基于隐私保护的联邦推荐算法综述

张洪磊[1] 李浥东[1] 邬俊[1] 陈乃月[1] 董海荣[2]

摘 要 推荐系统通过集中式的存储与训练用户对物品的海量行为信息以及内容特征, 旨在为用户提供个性化的信息服务与决策支持. 然而, 海量数据背后存在大量的用户个人信息以及敏感数据, 因此如何在保证用户隐私与数据安全的前提下分析用户行为模式成为了近年来研究的热点. 联邦学习作为新兴的隐私保护范式, 能够协调多个参与方通过模型参数或者梯度等信息共同学习无损的全局共享模型, 同时保证所有的原始数据保存在用户的终端设备, 较之于传统的集中式存储与训练模式, 实现了从根源上保护用户隐私的目的, 因此得到了众多推荐系统领域研究学者们的广泛关注. 基于此, 对近年来基于联邦学习范式的隐私保护推荐算法进行全面综述、系统分类与深度分析. 具体的, 首先综述经典的推荐算法以及所面临的问题, 然后介绍基于隐私保护的推荐系统与目前存在的挑战, 随后从多个维度综述结合联邦学习技术的推荐算法, 最后对该方向做出系统性的总结并对未来研究方向与发展趋势进行展望.

关键词 推荐系统, 联邦学习, 隐私保护, 协同过滤

引用格式 张洪磊, 李浥东, 邬俊, 陈乃月, 董海荣. 基于隐私保护的联邦推荐算法综述. 自动化学报, 2022, **48**(9): 2142−2163

DOI 10.16383/j.aas.c211189

A Survey on Privacy-preserving Federated Recommender Systems

ZHANG Hong-Lei[1] LI Yi-Dong[1] WU Jun[1] CHEN Nai-Yue[1] DONG Hai-Rong[2]

Abstract Recommender systems aim to provide users with personalized information services and decision support, by mining the centrally stored historical behaviors of users on items and their inherent attributes. However, there is numerous users′sensitive information behind the massive data, therefore, how to mine users′behavior patterns on the premise of ensuring users′privacy and data security has become a hotspot. As an emerging privacy-preserving paradigm, federated learning can coordinate multiple participants to jointly train a lossless global shared model by transmitting model parameters or gradients, and ensure that all original data are saved in the local terminal devices, compared with the traditional centralized storage and training mode. Therefore, it has been widely concerned by many researchers in the field of recommender systems. Based on this, the paper will provide a comprehensive survey, systematic taxonomy, and in-depth analysis of federated recommender systems. Specifically, we first summarize the classical recommendation algorithms and potential problems; then introduce the taxonomy and current challenges on privacy-preserving recommendation methods, and then summarize the privacy-preserving federated recommendation models from multiple dimensions. Finally, we conclude this paper and discuss possible research directions in this area.

Key words Recommender systems, federated learning, privacy protection, collaborative filtering

Citation Zhang Hong-Lei, Li Yi-Dong, Wu Jun, Chen Nai-Yue, Dong Hai-Rong. A survey on privacy-preserving federated recommender systems. *Acta Automatica Sinica*, 2022, **48**(9): 2142−2163

随着移动互联网络的飞速发展, 人们所持有的用户设备逐渐多元化, 进而使得用户能够越来越便捷上传所生成的内容数据, 因此海量用户行为与内容数据由此产生. 另外, 随着计算机硬件与人工智能技术的持续进步, 出色的计算能力与大规模算法模型也为海量数据的产生与处理提供了先决条件. 然而, 互联网产生数据的速度远远超过用户所能处理数据的速度, 以至于造成用户不能及时运用有效信息的情况, 这就产生了信息生产者与内容消费者之间的尖锐矛盾, 最终导致信息过载现象的发生[1].

推荐系统作为缓解信息过载问题的有效途径[2], 其通过利用用户与物品的历史交互数据以及各自固有的内容属性特征进行个性化建模以此实现对于用户未来可能感兴趣的物品进行精准预测的功能, 因而该技术得到了许多学者们的广泛关注[3]. 并且由

收稿日期 2021-12-13 录用日期 2022-06-23
Manuscript received December 13, 2021; accepted June 23, 2022
国家自然科学基金 (U1934220) 资助
Supported by National Natural Science Foundation of China (U1934220)
本文责任编委 张敏灵
Recommended by Associate Editor ZHANG Min-Ling
1. 北京交通大学计算机与信息技术学院 北京 100044 2. 北京交通大学轨道交通控制与安全国家重点实验室 北京 100044
1. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044 2. State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044

于其巨大的商业价值, 推荐算法也在工业界在线平台上 (比如社交[4]、新闻[5]、购物[6] 等) 成为了必不可少的重要组件. 推荐系统根据其推荐原理以及所利用具体数据的不同, 可进一步划分为利用属性信息的基于内容的方法[7]、利用用户对物品历史行为信息的协同过滤方法[8] 以及利用多种信息源的混合推荐方法. 近年来, 由于深度学习出色的表示能力, 基于深度学习的推荐算法[9] 能够高效利用海量训练样本, 并且能够有效整合多种附加信息 (比如社交信息[10]、文本信息[11]、图像信息[12] 等), 以此缓解推荐系统固有的数据稀疏与冷启动问题[13].

然而, 融合用户大量个人信息固然可以提升推荐算法的预测精度, 但往往会对用户的隐私和数据安全问题产生担忧. 具体地, 文献 [14−16] 表明仅利用用户所产生的内容数据或者历史行为信息可以反推出用户的敏感属性特征, 另外引入社交网络等附加信息可以实现更低成本的隐私泄露. 由于海量信息中不可避免的存在用户个人数据以及敏感信息, 因此平台需要收集更多的训练数据以提升推荐性能与用户为保护隐私而尽可能少的共享个人数据间的矛盾逐渐凸显. 另外, 随着中国对于数据安全与隐私问题越来越重视, 因此, 如何在保证用户隐私和安全的前提下有效融合更多数据以提升推荐性能成为了数据挖掘领域关注的重点. 所以, 基于隐私保护的推荐算法逐渐得到大家的广泛关注[17−19].

传统的隐私保护推荐算法主要采用差分隐私等机制添加数据扰动[20] 或者利用加密的方式 (比如同态加密[21] 与安全多方计算[22] 等) 实现对于个人敏感信息的隐私保护. 然而添加扰动的方法需要严格的数学假设并且不可避免的对原始数据引入偏差, 而加密的方式虽然能够实现对于原始数据的无损保护, 但加密操作往往需要更大的计算量最终使得模型的实时性大打折扣. 值得一提的是, 上述传统隐私保护推荐算法需要将个人数据收集到中心服务端进行存储与训练, 因此在原始数据传输等过程中仍然存在隐私泄露与安全威胁的问题. 另外, 由于上述隐私与安全问题的担忧造成了多参与方不能安全高效的进行数据共享, 最终导致数据孤岛现象进而影响整体模型的预测性能.

得益于近年来分布式学习与边缘计算的飞速发展, 以及互联网生态逐渐移动化与开放化, 使得用户终端设备有能力存储并训练相当容量的数据. 联邦学习[23] 充分发挥终端设备的计算能力并协同服务端联合优化全局模型, 同时能够使得原始数据保留在本地而较好地保护用户隐私信息, 这一新兴的隐私保护范式逐渐得到大家的认可[24]. 另外, 由于推荐系统的数据来源存在天然的分布式特性, 以及用户对于推荐服务严苛的实时性要求, 因此近年来端云架构下结合联邦学习的推荐算法取得了较大的进展[25−32]. 然而, 目前国内相关文献缺乏对于此研究方向的细致梳理与归纳总结. 基于以上动机, 本文对联邦学习赋能的推荐系统进行了全面综述, 细致整理了近 3 年发表在相关领域会议和期刊中此方向的文献, 旨在为该领域梳理出一条清晰的研究脉络, 为基于隐私保护的推荐算法提供更加全面的理论基础与研究框架 (对于本文所收集的论文列表可访问链接 https://github.com/hongleizhang/RSPapers).

本文第 1 节对推荐模型的发展历程进行分类介绍, 结构如下: 包括传统推荐算法、基于深度学习的推荐算法以及基于隐私保护的推荐算法. 第 2 节详细阐述基于联邦学习范式的隐私保护推荐算法的基本框架并对其扩展工作进行分类介绍. 第 3 节介绍联邦推荐系统所使用的开源工具库以及用于实验评估的常用数据集. 第 4 节总结本文并分析现有方法存在的问题并对未来可能的研究方向和发展趋势加以展望.

1 推荐系统概述

推荐系统作为缓解信息过载问题的重要手段, 其通过过滤无用信息进而筛选出用户可能感兴趣的物品以此达到提升用户体验和商户利润的目的[33−35]. 在众多推荐算法中, 协同过滤技术由于其出色的推荐性能与良好的可扩展性, 成为了学术界和工业界中最受欢迎的技术主题之一. 更具体地, 协同过滤技术基于以下假设: 即用户在过去所表现出的兴趣偏好在将来时间段仍然会保持类似的选择倾向, 并且可以根据其他相似用户的行为数据或者相似物品的浏览数据来推断目标用户对于未浏览物品的偏好[36]. 通过对协同过滤算法的发展趋势进行总结, 可将其大致分为以下两个阶段, 即推荐系统发展初期主要关注准确性指标阶段和推荐系统发展后期所关注的复合指标阶段[37]. 实际上在推荐系统发展早期人们主要是通过利用更复杂模型或者融合更多的数据来提升推荐准确性指标. 随着用户对推荐体验要求的逐渐提高, 使得研究人员开始研究包括隐私性在内的更加人性化的复合指标. 如图 1 所示, 将关注准确性指标阶段细分为传统的推荐算法和基于深度学习的推荐算法; 将后期所关注的复合指标聚焦在考虑隐私性指标前提下的推荐准确性 (图 1 中所提及文献用英文简写形式表示, “*”表示经典的隐私保护方法, 下划线表示联邦推荐算法).

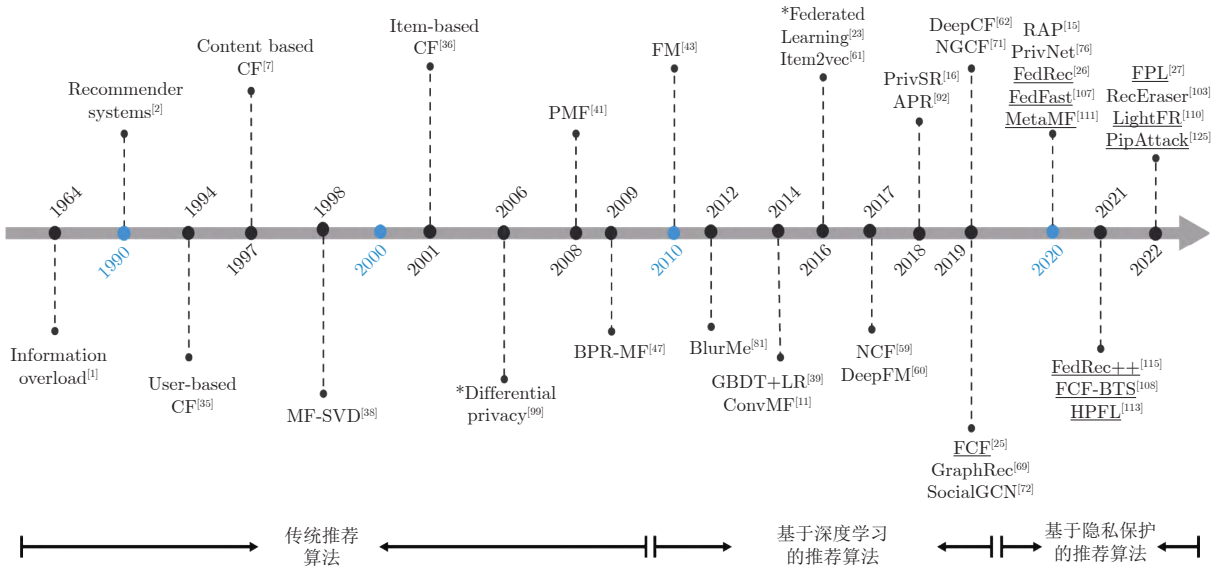


图 1 主流推荐模型发展历程

Fig. 1 Timeline of mainstream recommendation models

1.1 传统推荐算法

传统协同过滤算法作为推荐系统核心技术之一, 被长期应用在真实的推荐场景中. 其主要是通过将用户的历史行为信息转化为用户—项目行为矩阵的方式进行存储训练, 并且传统协同过滤方法能够擅长挖掘用户对物品直接近邻的属性特征. 根据其运用学习范式的不同可分为基于领域的推荐方法[36]和基于模型的推荐方法[38−40] 两大类. 基于领域的方法侧重于寻找当前用户 (物品) 的最近邻, 然后基于近邻做出物品推荐. 基于模型的方法利用机器学习技术将整个用户—项目评分信息或者部分数据作为训练集来产生预测模型, 然后使用训练好的模型为用户提供个性化推荐. 其中矩阵分解技术[41] 由于其高准确度和高扩展性等优点, 近年来得到了许多研究者的青睐.

矩阵分解技术通过学习用户和项目的低维表示进而达到个性化推荐的目的[41−43], 直观来讲, 矩阵分解技术将原始用户—项目评分矩阵 $\boldsymbol{R} \in \mathbf{R}^{n\times m}$ 分解为两个维度相同的较小矩阵 (用户隐含特征矩阵 $\boldsymbol{P} \in \mathbf{R}^{f\times n}$ 和项目隐含特征矩阵 $\boldsymbol{Q} \in \mathbf{R}^{f\times m}$), 然后将两者相乘来还原到原始的高维空间, 同时完成矩阵补全的任务. 典型的矩阵分解损失函数如式 (1) 所示, 通过在训练集中利用最小二乘法来建模真实值与预测值之间的误差, 然后利用梯度下降等优化算法迭代的更新用户和项目隐含特征向量使得误差降低到最小, 最终达到在未观测数据上具有泛化能力的目的.

$$L_{MF} = \frac{1}{2}\sum_{(u,\,i)\in\Omega}\left(r_{ui} - \boldsymbol{p}_u^{\mathrm{T}}\boldsymbol{q}_i\right)^2 + \frac{\lambda}{2}\left(\|\boldsymbol{p}_u\|^2 + \|\boldsymbol{q}_i\|^2\right) \tag{1}$$

式中, Ω 为训练数据集中二元对 (u, i) 的集合. 另外, $\boldsymbol{p}_u \in \mathbf{R}^f$ 和 $\boldsymbol{q}_i \in \mathbf{R}^f$ 分别代表具有共同维度为 f 的用户和物品隐含特征向量. 其中 λ 为正则项权重, 用来缓解模型过拟合问题. 矩阵分解作为基于模型的推荐算法中预测性能精准以及扩展性能优良的模型之一, 其可以灵活地融合各种附加信息[44−46].

除了上述考虑单一样本的建模方式外, 更为实际的假设为对于训练集中任意两个具有偏序关系的训练样本对作为一个训练样例, 该类方法统称为成对的建模方式[47−49], 其基本假设为用户所感兴趣的物品应该排在用户所不感兴趣物品的前边. 另外, 基于列表的建模方式将用户所对应的所有物品排序列表作为一个训练样例以此更加全面地考虑不同物品间的序列关系[50−54].

1.2 基于深度学习的推荐算法

由于深度学习强大的拟合能力以及高度非线性的表示能力, 其已经在推荐系统领域取得了巨大的成功[9]. 通过利用深度学习技术能够高效的融合各类附加信息, 使得推荐模型能够更加关注推荐机制本身的性能提升. 基于深度学习的推荐算法主要采用独热编码的存储方式进行模型训练, 并且其擅长利用高度非线性的特征表示能力挖掘用户对物品的潜在多阶近邻的属性特征. 本文根据深度学习模型

自身特性以及融合到推荐场景中附加信息的不同, 主要分为基于自编码器的推荐算法[55−57]、基于多层感知机的推荐算法[58−62]、基于卷积神经网络的推荐算法[63−65]、基于循环神经网络的推荐算法[66−68] 以及基于图神经网络的推荐算法[69−72]. 除了上述介绍的单一深度网络模型应用于推荐任务外, 集成多种深度模型的长处可以得到性能表现更加优良的集成模型[73].

尽管上述提及的深度学习推荐模型能够在预测性能方面得到显著提升, 但有相关的文献表明推荐模型在多种不同的攻击类型中存在一定的脆弱性, 最终给用户的敏感隐私信息带来严重的安全威胁[74]. 早在推荐系统研究初期, 来自得克萨斯大学的研究员通过将公开的用户行为数据集与互联网电影数据库进行关联识别出了匿名用户的真实身份[14]. 由于此次严重的隐私泄露问题最终导致网飞大赛因隐私原因被叫停, 该发现也为学者们重点研究推荐系统的攻击威胁与隐私保护提供了全新的思路, 因此下文将重点介绍基于隐私保护机制的推荐系统.

1.3　基于隐私保护的推荐算法

基于隐私保护的推荐算法的目标是一方面需要保护用户的个人隐私数据不被轻易泄露, 一方面需要防御来自不同背景不同类型的攻击威胁. 其中, 根据攻击者攻击手段与攻击目标的不同[75], 大致分为用户属性攻击、推理攻击和托攻击. 根据攻击者攻击阶段的不同, 大致分为中毒攻击与逃逸攻击. 根据攻击者掌握攻击环境程度的不同分为了白盒攻击 (掌握全部的攻击环境数据)、灰盒攻击 (掌握部分的攻击环境数据) 与黑盒攻击 (掌握极少的攻击环境数据). 由于上述多种不同类型的攻击手段, 使得推荐模型在整个机器学习训练过程中都有可能面临严重的安全威胁, 因此如何针对不同的攻击方式进行有效防御进而实现鲁棒的推荐系统是目前信息安全领域学者们研究的重点. 为有效应对上述攻击威胁进而更好地保护用户的个人隐私, 需要全方位的保护推荐系统各流程的敏感信息, 包括在数据收集阶段的数据集隐私保护、训练过程中的隐私保护、测试阶段的隐私保护等[76]. 周俊等[77] 通过根据经典的隐私保护方法来对传统的基于隐私保护的推荐算法进行综述介绍, 但该工作调研的方向侧重于安全领域并且缺乏对于机器学习领域新兴方法的补充 (比如对抗学习等新兴的机器学习范式).

基于此, 本文根据所使用防御机制的不同, 以更加全面的分类方式来进行介绍, 大致分为基于匿名化的隐私保护方法[78−80]、基于数据扰动的隐私保护方法[81−87]、基于密码学的隐私保护方法[88−90]、基于对抗学习的隐私保护方法[91−94] 与基于联邦学习的方法[95−97] 等, 具体实现机制与详细分析见表 1. 除了上述介绍的直接对某些隐私度量进行优化的隐私保护方法外[98−100], 还有一些特定的安全执行环境以及为了实现隐私保护而改造的模型训练方式. 比如可信执行环境[101]、分离学习[102]、机器遗忘学习[103] 以及联邦学习[95]. 其中, 联邦学习是一种充分发挥终端设备计算能力并协同服务端联合优化全局模型的分布式学习框架, 第 2.1 节将重点介绍其定义与分类.

2　基于联邦学习的推荐系统

本节首先介绍联邦学习的定义、分类以及主要执行步骤, 随后介绍联邦推荐系统的基本框架, 最后详细介绍联邦学习在推荐系统中的主要研究进展.

2.1　联邦学习

传统隐私计算方法通过在中心存储的数据集上进行加密或者扰动机制来实现安全可靠的数据发布与挖掘, 然而这些方法奏效的前提是需要多个参与方将私有数据汇聚到中心服务端进行统一管理. 但往往由于商业限制以及法律法规的约束, 数据不能

表 1　基于隐私保护的推荐算法总结

Table 1　Summary of privacy-preserving recommendation algorithms

隐私保护方法	保护阶段	具体实现机制	优点	缺点	代表文献
匿名化方法	数据收集	泛化、抑制、聚类等	实现简单, 可快速获取发布数据	容易受到去匿名化与差分攻击等威胁	[14, 78–80]
数据扰动方法	模型训练 模型测试	随机扰动、差分隐私	可以从理论角度保证数据隐私与安全	假设太强, 往往导致数据的可用性降低	[81–87]
密码学方法	模型训练 模型测试	多方安全计算、同态加密等	可提供安全可靠的加密数据	计算复杂度高, 需要加密与解密过程	[20–22, 88–90]
对抗学习方法	模型训练 模型测试	常规对抗训练、虚拟对抗训练等	可根据攻击目标灵活设计损失函数进行端到端训练	模型训练过程难以收敛, 容易出现模式崩塌等问题	[15, 37, 91–94]
联邦学习方法	数据收集 模型训练 模型测试	横向、纵向、迁移联邦学习等	保护隐私的同时实现分布式训练以解决数据孤岛问题	需要克服数据异质性以及通信效率等问题	[23–25, 95–97]

轻易地移交给其他第三方服务器, 因此导致了数据孤岛现象. 为有效应对上述情况, 联邦学习技术在不传输本地原始数据的前提下通过协同服务器端与多个本地模型进行联合优化, 进而聚合多个本地客户端模型的中间参数来得到全局较优的模型. 联邦学习通过将客户端的个人数据保留在本地以此实现原始数据的物理隔离, 从而确保个人数据不会被直接泄露, 使之满足隐私保护和数据安全需求. 进一步地, 联邦学习可以在保证各参与方独立性的情况下传输中间计算结果 (而非原始数据) 并且可以对其进行加密传输, 使其可以实现更严格的数据安全共享与公平合作; 另外, 联邦学习技术作为机器学习范式的一种可信分布式框架, 其能够高效融合来自更多机构或者用户间的训练数据以此来缓解集中式学习存在的有效训练数据不足的问题. 同时, 通过设计高效的联合优化算法能够实现服务端与客户端间全局模型的快速收敛, 并且可以有选择的对客户端模型进行合理聚合以此学习更优的机器学习模型. 综上, 联邦学习范式可以从根源上缓解用户的隐私保护问题并且能够保持模型优越的预测性能[23].

联邦学习作为近年来具有潜力的机器学习技术, 最早由谷歌公司为解决安卓设备的更新问题而被首次提出[24]. 根据原始数据的分布规律, 常用的联邦学习模式主要有横向联邦学习和纵向联邦学习两种[97]. 横向联邦学习场景是指当两个组织间的数据用户重叠较少, 而用户特征重叠较多时, 把数据集按照横向 (即样本维度) 切分, 并取出双方用户特征相同而用户不完全相同的部分数据进行训练; 纵向联邦学习场景是指当两个组织间的数据用户重叠较多而用户特征重叠较少时, 把数据集按照纵向 (即特征维度) 切分, 并取出双方用户相同而用户特征不完全相同的部分数据进行训练.

通用的联邦学习训练框架为: 首先服务端下发模型参数进行本地模型初始化与训练, 然后客户端发送中间梯度到服务器端, 其次服务器端聚合客户端的参数并更新全局模型, 最后下发最新参数并更新本地模型[24]. 在此们假设以多轮通信来执行同步的更新方案, 假设联邦学习系统中的客户端集合为 $K = \{1, 2, \cdots, k\}$, 其中服务端的全局模型表示为 $f(w)$, 第 k 个客户端的本地模型表示为 $f_k(w)$, 其通过利用各自的私有数据进行局部训练, 客户端的私有数据表示为 $D_k = \{x_k^j, y_k^j\}_{j=1}^{n_k}$. 为了达到高效的训练目的, 只选择部分比例的客户端进行更新, 即在每轮更新前初始化客户端集合的随机选择比例 C, 然后客户端将全局模型的参数状态进行下发, 每个被选中的客户端根据下发的全局模型以及私有数据进行 E 迭代次数的局部训练, 随后上传各自的最新参数供服务端进行聚合更新, 上述更新过程执行 T 轮直到模型收敛. 其中, 服务端的全局模型 $f(w)$ 具体表示为多个客户端模型的聚合形式:

$$\min_{w\in\mathbf{R}^d} f(w), \quad f(w) \stackrel{\text{def}}{=} \frac{1}{n}\sum_{k=1}^{n} f_k(w) \tag{2}$$

式中, d 表示为模型参数的特征维度, n 表示参与的客户端数量 $n = C/|K|$. 对于典型的机器学习问题, 定义损失函数为 $f_k(w) = l(x_i, y_i; w)$, 如果是分类任务一般为交叉熵损失函数, 回归任务一般为平方损失函数, 通过在本地执行梯度下降优化算法来获得最优解. 后续联邦学习的前沿进展基本, 都是围绕上述公式展开的, 比如如何更好地聚合本地模型[104]、如何更好地挑选具有代表性的客户端[105] 以及设计不同的个性化客户端模型[106] 等.

另外, 随着联邦学习技术的逐渐成熟, 研究者们逐渐设计出一系列联邦学习在计算机视觉、自然语言处理以及推荐系统领域的应用, 以上创新工作推动了联邦学习技术的发展与应用落地. 第 2.2 节将详细介绍联邦学习与推荐系统领域结合而诞生的基于联邦学习范式的推荐系统, 期望能够为学者们提供全面的综述与新的研究思路.

2.2 联邦推荐系统

推荐系统通过充分挖掘用户对物品的历史行为信息以及各自固有的属性特征以此发现用户的潜在兴趣偏好. 其中, 当前主流推荐模型的训练框架首先收集所有用户的个人信息到集中存储的中心服务端, 然后在中心服务端统一训练推荐模型 (其中大致经历召回、粗排、精排以及重排序阶段), 最后生成对于每个用户的个性化推荐结果. 然而, 用户上传的行为数据往往包含大量的个人敏感信息, 因此集中式训练的模式会存在潜在的隐私泄露风险与安全隐患[77]. 另外, 由于用户对于个人隐私的担忧, 大多数人们不乐意将自己的原始数据进行上传, 因此导致集中式的训练模式缺乏足够的训练数据而使得模型预测性能下降. 基于以上两种原因, 推荐系统亟需一种能够保护用户个人原始数据同时能够确保推荐算法预测性能的新颖学习框架.

联邦学习作为一种保护隐私的分布式机器学习框架, 其通过将用户个人原始数据保留在本地, 利用服务端与客户端的中间参数进行协同优化, 最终在保护用户个人隐私的同时保障了机器学习模型的预测性能[24]. 推荐算法为了实现保护用户隐私的需求, 自然的想法是将集中式学习框架迁移到联邦学习范式的场景中, 于是基于隐私保护的联邦推荐系

统得到了研究者的广泛关注. 基于联邦学习范式的推荐算法通用训练流程如图 2 所示. 具体地, 每个客户端在进行本地模型训练的前期工作主要是收集各自的行为数据, 其中主要包含用户的显式评分数据 (比如用户对物品的评分与评论数据) 以及隐式反馈数据 (比如对物品的点击、喜欢以及收藏数据等). 后续模型更新的详细步骤为:

步骤 1. 服务端下发全局推荐模型到客户端, 该模型可以是随机初始化模型或者预训练模型.

步骤 2. 客户端利用本地交互数据进行局部模型训练并更新本地模型.

步骤 3. 客户端将待更新的模型参数或者中间参数上传到中心服务端.

步骤 4. 服务端聚合来自本地客户端的模型参数或者中间参数.

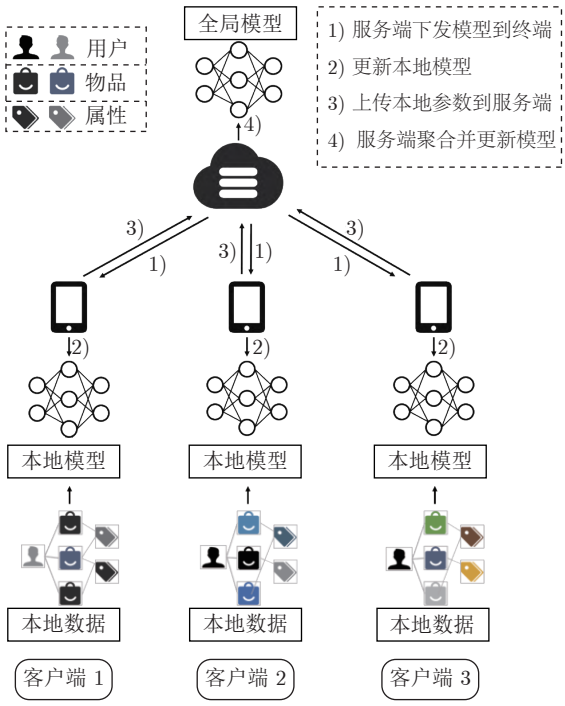


图 2　联邦推荐系统训练流程图

Fig. 2　The procedure of federated recommender systems

上述步骤进行多轮迭代直至全局模型收敛, 然后利用本地模型进行推理预测. 基于联邦学习的推荐算法框架与传统的联邦学习框架类似, 其将每个用户看做一个客户端, 用户所产生的个人行为数据 (比如浏览历史、点赞收藏历史等) 保存在本地, 通过与中心服务端进行协同优化, 最终达到个人原始数据不出本地而进行有效训练的目的. 不同之处在于推荐系统涉及的客户端众多, 因此选择哪些客户端进行更新是其主要面临的挑战. 另外, 推荐系统本地客户端存储的数据不同于传统的视觉数据, 其不仅存在数据异质性的问题还存在数据稀疏、长尾分布以及冷启动用户 (物品) 等复杂情况.

因此基于联邦学习的推荐系统会面临更多更严峻的挑战. 根据以上步骤, 研究者针对其中涉及到的每个部分进行了更进一步的研究, 研究的方向主要包括: 如何有效挖掘符合实际场景的异质数据, 如何挑选有代表性的本地模型参与训练, 如何在服务端进行更加有效的参数聚合, 如何减少通信成本并保证模型收敛以及如何实现参数传输过程中的隐私保护问题等. 基于以上研究问题, 第 2.3 ~ 2.8 节详细介绍基础联邦学习推荐算法框架[25−32]、基于效率增强的联邦推荐算法[107−110]、缓解异质性的个性化联邦推荐算法[111−114]、基于性能增强的联邦推荐算法[115−118]、基于隐私增强的联邦推荐算法[119−124] 以及防御攻击的鲁棒联邦推荐算法[125−128]. 图 3 展示了上述各研究方向之间的关系, 其中基础联邦推荐算法框架旨在为推荐场景常见的数据形式设计合理的联邦学习框架, 其余方向则是在此基础上的延伸 (分别考虑了效率性、异质性、有效性、隐私性以及鲁棒性), 以此建立一个全面的联邦学习推荐系统. 表 2 总结了基于联邦学习范式的推荐算法在各个方向上详细的研究目标、需要克服的挑战、主要实现机制以及代表性的参考文献, 希望能够为研究者们提供一个清晰的研究框架.

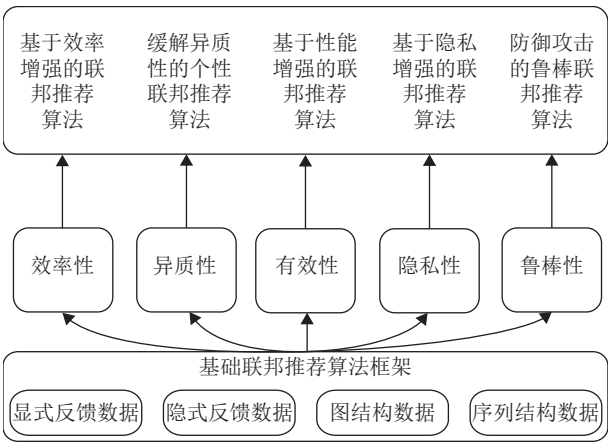


图 3　联邦推荐系统研究方向总结

Fig. 3　Summary of research directions for federated recommender systems

2.3　基础联邦推荐算法框架

基于通用的分布式训练框架, Ammad 等[25] 提出了针对隐式反馈数据设计的首个基于联邦学习框架的推荐算法 (Federated collaborative filtering, FCF), 该算法在中心服务端维护全局的矩阵分解模

表 2 联邦推荐算法主要研究方向以及实现机制总结

Table 2 Summary of main research directions and realization mechanisms of federated recommender systems

研究方向	潜在挑战	研究目的	适用场景	具体实现机制	代表文献
基础联邦推荐算法框架	如何针对基础推荐模型以及推荐场景设计合理的联邦学习框架	根据具体场景设计合理的联邦推荐算法	数据来源单一且数据噪声小	基于显式/隐式数据的联邦推荐框架、基于图/序列数据的联邦推荐框架	[5, 25–32]
基于效率增强的联邦推荐算法	如何保证联邦推荐算法模型的快速收敛	通过压缩与聚类等技术实现较低通信成本	大规模推荐系统	利用强化学习减少参数通信成本、利用聚类实现模型的快速收敛等	[107–110]
缓解异质性的个性联邦推荐算法	如何有效建模多种复杂异质性的关系	利用个性化联邦缓解客户端分布偏斜问题	数据来源多样且复杂	层次化建模、元学习方法以及迁移学习等个性化联邦技术	[111–114]
基于性能增强的联邦推荐算法	如何有效防止分布式训练过程中的信息丢失	利用去噪等机制弥补与集中式模型的差距	数据噪声多且对推荐精度要求高	负样本修正、模型正则化、梯度去噪以及迁移学习等技术	[31, 115–118]
基于隐私增强的联邦推荐算法	如何在保证有效性同时提高隐私保护能力	利用辅助技术实现隐私保护的有效提升	对隐私要求严格的场景, 比如金融、医疗等行业	差分隐私、本地差分隐私、同态加密以及秘钥共享等技术	[119–124]
防御攻击的鲁棒联邦推荐算法	如何实现有效攻击并提出对应的防御机制	通过分析攻击的可行性来提高其鲁棒性	用户设备不稳定且容易被攻击	中毒攻击、托攻击以及拜占庭攻击等	[125–128]

型, 每个客户端维护私有的矩阵分解模型, 然后通过本地私有的隐式反馈数据进行本地更新并上传梯度信息到中心服务端进行聚合优化, 更直观地理解可以参考图 4 算法示意图[27]. 具体地, 中心服务端维护所有物品的最新低维特征矩阵 $\boldsymbol{Q} \in \mathbf{R}^{f\times m}$, 每个用户客户端 u 维护各自私有的用户低维特征向量 $\boldsymbol{p}_u$ 以及从服务端下发的全局物品特征矩阵 $\boldsymbol{Q}$. 由于每个用户的私有数据 $D_u \in \{(u, i)|i \in N_u\}$ 以及特征向量 $\boldsymbol{p}_u$ 不会上传到服务端以及物品特征矩阵通过中间梯度信息 $\Delta\boldsymbol{Q}$ 进行更新, 通过以上机制实现了隐私保护的联邦学习协同过滤算法 FCF. 具体地, 对于用户 u 的特征向量 $\boldsymbol{p}_u$ 利用梯度下降算法的更新公式如下:

$$\boldsymbol{p}_u = \boldsymbol{p}_u + \eta \sum_{(u,i)\in D_u} (c_{ui}(r_{ui} - \boldsymbol{p}_u^{\mathrm{T}}\boldsymbol{q}_i))\boldsymbol{q}_i + \lambda \boldsymbol{p}_u \quad (3)$$

式中, D_u 表示用户 u 的私有隐式反馈数据, $c_{ui} = 1 + \alpha r_{ui}$ 表示用户 u 对物品 i 交互的置信度级别, α 通常取大于 0 的值, λ 为正则项系数, η 表示学习率. 通过该式 (3) 可以看出, 只利用本地数据就可以更新用户私有的特征向量以此保护用户的隐私信息. 对于物品 i 的特征向量 $\boldsymbol{q}_i$ 的更新需要在服务端进行, 并且需要聚合来自不同客户端 u 对于物品 i 的更新梯度信息, 因此具体更新物品向量的公式如下:

$$\boldsymbol{q}_i := \boldsymbol{q}_i + \eta \sum_{u\in N_i} f(u, i) + \lambda \boldsymbol{q}_i \quad (4)$$

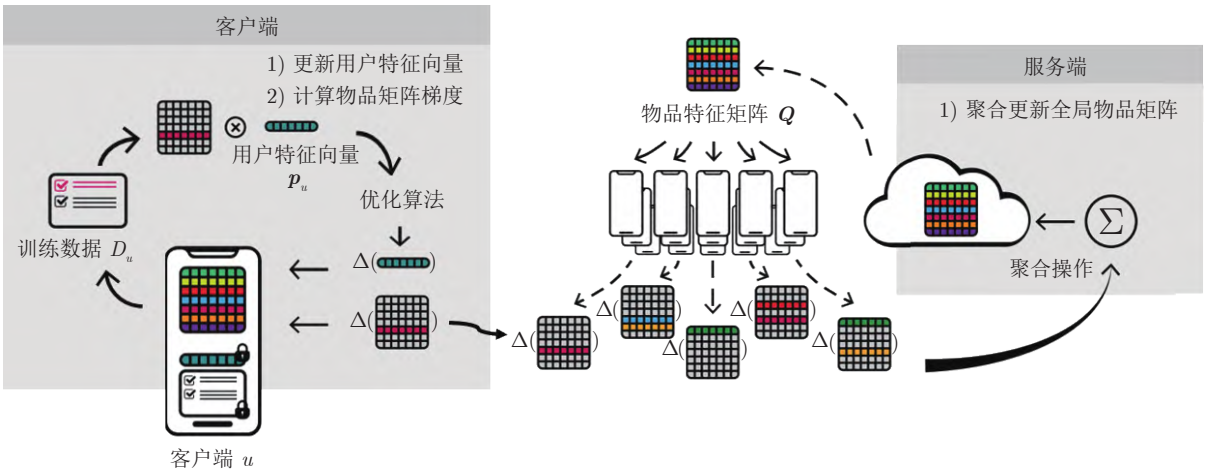


图 4 联邦推荐算法基本框架

Fig. 4 The general framework for federated recommender systems

式中, N_i 表示对于物品 i 产生行为记录的客户端集合, $f(u, i)$ 表示来自客户端 u 对于物品 i 的具体梯度信息 $f(u, i) = (c_{ui}(r_{ui} - p_u^{\mathrm{T}} q_i))p_u$. 通过上传对于物品特征的梯度信息而非原始数据可以实现对于物品特征矩阵的信息保护. 后续有相关文献表明, 上传的明文梯度信息中往往存在敏感信息[129], 因此如何实现联邦学习框架的强隐私保护值得被深入研究.

相比于隐式反馈数据, 针对于显式反馈数据的联邦推荐系统更具有挑战性. 具体体现在: 1) 隐私保护方面的挑战. 由于显式反馈数据在传输梯度信息时只上传用户 u 所产生交互的物品集合 I_u, 因此很容易被服务端所识别并造成隐私泄露; 2) 计算与通信方面的挑战. 如果仿照基于隐式反馈数据的联邦协同过滤方法 FCF 将所有未产生交互的物品当做负样本, 无疑会增加模型的偏差并且带来巨大的计算与通信开销. 基于以上挑战, Lin 等[26] 提出基于显式反馈的联邦推荐算法 (Federated recommendation with explicit feedback, FedRec), 该方法提出了两种简单且有效的机制, 即用户平均方法和混合填充方法, 来生成虚拟交互物品集合 I'_u (通过引入虚拟交互物品可以降低真正产生交互物品的被攻击概率, 从而达到隐私保护的目的) 以及对应的评分集合 R'_u 以此提高梯度信息在传输过程中的隐私保护能力. 具体地, 首先从每个用户 u 未交互过的物品集合中随机采样出虚拟交互物品集合 $I'_u \subseteq I \backslash I_u$, 然后根据式 (5) 来计算用户的平均评分作为生成的对应虚拟评分信息.

$$r'_{ui} = \bar{r}_u = \frac{\sum\limits_{k=1}^{m} y_{uk} r_{uk}}{\sum\limits_{k=1}^{m} y_{uk}} \tag{5}$$

式中, y_{uk} 表示用户 u 是否点击过物品 k, $y_{uk} = 1$ 表示产生过交互行为, $y_{uk} = 0$ 则表示之间没有产生过交互行为. 除了上述将用户平均评分作为虚拟评分信息外, 混合填充方法则将模型预测评分 $r'_{ui} = \hat{r}_{ui}$ 作为最终的虚拟评分. 通过引入虚拟交互物品与评分可以实现在梯度传输过程中的信息保护. 为了更加有效地建模隐式反馈数据, 另一种行之有效的方案是利用成对训练的思想来建模用户的相对偏好, 因此 Anelli 等[27] 提出了首个基于成对训练的联邦推荐算法, 并且通过实验分析了数据使用量与推荐模型预测性能的关系.

除了将上述经典的矩阵分解模型设计为具有隐私保护能力的联邦学习框架外, 为充分利用深度神经网络模型出色的拟合能力以及高度的非线性特征抽取能力, Perifanis 等[28] 提出了联邦学习设置下的神经协同过滤算法 (Federated neural collaborative filtering, FedNCF). 该算法是首个将传统神经协同过滤算法迁移到联邦学习的设置中并应用于序列推荐任务的模型. 具体地, 该算法采用联邦平均的训练模式将通用的矩阵分解模型、多层感知机模型以及两者相结合的模型进行了联邦学习框架的设计, 并且提出了安全的聚合协议来加密传输梯度信息以保证模型参数信息的隐私内容不被泄露. 通过丰富的实验验证了所提方法在预测性能与隐私性方面的优越性, 并且验证了所提出的安全聚合协议相比于传统的同态加密机制具有更少的计算开销.

随着图神经网络在推荐系统领域的快速发展, 其已经被学术界与工业场景证明了其有效性. 但目前主流的图神经网络推荐算法需要收集所有用户的信息到中心服务器进行集中式训练, 这就造成了用户对于个人隐私的担忧. 为提高图神经网络模型的隐私保护能力, Wu 等[29] 提出了基于联邦学习框架的图神经网络推荐算法 (Federated graph neural network for privacy-preserving recommendation, FedGNN), 该方法是首个将图神经网络推荐系统设计为联邦学习框架的模型, 其在充分挖掘高阶的交互信息的同时能够很好的保护用户的个人隐私信息. 具体地, 每个用户客户端利用私有的交互信息局部训练各自客户端的图神经网络模型, 随后每个客户端上传本地的梯度信息至服务器进行聚合更新. 由于传输的局部梯度信息中可能包含丰富的个人敏感信息, 该文提出利用本地差分隐私技术应用到待传输的梯度数据上以保护用户隐私. 另外, 为了进一步保护用户所交互过的物品集合, 本文提出将随机采样的物品集合作为伪交互物品集合以起到匿名化的作用. 最后, 为充分挖掘用户高阶的交互信息, 该文提出利用图扩充技术在隐私保护的情况下找到具有相互交互物品的相邻用户并交换他们的嵌入特征信息.

上述方法主要是将评分预测任务以及二分类等任务迁移到联邦推荐的框架上, 但现实场景中的数据大多是以序列的形式存在, 因此如何将序列推荐任务迁移到联邦学习框架上成为了研究的难点. Han 等[30] 提出 On-device deep learning for privacy-preserving sequential recommendation (DeepRec) 算法首次将序列化推荐任务迁移到联邦推荐算法框架上. 具体地, 该算法首先利用欧盟通用数据保护条例出台之前的数据构建全局模型, 然后在其终端用户设备上进行不断的微调操作. 另外, 该算法还利用模型剪枝以及嵌入稀疏性等技术来减小计算与网

络开销, 这样的操作使得模型训练过程在不需要传输用户原始数据的前提下能够有效地在计算资源受限的移动设备上进行操作. 通过将该算法应用在淘宝数据集上, 该算法实现了在计算资源与带宽资源更小情况下与集中式推荐算法相似的推荐精度的效果.

综上, 由于不同推荐算法模型结构的不同, 需要针对不同的基础模型进行有针对性的设计联邦学习框架. 除了上述介绍的对于基本矩阵分解、神经协同过滤模型以及基于图神经网络推荐算法进行专门设计联邦学习框架外, 针对于不同的推荐场景进行专门的联邦学习框架设计同样是具有潜力的研究方向, 比如新闻推荐场景[5]、序列化推荐场景[30]、跨域推荐场景[31] 以及社会化推荐场景[32] 等.

2.4 基于效率增强的联邦推荐算法

传统的基于联邦学习框架的推荐算法同样面临在优化过程中通信成本高的挑战, 即通信轮次过多以及通信过程中的通信量过大问题, 因此如何设计高效的梯度更新策略用以减轻通信开销是其关注的重点方向之一. 标准的联邦学习框架随机的挑选客户端来进行多轮更新, 并且在服务端直接对挑选的客户端的整个模型进行简单平均来作为最终的全局模型, 这样的更新操作使得联邦推荐模型在达到令人满意的推荐精度前需要进行多轮的通信操作.

针对标准联邦学习框架随机选取客户端以及简单聚合操作导致模型收敛慢速的问题, Muhammad 等[107] 提出了对于上述两步进行改进的联邦推荐方法 Going beyond average for faster training of federated recommender systems (FedFast), 该方法具体包括用户采样机制 (Active sampling, ActvSAMP) 以及模型更新机制 (Active aggregation, ActvAGG), 该算法框架如图 5 所示, 通过所提出的用户采样机制与模型更新策略可以实现快速收敛的目的. 具体地, 该方法首先对参与更新的客户端实行 ActvSAMP 采样机制, 即首先对客户端进行聚类操作, 使得具有相同分布以及相同计算能力的客户端处于同一个簇内, 随后在每个簇内选取代表作为选中的待更新的客户端. 然后进行 ActvAGG 聚合操作, 即将更新的代表客户端的参数直接同步到簇内其他客户端的模型上, 以此实现快速的模型训练目的. 该方法通过挑选具有差异性的客户端进行参数传递与更新以及对于相似客户端进行直接的参数交换保证了模型的快速收敛. 该文以通用矩阵分解模型为基础, 将其按照联邦学习框架的设置进行设计, 通过实验

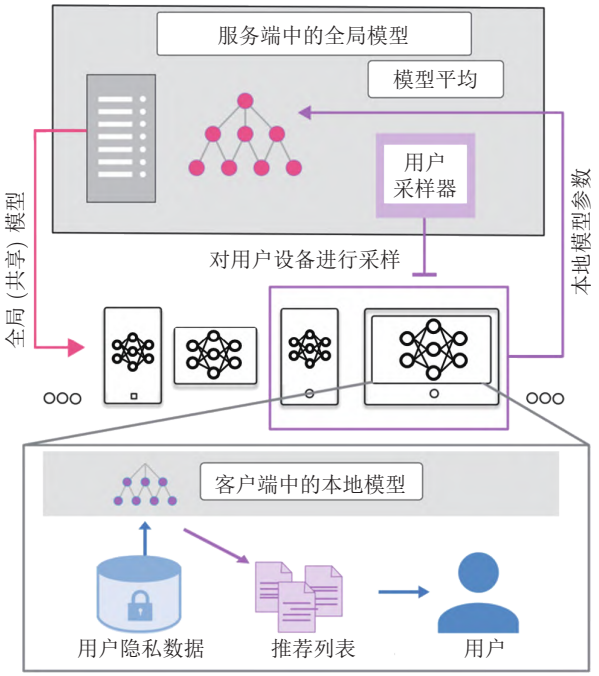


图 5 FedFast 算法示意图

Fig. 5 The diagram of FedFast model

证明其在推荐性能以及模型收敛速度上都具有优异表现.

根据基本的联邦学习推荐系统的设置, 在更新模型参数的过程中需要传输物品特征矩阵的梯度信息 $\Delta \boldsymbol{Q}$ 进而完成服务端的聚合优化. 然而随着物品数量的增加, 模型在传输过程中的参数量也逐渐加大, 比如在 1 千万规模的真实推荐系统场景中, 物品特征矩阵的存储量将达到 1.6 GB 的量级, 这也就说明需要传输 1.6 GB 的数据来完成一次迭代更新. 因此, 针对于在联邦学习传输参数过程中推荐模型过大的问题, Khan 等[108] 通过利用强化学习技术提出一种负载优化的联邦推荐方法 Bayesian Thompson sampling for federated collaborative filtering (FCF-BTS). 具体地, 该文将对于矩阵分解模型中的物品特征矩阵 $\boldsymbol{Q}$ 的优化过程建模为多臂老虎机问题. 首先在服务端利用初始的贝叶斯汤姆森采样方法选取待更新物品的子集 M_s, 然后基于 M_s 选取物品特征矩阵 $\boldsymbol{Q}$ 的子集, 记为 $\boldsymbol{Q}^*$. 随后将物品特征矩阵子集 $\boldsymbol{Q}^*$ 下发到具体地客户端, 然后本地客户端利用私有数据进行更新并回传梯度信息 $\Delta \boldsymbol{Q}^*$ 至服务端, 同时在本地客户端利用回报函数, 即式 (6) 计算第 t 轮对于物品 j 的回报分数 r_t^j, 并根据回报分数更新贝叶斯汤姆森采样器. 经过多轮迭代直到找到合适的待更新物品的子集并达到模型的最终收敛.

$$r_t^j = (1-\gamma t)\cos\left(v_t^j, \nabla^j \boldsymbol{Q}_t^*\right) + \frac{\gamma}{t}\sum_{k=1}^{f}\left|\nabla^j \boldsymbol{Q}_{t-1} - \nabla^j \boldsymbol{Q}_t^*\right| \tag{6}$$

式中, γ 为正则项系数, f 为物品特征向量的嵌入维度, v_t^j 表示在第 t 轮迭代对于物品 j 历史梯度信息的指数衰减系数. 通过该文设计的新颖回报函数可以快速找到待更新的物品子集以此实现减少模型参数传输量的问题.

与上述利用强化学习技术来减少传输通信量的研究思路不同, Yi 等[109] 提出了基于模型分解的高效联邦推荐算法 (Efficient federated learning framework for privacy-preserving news recommendation, Efficient-FedRec). 具体地, 该算法立足于新闻推荐场景, 并根据实验观察发现新闻推荐模型的大部分参数来自于新闻的特征表示, 因此将整个新闻推荐模型分解为大型新闻表示模型和轻量级用户表示模型. 在该方法模型训练过程中, 只需向服务端请求小型的用户表示模型和与其相关联的小规模新闻特征表示, 通过模型分解方式大大减少了模型传输过程中的通信开销. 为了在模型训练过程中保护用户隐私, 文献 [109] 还提出了一种基于多方计算框架的安全梯度聚合协议. 该协议通过对原始交互记录集合进行逆向变换操作, 从而得到全新的梯度表示, 随后将其发送到服务端进行安全梯度聚合, 从而保护原始梯度的隐私信息. 通过大量实验表明, 所提方法可以有效地减少新闻推荐模型训练的计算开销与通信成本.

综上, 提高联邦学习推荐算法框架训练效率的途径主要包括选取合适的客户端进行更新、利用合理的聚合机制、增加本地模型的计算来减少通信轮次以及缩小传输的模型参数量等.

2.5　缓解异质性的个性化联邦推荐算法

与传统集中式训练的推荐模型相比, 基于联邦学习框架的推荐算法在异质性方面面临更加严峻的挑战. 其主要体现在数据异质性以及模型异质性两个方面. 数据异质性是指不同的用户所偏好的物品类别不同, 因此导致用户终端上存储的行为数据不能满足常规的独立同分布的假设. 另外由于不同的用户所产生的交互行为数量也不尽相同, 因此也导致了数据规模的不平衡现象以及推荐系统领域常见的冷启动用户 (物品) 的情况. 模型异质性是指由于不同用户终端的存储能力、计算性能、通信能力的不同以及数据异质性的存在而需要个性化设计模型的情况. 以上两种异质性在传统的联邦学习框架下已经存在, 但由于推荐领域对于用户个性化需求的满足加剧了上述现象的发生, 因此解决联邦学习框架的推荐模型异质性问题是当前研究的重点与难点问题.

针对数据异质性挑战, Wu 等[113] 设计开发了一种基于层次化个性建模的联邦推荐算法 (Hierarchical personalized federated learning for user modeling, HPFL), 算法框架如图 6 所示. 该算法不同于其他文献将用户的全部个人信息看做是不能直接分享的隐私信息, 而是提出了隐私层面的异质性. 即根据是否具有公共属性而将用户的个人行为信息通过层次划分来生成公开信息部分与隐私信息部分. 比如, 物品的属性信息以及标签数据属于公开信息, 而用户的个人行为信息则属于隐私信息. 该模型只对隐私信息部分进行加密处理, 而对于公开信息部分可以直接进行信息交换. 基于以上层次化信息, 该方法设计了包含公开信息组件与隐私信息组件的用户模型. 在客户端模型训练阶段, 客户端可以直接上传公开组件的信息, 而对于隐私部分的组件需要进行加密处理以此来保护客户端数据的隐私性. 在服务端聚合阶段中, 其直接聚合来自客户端的公开组件的参数信息以此获得最新的全局公开组件. 对于隐私组件, 服务端需要聚合来自客户端加密后的隐私组件以此来获取最终的全局隐私组件. 该模型通过生成的层次化信息以及个性化更新策略与聚合机制较好地实现了缓解数据异质性、模型异质性以及隐私异质性的问题.

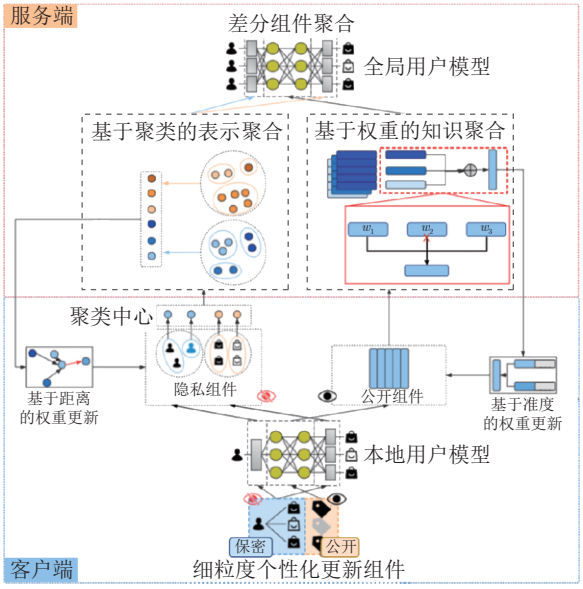


图 6　HPFL 算法示意图

Fig. 6　The diagram of HPFL model

针对常规联邦学习设置中固有的数据异质性问题, 利用元学习方法基于少量样本为不同任务 (客户端) 学习不同的个性化模型是当前的主流方案. 元学习旨在让模型获得特定 "学会学习"的能力, 使其可以在获取已有知识的基础上快速学习新的任务. 当前元学习的方法维度多种多样, 根据采用元知识形式的不同主要关注基于网络结构的元学习方法以及基于权重的元学习方法[130]. 其中基于网络结构的元学习方法是指利用学习机制来自动生成机器学习模型的结构以及参数, 而基于权重的元学习方法主要指利用模型无关的元学习方法来学习较优的初始化权重用以快速实现在其他任务上的适配, 但该方法需要进行二阶梯度计算以及需要对原始数据进行划分然后再进行分阶段训练, 这样的操作会在客户端造成大量的计算成本. 基于此, Wang 等[112] 提出基于改进的元学习个性化联邦推荐算法, 以此来缓解数据异质性问题. 该算法提出利用近似一阶梯度信息进行模型训练, 不仅可以达到良好的算法性能, 同时能够大大减少客户端的计算成本. 另外该算法不需要对数据进行重复划分操作, 因此其适用于联邦学习环境下的冷启动推荐场景中.

当前主流的联邦学习推荐系统框架通常假设服务端的全局模型与客户端的用户模型规模一致, 而忽略了用户终端对于存储、内存以及通信带宽的局限性, 因此需要对不同客户端进行个性化的模型设计以充分考虑其自身的设备能力. 针对上述模型异质性的挑战, Lin 等[111] 提出了基于网络结构元学习的联邦矩阵分解算法 (Meta matrix factorization for federated rating predictions, MetaMF). 具体地, 该算法模型由协同记忆模块、元推荐模块以及评分预测模块构成. 其中协同记忆模块负责融合来自邻居用户的协同信息, 元推荐模块用于生成私有的物品特征矩阵以及用户的私有评分预测模型, 评分预测模块用来根据上述生成的私有物品特征矩阵以及私有评分模型进行评分预测任务. 由于物品数量巨大以及物品特征维度高的特点, 直接为用户生成私有的项目特征矩阵具有很大的挑战性. 为了解决上述问题, 该文提出利用矩阵分解的操作首先生成两个低维的物品特征矩阵以及升维矩阵, 然后将其传输到客户端进行乘积操作来还原出原始规模的物品特征矩阵. 通过将大型的协同记忆模块与元推荐模块部署在服务端而把小型的用户私有评分预测模块部署在客户端实现了联邦推荐模型的个性化设计, 同时在充分考虑设备自身能力的前提下保证了推荐模型的预测性能. 另外, Müllner 等[124] 在严格的隐私约束下证明了元学习模块在保证模型鲁棒性方面有着重要意义.

综上所述, 由于推荐算法对于个性化偏好的要求, 因此基于联邦学习的推荐算法面临更加严峻的异质性挑战, 其具体体现在个人交互行为上的数据规模与类别的差异性等. 为有效缓解异质性带来的挑战, 主要通过层次化建模、元学习方法等设计个性化的联邦学习模型以此来拟合不同客户端的数据分布, 实现对于模型泛化能力的提升.

2.6 基于性能增强的联邦推荐算法

基于联邦学习范式的推荐算法由于可以保留用户的原始个人行为数据在本地, 而通过中间参数 (模型权重或者梯度信息) 协同服务端与客户端模型进行联合优化, 其可以很大程度上保护用户的隐私信息同时能够得到良好的预测性能. 然而正是由于分布式训练的特性以及通过模型中间参数来执行整个优化过程的原因, 导致联邦学习的模型预测精度要在整体上弱于集中式训练的模型精度. 因此, 设计高效的性能提升方法来弥补联邦学习推荐系统模型与集中式推荐模型的差距也是当前研究的重要方向之一.

通过模型的中间参数执行服务端与客户端之间的协同优化, 可以在保护数据隐私的前提下实现模型的分布式训练. 然而模型的中间参数数据中往往包含大量的敏感信息, 比如目标用户对于特定物品的评分信息以及用户所产生的历史点击物品集合等信息, 因此通常的做法是在上述待上传的信息中添加虚拟的点击物品集合以及与其对应的评分记录来进行扰动, 以此实现服务端不能轻易识别出具体的用户以及物品等信息的功能, 进而达到避免敏感信息泄露的目的. 然而向原始数据中添加虚拟行为记录数据的做法不可避免的在模型训练过程中添加了噪声信息, 最终导致推荐算法预测性能的下降.

基于上述挑战, Liang 等[115] 提出基于显式评分数据去噪机制的无损联邦推荐算法 (Lossless federated recommendation with explicit feedback, FedRec++), 算法框架如图 7 所示. 为了消除添加随机采样的物品以及评分所引入的梯度噪声, 该算法提出通过分配一些具有去噪功能的客户端来实现无损的模型优化. 具体地, 服务端首先聚合来自正常用户 u 对物品 i 的梯度信息 $\Delta \boldsymbol{q}_i^u$, 然后计算物品 i 的梯度信息聚合形式为:

$$\Delta \boldsymbol{Q}_i = \sum_{u \in U \setminus \tilde{U}} \Delta \boldsymbol{q}_i^u \tag{7}$$

式中, U 表示正常用户集合, 而 $\tilde{U}$ 则表示去噪用户集合. 由于 $\Delta \boldsymbol{Q}_i$ 中包含虚拟生成的物品信息, 因此

服务端不能轻易识别出用户真正产生过交互的物品集合以此达到隐私保护目的. 为了提高模型训练的精度, 该算法提出利用去噪客户端 $\tilde{U}$ 来消除上述梯度噪声信息, 即按照式 (8) 服务端收到来自去噪客户端的梯度信息后作为最终的梯度信息:

$$\Delta \boldsymbol{Q}_i = \Delta \boldsymbol{Q}_i - \sum_{\tilde{u}\in\tilde{U}} \Delta \boldsymbol{q}^s(\tilde{u}, i) \tag{8}$$

式中, $\Delta \boldsymbol{q}^s(\tilde{u}, i)$ 表示来自去噪客户端 $\tilde{u}$ 对于物品 i 的梯度信息. 通过对去噪客户端合理的选取, 可以实现在显式评分预测场景下的无损失联邦学习的目的.

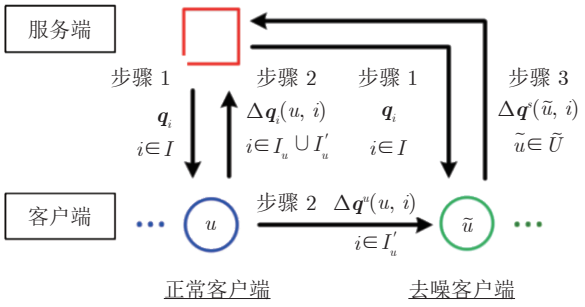


图 7　FedRec++算法示意图

Fig. 7　The diagram of FedRec++ model

传统推荐模型预测性能之所以能够表现优异的原因主要得益于在训练过程中正样本与负样本的密切配合. 其中, 正样本负责将训练样本对 (如用户、物品) 在嵌入空间中拉拢的尽可能的近, 而负样本则负责将不相关的训练样本对的嵌入距离分离的尽可能的远. 通常负样本存在的意义在于防止嵌入空间的模式崩塌, 即如果训练过程中只有正样本存在会让所有样本学习到的表示趋于近似, 因此不再能够提供有区分性的特征. 往往推荐系统场景中只包含用户的正反馈信息, 因此通常的做法是在训练过程中人为的采样负样本来进行模型的正常训练.

在传统的集中式模型训练过程中可以从整体训练数据分布中抽取可靠的负样本数据. 然而, 在联邦学习设置的环境下由于用户个人行为数据是由客户端根据其所处环境进行本地生成的. 这就意味着在每台客户端上可能不存在所需的负样本信息. 即使负样本确实存在, 但也相对较少且相对相似. 通过实验观察可以看出, 当在联邦学习场景下, 简单地应用这些负样本, 会导致模型预测性能的显著下降. 针对上述问题, Ning 等[116] 在联邦学习框架下分析了这种现象并认为性能下降的主要原因是由非独立同分布数据下的负样本采样不精准而导致的, 并不是传统联邦学习设置中的客户端漂移问题. 另外, 作者提出了一种批次不敏感的损失函数 (Batch-insensitive loss, BI) 来缓解数据异质场景下的负样本偏差问题, 具体损失函数如下:

$$\mathcal{L}_{BI}(X, Y) = \frac{1}{N}\sum_{i=0}^{N} \mathcal{L}_{BI}(X_i, Y_i) \tag{9}$$

式中, X 和 Y 表示具有 N 个数据量的不同样本批次. 上述公式直观地意味着, 不管单个样本是如何进行批处理的, 其在并行的不同批次数据上应用损失函数都会产生相同的平均损失和梯度更新. 当把该特性应用到联邦学习框架下时可以看到, 不管数据在客户端之间被怎样分割, 当客户端执行本地训练的一个迭代时, 批次不敏感的损失函数会在训练结束后产生相同的最终服务端更新结果. 通过在联邦学习推荐系统的框架下引入批次不敏感损失函数, 可以很好地解决数据异质场景下负样本生成不准确的问题, 最终实现推荐性能的显著提升.

为更加精准地建模用户的行为偏好, 另一种行之有效的方案是利用来自其他领域的知识来辅助本领域的推荐任务, 该类问题也称之为跨域推荐. 然而在跨域推荐的场景中需要对源域学到的知识直接迁移到目标领域, 这就给用户带来了隐私安全方面的担忧. 因此, 如何在跨域推荐场景下实现性能提升同时保护个人数据的隐私问题是目前具有挑战的研究方向. 目前主流的跨域推荐方法是通过在云上的方式在不同域之间进行原始数据的信息共享以此来获取其他领域的知识, 然而上述方法存在隐私泄露的风险. 针对上述问题, Liu 等[31] 设计了一种协同迁移的个性化联邦推荐算法 (Federated collaborative transfer for recommendation, FedCT). 该方法证明了可以通过在智能终端等边缘设备上进行高效的间接信息共享来克服这些问题, 并将跨域推荐问题形式化为带有多个领域服务端的分布式计算环境, 更直观理解见图 8. 具体地, 该算法在每个用户的个人空间上学习和维护去中心化的用户编码, 并基于变分推理框架进行优化, 其目标是最大化用户编码和来自所有交互过的特定领域内用户信息之间的互信息. 通过实验分析, 所提出的方案在保护数据隐私的前提下实现了性能提升并且提供了一种不依赖于具体领域数量的高效推理机制.

经典的跨域推荐问题主要涉及两个领域之间的信息共享, 后续为了进一步提升目标领域的推荐性能, Flanagan 等[117] 沿着添加辅助信息的研究思路提出了联邦多视角矩阵分解算法来安全的融合多数据源的评分信息, 该算法通过在矩阵分解框架的基础上引入多视角学习以及联邦学习, 使得多种信息源的原始数据不需要上传到中心服务端而是通过利

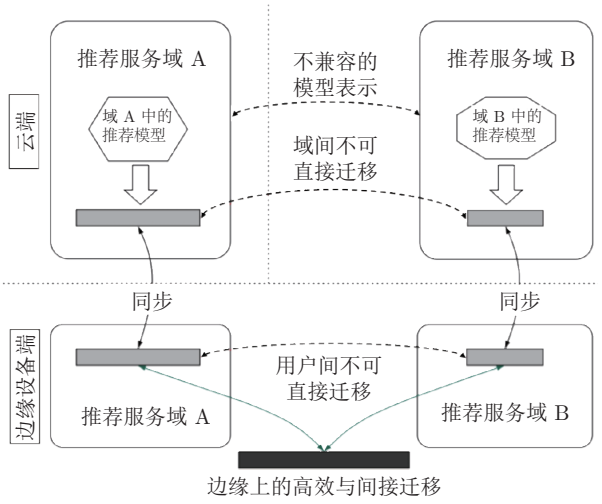


图 8 FedCT 算法示意图

Fig. 8 The diagram of FedCT model

用参数共享的方式来获得额外的知识, 该算法在冷启动联邦推荐场景下也有显著的性能提升.

综上, 通过在联邦学习框架下引入合理的去噪机制、融合高效的表示学习等技术以及解决由数据异质性导致的负样本生成不准确等问题可以实现推荐模型显著的性能提升. 因此, 在未来的研究中可以考虑融入对比学习以及迁移学习等知识来提高联邦推荐模型的泛化能力.

2.7 基于隐私增强的联邦推荐算法

由于联邦学习框架可以保留用户的个人行为数据在本地而通过模型中间参数进行协同优化, 因此通过将集中式训练的推荐模型迁移到联邦学习的框架上可以从根源上保护用户行为信息的隐私问题. 然而, 最新的研究文献表明传输模型的梯度信息仍然可能遭受逆向攻击进而泄露用户隐私以及模型的结构信息[131]. 不同于传统的机器学习任务, 由于在推荐系统场景中存在大量的用户个人敏感行为信息以及受保护的用户属性信息, 因此在联邦学习框架基础上增强隐私保护能力是当前推荐系统领域研究的重要课题.

与常规联邦学习模型增强隐私保护能力的研究路线类似, 实现隐私增强的联邦推荐算法的主要途径是在基础框架下引入数据扰动以及密码学等技术, 以保证数据安全运行的同时实现精准推荐的目标. 针对显式评分数据在参数优化过程中容易被服务端识别进而造成用户信息泄露的问题, Lin 等[26] 提出基于数据扰动的隐私保护联邦推荐算法 FedRec, 该方法提出了两种简单且有效的数据扰动机制, 即用户平均方法和混合填充方法, 来生成伪交互物品集合 I'_u 以及对应的评分集合 R'_u, 通过在参数更新过程中上传用户真实的交互集合 I_u 以及伪交互集合 I'_u 以此提高梯度信息在传输过程中的隐私保护能力.

另外, 为防止基于隐式反馈数据的联邦推荐系统隐私泄露问题, Minto 等[119] 提出利用差分隐私机制等数据扰动技术来保护用户数据安全性的算法 (Local differential privacy based federated recommendation, LDP-FedRec), 算法整体框架见如图 9. 具体地, 保存在客户端的模型包含该用户 u 的隐特征向量 $\boldsymbol{p}_u$ 以及与用户无关的全部物品的隐特征矩阵 $\boldsymbol{Q}$. 对于用户向量的更新由于不需要上传到服务器而得到很好的保护. 对于客户端得到的物品更新梯度矩阵 $\Delta\boldsymbol{Q}$ 通过利用本地差分隐私 (Local differential privacy, LDP) 机制以及代理网络来得到不包含用户元数据的具有隐私保护功能的物品更新梯度矩阵 $\Delta\tilde{\boldsymbol{Q}}$, 随后再进行平均聚合. 通过利用匿名化以及扰动机制可以实现不被服务端轻易识别进而保护用户隐私的目标.

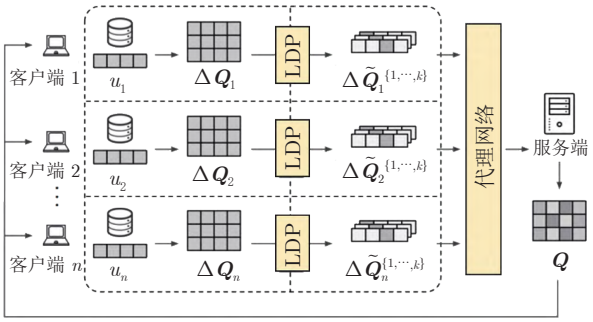


图 9 LDP-FedRec 算法示意图

Fig. 9 The diagram of LDP-FedRec model

为保护梯度信息在传输过程中不泄露用户原始数据的问题, 除了利用差分隐私等扰动机制来保护参数外, 利用密码学等技术可以实现严格的数据隐私保护能力. 文献 [120] 证明了利用中间梯度信息可以反推出用户的原始评分记录, 并提出一种利用同态加密技术来保护梯度信息不被泄露的方法. 具体地, 首先生成公开秘钥与私有秘钥. 公开密钥可以被任何参与者共享, 而私有秘钥只在用户间进行识别; 然后进行模型参数的初始化工作, 即在服务端初始化物品矩阵以及在每个用户端进行用户特征向量的初始化工作; 最后执行在同态加密环境下的矩阵分解操作, 以此实现保护模型的中间参数不被恶意第三方攻击的目标.

为增强联邦学习推荐系统的隐私保护能力, 当前的方法主要采用同态加密以及差分隐私机制对中间的计算结果进行保护. 然而, 前者带来了额外的

通信和计算成本, 后者由于严格的数学假设不可避免的对模型的准确性有所影响. 因此以上方法不能同时满足推荐系统的实时反馈和准确的个性化需求. 为此 Yang 等[121] 提出了一种新颖的联邦推荐框架. 该方法可以在不牺牲效率和有效性的前提下保护联邦推荐系统中的数据隐私问题. 具体地, 该算法利用秘密共享技术来结合联邦矩阵分解的安全聚合过程. 此外, 该算法还引入了个性化掩码的新思想, 并将其应用于所提出的联邦掩码矩阵分解框架中. 个性化掩码机制可以进一步提高模型的训练效率以及模型的预测精度. 通过实验结果展示了所设计的模型在不同的真实数据集上的优越性. 此外, Lin 等[122] 利用虚假标记以及秘密共享技术来修改客户端上传到服务器的参数数据, 通过该机制实现了在不损失模型准确性的前提下保护用户隐私的目标. 该算法是一种通用的跨客户端设备的联邦学习框架, 可以方便地迁移到评分预测、物品排序以及序列化推荐场景.

综上所述, 为增强联邦学习框架下推荐算法模型的隐私保护能力, 主要通过利用差分隐私等扰动机制以及同态加密等密码学技术来保护分布式优化过程中的梯度信息. 然而, 权衡推荐算法的模型精度与隐私保护的效用程度是隐私增强的联邦学习推荐算法需要重点考虑的问题.

2.8 防御攻击的鲁棒联邦推荐算法

基于联邦学习框架的推荐算法由于可以保留用户的敏感交互记录在本地, 因此可以从根源上保护用户的个人隐私信息. 然而, 正是由于其分布式存储数据的特性以及推荐场景对于用户个性化指标的追求, 使得基于联邦学习框架的推荐算法较之于常规联邦学习模型更容易受到低成本的攻击方法的破坏, 比如中毒攻击 (托攻击) 以及拜占庭攻击等. 因此, 研究对于联邦推荐系统攻击的可行性及其防御机制能够为鲁棒联邦推荐算法的安全稳定运行提供重要依据与理论支撑.

联邦学习推荐场景下中毒攻击的目标是通过干扰训练数据集及其训练过程来提升敌手对于目标物品的曝光频率以此达到促销某物品的不正当目的. 文献 [125] 提出了一种系统性的攻击方法来对联邦推荐系统进行后门攻击进而推广某种目标物品. 该算法的核心策略是利用基于数据驱动的推荐系统中普遍存在的流行度偏差的固有属性. 由于热门商品更容易出现在推荐列表中, 因此通过精心设计的攻击模型使目标商品在嵌入空间中具有热门商品的普遍特征. 然后通过在模型更新期间通过少数恶意用户上传精心制作的梯度, 最终可以有效地增加联邦推荐系统中不受欢迎的目标物品的曝光率. 该算法通过在真实的数据集上评估表明, 所提出的攻击模型可以显著提高目标物品的曝光率, 并且不会损害当前推荐算法的准确性. 另外通过实验指出现有的防御措施不够有效, 并突出强调了针对联邦推荐系统的本地模型设计中毒攻击新防御措施的必要性.

针对上述提及的当前防御措施不能有效应用于联邦学习推荐系统场景下的问题, Jiang 等[126] 首次系统性地研究了联邦学习背景下的托攻击问题, 并提出了一种有效的检测方法, 联邦托攻击检测器来有效检测联邦学习推荐系统场景下针对协同过滤算法的托攻击. 该文献首先展示了在联邦学习推荐系统中实施托攻击的可行性. 其次, 该算法专门设计了四个基于客户端间交换梯度的新特征. 通过结合这些基于梯度的特征, 可以训练一个半监督贝叶斯分类器来有效地识别托攻击. 最后, 通过在真实数据集上进行大量的实验证明了所提出方法的有效性.

联邦推荐系统可以在不收集用户隐私数据的情况下提供良好的模型预测性能. 然而, 由于联邦学习分布式存储的特性以及客户端高控制权的特点, 使得模型容易受到来自客户端的拜占庭攻击, 即客户端向服务器发送任意值的拜占庭梯度, 而不是计算得到的真实梯度从而导致整个联邦学习系统的模型预测性能恶化的现象. 针对上述攻击, Chen 等[127] 开发了一种新颖的联邦推荐技术, 其能够对拜占庭客户端产生的恶意梯度攻击具有健壮性. 该文献认为检测拜占庭攻击的关键因素在于监测来自客户端模型参数的梯度信息. 随后其提出一种鲁棒学习策略, 即在服务端计算并利用梯度数据 (而不是使用模型参数) 来过滤恶意的拜占庭客户端. 最后, 通过所提出的拜占庭弹性定义从理论角度与实验层面证明了其鲁棒学习策略的有效性.

综上, 基于联邦学习范式的推荐模型由于存在天然的分布式数据存储特性、客户端高自主权与控制权的特点以及服务端难以识别有效梯度等挑战, 使得模型更容易受到来自客户端以及传输过程中的恶意攻击行为, 比如中毒攻击 (托攻击)、拜占庭攻击等. 为有效应对上述攻击, 可以从客户端的梯度信息入手, 设计高效的恶意梯度检测方法以及提取有效反映梯度信息的特征等是目前行之有效的解决方案.

3 联邦推荐系统学术资源总结

本节将对上述基于联邦学习的推荐系统所涉及的学术资源进行全面总结, 具体包括在算法实现过

程中所用到的开源工具库以及用于实验评估的数据集. 期望通过对上述学术资源的分类介绍, 能够为基于联邦学习的推荐系统这一新兴领域提供全面的研究基础.

3.1 开源工具库

本节对基于联邦学习的推荐系统方向相关的开源工具库进行调研与总结, 其主要是对原有联邦学习框架的改进与二次开发, 其中包括微众银行开发的面向工业界与学术界的联邦学习框架 (Federated artificial intelligent technology enabler, FATE) 以及仅面向学术研究的谷歌开发的联邦学习框架 (Tensorflow federated, TFF)、百度公司开发的基于飞桨框架的联邦学习库 (Paddle federated learning, PaddleFL) 以及南加州大学开发的联邦学习库 (Federated machine learning, FedML) 等通用性联邦学习框架. 其中, FATE 框架由于广泛的适用场景与众多的隐私保护机制受到了学术界与工业界的广泛关注, 包括设计了横向、纵向以及联邦迁移学习场景以及实现了多方安全计算、同态加密与差分隐私等众多隐私保护算法. 另外, 通过对联邦推荐系统领域的调研, 总结归纳了一些直接对联邦推荐系统框架进行设计的优秀开源工具库, 比如微众银行开发的联邦推荐算法库 (Federated recommendation systems, FederatedRec)、阿里开发的弹性联邦学习库 (Elastic federated learning solution, EFLS)、联邦贝叶斯个性化排序算法 (Federated bayesian personalized ranking, FedBPR)、联邦图神经网络库 (Federated graph neural network, FedGNN) 以及针对于联邦推荐算法的中毒攻击算法 (Model poisoning attack to federated recommendation, FedAttack). 其中, FederatedRec 框架包含了 6 种推荐系统场景常用的算法, 具体包括 5 种纵向联邦推荐算法和 1 种横向联邦算法, 其可用于解决联邦学习场景下的评分预测与物品排序等任务, 其通过同态加密与差分隐私机制实现隐私增强的作用; EFLS 框架则是一个跨企业跨部门合作的联邦推荐框架, 其已在大规模工业场景中进行验证, 该框架具有大规模以及高可用的云原生架构, 其集成了多种隐私保护算法 (比如隐私集合求交算法、前向加密算法和差分隐私算法等). 另外 3 种开源工作则分别实现了对成对贝叶斯个性化推荐算法、图神经网络推荐算法以及对联邦推荐场景的攻击算法的工作. 通过分析可以发现, 以上三种框架除了经典的差分隐私机制外, 另外专门设计了适用于各自数据的隐私保护机制, 比如 FedBPR 算法通过上传单一样本的梯度进而使得服务端无法识别出是来自正样本的梯度还是来自负样本的梯度进而达到隐私保护的目的; FedGNN 框架则是通过扩充原有交互样本集合以及随机生成伪交互标签的方式达到隐私保护的目的; FedAttack 算法通过利用翻转正负样本的机制达到难以攻击的目的进而达到隐私保护的目的. 期望通过总结上述开源工作可以促进该领域更多优秀开源工作的诞生. 上述所提及框架的详细总结见表 3. 表 3 整理了所有框架在受众定位、适用场景、隐私保护机制以及代码库链接等方面的内容.

表 3 联邦推荐算法常用工具库总结

Table 3 Summary of commonly used repositories in federated recommender systems

工具库名称	受众定位	适用场景	隐私保护机制	代码库链接	发布单位
FATE	工业产品 学术研究	横向联邦学习 纵向联邦学习 联邦迁移学习	多方安全计算 同态加密 差分隐私	https://github.com/FederatedAI/FATE	微众银行
TFF	学术研究	横向联邦学习	差分隐私	https://github.com/tensorflow/federated	谷歌
PaddleFL	学术研究	横向联邦学习 纵向联邦学习	多方安全计算 差分隐私	https://github.com/PaddlePaddle/PaddleFL	百度
PySyft	学术研究	横向联邦学习	多方安全计算 同态加密 差分隐私	https://github.com/OpenMined/PySyft	OpenMind
OpenFL	学术研究	横向联邦学习	可信执行环境	https://github.com/intel/openfl	英特尔
FedML	学术研究	横向联邦学习 纵向联邦学习	差分隐私 密码学算法	https://github.com/FedML-AI/FedML	南加州大学
FederatedRec	学术研究	横向联邦学习 纵向联邦学习	同态加密 差分隐私	https://fate.fedai.org/federatedml/	微众银行
EFLS	工业产品 学术研究	纵向联邦学习	差分隐私 前向加密	https://github.com/alibaba/Elastic-Federated-Learning-Solution	阿里巴巴
FedBPR	学术研究	横向联邦学习	单一梯度上传	https://github.com/sisinflab/FedBPR	SisinfLab
FedGNN	学术研究	横向联邦学习	差分隐私 伪标签生成	https://github.com/wuch15/FedGNN	微软亚洲研究院
FedAttack	学术研究	横向联邦学习	标签翻转	https://github.com/rdz98/FedRecAttack	清华大学

联邦推荐系统的实验模拟需要处理与传统机器学习模型不同的挑战, 比如如何高效的划分中心式的数据集、在不同的模拟终端设备上高效运行计算以及如何合理地执行协同优化等.

通过对基于联邦学习的推荐算法所使用的工具库总结发现, 仍然可以根据原始联邦学习的适用场景进行划分, 即横向联邦推荐系统、纵向联邦推荐系统以及联邦迁移推荐系统. 其中, 横向联邦推荐系统从用户 (样本) 维度来划分原始的数据集, 将每个用户的交互记录看作单独的客户端用来与服务端进行联合训练; 纵向联邦推荐系统则从物品 (特征) 维度来对原始集中式数据集进行划分, 将不同特征的用户集合看作单独的客户端用于与中心服务端进行协同训练; 联邦迁移推荐系统则是在用户和物品维度都存在样本不足的情况下, 利用迁移学习技术来完成客户端与服务端的联合协同训练. 通过对上述相关文章应用场景的调研, 横向联邦推荐系统在所介绍文献中的应用最广, 纵向联邦以及联邦迁移推荐系统的应用较少. 另外, 通过对上述基于联邦学习的推荐系统的开源情况进行规律总结, 发现绝大多数的文章没有公布用于实验评估的源代码, 这就为该领域的持续健康发展带来了阻力. 其次, 上述调研的相关文献的实验设置存在不统一以及不公平对比的情况, 这就为后续从事相关领域的学者带来了实验复现方面的挑战. 因此, 设计与构建用于统一评测的联邦推荐系统基准库能够为该领域的稳定持续发展奠定基础.

3.2　评估数据集

基于联邦学习的推荐系统所使用的数据集主要来自对原始集中式存储数据的改进, 其中包括 MovieLens、Amazon、Last.FM、Yelp、Book-Crossings、MIND、Douban、Ciao、Epinions、Filmtrust 等. 需要说明的是, 为了适用于联邦推荐系统的研究需要提前划分好特定格式的数据集. 具体地, 针对于横向联邦推荐系统, 需要将每个用户看作一个客户端, 因此需要按照用户维度进行划分的方式来构成用于联邦学习研究的数据集; 针对于纵向联邦推荐系统则需要按照特征维度进行划分, 即将不同域的数据看作不同的客户端. 典型的应用场景是豆瓣平台, 即同一个用户既有电影相关的信息, 又存在书籍相关的数据. 表 4 将列举出相关数据集的主要统计信息, 其中, 引用次数是指出现在本文综述中的基于联邦学习的推荐系统文献所应用的数据集的引用次数总和. 除了介绍所用数据集的基本描述信息, 还总结归纳了每个数据集所存在的潜在隐私泄露风险, 比如 Movielens数据集中存在用户对电影的观看记录以及用户自身存在的属性信息 (性别、年龄、地理位置等信息), 因此观看记录会存在用户行为模式的隐私泄露风险以及用户的属性信息会存在用户属性攻击等潜在风险[131]. 而 Filmtrust 数据集除了存在行为信息泄露风险外, 还可能存在用户社交链接的泄露可能[132].

通过对基于联邦学习的推荐算法文献所应用的数据集的总结发现, 大部分的文献选择使用电影评分数据集 MovieLens 作为其评估的主要数据来源. 另外, 通过对上述文献所应用的数据集进行规律总结可以看出, 基于联邦学习的推荐算法相比于其他推荐系统研究方向来看, 其数据规模呈现出相对较小的特征, 其主要原因是基于联邦学习的实验设置需要对每个用户进行客户端模拟, 因此在模拟分布式训练框架的过程中容易造成计算资源过高的问

表 4　联邦推荐算法常用数据集总结

Table 4　Summary of commonly used datasets in federated recommender systems

数据集名称	场景	主要描述信息	敏感隐私信息	评分范围	引用次数
MovieLens-1M	电影	该数据集包含 6040 个 用户对 3952 部电影共 1000209 个评分记录	用户行为记录以及用户属性信息	1 ~ 5	15
MovieLens-100k	电影	该数据集包括 943 个用户对 1682 部电影共 100000 个评分记录	用户行为记录以及用户属性信息	1 ~ 5	6
Amazon	综合	该数据集包含多种领域, 如音乐、电影、书籍、体育等多个子数据集	用户行为记录	0 ~ 5	3
Last.FM	音乐	该数据集包括 1892个用户, 17632 首歌曲, 以及 92834 个评分记录	用户收听记录	0 ~ 1	2
MIND-small	新闻	该数据集包含 50001 个用户对 25659 条新闻共 8584442 个评分记录	用户阅读记录	0 ~ 1	2
Douban	电影	该数据集包括 129490 个用户对 58541 部电影共 16830839 个评分记录	用户行为记录以及社交信息	0 ~ 5	2
Ciao	电影	该数据集包括 7375 个用户对 105114 部电影共 284086 个评分记录	用户行为记录以及社交信息	1 ~ 5	2
Filmtrust	电影	数据集包括 1508 个用户对 2071 部电影共 35497 个评分记录	用户行为记录以及社交信息	0.5 ~ 4	1
Book-Crossings	书籍	该数据集包括 105284 个用户, 340557 本书, 以及 1149780 个评分记录	用户行为记录与用户属性信息	1 ~ 10	1
Epinions	购物	该数据集包括 116260 个用户对 41269 个物品共 188478 个评分记录	用户行为记录以及社交信息	1 ~ 5	1
Yelp	购物	该数据集包括 7975 个用户, 9323 个物品以及 79087 个交互记录	用户购买记录与标签信息	1 ~ 5	1
MovieLens-10M	电影	该数据集包括 138493 个用户对 27278 部电影共 20000263 个评分记录	用户行为记录与用户属性信息	0.5 ~ 5	1

题. 所以后续该研究方向的研究趋势开始向基于大规模的终端设备的联邦推荐算法演进. 另外, 目前主流的评估方式仍然是采用面向学术界相对静态的数据集以及离线评估的实验设置, 后续可以考虑在现实工业场景进行实时的在线数据集评测. 其次, 目前的数据集仍然是对传统集中式数据集的改进, 即通过人工提前设置的方式来模拟基于联邦学习的实验环境, 因此后续可以考虑构建面向真实场景的基于联邦学习推荐系统的数据集同样是值得考虑的基础工程.

4 总结与展望

本文首先对近年来推荐系统领域的研究进展进行了综述, 并按照传统推荐算法、基于深度学习的推荐算法以及基于隐私保护的推荐算法进行了详细分类介绍. 其中, 基于隐私保护的推荐算法根据其所利用原理的不同分为了匿名化方法、数据扰动方法、密码学方法、对抗学习方法, 并对其进行详细介绍. 最后系统性的综述了联邦学习与推荐系统领域相结合的最新研究进展, 首先介绍了联邦学习以及联邦推荐系统的定义, 随后按照基础联邦学习推荐算法框架、基于效率增强的联邦推荐算法、缓解异质性的个性化联邦推荐算法、基于性能增强的联邦推荐算法、基于隐私增强的联邦推荐算法以及防御攻击的鲁棒联邦推荐算法 6 个方面进行详细介绍. 最后详细介绍和总结了该方向常用的开源工具库以及经典数据集, 以此便于对基于联邦学习的推荐系统领域进行实验评估.

通过对基于隐私保护的联邦推荐算法进行全面的调研与综述, 发现当前的研究成果已经在一定程度上保护了用户敏感数据的隐私安全同时保障了推荐模型的预测精度, 但仍然存在如下的研究难点与热点.

1) 联邦推荐系统的激励机制. 激励机制旨在建立一个公平高效的平衡机制使得各参与方能够持续地参与到联邦学习的全生命周期中, 以此最大化集合体的全局效用且最小化各参与方的局部损失与训练成本. 不同于其他联邦学习应用场景, 联邦推荐系统中的客户端代表真实的用户个体, 因此如何评估每个用户的模型训练贡献以及如何设计高效的调度算法以此持续激励用户进行数据共享和提供客户端算力是目前具有潜力的研究方向.

2) 联邦推荐系统的冷启动挑战. 冷启动问题是指新用户或者新物品在进入既有系统时存在的交互数据稀缺的情况. 集中式推荐模型的冷启动问题已经形成了较为全面的研究体系. 然而, 由于联邦推荐系统场景下的冷启动问题更具有挑战性, 比如如何在资源受限的联邦设置下融合并建模更多有效的附加信息来缓解终端用户的数据稀疏问题, 因此当前的研究工作还处于初级阶段.

3) 联邦推荐系统的异质性挑战. 异质性在传统联邦学习设置中已经进行了广泛的研究, 主要体现在数据异质性与模型异质性方面. 在推荐系统场景中由于参与方为真实的用户个体使得异质性更加具有挑战性, 比如个人行为数据存在严重的特征偏斜情况以及所参与的用户设备数量众多且设备各异等问题, 因此如何在联邦学习框架下细粒度的建模数据异质性以及模型异质性是目前推荐系统领域的主要挑战.

4) 联邦推荐系统的实时性挑战. 实时性是保障机器学习系统能够稳定部署在真实场景中的重要指标, 其主要体现在模型的更新周期以及部署效率上. 集中式推荐模型由于可以在计算能力以及存储能力更强的服务器端完成实时的模型训练以及线上更新, 使得用户兴趣能够及时被推荐模型捕捉. 然而联邦推荐系统在集中式推荐模型挑战的基础上还要重点关注模型参数在服务端与用户终端间的上传与下载的传输时延等复杂情况, 因此如何提高模型参数的传输效率以及优化本地模型的更新机制以此来提高联邦推荐模型的实时性有利于进一步改善联邦推荐场景的用户体验.

References

1 Jacoby J. Perspectives on information overload. *Journal of Consumer Research*, 1984, **10**(4): 432−435

2 Goldberg D, Nichols D, Oki B M, Terry D. Using collaborative filtering to weave an information tapestry. *Communications of the ACM*, 1992, **35**(12): 61−70

3 Rao Zi-Yun, Zhang Yi, Liu Jun-Tao, Cao Wan-Hua. Recommendation methods and systems using knowledge graph. *Acta Automatica Sinica*, 2021, **46**(9): 2061−2077
(饶子昀, 张毅, 刘俊涛, 曹万华. 应用知识图谱的推荐方法与系统. 自动化学报, 2021, **46**(9): 2061−2077)

4 Tang J, Hu X, Liu H. Social recommendation: A review. *Social Network Analysis and Mining*, 2013, **3**(4): 1113−1133

5 Qi T, Wu F, Wu C, Huang Y, Xie X. Privacy-preserving news recommendation model learning. In: Proceedings of the Findings of the Conference on Empirical Methods in Natural Language Processing. Virtual Event: 2020. 1423−1432

6 Cheng H T, Koc L, Harmsen J, Shaked T, Chandra T, Aradhye H, et al. Wide & deep learning for recommender systems. In: Proceedings of the 1st Workshop on Deep Learning for Recommender Systems. Boston, MA, USA: 2016. 7−10

7 Pazzani M J, Billsus D. Content-based recommendation systems. In: Proceedings of the Adaptive Web. Berlin, Heidelberg: 2007. 325−341

8 Shi Y, Larson M, Hanjalic A. Collaborative filtering beyond the user-item matrix: A survey of the state of the art and future challenges. *ACM Computing Surveys*, 2014, **47**(1): 1−45

9 Zhang S, Yao L, Sun A, Tay Y. Deep learning based recommender system: A survey and new perspectives. *ACM Computing Surveys*, 2019, **52**(1): 1−38

10 Zhang H, Liu G, Wu J. Social collaborative filtering ensemble. In: Proceedings of the Pacific Rim International Conference on Artificial Intelligence. Nanjing, China: 2018. 1005−1017

11 Kim D, Park C, Oh J, Lee S, Yu H. Convolutional matrix factorization for document context-aware recommendation. In: Proceedings of the 10th ACM Conference on Recommender Systems. Boston, MA, USA: 2016. 233−240

12 He R, McAuley J. VBPR: Visual Bayesian personalized ranking from implicit feedback. In: Proceedings of the AAAI Conference on Artificial Intelligence. Phoenix, Arizona, USA: 2016. 144−150

13 Han D, Li J, Yang L, Zeng Z. A recommender system to address the cold start problem for app usage prediction. *International Journal of Machine Learning and Cybernetics*, 2019, **10**(9): 2257−2268

14 Narayanan A, Shmatikov V. Robust deanonymization of large sparse datasets. In: Proceedings of the IEEE Symposium on Security and Privacy. Oakland, California, USA: 2008. 111−125

15 Beigi G, Mosallanezhad A, Guo R, Alvari H, Nou A, Liu H, et al. Privacy-aware recommendation with private-attribute protection using adversarial learning. In: Proceedings of the 13th International Conference on Web Search and Data Mining. Houston, TX, USA, 2020. 34−42

16 Meng X, Wang S, Shu K, Li J, Chen B, Liu H, et al. Personalized privacy-preserving social recommendation. In: Proceedings of the AAAI Conference on Artificial Intelligence. New Orleans, Louisiana, USA: 2018. 3796−3803

17 Zhan J, Hsieh C L, Wang I C, Hsu T S, Liau C J, Wang D W. Privacy-preserving collaborative recommender systems. *IEEE Transactions on Systems, Man, and Cybernetics*, 2010, **40**(4): 472−476

18 Zhang Feng, Chang Hui-You. Research on privacy-preserving collaborative filtering recommendation based on distributed data. *Chinese Journal of Computers*, 2006, **8**: 1487−1495
(张锋, 常会友. 基于分布式数据的隐私保持协同过滤推荐研究. 计算机学报, 2006, **8**: 1487−1495)

19 Polat H, Du W. Privacy-preserving collaborative filtering using randomized perturbation techniques. In: Proceedings of the Third IEEE International Conference on Data Mining. Melbourne, Florida, USA: IEEE, 2003. 625−628

20 Berlioz A, Friedman A, Kaafar M A, Boreli R, Berkovsky S. Applying differential privacy to matrix factorization. In: Proceedings of the 9th ACM Conference on Recommender Systems. Vienna, Austria: 2015. 107−114

21 Kim S, Kim J, Koo D, Kim Y, Yoon H, Shin J. Efficient privacy-preserving matrix factorization via fully homomorphic encryption. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. Xi′ an, China: 2016. 617−628

22 Shmueli E, Tassa T. Secure multi-party protocols for item-based collaborative filtering. In: Proceedings of the Eleventh ACM Conference on Recommender Systems. Como, Italy: 2017. 89−97

23 Konecny J, McMahan B, Ramage D. Federated optimization: Distributed optimization beyond the datacenter[Online], available: https://arxiv.org/abs/1511.03575, November 11, 2015

24 McMahan B, Moore E, Ramage D, Hampson S, Arcas B A. Communication-efficient learning of deep networks from decentralized data. In: Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. Fort Lauderdale, USA: 2017. 1273−1282

25 Ammad M, Ivannikova E, Khan S A, Oyomno W, Fu Q, Tan K E, et al. Federated collaborative filtering for privacy-preserving personalized recommendation system[Online], available: https://arxiv.org/abs/1901.09888, January 29, 2019

26 Lin G, Liang F, Pan W, Ming Z. Fedrec: Federated recommendation with explicit feedback. *IEEE Intelligent Systems*, 2020, **36**(5): 21−30

27 Anelli V W, Deldjoo Y, Di Noia T, Ferrara A, Narducci F. User-controlled federated matrix factorization for recommender systems. *Journal of Intelligent Information Systems*, 2022, **58**(2): 287−309

28 Perifanis V, Efraimidis P S. Federated neural collaborative filtering. *Knowledge-Based Systems*, 2022, **242**: 108441

29 Wu C, Wu F, Cao Y, Huang Y, Xie X. Fedgnn: Federated graph neural network for privacy-preserving recommendation [Online], available: https://arxiv.org/abs/2102.04925, February 9, 2021

30 Han J, Ma Y, Mei Q, Liu X. DeepRec: On-device deep learning for privacy-preserving sequential recommendation in mobile commerce. In: Proceedings of the Web Conference. Virtual Event: 2021. 900−911

31 Liu S, Xu S, Yu W, Fu Z, Zhang Y, Marian A. FedCT: Federated collaborative transfer for recommendation. In: Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval. Virtual Event: 2021. 716−725

32 Liu Z, Yang L, Fan Z, Peng H, Yu P S. Federated social recommendation with graph neural network. *ACM Transaction on Intelligent Systems and Technology*, 2022, **13**(4): 1−24

33 Smith B, Linden G. Two decades of recommender systems at amazon.com. *IEEE Internet Computing*, 2017, **21**(3): 12−18

34 Gomez-Uribe C A, Hunt N. The netflix recommender system: Algorithms, business value, and innovation. *ACM Transactions on Management Information Systems*, 2015, **6**(4): 1−19

35 Resnick P, Iacovou N, Suchak M, Bergstrom P, Riedl J. Grouplens: An open architecture for collaborative filtering of netnews. In: Proceedings of the Conference on Computer Supported Cooperative Work. Chapel Hill, NC, USA: 1994. 175−186

36 Sarwar B, Karypis G, Konstan J, Riedl J. Item-based collaborative filtering recommendation algorithms. In: Proceedings of the 10th International Conference on World Wide Web. Hong Kong, China: 2001. 285−295

37 Deldjoo Y, Di Noia T, Merra F A. Adversarial machine learning in recommender systems: State of the art and challenges. In: Proceedings of the 13th International Conference on Web Search and Data Mining. New York, NY, USA: 2020. 869−872

38 Billsus D, Pazzani M J. Learning collaborative information filters. In: Proceedings of the Fifteenth International Conference on Machine Learning. Madison, Wisconsin, USA: 1998. 46−54

39 He X, Pan J, Jin O, Xu T, Liu B, Xu T, et al. Practical lessons from predicting clicks on ads at facebook. In: Proceedings of the Eighth International Workshop on Data Mining for Online Advertising. New York, NY, USA: 2014. 1−9

40 Koren Y, Bell R, Volinsky C. Matrix factorization techniques for recommender systems. *Computer*, 2009, **42**(8): 30−37

41 Mnih A, Salakhutdinov R R. Probabilistic matrix factorization. In: Proceedings of the Twenty-first Annual Conference on Neural Information Processing Systems. Vancouver, British Columbia, Canada: 2008. 1257−1264

42 Johnson C C. Logistic matrix factorization for implicit feedback data. In: Proceedings of the Annual Conference on Neural Information Processing Systems. Vancouver, British Columbia, Canada: 2014. **27**(78): 1−9

43 Rendle S. Factorization machines. In: Proceedings of the IEEE International Conference on Data Mining. Sydney, Australia: IEEE, 2010. 995−1000

44 Koren Y. Factorization meets the neighborhood: A multi-faceted collaborative filtering model. In: Proceedings of the 14th ACM SIGKDD International Conference on Knowledge discovery and data mining. Las Vegas, Nevada, USA: 2008. 426−434

45 Hu L, Sun A, Liu Y. Your neighbors affect your ratings: On geographical neighborhood influence to rating prediction. In: Proceedings of the 37th International ACM SIGIR Conference on Research & Development in Information Retrieval. Gold Coast, QLD, Australia: 2014. 345−354

46 Li Hui, Ma Xiao-Ping, Shi Jun, Li Cun-Hua, Zhong Zhao-Man, Cai Hong. A recommendation model by means of trust transition in complex network environment. *Acta Automatica Sinica*, 2018, **44**(2): 363−376
(李慧, 马小平, 施珺, 李存华, 仲兆满, 蔡虹. 复杂网络环境下基于信任传递的推荐模型研究. 自动化学报, 2018, **44**(2): 363−376)

47 Rendle S, Freudenthaler C, Gantner Z. BPR: Bayesian personalized ranking from implicit feedback. In: Proceedings of the Twenty-fifth Conference on Uncertainty in Artificial Intelligence. Montreal, Canada: 2009. 452−461

48 Mao K, Zhu J, Wang J, Dai Q, Dong Z, Xiao X, et al. SimpleX: A simple and strong baseline for collaborative filtering. In: Proceedings of the 30th International Conference on Information and Knowledge Management. Virtual Event: 2021. 1243−1252

49 Hsieh C K, Yang L, Cui Y. Collaborative metric learning. In: Proceedings of the 26th International Conference on World Wide Web. Perth, Australia: 2017. 193−201

50 Weimer M, Karatzoglou A, Le Q. Cofirank: Maximum margin matrix factorization for collaborative ranking. In: Proceedings of the 21st Annual Conference on Neural Information Processing Systems. Vancouver, British Columbia, Canada: 2007. 222−230

51 Shi Y, Karatzoglou A, Baltrunas L, Larson M, Oliver N, Hanjalic. Climf: Learning to maximize reciprocal rank with collaborative less-is-more filtering. In: Proceedings of the sixth ACM Conference on Recommender Systems. Dublin, Ireland: 2012. 139−146

52 Liu W, Xi Y, Qin J, Sun F, Chen B, Zhang W, et al. Neural re-ranking in multi-stage recommender systems: A review[Online], available: https://arxiv.org/abs/2202.06602, February 14, 2022

53 Xia F, Liu T Y, Wang J. Listwise approach to learning to rank: Theory and algorithm. In: Proceedings of the 25th International Conference on Machine learning. Helsinki, Finland: 2008. 1192−1199

54 Li Jin-Zhong, Liu Guan-Jun, Yan Chun-Gang, Jiang Chang-Jun. Research advances and prospects of learning to rank. *Acta Automatica Sinica*, 2018, **44**(8): 1345−1369
(李金忠, 刘关俊, 闫春钢, 蒋昌俊. 排序学习研究进展与展望. 自动化学报, 2018, **44**(8): 1345−1369)

55 Sedhain S, Menon A K, Sanner S. Autorec: Autoencoders meet collaborative filtering. In: Proceedings of the 24th International Conference on World Wide Web. Florence, Italy: 2015. 111−112

56 Wu Y, DuBois C, Zheng A X, Ester M. Collaborative denoising auto-encoders for top-n recommender systems. In: Proceedings of the ninth ACM International Conference on Web Search and Data Mining. San Francisco, USA: 2016. 153−162

57 Liang D, Krishnan R G, Hoffman M D. Variational autoencoders for collaborative filtering. In: Proceedings of the 2018 World Wide Web Conference. Lyon, France: 2018. 689−698

58 Hornik K, Stinchcombe M, White H. Multi-layer feedforward networks are universal approximators. *Neural Networks*, 1989, **2**(5): 359−366

59 He X, Liao L, Zhang H, Nie L, Hu X, Chua T S. Neural collaborative filtering. In: Proceedings of the 26th International Conference on World Wide Web. Paris, France: 2017. 173−182

60 Guo H, Tang R, Ye Y. DeepFM: A factorization-machine based neural network for CTR prediction. In: Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence. Melbourne, Australia: 2017. 1725−1731

61 Barkan O, Koenigstein N. Item2vec: Neural item embedding for collaborative filtering. In: Proceedings of the 26th International Workshop on Machine Learning for Signal Processing. Vietri sul Mare, Salerno, Italy: 2016. 1−6

62 Deng Z H, Huang L, Wang C D. Deepcf: A unified framework of representation learning and matching function learning in recommender system. In: Proceedings of the AAAI Conference on Artificial Intelligence. Honolulu, Hawaii, USA: 2019. 61−68

63 Zheng L, Noroozi V, Yu P S. Joint deep modeling of users and items using reviews for recommendation. In: Proceedings of the tenth ACM International Conference on Web Search and Data Mining. Cambridge, UK: 2017. 425−434

64 Tang J, Wang K. Personalized top-n sequential recommendation via convolutional sequence embedding. In: Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining. Marina Del Rey, CA, USA: 2018. 565−573

65 Feng Yong, Chen Yi-Gang, Qiang Bao-Hua. Social and comment text CNN model based automobile recommendation. *Acta Automatica Sinica*, 2019, **45**(3): 518−529
(冯永, 陈以刚, 强保华. 融合社交因素和评论文本卷积网络模型的汽车推荐研究. 自动化学报, 2019, **45**(3): 518−529)

66 Huang J, Zhao W X, Dou H. Improving sequential recommendation with knowledge-enhanced memory networks. In: Proceedings of the 41st International ACM SIGIR Conference on Research & Development in Information Retrieval. Ann Arbor, USA: 2018. 505−514

67 de Souza Pereira Moreira G, Rabhi S, Lee J M. Transformers4Rec: Bridging the gap between NLP and sequential /session-based recommendation. In: Proceedings of the Fifteenth ACM Conference on Recommender Systems. Amsterdam, Netherlands: 2021. 143−153

68 Tim Donkers, Benedikt Loepp, Jurgen Ziegler. Sequential user-based recurrent neural network recommendations. In: Proceedings of the Eleventh ACM Conference on Recommender Systems. Como, Italy: 2017. 152−160

69 Fan W, Ma Y, Li Q, He Y, Zhao E, Tang J, et al. Graph neural networks for social recommendation. In: Proceedings of the World Wide Web Conference. San Francisco, CA, USA: 2019. 417−426

70 Hu J, Qian S, Fang Q. Efficient graph deep learning in tensorflow with TF_geometric. In: Proceedings of the ACM International Conference on Multimedia. Virtual Event: 2021. 3775−3778

71 Wang X, He X, Wang M. Neural graph collaborative filtering. In: Proceedings of the 42nd International ACM SIGIR Conference on Research and development in Information Retrieval. Paris, France: 2019. 165−174

72 Wu L, Sun P, Hong R. Socialgcn: An efficient graph convolutional network based model for social recommendation [Online], available: https://arxiv.org/abs/1811.02815, November 7, 2018

73 Zhang Q, Wang J, Huang H, Huang X, Gong Y. Hashtag recommendation for multimodal microblog using co-attention network. In: Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence. Melbourne, Australia: 2017. 3420−3426

74 Canny J. Collaborative filtering with privacy via factor analysis. In: Proceedings of the 25th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. Tampere, Finland: 2002. 238−245

75 Bilge A, Kaleli C, Yakut I, Gunes I, Polat H. A survey of privacy-preserving collaborative filtering schemes. *International Journal of Software Engineering and Knowledge Engineering*, 2013, **23**(8): 1085−1108

76 Hu G, Yang Q. PrivNet: Safeguarding private attributes in transfer learning for recommendation. In: Proceedings of the Findings of the Conference on Empirical Methods in Natural Language Processing. Virtual Event: 2020. 4506−4516

77 Zhou Jun, Dong Xiao-Lei, Cao Zhen-Fu. Research advances on privacy preserving in recommender systems. *Journal of Computer Research and Development*, 2019, **56**: 2033−2048
(周俊, 董晓蕾, 曹珍富. 推荐系统的隐私保护研究进展. 计算机研究与发展, 2019, **56**: 2033−2048)

78 Chang C C, Thompson B, Wang H. Towards publishing recommendation data with predictive anonymization. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing, China: 2010. 24−35

79 Sakuma J, Osame T. Recommendation with k-anonymized ratings. *Transactions on Data Privacy*, 2018, **11**(1): 47−60

80 Ruoxuan Wei, Hui Tian, Hong Shen. Improving k-anonymity based privacy preservation for collaborative filtering. *Computers & Electrical Engineering*, 2018, **67**: 509−519

81 Weinsberg U, Bhagat S, Ioannidis S. BlurMe: Inferring and obfuscating user gender based on ratings. In: Proceedings of the sixth ACM Conference on Recommender Systems. Dublin, Ireland: 2012. 195−202

82 Parra-Arnau J, Rebollo-Monedero D, Forné J. Optimal forgery and suppression of ratings for privacy enhancement in recommendation systems. *Entropy*, 2014, **16**(3): 1586−1631

83 McSherry F, Mironov I. Differentially private recommender systems: Building privacy into the netflix prize contenders. In: Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. Paris, France: 2009. 627−636

84 Jorgensen Z, Yu T. A privacy-preserving framework for personalized, social recommendations. In: Proceedings of the 17th International Conference on Extending Database Technology. Athens, Greece: 2014. 582

85 Jingyu H, Chang X, Sheng Z. Differentially private matrix factorization. In: Proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence. Buenos Aires, Argentina: 2015. 1763−1770

86 Zhu X, Sun Y. Differential privacy for collaborative filtering recommender algorithm. In: Proceedings of the 2016 ACM on International Workshop on Security And Privacy Analytics. New Orleans, LA, USA: 2016. 9−16

87 Shin H, Kim S, Shin J. Privacy enhanced matrix factorization for recommendation with local differential privacy. *IEEE Transactions on Knowledge and Data Engineering*, 2018, **30**(9): 1770−1782

88 Chaochao C, Liang L, Bingzhe W. Secure social recommendation based on secret sharing. In: Proceedings of the 24th European Conference on Artificial Intelligence. Santiago de Compostela, Spain: 2020. 506−512

89 Shmueli E, Tassa T. Mediated secure multi-party protocols for collaborative filtering. *ACM Transactions on Intelligent Systems and Technology*, 2020, **11**(2): 1−25

90 Jinsu K, Dongyoung K, Yuna K, Hyunsoo Y, Junbum S, Sungwook K. Efficient privacy-preserving matrix factorization for recommendation via fully homomorphic encryption. *ACM Transactions on Privacy and Security*, 2018, **21**(4): 1−17

91 Goodfellow I J, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. In: Proceedings of the 3rd International Conference on Learning Representations. San Diego, CA, USA, 2015.

92 He X, He Z, Du X, Chua T S. Adversarial personalized ranking for recommendation. In: Proceedings of the 41st International ACM SIGIR Conference on Research & Development in Information Retrieval. Ann Arbor, MI, USA: 2018. 355−364

93 Li K, Luo G, Ye Y. Adversarial privacy-preserving graph embedding against inference attack. *IEEE Internet of Things Journal*, 2020, **8**(8): 6904−6915

94 Xiao T, Tsai Y H, Sohn K. Adversarial learning of privacy-preserving and task-oriented representations. In: Proceedings of the AAAI Conference on Artificial Intelligence. New York, USA: 2020. 12434−12441

95 Kairouz P, McMahan H B, Avent B. Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*. **14**(1−2): 1−210

96 Li Q, Wen Z, Wu Z, Hu S, Wang N, Li Y, et al. A survey on federated learning systems: Vision, hype and reality for data privacy and protection[Online], available: https://arxiv.org/abs/1907.09693, July 23, 2019

97 Yang Q, Liu Y, Chen T. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, 2019, **10**(2): 1−19

98 Mireshghallah F, Taram M, Vepakomma P, Singh A, Raskar R, Esmaeilzadeh H. Privacy in deep learning: A survey [Online], available: https://arxiv.org/abs/2004.12254, April 25, 2020

99 Dwork C, Roth A, Others. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 2014, **9**(3−4): 211−407

100 Rebollo-Monedero D, Parra-Arnau J, Forné J. An information-theoretic privacy criterion for query forgery in information retrieval. In: Proceedings of the International Conference on Security Technology. Jeju Island, Korea: 2011. 146−154

101 Mo F, Shamsabadi A S, Katevas K. Darknetz: Towards model privacy at the edge using trusted execution environments. In: Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services. Toronto, Canada: 2020. 161−174

102 Gupta O, Raskar R. Distributed learning of deep neural network over multiple agents. *Journal of Network and Computer Applications*, 2018, **116**: 1−8

103 Chong C, Fei S, Min Z, Bolin D. Recommendation unlearning. In: Proceedings of the ACM Web Conference. Virtual Event: 2022. 2768−2777

104 Zhang M, Sapra K, Fidler S, Yeung S, Alvarez J M. Personalized federated learning with first order model optimization. In: Proceedings of the 9th International Conference on Learning

Representations. Virtual Event. 2021.

105 Liu B, Guo Y, Chen X. PFA: Privacy-preserving federated adaptation for effective model personalization. In: Proceedings of the Web Conference. Ljubljana, Slovenia: 2021. 923−934

106 Collins L, Hassani H, Mokhtari A, Shakkottai S. Exploiting shared representations for personalized federated learning. In: Proceedings of the 38th International Conference on Machine Learning. Virtual Event: 2021. 2089−2099

107 Muhammad K, Wang Q, Reilly-Morgan D, Tragos E, Smyth B, Hurley N, et al. Fedfast: Going beyond average for faster training of federated recommender systems. In: Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. Virtual Event: 2020. 1234−1242

108 Khan F K, Flanagan A, Tan K E. A payload optimization method for federated recommender systems. In: Proceedings of the Fifteenth ACM Conference on Recommender Systems. Amsterdam, Netherlands: 2021. 432−442

109 Yi J, Wu F, Wu C, Liu R, Sun G, Xie X. Efficient-FedRec: Efficient federated learning framework for privacy-preserving news recommendation. In: Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing. Virtual Event: 2021. 2814−2824

110 Zhang H, Luo F, Wu J, He X, Li Y. LightFR: Lightweight federated recommendation with privacy-preserving matrix factorization [Online], available: https://arxiv.org/abs/2206.11743, June 23, 2022

111 Lin Y, Ren P, Chen Z. Meta matrix factorization for federated rating predictions. In: Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval. Virtual Event: 2020. 981−990

112 Wang Q, Yin H, Chen T, Yu J, Zhou A, Zhang X. Fast-adapting and privacy-preserving federated recommender system. *The VLDB Journal*, 2021: 1−20

113 Wu J, Liu Q, Huang Z, Ning Y, Wang H, Chen E, et al. Hierarchical personalized federated learning for user modeling. In: Proceedings of the Web Conference. Virtual Event: 2021. 957−968

114 Chen Ming, Zhang Lei, Ma Tian-Yi. Recommendation approach based on attentive federated distillation. *Journal of Software*, 2021, **32**(12): 3852−3868
(谌明, 张蕾, 马天翼. 一种基于注意力联邦蒸馏的推荐方法. 软件学报, 2021, **32**(12): 3852−3868)

115 Liang F, Pan W, Ming Z. FedRec++: Lossless federated recommendation with explicit feedback. In: Proceedings of the AAAI Conference on Artificial Intelligence. Virtual Event: 2021. 4224−4231

116 Ning L, Singhal K, Zhou E X. Learning federated representations and recommendations with limited negatives[Online], available: https://arxiv.org/abs/2108.07931, August 18, 2021

117 Flanagan A, Oyomno W, Grigorievskiy A, Tan K E, Khan S A, Ammad-Ud-Din M. Federated multi-view matrix factorization for personalized recommendations. In: Proceedings of European Conference on Machine Learning and Knowledge Discovery in Databases. Ghent, Belgium: 2020. 324−347

118 Saikishore Kalloori, Severin Klingler. Horizontal cross-silo federated recommender systems. In: Proceedings of the Fifteenth ACM Conference on Recommender Systems. Amsterdam, Netherlands: 2021. 680−684

119 Minto L, Haller M, Livshits B. Stronger privacy for federated collaborative filtering with implicit feedback. In: Proceedings of the Fifteenth ACM Conference on Recommender Systems. Amsterdam, Netherlands: 2021. 342−350

120 Chai D, Wang L, Chen K, Yang Q. Secure federated matrix factorization. *IEEE Intelligent Systems*, 2020, **36**(5): 11−20

121 Yang L, Tan B, Liu B, Zheng V W, Chen K, Yang Q. Practical and secure federated recommendation with personalized masks [Online], available: https://arxiv.org/abs/2109.02464, Au-gust 18, 2021

122 Lin Z, Pan W, Ming Z. FR-FMSS: Federated recommendation via fake marks and secret sharing. In: Proceedings of the Fifteenth ACM Conference on Recommender Systems. Amsterdam, Netherland: 2021. 668−673

123 Li T, Song L, Fragouli C. Federated recommendation system via differential privacy. In: Proceedings of the IEEE International Symposium on Information Theory. Los Angeles, USA: IEEE, 2020. 2592−2597

124 Müllner P, Kowald D, Lex E. Robustness of meta matrix factorization against strict privacy constraints. In: Proceedings of the 43rd European Conference on Information Retrieval Research. Virtual Event: 2021. 107−119

125 Zhang S, Yin H, Chen T. PipAttack: Poisoning federated recommender systems for manipulating item promotion. In: Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining. New York, USA: 2022. 1415−1423

126 Jiang Y, Zhou Y, Wu D, Li C, Wang Y. On the detection of shilling attacks in federated collaborative filtering. In: Proceedings of the 2020 International Symposium on Reliable Distributed Systems. Shanghai, China: IEEE, 2020. 185−194

127 Chen C, Zhang J, Tung A K, Kankanhalli M, Chen G. Robust federated recommendation system [Online], available: https://arxiv.org/abs/2006.08259, June 15, 2020

128 Wu C, Wu F, Qi T, Huang Y, Xie X. FedAttack: Effective and covert poisoning attack on federated recommendation via hard sampling [Online], available: https://arxiv.org/abs/2202.04975, February 10, 2022

129 Orekondy T, Oh S J, Zhang Y, Schiele B, Fritz M. Gradient-leaks: Understanding and controlling deanonymization in federated learning [Online], available: https://arxiv.org/abs/1805.05838, May 15, 2018

130 Hospedales T, Antoniou A, Micaelli P, Storkey A. Meta-learning in neural networks: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, DOI: 10.1109/TPAMI.2021.3079209

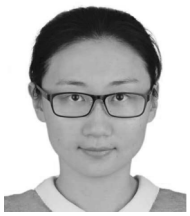
131 Wang Z, Song M, Zhang Z, Song Y, Wang Q, Qi H. Beyond inferring class representatives: User-level privacy leakage from federated learning. In: Proceedings of the IEEE Conference on Computer Communications. Paris, France: IEEE, 2019. 2512−2520

132 He X, Jia J, Backes M, Gong N Z, Zhang Y. Stealing links from graph neural networks. In: Proceedings of the 30th USENIX Security Symposium. Virtual Event: 2021. 2669−2686

张洪磊 北京交通大学计算机与信息技术学院博士研究生. 主要研究方向为推荐系统与隐私保护.
E-mail: honglei.zhang@bjtu.edu.cn
(**ZHANG Hong-Lei** Ph.D. candidate at the School of Computer and Information Technology, Beijing Jiaotong University. His research interest covers recommender systems and privacy protection.)

李浥东 北京交通大学计算机与信息技术学院教授. 主要研究方向为大数据分析与安全, 数据隐私保护与先进计算. E-mail: ydli@bjtu.edu.cn
(**LI Yi-Dong** Professor at the School of Computer and Information Technology, Beijing Jiaotong University. His research interest covers big data analysis and security, data privacy protection, and advanced computing.)

邬 俊 北京交通大学计算机与信息技术学院副教授. 主要研究方向为信息检索与推荐系统.
E-mail: wuj@bjtu.edu.cn
(**WU Jun** Associate professor at the School of Computer and Information Technology, Beijing Jiaotong University. His research interest covers information retrieval and recommender systems.)



陈乃月 北京交通大学计算机与信息技术学院讲师. 主要研究方向为社交网络, 数据挖掘与联邦学习. 本文通信作者. E-mail: nychen@bjtu.edu.cn
(**CHEN Nai-Yue** Lecturer at the School of Computer and Information Technology, Beijing Jiaotong University. Her research interest covers social networks, data mining, and federated learning. Corresponding author of this paper.)

董海荣 北京交通大学轨道交通控制与安全国家重点实验室教授. 主要研究方向为列车运行智能控制与优化和调度控制一体化.
E-mail: hrdong@bjtu.edu.cn
(**DONG Hai-Rong** Professor at the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University. Her research interest covers intelligent control and optimization of train operation, and integration of scheduling and control.)