计算机科学
COMPUTER SCIENCE

基于联邦学习的网络化ICU呼吸机和镇静剂管理方法

曹林霄, 刘佳, 朱怡飞, 周浩泉, 龚伟, 于卫华, 李朝友

引用本文

曹林霄, 刘佳, 朱怡飞, 周浩泉, 龚伟, 于卫华, 李朝友. 基于联邦学习的网络化ICU呼吸机和镇静剂管理方法[J]. 计算机科学, 2023, 50(10): 165-175.

CAO Linxiao, LIU Jia, ZHU Yifei, ZHOU Haoquan, GONG Wei, YU Weihua, LI Chaoyou. Ventilator and Sedative Management in Networked ICUs Based on Federated Learning [J]. Computer Science, 2023, 50(10): 165-175.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220900177

基于联邦学习的网络化ICU呼吸机和镇静剂管理方法

曹林霄[1] 刘 佳[2] 朱怡飞[3] 周浩泉[4] 龚 伟[4] 于卫华[5] 李朝友[6]
1 中国科学技术大学大数据学院 合肥 230026
2 安徽医科大学附属省立医院儿科 合肥 230001
3 上海交通大学密西根学院 上海 200240
4 中国科学技术大学附属第一医院儿科 合肥 230001
5 合肥市第一人民医院护理部 合肥 230061
6 合肥市第一人民医院儿科 合肥 230061
(linxiaocao@mail.ustc.edu.cn)

摘 要 医疗物联网设备的激增和丰富的医疗数据为智慧医疗提供了新的可能。重症监护室(ICU)的病人依靠众多医疗边缘设备来持续监测管理患者的健康状况。在ICU常见的治疗干预措施中,有创机械通气和镇静剂的注射多用于维持患者的呼吸功能,提高治疗质量,而现有的治疗干预措施很大程度上依赖于医生的判断。文中提出了一种基于联邦学习的临床辅助决策方法——MFed,可以基于网络化ICU分布式协作学习最佳干预政策。该方法应用基于差分隐私的联邦学习方法,打破了医疗数据隐私方面的限制以及医疗数据孤岛的窘境;用分布鲁棒优化确保最坏情况下的性能并结合伪孪生网络实现自适应地滤除噪声数据。最后,在现实ICU数据集上的实验表明,与其他最先进的基线相比,所提方法的准确率提高了36.75%。

关键词:联邦学习;医疗物联网;分布式鲁棒优化;医疗数据噪声;医疗数据隐私
中图法分类号 TP391

Ventilator and Sedative Management in Networked ICUs Based on Federated Learning

CAO Linxiao[1],LIU Jia[2],ZHU Yifei[3],ZHOU Haoquan[4],GONG Wei[4],YU Weihua[5] and LI Chaoyou[6]
1 School of Data Science,University of Science and Technology of China,Hefei 230026,China
2 Department of Pediatrics,Provincial Hospital Affiliated to Anhui Medical University,Hefei 230001,China
3 University of Michigan-Shanghai Jiao Tong University Joint Institute,Shanghai Jiao Tong University,Shanghai 200240,China
4 Department of Pediatrics,The First Affiliated Hospital of USTC,Hefei 230001,China
5 Department of Nursing,The First People's Hospital of Hefei,Hefei 230061,China
6 Department of Pediatrics,The First People's Hospital of Hefei,Hefei 230061,China

Abstract The proliferation of medical IoT devices and the abundance of medical data open up new possibilities for smart healthcare. Patients in the intensive care unit (ICU) rely on numerous medical IoT devices to continuously monitor and manage patients' health status. Among the common therapeutic interventions in ICUs, invasive mechanical ventilation and sedation are mostly administered to maintain patients' respiratory function and enhance the care quality. While the existing therapeutic interventions rely heavily on physician judgment. This paper proposes a data-driven optimal policy learning framework named MFed that allows distributed learning of optimal intervention policies on networked ICUs. A differentially private federated learning method is constructed to overcome privacy limitations in medical data. MFed further ensures worst-case performance with distributionally robust optimization and adaptively filters out noisy data. Extensive experiments on a real-world ICU dataset show that the proposed method improves accuracy by 36.75% compared to other state-of-the-art baselines.

Keywords Federated learning,Medical IoT,Distributionally robust optimization,Medical data noise,Medical data privacy

1 引言

随着物联网设备在医疗领域的广泛应用,大量的临床数据也相应产生。近期,Dell Technologies的一项全球范围内的调研报告显示[1],在过去的两年中,医疗领域的数据增长超过878%,且增长的趋势也一直未见减缓。而这些数据

到稿日期:2022-09-17 返修日期:2023-02-10
基金项目:合肥市自主创新政策"借转补"项目(J2020Y03)
This work was supported by the Hefei Healthcare Grant(J2020Y03).
通信作者:周浩泉(zhouhq2005@qq.com)

大部分都来源于医院中各种各样的医疗物联网设备对患者生命体征的持续长时间的测量[2]。数据丰富的现代医疗环境为新兴人工智能与传统医疗技术的融合和智慧医疗的发展提供了沃土[3]。

重症监护室(Intensive Care Unit,ICU)是医院专为病情较重的患者所设立的特殊病房,以对病人实现更加精确的治疗和护理。在ICU中,存在着大量带有各类传感器的医疗物联网设备,例如呼吸机、监护仪、心电图机等,这些设备时刻监督着病人的生命体征,方便医生在病人病情出现不良变化时可以实时干预。传统意义上,医生需要理解这些由边缘设备采集到的复杂异构的数据,从而做出正确的临床决策。而在这样的背景下,缺乏一个严谨和最佳的治疗指导无疑会使不同医生所提出的治疗方案存在差异[4]。智能医疗干预一般指利用人工智能技术从这些复杂多模态的临床数据中获取最佳的治疗策略,提升治疗效果,完善医治的方案指导,如图1所示。

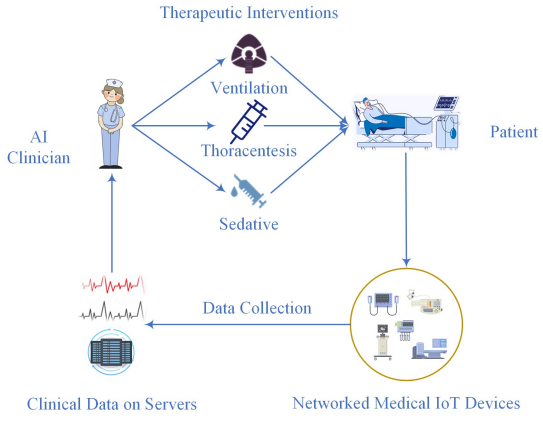


图1 智慧医疗干预示意图

Fig. 1 Illustration of intelligent therapeutic interventions

有创呼吸机是ICU中常用的医疗干预手段,为已经无法自主呼吸的患者提供基本的呼吸功能,以维持生命和基本生理需求。而呼吸机的使用时长,即患者的通气时长,无论是对医院还是对患者都非常重要。已有工作显示[5],过早地拔管会给病人的病情恢复带来负面影响甚至会危及生命;同样,保守地延迟拔管时间,一方面会增加病人感染的风险,另一方面也不利于病人的身体康复,同时还会带来额外的经济负担。而有创呼吸机的使用通常需要切开病人的气管来进行操作,会给患者带来极大的痛苦。因此在实际治疗过程中,有创呼吸机通常又和镇痛镇静剂配合使用,以减少病人的痛楚,保证患者在通气情况下能保证生理稳定。然而,不同患者生理因素的天然相异,导致不同的患者对相同剂量的镇静剂药物所产生的反应也同样存在着差别[6]。因此设计个性化的镇静剂使用策略来提升ICU的治疗效果和护理质量,也是目前的潜在需求。

当前,随着医疗物联网设备在ICU中被广泛使用以及人工智能技术的突飞猛进,ICU中部署的这些分散的医疗终端设备构成了天然的边缘计算的场景,充分利用这些设备所采集的数据,构建一个临床呼吸机和镇静剂联合管理的辅助决策工具,优化原有的治疗方案,减小患者在ICU中的死亡率,提升ICU的治疗水平,引起了人们的广泛关注。

一般来说,传统的机器学习方法通常都要求拥有一个多样的、综合全面的数据集,各类机器学习方法从中学习到高质量的策略模型。而考虑现实中医疗资源的不均匀分布,各级医疗机构间的治疗水平也参差不齐,在这样的设定下,仅通过个别医疗机构的数据来构建这样完备的数据环境是有挑战的。而利用这样的数据集所训练出的模型在面对未知的数据时,其表现通常会大打折扣,模型的泛化能力堪忧。因此,协同多家医疗机构的临床数据,联合搭建治疗策略模型(见图2),是目前亟需解决的问题。

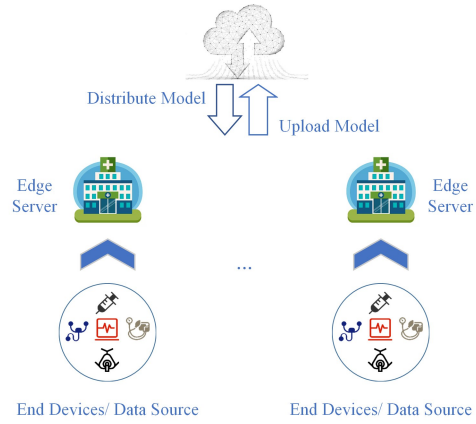


图2 分布式网络化医疗环境协作学习

Fig. 2 Illustration of collaborative learning in distributed networked healthcare environment

为了实现上述目标,我们将会面临着以下几项挑战。首先是隐私问题,医疗数据通常都会涉及患者的隐私以及道德伦理层面的问题,一旦遭到泄露或者被滥用,都会对医患双方产生一系列非常严重的后果[7]。因此,简单的聚合或者共享这些医疗机构彼此之间的数据在实际操作过程中是不可行的[8],而已有的工作证明,一般的联邦学习在参数传递的过程中同样会带来隐私顾虑[8]。因此如何在保证病人的数据隐私不被泄露的前提下,联合各家医院的数据共同训练一个临床决策工具是值得探索的。其次,在分布式医疗场景下,利用分散异构的训练数据所得到的策略模型理应在各站点的测试集上均有不俗的表现。因此,如何保证全局模型在各家医院数据分布不同的情况下都能有较好的性能,也是值得深究的问题。最后,在医疗领域中,由于不正确的输入和注释、不一致的命名和编码习惯等,电子健康记录(EHR)数据中很容易掺入不同类型的噪声,进而导致数据质量低下,而这样的数据可能在一定程度上造成模型的性能损失。因此,如何减轻数据噪声对模型训练的影响并生成一个可适用的模型也并非易事。

针对上述挑战,本文提出了一个基于差分隐私的联邦学习框架MFed,该框架充分利用不同医院ICU中的数据,来学习最佳的呼吸机和镇静剂管理策略。具体来说,每个医院的边缘服务器利用差分隐私扰动本地模型参数后,将其上传到云端服务器,所有上传云端的模型参数将会以特定规则被聚合,然后分发给参与模型训练的边缘服务器,而每个医院的原始数据在整个训练过程中不会被传递,以保证数据隐私。

我们采用分布鲁棒优化（Distributionally Robust Optimization，DRO）来缓解数据异构性的负面影响，保证模型在最坏情况下的性能。同时，我们使用伪孪生网络对有数据噪声的边缘服务器进行协同损失剪裁，以减轻数据噪声对模型训练的影响。

本文的主要贡献如下：

1）MFed 提出了在 ICU 智慧医疗领域应用差分隐私和联邦学习相结合的方式，来解决呼吸机和镇静剂决策问题。

2）MFed 使用分布鲁棒优化，通过最小化模型训练数据分布附近的最坏情况分布的损失，来优化全局模型，以使模型更契合每个边缘服务器的本地数据。

3）MFed 用边缘服务器的本地模型参数和云服务器的聚合参数构建了伪孪生网络结构，使用协同损失函数，选择损失小的数据样本训练模型，来减轻噪声标签造成的负面影响。

4）在 ICU 数据集上进行的大量实验表明，MFed 在不共享原始数据的情况下就能达到和集中式机器学习方法相抗衡的性能。

本文第 2 章介绍了研究背景和相关工作；第 3 章描述了 MFed 的详细设计；第 4 章展示了 MFed 的实验结果以及进行了性能评估；最后总结全文。

2 研究背景与相关工作

2.1 联邦学习在医疗领域的应用

联邦学习（Federated Learning，FL）是一种分布式机器学习范式，可以有效解决数据孤岛的问题，允许参与者在不共享原始数据的情况下协作训练神经网络模型[9]。训练过程通常由服务器协调，以迭代的方式执行，直到获得全局模型收敛。具体来说，服务器初始化模型参数并将其分发给参与训练的客户端。被选中的参与者用自己所下载的模型参数初始化他们的本地模型，并使用其本地所采集的数据训练本地模型。然后，每个客户端将本地更新的模型参数发送到服务器上。服务器根据不同的聚合规则聚合客户端上传的本地模型来更新全局模型。更新后的全局模型被分发回参与训练的客户端，进行下一轮的本地训练和全局聚合。由于对数据隐私和医疗智能化的迫切需求，联邦学习已经成为连接不同医疗机构的 EHR 数据的可选方案[10]。它已被广泛应用于各种医疗保健场景，包括医学图像分析、疾病诊断等。

2.1.1 联邦学习应用于医疗影像分析

联邦学习适合处理多源分散的医学图像数据这样的任务，即不同的医疗机构需要处理相同的任务，但对应的病人不同[11]。Yan 等[12]最近提出了一种联邦学习方法，通过将所有客户端的图像转化到公共图像空间来解决不同机构之间可能存在的差异，并将其应用于前列腺癌的分类任务。Sheller 等[13]训练了一个具有分布式结构的深度神经网络，来划分脑瘤患者的 MRI 扫描图像。Zhang 等[14]提出了一种新型的基于动态融合的联邦学习，用于医学图像诊断分析，检测 COVID-19 感染情况。Guo 等[15]提出了用于磁共振图像重构的跨客户端建模，在不同源域客户端之间学习和目标客户端潜在分布一致的中间潜在特征，从而从欠采样数据中重新准确地构建磁共振图像。Malekzadeh 等[16]提出了一个为检测糖尿病视网膜病变而设计的医疗决策工具，该工具采用了结合差分隐私随机梯度下降的联邦学习，通过安全聚合来权衡隐私和准确性。

2.1.2 联邦学习应用于其他智慧医疗领域

Lu 等[17]提出了一个无中心服务器概念的联邦学习框架，用于处理 EHR 数据，并对心脏和精神状况的诊断问题进行数学建模，以实现智能辅助治疗。Wu 等[18]提出了一个基于云边缘的联邦学习框架，该框架从不同的客户端学习全局模型，用于家庭健康监测，并使用卷积自动编码器来处理数据异构性的影响。Xu 等[19]提出了一个通用的多视图联邦学习框架，使用移动设备上的数据来检测抑郁症，然后使用后期融合方法来解决多视图数据时间序列不一致的问题。Tan 等[20]提出了一种基于树的模型平均方法，使用来自其他潜在异构站点的模型来提高目标站点治疗的准确性，并通过验证氧疗法对患者生存率的影响证实了该方法的可行性。Elayan 等[21]提出了一个联邦学习框架，自动捕捉训练数据，以便利用可穿戴的物联网设备检测皮肤病。

2.2 差分隐私

现有的研究表明，联邦学习在客户端和服务器端的每次交互过程中的参数同样存在泄露隐私的可能，即攻击者利用相关参数在相邻轮次进行差异分析，这可能会导致部分患者的临床数据被暴露[22]。差分隐私（Differential Privacy，DP）可以为分布式数据处理系统的隐私保护提供一个强有力的保障，通常通过给模型参数添加噪声扰动，来防止敏感的数据被暴露[23]。如果随机算法 $f(D)$ 在任意相差一条记录的 D 和 D' 数据集满足：

$$\Pr[f(D)\in S]\leqslant e^{\epsilon}\Pr[f(D')\in S] \tag{1}$$

则随机算法 $f(D)$ 满足 ϵ-DP，其中 ϵ 是隐私参数，决定了隐私保护程度。这样就意味着数据集中的任何一条记录都不会对算法的输出分布产生重大影响[24]。基于差分隐私的联邦学习方法根据场景的不同被划分为中心化差分隐私和本地差分隐私。中心化差分隐私通常对云端服务器聚合的参数加入噪声扰动，而面向客户端的差分隐私保护，一般在客户端参数上传前对模型参数进行扰动。基于差分隐私的联邦学习方法已经有大量的应用。Choudhury 等[25]将融合联邦学习和差分隐私的方法应用于现实世界的健康数据，提供两层隐私保护机制。首先，模型训练过程中原始数据并不会跨组织流动；其次，差分隐私机制的引入可以保护模型免受潜在的隐私攻击。Adnan 等[26]利用联邦学习实现分布式分析癌症基因图谱，并达到与传统训练相近的性能，应用差分隐私保护技术能进一步提升数据的安全性。

2.3 噪声标签处理

在医疗任务中，EHR 数据中存在噪声标签的原因为编码不准确、命名规则不一致等。本地数据噪声通常指个别医院在本地收集或处理病人数据时引入的噪声。不准确的测量和错误的输入同样是 ICU 中噪声标签数据的主要来源。关于医疗数据噪声的更详细的描述可以参照 Lee 等[27]的工作。

众多研究者已经意识到这个问题的重要性，并一直试图理解标签噪声，开发新颖而稳健的学习方法来解决它们。Co-teaching[28]在选定的或加权的样本上进行训练，简单地说，

Co-teaching 会同时训练两个网络，通过逐步选择模型中损失较小的数据样本，在另一个模型上进行训练和更新，并在两个模型之间不断交换自己模型中损失较小的数据，利用两个网络提供的不同视角来实现噪声控制。JoCoR[29]的架构与 Co-teaching 相似，但两个模型的损失是联合计算的，模型是联合更新的。一般认为，不同的模型会在大多数样本的正确标签上达成一致，而在错误的标签上不太可能达成一致。在 JoCoR 训练过程中，有两种损失，一种是两个模型各自的输出和标签之间的分类损失，另一种是两个预测之间的距离损失，其中距离损失是为了使两个模型尽可能一致。

2.4 MFed 与已有工作的差异

Prasad 等[30]使用 off-policy 强化学习算法来根据所提供的病人历史轨迹选择适当的干预措施。而 Yu 等[31]利用贝叶斯逆强化学习方法，通过推断特定潜在奖励函数内部的权重来平衡评价标准的各个方面。与之前的工作相比，MFed 是一个临床决策工具，它在分散的场景下跨边缘设备工作，实现相同的任务，同时利用联邦学习结合差分隐私来解决医疗数据孤岛所带来的挑战。MFed 是在分布式场景中，在保护患者数据隐私的前提下，实现临床决策，并缓解了医疗数据存在噪声的影响。MFed 是利用联邦学习结合差分隐私建立的 ICU 智能决策框架，利用基于医疗物联网边缘设备采集的数据对 ICU 中的呼吸机和镇静剂两个常见医疗干预手段进行联合管理，并对患者的隐私高度保密。此外，MFed 使用 DRO 优化最差分布下的模型表现，结合协同损失训练，可以自适应地过滤掉有噪声标签的数据，减轻医疗数据噪声的负面影响，进一步提高模型的鲁棒性。

3 框架设计

本章将介绍 MFed 的详细设计，在分布式场景下，以保护患者敏感数据为前提，跨组织地从存在有噪声标签的医疗数据中学习到最佳决策策略。

3.1 MFed 整体框架

MFed 的整体框架如图 3 所示。MFed 的主要特征就是基于差分隐私的联邦学习方法，实现在不共享本地数据的情况下，基于联邦学习训练一个全局适用的模型。我们在 ICU 中使用医疗物联网终端设备监测病人的体征，以确定病人是否准备好拔管以及对镇静剂的药物反应。具体来说，当边缘服务器接收到来自云端服务器所下发的模型参数，边缘服务器由下载的全局模型和上轮迭代的本地模型构建伪孪生结构，利用逆强化学习方法通过边缘物联网设备采集的本地私有数据完成本地策略模型的联合训练。MFed 在所有边缘服务器上传的梯度中混入高斯噪声，并将其上传到云服务器，以便实现多家医院的跨机构全局模型的构建。云服务器将各边缘服务器上传的参数以与样本量比例相关的权重汇总，更新全局模型，然后将聚合后的模型参数分发到各边缘服务器。本地的边缘服务器下载由云服务器下发提供的模型参数，并将其配置为本地模型的初始参数，开始新一轮的本地模型训练。值得注意的是，边缘服务器和云服务器之间的整个交互过程中只传输了加噪声后的模型参数，一方面不会涉及病人的原始临床数据，另一方面还可以防止潜在的隐私攻击，从而实现保护病人的临床数据的目的。算法 1 给出了更详细的描述。

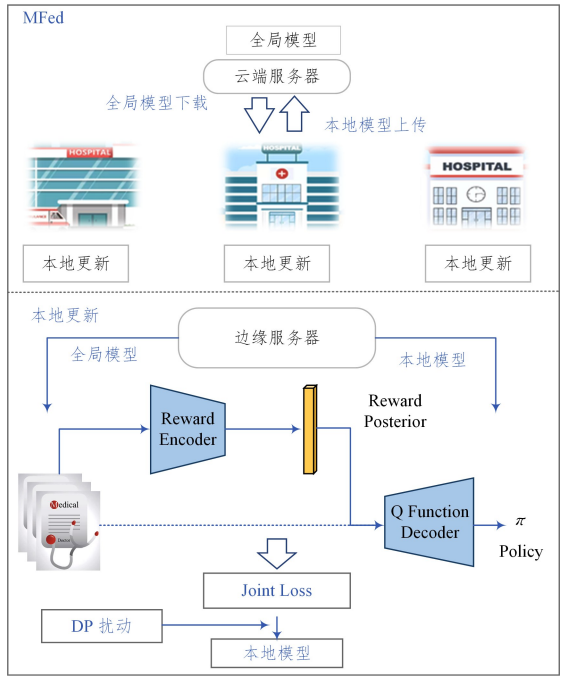


图 3 MFed 整体框架图

Fig. 3 Overall framework of MFed

算法 1 MFed

输入：边缘服务器数量 N，总迭代次数 T，云端服务器学习率 η，γ，初始模型参数 θ_0

输出：最终全局模型 θ

1. 初始化云端模型参数 θ_0
2. for t=0 to T do
3. 云端服务器下发模型参数 θ_0 给边缘服务器
4. for client i∈N in parallel do
5. θ_t^i=本地更新 Local Update (i, θ_t)
6. end for
7. $\overline{\theta_t}=\sum\omega_i\theta_t^i$
8. θ_{t-1}=云端更新 Server Update($\overline{\theta_t}$)
9. end for
10. Return θ

3.2 结合差分隐私的协同策略学习

强化学习(Reinforcement Learning，RL)已经成为解决复杂的贯序决策问题的范式。它是一种目标导向的方法，强调定义的 agent 通过与环境的互动来学习，以实现一个特定的目标，而不需要可模仿的监督信号或对周围环境的完整建模[32]。目前，强化学习的应用已经在各种环境中进行了探索。但实际上，在医疗场景中直接获得与动作相关的反馈通常是具有挑战性的。逆强化学习(Inverse Reinforcement Learning，IRL)是一种从给定的政策或专家示例中反向推导出马尔可夫决策过程(Markov Decision Process，MDP)的奖励函数的方法，允许 agent 通过专家的轨迹示范学习如何对复杂问题进行决策，而这种形式的方法会更贴合于医疗场景的应用[33]。在 MFed 中，我们应用逆强化学习方法来主导边缘服务器上的模型更新。一般来说，RL 解决临床决策

问题需要将整个治疗过程建模为一个 MDP 模型，由元组(S,A,P,R)组成。在我们的任务场景中，它可以被认为是 MDP\PR，这可以解释为由于缺乏对 P 的了解，即无法直接获得潜在的奖励或状态转移函数，不能模拟环境来采样。但是相比 P 和 R 的难以获取，我们很容易获得一些权威的演示数据，例如经验丰富的医生的治疗记录。我们需要完成的就是从这些治疗记录中学习到解释示范动作的奖赏函数和策略模型。首先，我们定义 MDP 模型中的其余两个元素：

1）State：$s_t \in S$ 表示患者在 t 时刻的生理状态。在状态空间设计的过程中，我们将一些可以反应患者状态的生理指标纳入其中。本文模型可以依赖这些指标判断患者是否已经准备好进行拔管的操作以及患者对于镇静剂的药物反应情况。患者在 t 时刻的状态由一组 37 维的向量来表示，包括患者的一些基本信息，如身高、年龄、体重等；同时也有一些由医疗 IoT 设备所采取的生理指标，如心率、呼吸频率、呼吸机潮气量等。这些指标共同构成表征患者状态的矢量。

2）Action：$a_t \in A$ 表示对于患者在 t 时刻状态所做出的医疗干预手段。我们考虑将呼吸机和镇静剂两种现实生活中常常联合使用的医疗干预措施进行联合考虑。我们将动作空间分成两个部分，分别表示呼吸机和镇静剂所对应的状态。具体来说，将呼吸剂开关状态表示为 $a_t[0] \in [0,1]$，将 6 种常用的镇静剂，例如丙泊酚等，映射到相同的剂量量表中，并将其分为 4 个等级，分别表示不同剂量的镇静剂输入。因此，整个动作空间可以表示为：

$$A=\left\{\begin{bmatrix}0\\0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0\\2\end{bmatrix}\begin{bmatrix}0\\3\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1\\2\end{bmatrix}\begin{bmatrix}1\\3\end{bmatrix}\right\}$$

在时刻 t，由患者的状态以及医生的临床操作共同组成治疗的轨迹数据，构成了我们的数据集 $D=\{(s_1^i,a_2^i,s_2^i a_3^i,\cdots,s_\tau^i a_{\tau+1}^i)\}_{i=1}^m$，其中 m 为患者的数量，τ 为该患者的最后治疗时刻。

在边缘服务器上，我们在完成数据预处理后使用逆强化学习算法来训练本地模型，并对模型参数掺入对应隐私预算的高斯噪声，以扰动参数。在我们的任务中，使用 AVRIL[34] 来完成本地端模型的训练。AVRIL 的核心思想是训练两个神经网络，一个是学习复现专家演示中的决策策略，另一个是学习第一个神经网络学到的策略的奖励分布，通过调整奖励函数的分布来使真实策略和所学的 Q 函数之间误差最小。具体来说，AVRIL 定义参数化奖励分布为 r_φ，这里将奖励函数的分布初始化为均值为 0、方差为 1 的高斯分布 $r_\varphi=N(R,\mu,\sigma)$，用于构建优化目标，最小化该分布 r_φ 与奖励函数的后验分布的 Kullback-Leibler（KL）距离，记作：

$$\min_{\varphi} D_{\mathrm{KL}}(r_\varphi(R)\,||\,p(R|D)) \tag{2}$$

但是此时两个分布之间的距离依然很难评估，因为 ELBO（Evidence Lower BOund）中依然包含似然项。

$$F(\phi)=E_{q_\phi}[\log p(D|R)]-D_{\mathrm{KL}}(q_\phi(R)\,\|\,p(R)) \tag{3}$$

AVRIL 根据 Boltzmann 合理性假设，对式(3)进行变换得到：

$$F(\phi)=-D_{\mathrm{KL}}(q_\phi(R)\,\|\,p(R))+E_{q_\varphi}\left[\sum_{(s,a)\in D}\log\frac{\exp(\beta Q_R^{\pi^D}(s,a))}{\sum_{b\in A}\exp(\beta Q_R^{\pi^D}(s,b))}\right] \tag{4}$$

但是对 $Q_R^{\pi^D}$ 进行评估仍存在困难。AVRIL 定义了一个参数为 θ 的 Q 网络，利用变分后验来联合优化 θ,ϕ。AVRIL 利用策略神经网络 Q_θ 来反映与预期奖励所关联的策略。而简单地对两个参数分别进行优化事实上是不可取的，因为学习的策略和奖励分布本身是密切相关的。我们尝试通过相同的优化目标来对两个参数进行约束，特别是策略所表达的隐藏奖励函数和奖励函数分布的后验分布是相近的，AVRIL 获得了一个共同的约束优化目标。

$$\max_{\phi,\theta}\sum_{(s,a)\in D}\log\frac{\exp(\beta Q_\theta(s,a))}{\sum_{b\in A}\exp(\beta Q_\theta(s,b))}-D_{\mathrm{KL}}(q_\phi(R)\,\|\,p(R))$$
$$\text{s.t. } E_{\pi,T}[-\log q_\phi(Q_\theta(s,a)-\gamma Q_\theta(s',a'))]<\epsilon \tag{5}$$

利用拉格朗日乘子法和 KKT 条件重写式(5)，得到由参数 λ 控制约束强度的优化目标：

$$F(\phi,\theta,D)=-D_{\mathrm{KL}}(q_\phi(R)\,\|\,p(R))+\lambda\log q_\phi(Q_\theta(s,a)-\gamma Q_\theta(s',a'))+E_{q_\phi}\left[\sum_{(s,a)\in D}\log\frac{\exp(\beta Q_R^{\pi^D}(s,a))}{\sum_{b\in A}\exp(\beta Q_R^{\pi^D}(s,b))}\right] \tag{6}$$

本文利用式(6)联合训练奖励函数分布参数和策略网络参数。在本地端，各家医院利用本地私有的数据，来完成本地模型的更新。我们将这两个网络的模型参数混入适量的高斯噪声，并上传给云端服务器，这样可以保证在参数传递中，潜在的隐私攻击者无法根据相邻的参数的变化推断出敏感的数据。本地更新算法的整体过程如算法 2 所示。

算法 2 本地更新

输入：数据集 D，状态 S，动作 A，学习率 η，隐私保护级别

输出：奖励变分分布参数 α，策略函数参数 β

1. 初始化参数 α,β
2. while not converged do
3. 从数据集 D 抽取 D_{mini} 参与训练
4. $f(\alpha,\beta,D)=E\left[\frac{n}{\xi}f(\alpha,\beta,D_{\mathrm{mini}})\right]$
5. $(\alpha',\beta')=(\alpha,\beta)+\eta\nabla_{\alpha,\beta}f(\alpha,\beta,D)$
6. $\alpha,\beta\leftarrow\alpha'+\mathcal{N}(0,\sigma^2),\beta'+\mathcal{N}(0,\sigma^2)$
7. end while
8. Return α,β

具体来说，对于边缘服务器和云服务器之间的每一次交互，边缘服务器利用本地端的边缘设备收集临床数据，通过 AVRIL 训练获得本地模型参数，分别表示动作策略和奖励的分布。边缘服务器将这些模型参数依据隐私预算加入高斯噪声并上传到云服务器，云服务器将本地参数以特定的规则进行聚合，这样一方面可以保证原始数据一直保留在各个边缘服务器的本地，而另一方面也保证在参数传递过程中，攻击者无法轻易从这些模型参数中分析出患者的敏感信息。本文使用了一种常见的方法，即聚合参与者的加权损失函数、权重与样本量成正比[8]。最终得到一个模型，其模型参数 $\theta\in\Theta$，使边缘服务器损失函数的加权平均值最小。

$$\min_\theta f(\theta)=\sum_{i=1}^N p_i f_i(\theta) \tag{7}$$

其中，N 是参与该轮迭代的边缘服务器的数量，而每个边缘服务器上又拥有 m_i 条临床数据。因此，总的训练样本数为

$M=\sum_{i=1}^{N} m_i$，则其对应的加权比例为 $p_i=m_i/M$。在全局模型聚合完成以后，云服务器将聚合后的模型参数分发给下轮参与训练的边缘服务器来结束当前轮的交互。

3.3 分布鲁棒优化应用于数据噪声

如前文所述，我们在分布式环境中实现了一个跨机构的呼吸机和镇静剂管理的临床决策工具的开发。然而，在相对保守和严谨的医疗领域应用中，确保策略在不同的边缘服务器上表现良好是至关重要的。因为不同的边缘服务器上存储的本地数据可能是非均匀、不平衡的。另外，我们还考虑了来自不同边缘服务器的数据中存在噪声标签的现象。

MFed 引入了分布鲁棒优化(DRO)，这是一种通用的学习范式，它通过最小化最坏情况下的经验风险，来迫使学到的模型在最坏情况下表现良好，并以协同训练的方式优化噪声标签。在我们的任务中，由于医疗资源分布不均匀，不同规模的医院所收集的数据存在差异。我们很难要求每个边缘服务器上的临床数据是平衡的，但我们却需要保证模型的泛化能力，也就是说，训练后的模型需要适用于每个医院。

受已有工作[35]的启发，将不同的局部损失函数与可学习的权重相结合，并在每次迭代中根据更新的参数将抽样参与者纳入协同更新过程中，使用 DRO 来减轻数据异构造成的影响。

$$\min_{\theta\in\Theta}\max_{\lambda\in\Lambda}=\sum_{i=1}^{N}\lambda_i f_i(\theta) \tag{8}$$

其中，$\lambda\in\Lambda$ 是每个局部损失函数的全局权重。MFed 利用 DRO 并结合协同训练的方式来处理噪声标签，以实现一个适应所有参与训练的边缘服务器的全局模型。我们将通过描述算法的整个流程来说明这两种本地更新方法的区别，具体过程如算法 3 所示。

算法 3 MFed(DRO)

输入：边缘服务器数量 N，总迭代次数 K，本地迭代次数 T，云端服务器学习率 η,γ，初始模型参数 θ_0

输出：最终全局模型 θ_K

1. 初始化云端模型参数 θ_0
2. for k= 0 to K do
3. 云端服务器随机选取时刻 $t\in[0,T]$
4. 云端服务器下发模型参数 θ_0 和时间常数 t
5. for client $i\in N$ in parallel do
6. $\theta_k^i,\theta_t^i=$ Joint Loss Training(i,θ_i,t,j)
7. end for
8. $\overline{\theta}_k=\sum_{i\in N}\omega_i\theta_k^i$
9. $\overline{\theta}_{k,t}=\sum_{i\in N}\omega_i\theta_t^i$
10. 云服务器发送 $\overline{\theta}_{k,t}$ 给所有边缘服务器
11. 接收各边缘服务器返回的 $f_i(\overline{\theta}_{k,t},\xi)$
12. 判断存在噪声数据源，并标记噪声 ID j
13. end for
14. Return θ_K

与传统的联邦学习一样，我们从云服务器初始化模型，并将模型参数分发到每个边缘服务器。然而，MFed 除了模型参数外，还特别广播了一个随机时间点 $t\in T$，其中 T 表示本地模型训练的迭代次数。边缘服务器将云服务器提供的模型参数设置为本地初始模型，并根据医疗物联网设备收集的本地数据利用 AVRIL 进行模型优化。但此时，我们不仅要保留本地训练结束时的模型，还要保留时间点 t 的模型参数。边缘服务器将它们都上传到云服务器。与以前的工作相比，MFed 在云服务器和边缘服务器之间引入了一个额外的交互。MFed 在云端汇总每个边缘服务器在时间 t 的参数后，再次将其下发给边缘服务器，边缘服务器根据时间 t 的聚合模型来评估本地数据质量并将损失值传送给云服务器。云服务器根据损失值来确定数据质量更差、存在噪声的边缘服务器，并对该边缘服务器进行标记。为了保证整个过程中数据的安全性，我们对每一次的参数传递都加上指定隐私预算的高斯噪声，以减小潜在的信息安全的风险。

MFed 对标记噪声的客户端采用了不同的本地更新方法，以减轻对全局模型的负面影响。边缘服务器本地更新过程类似于文献[29]，即同时训练两个网络，共同计算两个模型的损失，并同步更新模型。通常来说，默认不同的模型通常会在大多数拥有正确标签的样本上达成一致，而不太可能在错误标签上达成一致。具体来说，如图 4 所示，被标记的服务器首先设置两个结构相同的模型，并为每个模型分配不同的初始状态。其中一个是来自云端所共享的模型参数，另一个参数是该边缘服务器在上一轮本地训练完成后所得到的模型。我们类似构建伪孪生网络结构来更新两个模型，也就是说，它们有不同的初始参数，但同时会被一个协同损失函数所更新。而这个协同损失除了包括现有的本地更新方法的损失，也附加了 Co-Regularization 带来的损失。然后本文根据这个协同损失函数选择损失值相对较小的样本来更新模型。

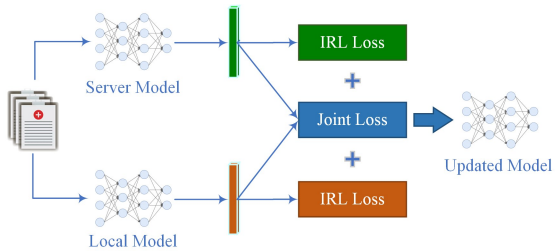


图 4 协同损失训练示意图

Fig. 4 Schematic of joint loss training

我们将这个协同损失函数定义为：

$$\mathcal{L}(\xi)=\mathcal{L}_{\text{IRL}}(\xi)+\mathcal{L}_{\text{Co-Reg}}(\xi) \tag{9}$$

其中，ξ 表示输入临床数据样本，$\mathcal{L}_{\text{IRL}}$ 表示由边缘服务器本地更新过程中产生的损失值，而 $\mathcal{L}_{\text{Co-Reg}}$ 表示协同正则化网络的两个预测分布的对比损失。Co-Regularization 有助于模型选择具有正确标签的数据参与模型训练，因为较小的协同损失意味着两个网络在预测上达成了一致。在本文的工作中，我们用 Kullback-Leibler Divergence 来量化两个预测分布之间的差异，具体如下：

$$\mathcal{L}_{\text{Co-Reg}}=D_{\text{KL}}(P_1\parallel P_2)+D_{\text{KL}}(P_2\parallel P_1) \tag{10}$$

其中，P_1 和 P_2 分别表示两个模型对相同输入所提供的预测分布。更详细的本地协同损失更新过程如算法 4 所示。

算法 4 Joint Loss Training

输入：初始模型参数 θ，边缘服务器 ID i，噪声标记 ID j，时间常数 t

输出：最终模型 θ_k^i 和 θ_t^i

1. if client ID i==noisy client ID j then
2. 初始化本地模型参数 1：$\theta^{i}_{server}=\theta_0$
3. 初始化本地模型参数 2：$\theta^{i}_{local,0}=\theta_{local,0}$
4. Fetch mini-batch ξ from dataset D
5. $P_1=f(\theta^{i}_{0},\xi)$
6. $P_2=f(\theta^{i}_{local,0},\xi)$
7. 利用 P_1 和 P_2 计算协同损失
8. 获得协同损失较小的样本数据 $\tilde{\xi}$
9. $L=\frac{1}{D}\sum_{\xi\in}l(\tilde{\xi})$
10. $\theta_{server}=\theta_{server}-\eta\nabla L$，$\theta_{local}=\theta_{local}-\eta\nabla L$
11. end if

3.4 时间复杂度分析

本节分析算法 MFed 的时间复杂度，MFed 方法主要由云端服务器端的全局模型更新算法和本地医院利用私有数据对本地模型进行更新的算法相组合，其中本地端的算法嵌套在云端服务器的全局更新算法中。我们定义云端服务器共完成云端和服务器端的通信次数为 T，参与方的数量为 N。在每次迭代时，本地端的时间复杂度为 $O(\log(N))$，则 MFed 的时间复杂度等于云端服务器的时间复杂度，为 $O(T\log(N))$。

4 实验设置与结果

本章将介绍本文实验的具体细节和实验设置，包括任务设置、数据集、数据预处理、基准、度量标准和参数设置，并给出实验结果。

4.1 实验设置

4.1.1 任务设定

假设共有 8 家医院的边缘服务器加入模型训练过程。8 家医院的边缘服务器不断从本地边缘物联网设备获取数据，用于实时监测病人，并根据这些数据完成本地模型的训练。同时，我们配置了一个云服务器，可以在整个过程中与每个边缘服务器进行通信，并充分结合每个边缘服务器的医疗数据资源，最终得到一个全局模型。

4.1.2 数据集

本文的数据来源主要分为国外重症监护数据库(MIMIC-III)数据集和国内 ICU 自采数据集。

1)MIMIC-III 数据库包含 2001 年至 2012 年 11 年间近 6 万份 ICU 住院病人的记录[36]。MIMIC-III 数据库主要有两类基础数据：一类是从 EHR 中提取的临床数据，包括患者人口学特征信息、诊断信息、实验室检查信息、医学影像信息等；另一类是床旁监护设备采集的时间序列数据和相关生命体征参数及事件记录。

2)国内数据集主要是我们从中国科学技术大学第一附属医院 ICU 中采集到的 50 位患者的数据，其中包含患者的基础体征信息和医疗设备的实时监测数据。

4.1.3 数据预处理

为了满足我们的任务需求，我们从数据库中筛选出通气时间超过 24 h 的患者，这是为了确保这些患者不是因为术后的正常过渡而需要呼吸机的介入。同时，我们还滤除了最终没有成功出院的患者，以排除那些和通气时间以及镇静剂量关联不大的死亡患者，也就是说，即使拥有更好的呼吸机或者镇静剂管理策略也不大可能对这类病人带来积极的影响。

最终，我们从 MIMIC III 数据库中的 ICU 入院病例中，提取了患者的生理数据以及医生的治疗手段记录。在过滤掉一些可能影响模型训练的样本后，我们插入生命体征测量的缺失值，来获得以 1h 为间隔的临床数据。经过一系列的数据处理，我们最终得到了 3 545 名患者每小时的临床数据，共 328 279 条轨迹。图 5 给出了几个相关生命体征随时间变化的曲线。我们将数据集按照病人为单位划分为训练集和测试集。数据准备完成后，在训练集中有 2 836 个病人，包括 260 559 个轨迹数据，在测试集中有 709 个病人，包括 67 720 个临床数据。

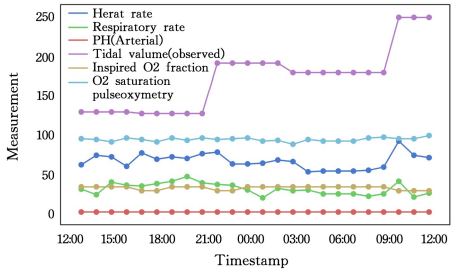


图 5 病人的生命体征随时间变化的曲线

Fig. 5 Typical patient timeline

同样，我们将从国内医院采集到 50 位病人共计 1 771 条的原始数据通过上述的数据预处理后，获得国内医院的数据，共计 4 139 条轨迹数据。我们将这些数据设定为单独的测试集来评估模型的性能。

最后，我们再将训练集按病人为单位分成 8 个子集，表示存储在 8 个边缘服务器上的临床数据，即每个医院所持有的病人数据。

4.1.4 基准方法

我们通过比较 MFed 和其他现有的方法的表现来评估方法的优劣。

1)Fitted Q Iteration(FQI)[37]是一种离线批量强化学习算法，利用极端随机树拟合 Q 函数。该方法已经被应用于相同的任务，在集中式数据集上为管理呼吸机和镇静剂的使用而开发的临床决策工具[30]。

2)AVRIL[32]。其是 MFed 中边缘服务器所利用的逆强化学习算法，通过学习奖励的近似后验分布，从复杂的状态空间中寻求适当的政策。我们在一个集中式数据集上测试 AVRIL，并观察其结果。

3)Fed-NFQI。其是一个联邦学习和 Neural Fitted Q Iteration(NFQI)的组合，通过局部更新和全局聚合不断优化政策，在整个通信过程中传递政策模型，而不分享本地的数据[38]。在现有的工作中，NFQI 已经在一个集中的数据集上实现一个相近的任务[30]。我们将其与联邦学习相结合[8]，并观察实验的输出。奖励函数是依据 Prasad 等[30]的工作中提到的方案而设计的，对长时间插管、二次插管、病人体征的急剧变化、超过自然阈值等情况进行惩罚。

4)MFed w/o DRO。其是 MFed 没有 DRO 模块的联邦学习方法，简单地将每个本地边缘服务器的数据关联起来，

建立一个决策工具，而不考虑数据噪声和数据分布偏移带来的不利影响。

4.1.5 衡量指标

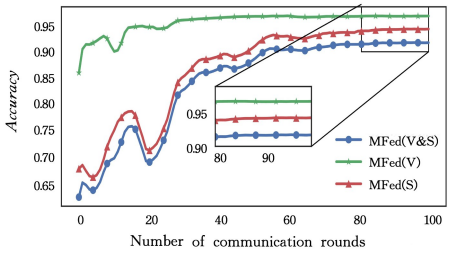
我们根据两个指标来考察模型的性能。第一个指标定义为准确性，即当模型预测的动作与医生的动作一致时，则认为该策略是正确的。而准确率又有3个方面：呼吸机准确率、镇静剂准确率和两者联合的准确率，其中我们把联合准确率作为评价模型最重要的标准。另外，我们把模型到达指定准确率需要边缘服务器和云服务器交流的轮数作为第二个指标。

4.1.6 参数设定

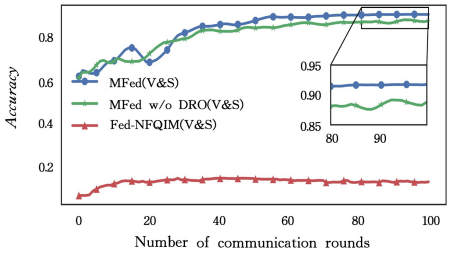
我们将云服务器和边缘服务器之间的通信次数设定为100，每两个通信间隔，本地模型迭代3000次。云服务器使用学习率为10^{-2}的Adam优化器，本地边缘服务器使用64个神经元的3层MLP网络结构，并使用学习率为10^{-4}的SGD优化器训练。模型参数开始时在云端服务器被随机初始化，并被发送到边缘服务器。

4.2 实验结果

MFed的性能表现如图6所示。图6(a)给出了MFed随着云端和本地的交互回合数的增加而不断提升的预测准确率。我们发现，MFed的最终准确率达到不错的程度且3项指标都有着较高的准确率，其中呼吸机管理的准确率为96.76%，镇静剂准确率为94.31%，联合动作的准确率为91.75%。然后尝试将MFed与其他两个联邦学习的方案进行分布式场景下的比较。图6(b)给出了3种方法在联合动作准确性方面的差异，即MFed，MFed w/o DRO和Fed-NFQI。与Fed-NFQI相比，MFed对通气、镇静剂和联合动作的准确性有了大幅度的提升。需要注意的是，第一个呈现的数据点已经代表第一轮训练后的表现。我们进一步观察MFed和MFed w/o DRO，MFed的表现相对来说都更加优异，3项指标都有了一定程度的提升，也证明DRO机制的设置对噪声处理有着积极的影响。



(a) MFed在呼吸机、镇静剂以及联合动作上的预测准确率



(b) MFed，MFed w/o DRO和Fed-NFQI在联合动作上的准确率对比

图6 MFed在MIMIC-III数据集上的性能表现

Fig. 6 Performance of MFed in MIMIC-III

本文综合考察了MFed与Fed-NFQI、MFed w/o DRO以及另外两种集中数据集上的方法FQI和AVRIL的准确率，具体如表1所列。其中FQI是Prasad等所尝试的相同任务，且处于集中式的设计中。与FQI相比，MFed针对任意指标都具有优势，呼吸机准确率提高了11.76%，镇静剂准确率提高了36.31%，联合动作准确率提高了36.75%。理论上来说，由于分布式环境的局限性，联邦学习算法的性能相比集中数据集上的性能通常会更差，这是不同机构间的数据壁垒造成的必然结果。而令人惊讶的是，虽然MFed的最终准确率比最先进的集中数据集上的方法AVRIL有所下降，但它在呼吸机的准确率方面甚至超过了AVRIL。

表1 MFed和其他方法准确率的对比

Table 1 Accuracy comparison of MFed and other methods

(单位：%)

Dataset	Method	V	S	$V\&S$
MIMIC-III	FQI	85.00	58.00	55.00
	AVRIL	96.38	96.71	93.43
	Fed-NFQI	71.89	16.89	14.38
	MFed w/o DRO	96.21	91.69	89.16
	MFed	96.76	94.31	91.75
国内数据集	Fed-NFQI	74.72	31.55	29.86
	MFed w/o DRO	97.79	80.26	79.36
	MFed	97.70	80.98	79.87

我们在国内的测试集上同样对3种联邦学习方法做了性能的评估，如图7所示。不难看出，Fed-NFQI的表现依旧没有MFed和MFed w/o DRO优异，而这两种方法的性能也非常接近，但相比在国外的数据集上两个模型在联合动作上的表现还是逊色了不少，但呼吸机的准确率却出乎意料的有所提升，结果如表1所列。原因可能是国内数据集目前的数据量依然不太乐观，作为测试集可能因为大小或分布偏移等因素而对模型性能的评估不稳定。而该数据采集也是我们一直在持续进行的。

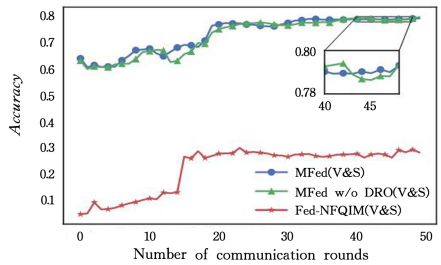


图7 MFed和其他方法在国内数据集上的表现

Fig. 7 Performance of MFed and other methods on domestic datasets

此外，我们还比较了MFed和其他两种联邦学习方法在收敛速度方面的差异，如表2所列。由于Fed-NFQI的最终准确率太低，我们将MFed w/o DRO的收敛至85%的联合动作准确率作为目标准确率基线，然后观察达到目标准确率所需的通信轮数。从表2中可以看出，与MFed w/o DRO相比，MFed达到目标准确率时减少了27.66%的轮次，可以更快收敛。总体来说，MFed在准确度方面明显优于其他联邦学习方法，而且与集中数据集上所应用的方法相比也很有竞争力。

表 2 MFed 和其他方法的收敛速度的对比

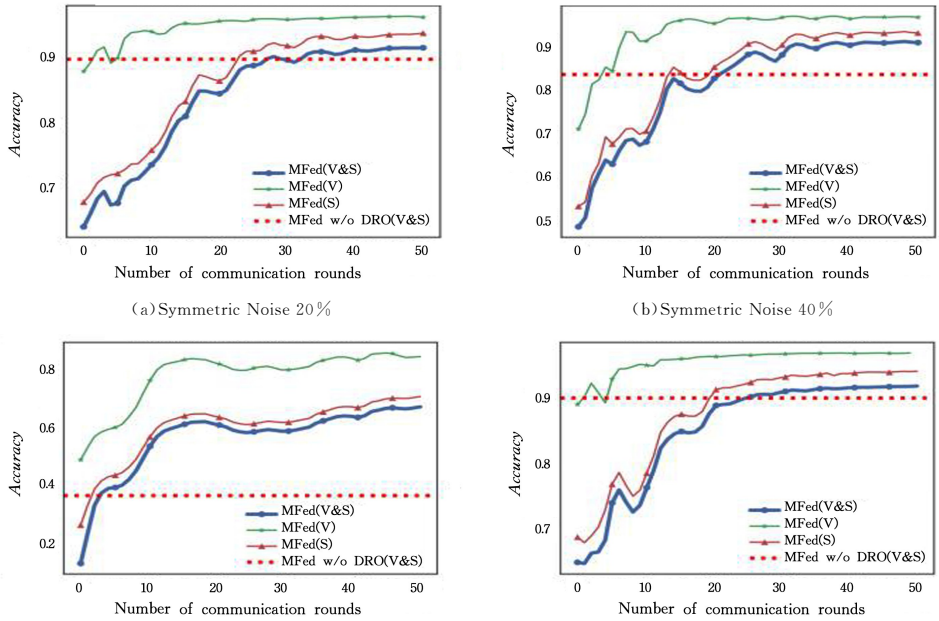
Table 2 Comparison of MFed and other methods in rounds to target accuracy

	Rounds to target accuracy	Improvement/%
Fed-NFQI	Can't reach	Not applicable
MFed w/o DRO	47	0
MFed	**34**	**27.66**

本文进一步验证了 MFed 克服噪声数据和数据分布偏移的能力。在数据噪声的情况下，我们重点观察 MFed 在不同噪声水平下的表现，以验证 MFed 可以缓解数据噪声带来的消极影响。为了验证 MFed 克服数据分布偏移的表现，我们主要验证 3 种算法在最差分布下的性能，以观察该模型对不同边缘服务器的适用性。

4.2.1 数据噪声

首先，我们翻转标签以掺入人为创造的噪声标签，并验证 MFed 在不同噪声情况下的工作。我们根据标签翻转的不同将噪声标签分为两类，即对称噪声标签和非对称噪声标签。对称噪音标签指呼吸机或镇静的当前动作被改为其相反的动作，例如插管被改为拔管。非对称性翻转指将选定的动作随机修改为任何其他动作。我们根据翻转的标签数量占总样本数的百分比来定义噪音水平。我们评估了 MFed 和 MFed w/o DRO 在对称噪声标签以及非对称噪声标签等 4 种不同噪声环境中的差异，如图 8 所示。MFed 在不同的噪声水平下表现强大。用联合动作作为主要衡量标准，以 MFed w/o DRO 在相同噪声条件下的最终准确率为基线，可以更清楚地看到这两种算法的差距随着噪声水平的提高而逐渐扩大。当数据中少于 40% 的标签被翻转时，MFed 的性能都不错，各项指标的准确性均可以达到较高的水平，MFed 受噪声影响的程度有限。



(a) Symmetric Noise 20%　(b) Symmetric Noise 40%

(c) Symmetric Noise 50%　(d) Asymmetric Noise 20%

图 8 MFed 在不同噪声环境下的表现

Fig. 8 Comparison of MFed performance at different noise levels

当噪声水平增加到 50% 时，MFed 的性能有了明显的下降，而尽管如此，准确率仍然可以保持在 67.13%，与基线相比优势依然很明显。

为了进一步证实 MFed 的抗噪声能力主要源于 DRO 模块的设计，我们详细记录了 MFed 和 MFed w/o DRO 在几种噪声环境下的性能表现，结果如表 3 所列。很明显，MFed 比 MFed w/o DRO 更优，而且随着噪声水平的增加，这种优势变得更加明显。在有 20% 对称噪声和 20% 不对称噪声的数据集上相比在有 40% 翻转标签的数据集上，MFed 比 MFed w/o DRO 两种方法的优势差异提升了接近 5%。当把标签翻转到 50% 时，MFed 的性能更是提升了 30.45%。而值得注意的是，对于原始数据，可能存在一些未知的数据噪声分布，DRO 的效果也同样被证明。因此，MFed 可以减轻边缘服务器上的数据中存在的噪声对模型训练的不利影响。

表 3 MFed 和 MFed w/o DRO 在不同噪声环境下的表现

Table 3 Terminal accuracy of MFed and MFed w/o DRO at different noise levels

(单位：%)

Noise Level	Method	*V*	*S*	*V*&*S*
Symmetric 20%	MFed w/o DRO	96.32	92.48	90.18
	MFed	97.09	94.19	92.01
Symmetric 40%	MFed w/o DRO	90.75	85.53	83.3
	MFed	96.47	93.05	90.82
Symmetric 50%	MFed w/o DRO	53.89	40.05	36.68
	MFed	84.41	70.69	67.13
Asymmetric 20%	MFed w/o DRO	96.56	92.59	89.96
	MFed	96.83	94.06	91.83
Original Data	MFed w/o DRO	96.21	91.69	89.16
	MFed	96.76	94.31	91.75

4.2.2 数据分布偏移

为了验证最终训练的模型在最坏数据分布情况下仍然表现良好，我们为每个边缘服务器保留一部分数据并将其作为

测试集，也就是不同的边缘服务器有不同的测试数据分布。我们使用每个边缘服务器持有的测试数据来评估最终得到的全局模型，以得出模型在联合动作方面的准确性，而这与模型的泛化和适用性密切相关。我们将观察 MFed 和其他联合解决方案在不同噪声环境下的表现。图 9 给出了 3 种算法在最差分布上的表现。非常明显的是，在数据分布最差的边缘服务器上，MFed 始终优于 MFed w/o DRO 和 Fed-NFQI，而且这种改进随着训练数据中的噪声标签的增加而提升。这也证明了 MFed 在每次迭代中 DRO 的设计选择性地将较差的边缘服务器数据加入协同损失训练的有效性。

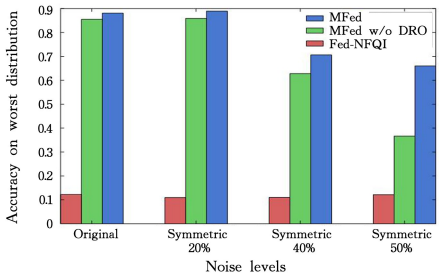


图 9 MFed 与其他方法在最差分布上的准确率表现

Fig. 9 Accuracy of MFed and benchmarks on the worst distribution

结束语 本文提出了 MFed，一个基于差分隐私的联邦学习能够实现呼吸机和镇静剂智能管理的医疗决策工具。它可以根据病人的体征状况，及时提供治疗干预建议。MFed 充分利用了 ICU 中各种传感器所采集的数据，并利用差分隐私的机制来进一步提升数据的隐私性。此外，为了解决医疗数据中的数据分布偏移和噪声问题，我们使用 DRO 来确保模型在所有参与训练的边缘服务器上表现良好，这使得在每次迭代中选择参与的边缘服务器的问题转化为最小最大化问题，并且我们利用协同损失训练来消除噪声标签的负面影响。实验结果表明，与 MFed w/o DRO 相比，MFed 具有更好的抗噪声能力，并且在最差的数据分布上优于其他解决方案。

本文方法适用于跨医疗机构的协同训练公用的临床决策工具并保证数据隐私性。但相比传统的联邦学习的本地端通信资源有限且用户量较大的设定，MFed 的适用范围不同。现实生活中，多个医疗机构协作训练的横向联邦学习框架通常对网络通信资源并没有明确的限制，因为相比其他类似于移动客户端或者通信节点的资源受限，医疗机构级别的边缘服务器与云端服务器通信的过程相对稳定。而 MFed 单次传输的模型大小仅为 0.088616 MB，这同样减小了通信压力，提升了通信效率。

未来值得尝试的方向包括，MFed 采用的差分隐私虽然可以保护参数传递过程中的隐私性，但同样噪声的加入会让模型的性能受到干扰。因此将更先进的加密技术应用于联邦学习的训练框架，以进一步权衡数据隐私和模型性能之间的关系是值得尝试的。此外，医疗场景下，数据中的异常标签也可能恰好是病人的特殊状态，纯粹的过滤可能会对模型的性能和对极端情况的泛化有不利影响。因此，加入更适度的噪声处理方法也是一个值得尝试的方向。

参 考 文 献

[1] DELL TECHNOLOGIES. Dell emc global data protection index survey[EB/OL]. [2022-08-10]. https://www.dellemc.com/en-us/data-protection/gdpi/index.htm.

[2] HUESCH M D, MOSHER T J. Using it or losing it? the case for data scientists inside health care[J/OL]. Nejm Catalyst, 2017, 3(3). https://catalyst.nejm.org/doi/full/10.1056/CAT.17.0493.

[3] RAZA M, AWAIS M, SINGH N, et al. Intelligent iot framework for indoor healthcare monitoring of parkinson's disease patient [J]. IEEE Journal on Selected Areas in Communications, 2020, 39(2): 593-602.

[4] CONTI G, MANTZ J, LONGROIS D, et al. Sedation and weaning from mechanical ventilation: time for 'best practice' to catch up with new realities? [J]. Multidisciplinary Respiratory Medicine, 2014, 9(1): 1-5.

[5] AMBROSINO N, GABBRIELLI L. The difficult-to-wean patien [J]. Expert Review of Respiratory Medicine, 2010, 4(5): 685-692

[6] PATEL S B, KRESS J P. Sedation and analgesia in the mechanically ventilated patient[J]. American Journal of Respiratory and Critical Care Medicine, 2012, 185(5): 486-497.

[7] ZHANG Y, HE D, OBAIDAT M S, et al. Efficient identity-based distributed decryption scheme for electronic personal health record sharing system[J]. IEEE Journal on Selected Areas in Communications, 2020, 39(2): 384-395.

[8] WANG J Z, KONG L W, HUANG Z C, et al. Research progress on privacy protection in federated learning [J]. Big Data, 2021, 7(3): 130-149.

[9] 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.

[10] ZHANG D Y, KOU Z, WANG D. Fedsens: A federated learning approach for smart health sensing with class imbalance in resource constrained edgecomputing[C]// IEEE INFOCOM 2021—IEEE Conference on Computer Communications. IEEE, 2021: 1-10.

[11] ELAYAN H, ALOQAILY M, GUIZANI M. Sustainability of healthcare data analysis IoT-based systems using deep federated learning[J]. IEEE Internet of Things Journal, 2021, 9(10): 7338-7346.

[12] YAN Z, WICAKSANA J, WANG Z, et al. Variation-aware federated learning with multi-source decentralized medical image data[J]. IEEE Journal of Biomedical and Health Informatics, 2020, 25(7): 2615-2628.

[13] SHELLER M J, REINA G A, EDWARDS B, et al. Multiinstitutional deep learning modeling w/o sharing patient data: A feasibility study on brain tumor segmentation[J]. MICCAI Brainlesion Workshop, 2019: 92-104.

[14] 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.

[15] GUO P,WANG P,ZHOU J,et al. Multi-institutional collaborations for improving deep learning-based magnetic resonance image reconstruction using federated learning[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2021:2423-2432.

[16] MALEKZADEH M,HASIRCIOGLU B,MITAL N,et al. Dopamine:Differentially private federated learning on medical data [J]. arXiv:2101. 11693,2021.

[17] LU S,ZHANG Y,WANG Y,et al. Learn electronic health records by fully decentralized federated learning[J]. arXiv:1912. 01792,2019.

[18] WU Q,CHEN X,ZHOU Z,et al. Fedhome:Cloud-edge based personalized federated learning for in-home health monitoring [J]. IEEE Transactions on Mobile Computing, 2020, 21(8): 2818-2832.

[19] XU X,PENG H,SUN L,et al. Fedmood:Federated learning on mobile health data for mood detection[J]. arXiv:2102. 09342, 2021.

[20] TAN X,CHANG C C H,TANG L. A tree-based federated learning approach for personalized treatment effect estimation from heterogeneous data sources[C]// International Conference on Machine Learning. PMLR,2022:21013-21036.

[21] ELAYAN H,ALOQAILY M,GUIZANI M. Deep federated learning for iot-based decentralized healthcare systems[C]// 2021 International Wireless Communications and Mobile Computing(IWCMC). IEEE,2021:105-109.

[22] LIU Y X,CHEN H,LIU Y H,et al. Privacy-Preserving Technologies in Federated Learning [J]. Journal of Software,2022, 33(3):1057-1092.

[23] YANG G,WANG Z S. Research progress of privacy protection in federated learning[J]. Journal of Nanjing University of Posts and Telecommunications(Natural Science Edition), 2020, 40(5):204-214.

[24] INAN A,GURSOY M E,SAYGIN Y. Sensitivity analysis for non-interactive differential privacy: bounds and efficient algorithms[J]. IEEE Transactions on Dependable and Secure Computing,2017,17(1):194-207.

[25] CHOUDHURY O,GKOULALAS-DIVANIS A,SALONIDIS T,et al. Differential privacy-enabled federated learning for sensitive health data[J]. arXiv:1910. 02578,2019.

[26] ADNAN M,KALRA S,CRESSWELL J C,et al. Federated learning and differential privacy for medical image analysis[J]. Scientific Reports,2022,12(1):1-10.

[27] LEE C,LUO Z,NGIAM K Y,et al. Big healthcare data analytics:Challenges and applications[M]// Handbook of Large-scale Distributed Computing in Smart Healthcare. 2017:11-41.

[28] HAN B,YAO Q,YU X,et al. Co-teaching:Robust training of deep neural networks with extremely noisy labels[J]. Advances in Neural Information Processing Systems,2018,31:8535-8545.

[29] WEI H,FENG L,CHEN X,et al. Combating noisy labels by agreement:A joint training method with co-regularization [C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020:13726-13735.

[30] PRASAD N,CHENG L F,CHIVERS C,et al. A reinforcement learning approach to weaning of mechanical ventilation in intensive care units[J]. arXiv:1704. 06300,2017.

[31] YU C,LIU J,ZHAO H. Inverse reinforcement learning for intelligent mechanical ventilation and sedative dosing in intensive care units[J]. BMC Medical Informatics and Decision Making, 2019,19(2):111-120.

[32] SUTTON R S,BARTO A G. Reinforcement learning:An introduction[M]. MIT Press,2018.

[33] NG A Y,RUSSELL S. Algorithms for inverse reinforcement learning[C]// ICML. 2000,1:2.

[34] CHAN J,VAN DER SCHAAR M. Scalable bayesian inverse reinforcement learning[J]. arXiv:2102. 06483,2021.

[35] DENG Y,KAMANI M M,MAHDAVI M. Distributionally robust federated averaging[J]. Advances in Neural Information Processing Systems,2020,33:15111-15122.

[36] JOHNSON E,POLLARD T J,SHEN L,et al. Mimic-iii,a freely accessible critical care database[J]. Scientific Data,2016,3(1): 1-9.

[37] ERNST D,STAN G B,GONCALVES J,et al. Clinical data based optimal sti strategies for hiv:a reinforcement learning approach[C]// Proceedings of the 45th IEEE Conference on Decision and Control. IEEE,2006:667-672.

[38] RIEDMILLER M. Neural fitted q iteration-first experiences with a data efficient neural reinforcement learning method [C]// European Conference on Machine Learning. 2005: 317-328.

CAO Linxiao, born in 2000, postgraduate. His main research interests include federated learning and reinforcement learning.

ZHOU Haoquan, born in 1968, master, chief physician. His main research interests include childhood respiratory disease, bronchoscopy, and smart healthcare.

(责任编辑:喻藜)