXiv preprint, 2018, arXiv:1806.00582.

[16] BRIGGS C, FAN Z, ANDRAS P. Federated learning with hierarchical clustering of local updates to improve training on non-IID data[C]//Proceedings of 2020 International Joint Conference on Neural Networks. Piscataway: IEEE Press, 2020: 1-9.

[17] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv preprint, 2016, arXiv:1602.05629.

[18] ARIVAZHAGAN M G, AGGARWAL V, SINGH A K, et al. Federated learning with personalization layers[J]. arXiv preprint, 2019, arXiv:1912.00818.

[19] KAIROUZ P, MCMAHAN H B, AVENT B, et al. Advances and open problems in federated learning[J]. Foundations and Trends® in Machine Learning, 2021, 14(1-2): 1-210.

[20] KONEČNÝ J, MCMAHAN H B, YU F X, et al. Federated learning: strategies for improving communication efficiency[J]. arXiv preprint, 2016, arXiv:1610.05492.

[21] HSU T M H, QI H, BROWN M. Measuring the effects of non-identical data distribution for federated visual classification[J]. arXiv preprint, 2019, arXiv:1909.06335.

[22] REDDI S, CHARLES Z, ZAHEER M, et al. Adaptive federated optimization[J]. arXiv preprint, 2020, arXiv:2003.00295.

[23] DUCHI J C, HAZAN E, SINGER Y. Adaptive subgradient methods for online learning and stochastic optimization[J]. Journal of Machine Learning Research, 2011, 12: 2121-2159.

[24] KINGMA D P, BA J. Adam: a method for stochastic optimization[J]. arXiv preprint, 2014, arXiv:1412.6980.

[25] ZAHEER M, REDDI S J, SACHAN D, et al. Adaptive methods for nonconvex optimization[C]//Proceedings of the 32nd International Conference on Neural Information Processing Systems. New York: ACM Press, 2018: 9815-9825.

[26] WANG H Y, YUROCHKIN M, SUN Y K, et al. Federated learning with matched averaging[J]. arXiv preprint, 2020, arXiv: 2002.06440.

[27] ARIVAZHAGAN M G, AGGARWAL V, SINGH A K, et al. Federated learning with personalization layers[J]. arXiv preprint, 2019, arXiv:1912.00818.

[28] LI T, SAHU A K, ZAHEER M, et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine Learning and Systems, 2020, 2: 429-450.

[29] KONEČNÝ J, MCMAHAN B, RAMAGE D. Federated optimization: distributed optimization beyond the datacenter[J]. arXiv preprint, 2015, arXiv:1511.03575.

[30] DENG Y Y, KAMANI M M, MAHDAVI M. Adaptive personalized federated learning[J]. arXiv preprint, 2020, arXiv: 2003.13461.

[31] KARIMIREDDY S P, KALE S, MOHRI M, et al. SCAFFOLD: stochastic controlled averaging for federated learning[J]. arXiv preprint, 2019, arXiv:1910.06378.

[32] LI T, HU S Y, BEIRAMI A, et al. Ditto: fair and robust federated learning through personalization[J]. arXiv preprint, 2020, arXiv:2012.04221.

[33] LI Q B, HE B S, SONG D. Model-contrastive federated learning[C]// Proceedings of 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2021: 10708-10717.

[34] KHODAK M, BALCAN M F, TALWALKAR A. Adaptive gradient-based meta-learning methods[J]. arXiv preprint, 2019, arXiv:1906.02717.

[35] VANSCHOREN J. Meta-learning: a survey[J]. arXiv preprint, 2018, arXiv: 1810.03548.

[36] VILALTA R, DRISSI Y. A perspective view and survey of meta-learning[J]. Artificial Intelligence Review, 2002, 18(2): 77-95.

[37] 李凡长, 刘洋, 吴鹏翔, 等. 元学习研究综述[J]. 计算机学报, 2021, 44(2): 422-446.
LI F Z, LIU Y, WU P X, et al. A survey on recent advances in meta-learning[J]. Chinese Journal of Computers, 2021, 44(2): 422-446.

[38] HSU K, LEVINE S, FINN C. Unsupervised learning via meta-learning[J]. arXiv preprint, 2018, arXiv: 1810.02334.

[39] KHODADADEH S, BOLONI L, SHAH M. Unsupervised meta-learning for few-shot image classification[J]. Advances in Neural Information Processing Systems, 2019, 32.

[40] SNELL J, SWERSKY K, ZEMEL R. Prototypical networks for few-shot learning[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. New York: ACM Press, 2017: 4080-4090.

[41] RAVI S, LAROCHELLE H. Optimization as a model for few-shot learning[J]. International Conference on Learning Representations, 2016.

[42] DUAN Y, SCHULMAN J, CHEN X, et al. RL2: fast reinforcement learning via slow reinforcement learning[J]. arXiv preprint, 2016, arXiv:1611.02779.

[43] ANDRYCHOWICZ M, DENIL M, COLMENAREJO S G, et al. Learning to learn by gradient descent by gradient descent[C]//Proceedings of the 30th International Conference on Neural Information Processing Systems. New York: ACM Press, 2016: 3988-3996.

[44] SANTORO A, BARTUNOV S, BOTVINICK M, et al. Meta-learning with memory-augmented neural networks[C]// Proceedings of the 33rd International Conference on Machine Learning. New York: ACM Press, 2016: 1842-1850.

[45] MISHRA N, ROHANINEJAD M, CHEN X, et al. A simple neural attentive meta-learner[J]. arXiv preprint, 2017, arXiv: 1707.03141.

[46] RAJESWARAN A, FINN C, KAKADE S, et al. Meta-learning with implicit gradients[J]. arXiv preprint, 2019, arXiv: 1909.04630.

[47] SONG X Y, GAO W B, YANG Y X, et al. ES-MAML: simple hessian-free meta learning[J]. arXiv preprint, 2019, arXiv: 1910.01215.

[48] SALIMANS T, HO J, CHEN X, et al. Evolution strategies as a scalable alternative to reinforcement learning[J]. arXiv preprint, 2017, arXiv:1703.03864.

[49] NICHOL A, ACHIAM J, SCHULMAN J. On first-order meta-learning algorithms[J]. arXiv preprint, 2018, arXiv: 1803.02999.

[50] RUSU A A, RAO D, SYGNOWSKI J, et al. Meta-learning with latent embedding optimization[J]. arXiv preprint, 2018, arXiv:1807.05960.

[51] SUNG F, ZHANG L, XIANG T, et al. Learning to learn: meta-critic networks for sample efficient learning[J]. arXiv preprint, 2017, arXiv:1706.09529.

[52] VINYALS O, BLUNDELL C, LILLICRAP T, et al. Matching networks for one shot learning[C]//Proceedings of the 30th International Conference on Neural Information Processing Systems. New York: ACM Press, 2016: 3637-3645.

[53] SNELL J, SWERSKY K, ZEMEL R. Prototypical networks for few-shot learning[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. New York: ACM Press, 2017: 4080-4090.

[54] KOCH G, ZEMEL R, SALAKHUTDINOV R. Siamese neural networks for one-shot image recognition[C]//Proceedings of ICML Deep Learning Workshop. [S.l.:s.n.], 2015.

[55] SANTORO A, RAPOSO D, BARRETT D G T, et al. A simple neural network module for relational reasoning[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. New York: ACM Press, 2017: 4974-4983.

[56] CHAWLA N V, BOWYER K W, HALL L O, et al. SMOTE: synthetic minority over-sampling technique[J]. Journal of Artificial Intelligence Research, 2002, 16: 321-357.

[57] INOUE H. Data augmentation by pairing samples for images classification[J]. arXiv preprint, 2018, arXiv:1801.02929.

[58] GOODFELLOW I, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial networks[J]. Communications of the ACM, 2020, 63(11): 139-144.

[59] CUBUK E D, ZOPH B, MANE D, et al. AutoAugment: learning augmentation policies from data[J]. arXiv preprint, 2018, arXiv:1805.09501.

[60] ZHANG H P, CAO Z, YAN Z A, et al. Sill-net: feature augmentation with separated illumination representation[J]. arXiv preprint, 2021, arXiv:2102.03539.

[61] RAJENDRAN J, IRPAN A, JANG E. Meta-learning requires meta-augmentation[C]// Proceedings of the 34th International Conference on Neural Information Processing Systems. New York: ACM Press, 2020: 5705-5715.

[62] ZHOU F W, LI J W, XIE C L, et al. MetaAugment: sample-aware data augmentation policy learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2021, 35(12): 11097-11105.

[63] ZHANG R X, CHE T, GHAHRAMANI Z, et al. MetaGAN: an adversarial approach to few-shot learning[C]//Proceedings of the 32nd International Conference on Neural Information Processing Systems. New York: ACM Press, 2018: 2371-2380.

[64] SUN P, OUYANG Y, ZHANG W, et al. MEDA: meta-learning with data augmentation for few-shot text classification[C]//Proceedings of 2021 International Joint Conference on Artificial Intelligence. [S.l.:s.n.], 2021: 3929-3935.

[65] CHEN F, LUO M, DONG Z H, et al. Federated meta-learning with fast convergence and efficient communication[J]. arXiv preprint, 2018, arXiv:1802.07876.

[66] JIANG Y H, KONEČNÝ J, RUSH K, et al. Improving federated learning personalization via model agnostic meta learning[J]. arXiv preprint, 2019, arXiv: 1909.12488.

[67] FALLAH A, MOKHTARI A, OZDAGLAR A. Personalized federated learning with theoretical guarantees: a model-agnostic meta-learning approach[J]. Advances in Neural Information Processing Systems, 2020, 33: 3557-3568.

[68] ZAFAR M B, VALERA I, GOMEZ RODRIGUEZ M, et al. Fairness beyond disparate treatment & disparate impact: learning classification without disparate mistreatment[C]//Proceedings of the 26th International Conference on World Wide Web. Switzerland: International World Wide Web Conferences Steering Committee, 2017: 1171-1180.

[69] LI T, SANJABI M, BEIRAMI A, et al. Fair resource allocation in federated learning[J]. arXiv preprint, 2019, arXiv: 1905.10497.

[70] KHODAK M, BALCAN M F, TALWALKAR A. Adaptive gradient-based meta-learning methods[J]. arXiv preprint, 2019, arXiv:1906.02717.

[71] ZHANG M, SAPRA K, FIDLER S, et al. Personalized Federated Learning with first order model optimization[C]//Proceedings of International Conference on Learning Representations. [S.l.:s.n.], 2020.

[72] ACAR D A E, ZHAO Y, ZHU R, et al. Debiasing model updates for improving personalized federated training[C]// Proceedings of International Conference on Machine Learning. [S.l.:s.n.], 2021: 21-31.

[73] SINGHAL K, SIDAHMED H, GARRETT Z, et al. Federated reconstruction: partially local federated learning[J]. arXiv preprint, 2021, arXiv: 2102.03448.

[74] YUE S, REN J, XIN J, et al. Efficient federated meta-learning over multi-access wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(5): 1556-1570.

[75] YUE S, REN J, XIN J, et al. Inexact-ADMM based federated meta-learning for fast and continual edge learning[C]// Proceedings of the 22nd International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing. New York: ACM Press, 2021: 91-100.

[76] ELGABLI A, ISSAID C B, BEDI A S, et al. Energy-efficient and federated meta-learning via projected stochastic

gradient ascent[C]//Proceedings of 2021 IEEE Global Communications Conference. Piscataway: IEEE Press, 2022: 1-6.

[77] YAO X, HUANG T C, ZHANG R X, et al. Federated learning with unbiased gradient aggregation and controllable meta updating[J]. arXiv preprint, 2019, arXiv: 1910.08234.

[78] EDMUNDS R, GOLMANT N, RAMASESH V, et al. Transferability of adversarial attacks in model-agnostic meta-learning[C]//Proceedings of 2017 Deep Learning and Security Workshop. [S.l.:s.n.], 2017.

[79] YIN C X, TANG J, XU Z Y, et al. Adversarial meta-learning[J]. arXiv preprint, 2018, arXiv:1806.03316.

[80] LIN S, YANG G, ZHANG J S. A collaborative learning framework via federated meta-learning[C]//Proceedings of 2020 IEEE 40th International Conference on Distributed Computing Systems. Piscataway: IEEE Press, 2021: 289-299.

[81] CHEN C L, GOLUBCHIK L, PAOLIERI M. Backdoor attacks on federated meta-learning[J]. arXiv preprint, 2020, arXiv: 2006.07026.

[82] YIN D, CHEN Y D, RAMCHANDRAN K, et al. Byzantine-robust distributed learning: towards optimal statistical rates[J]. arXiv preprint, 2018, arXiv: 1803.01498.

[83] ARAMOON O, CHEN P Y, QU G, et al. Meta federated learning[J]. arXiv preprint, 2021, arXiv:2102.05561.

[84] BONAWITZ K, IVANOV V, KREUTER B, et al. Practical secure aggregation for privacy-preserving machine learning[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 1175-1191.

[85] ZHENG W B, YAN L, GOU C, et al. Federated meta-learning for fraudulent credit card detection[C]//Proceedings of the 29th International Joint Conference on Artificial Intelligence. New York: ACM Press, 2021: 4654-4660.

[86] LI X F, LIU S H, LI Z F, et al. FlowScope: spotting money laundering based on graphs[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2020, 34(4): 4731-4738.

[87] DAL POZZOLO A, BORACCHI G, CAELEN O, et al. Credit card fraud detection: a realistic modeling and a novel learning strategy[J]. IEEE Transactions on Neural Networks and Learning Systems, 2018, 29(8): 3784-3797.

[88] ZHAO H, JI F, LI Q, et al. Federated meta-learning enhanced acoustic radio cooperative framework for ocean of things[J]. IEEE Journal of Selected Topics in Signal Processing, 2022, 16(3): 474-486.

[89] LIN Y J, REN P J, CHEN Z M, et al. Meta matrix factorization for federated rating predictions[C]//Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval. New York: ACM Press, 2020: 981-990.

[90] JALALIRAD A, SCAVUZZO M, CAPOTA C, et al. A simple and efficient federated recommender system[C]//Proceedings of the 6th IEEE/ACM International Conference on Big Data Computing, Applications and Technologies. New York: ACM Press, 2019: 53-58.

[91] BEEL J. Federated meta-learning: democratizing algorithm selection across disciplines and software libraries[J]. Science (AICS), 2018, 210: 219.

[92] 吴建汉, 司世景, 王健宗, 等. 联邦学习攻击与防御综述[J]. 大数据, 2022, 8(5): 12-32.
WU J H, SI S J, WANG J Z, et al. Threats and defenses of federated learning: a survey[J]. Big Data Research, 2022, 8(5): 12-32.

作者简介

张传尧（1998- ），男，中国科学技术大学硕士研究生，平安科技（深圳）有限公司算法工程师，主要研究方向为元学习和联邦学习。

司世景（1988- ），男，博士，平安科技（深圳）有限公司资深算法研究员，深圳市海外高层次人才，美国杜克大学人工智能博士后，中国计算机学会会员，主要研究方向为机器学习和及其在人工智能领域应用。

王健宗（1983- ），男，博士，平安科技（深圳）有限公司副总工程师，资深人工智能总监，联邦学习技术部总经理。美国佛罗里达大学人工智能博士后，中国计算机学会高级会员，中国计算机学会大数据专家委员会委员，曾任美国莱斯大学电子与计算机工程系研究员，主要研究方向为联邦学习和人工智能等。

肖京（1972- ），男，博士，平安集团首席科学家，2019年吴文俊人工智能杰出贡献奖获得者，中国计算机学会深圳分部副主席，主要研究方向为计算机图形学学科、自动驾驶、3D显示、医疗诊断、联邦学习等。

收稿日期： 2021-11-15
通信作者： 王健宗，jzwang@188.com
基金项目： 广东省重点领域研发计划“新一代人工智能”重大专项（No.2021B0101400003）
Foundation Item: The Key Research and Development Program of Guangdong Province (No.2021B0101400003)