

一种基于子序列的隐私保护多行为序列推荐方法

关浩荣 潘微科 明 仲

(深圳大学计算机与软件学院 广东 深圳 518060)

摘 要 随着互联网的飞速发展与大数据时代的到来,推荐系统在电子商务、社交媒体和短视频平台等众多领域愈发重要,成为解决信息过载、提升用户体验的重要手段。在实际应用场景中,用户历史交互数据具有多行为性和序列性等特征,以电商领域为例,用户通常会通过浏览、收藏和购买等行为与物品产生交互。相较于只考虑单一行为类型的传统推荐方法,融合多种行为类型与序列信息的推荐方法能更全面地理解用户偏好,进而提供更贴合用户兴趣的个性化推荐。随着我国《中华人民共和国个人信息保护法》和欧盟《通用数据保护条例》等隐私法规的出台,用户隐私意识随之提升,推荐系统需在严格合规的前提下精准挖掘多行为序列中的用户偏好,而多行为序列中不同交互行为间存在复杂的时序关联,联邦多行为序列推荐(Federated Multi-Behavior Sequential Recommendation, FMBSR)由此面临双重挑战:一方面,需解决多行为序列信息建模难题,以有效捕捉用户动态偏好;另一方面,FMBSR 虽可规避数据集中存储的隐私风险,但如何实现隐私保护与推荐性能的平衡,仍是其落地应用的主要障碍。为此,本文提出以可解释性强的协同过滤为核心框架的基于子序列的隐私保护协同推荐方法(Subsequence-based Privacy-preserving Collaborative Recommendation, SPCR),该方法主要包含三个模块:(1)密钥初始化:采用对称与非对称加密相结合的方式,为后续全流程隐私保护奠定基础;(2)计算相似度:设计兼具序列信息与多行为信息感知的相似度度量机制,将多行为序列信息融入用户相似度度量,提升相似度计算准确性;(3)预测评分:设计近期行为模式一致性模块,捕捉用户购买不同目标物品前的行为模式差异,动态调节相似度以适配目标物品。在 JD 和 UB 两个真实数据集上的实验表明,SPCR 兼具推荐性能与隐私保护的优势。相较于无隐私保护的方法,它优于 FLAG、NextIP 等基线模型,与 GEAR 相当;相较于 FedPerGNN、LP-GCN 等隐私保护类方法,它在推荐性能上具有显著优势。在 JD 数据集上,SPCR 性能略低于 GEAR,其 $Rec@10$ 为 0.1981、 $NDCG@10$ 为 0.1114,较次优基线 NextIP 分别提高约 10.86% 和 9.42%;在 UB 数据集上,SPCR 在 $Rec@10$ 上优于 GEAR,它的结果($Rec@10=0.0932$ 和 $NDCG@10=0.0604$)较次优基线 FLAG 分别提高约 4.48% 和 7.67%。同时,SPCR 与未结合隐私保护的中心化方法(SCR)在 $Rec@10$ 和 $NDCG@10$ 上结果完全一致,验证了隐私保护方案的无损性。SPCR 是 FMBSR 领域第一个实现多行为序列精准建模、隐私安全、性能无损与可解释性强的方法,在隐私保护、推荐性能与可解释性等方面取得了有效平衡。

关键词 联邦推荐;多行为序列推荐;协同推荐;用户相似度;隐私保护

中图法分类号 TP311

DOI 号 10.11897/SP.J.1016.2026.02111

A Subsequence-Based Privacy-Preserving Multi-Behavior Sequential Collaborative Recommendation Method

GUAN Hao-Rong PAN Wei-Ke MING Zhong

(College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, Guangdong 518060)

Abstract With the development of the Internet, and the advent of the big data era, recommender systems have become increasingly important in numerous fields such as e-commerce, social media, and short-video platforms, and have become an important means to address information overload and enhance user experience. In practical application scenarios, users' historical interac-

收稿日期:2025-09-18;在线发布日期:2026-03-23。本课题得到国家自然科学基金(Nos. 62461160311, 62272315)资助。关浩荣,硕士研究生,主要研究领域为推荐系统、联邦学习。E-mail:2400101025@mails.szu.edu.cn。潘微科(通信作者),博士,教授,中国计算机学会(CCF)会员,主要研究领域为推荐系统、深度学习、迁移学习、联邦学习。E-mail:panweike@szu.edu.cn。明 仲,博士,教授,中国计算机学会(CCF)会员,主要研究领域为软件工程、人工智能。

tion data have characteristics such as multi-behaviorality and sequentiality. Taking the e-commerce field as an example, users usually interact with items through behaviors such as browsing, collecting, and purchasing. Compared with traditional recommendation methods that only consider a single behavior type, recommendation methods that integrate multi-behavior types and sequential information can more comprehensively understand user preferences, thereby providing personalized recommendations that are more in line with users' interests. With the introduction of privacy regulations such as the "Personal Information Protection Law of the People's Republic of China" and the "European Union's General Data Protection Regulation", users' awareness of privacy has correspondingly increased. Recommender systems are required to accurately mine user preferences in multi-behavior sequences under the premise of strict compliance, while there are complex temporal correlations between different interactive behaviors in multi-behavior sequences, so federated multi-behavior sequential recommendation (FMBSR) thus faces dual challenges: on the one hand, it is necessary to address the difficulty of multi-behavior sequential information modeling to effectively capture user preferences; on the other hand, although FMBSR can avoid the privacy risks associated with centralized data storage, how to achieve a balance between privacy protection and recommendation performance remains a key obstacle to its practical application. To this end, this paper proposes a subsequence-based privacy-preserving collaborative recommendation method (SPCR) with a core framework of collaborative filtering featuring strong interpretability. The method consists of three main components: (1) Key Initialization: A combination of symmetric and asymmetric encryption is adopted to lay the foundation for subsequent full-process privacy protection; (2) Similarity Calculation: A similarity measurement mechanism that is both aware of sequential information and multi-behavior information is designed to integrate multi-behavior sequence information into user similarity measurement and improve the accuracy of similarity calculation; (3) Prediction Scoring: A recent behavior pattern consistency module is designed to capture the differences in behavior patterns of users before purchasing different target items and dynamically adjust the similarity to adapt to the target items. Experiments on two real-world datasets, i. e. , JD and UB, demonstrate that SPCR possesses the advantage of balancing recommendation performance and privacy protection. Compared with privacy-unprotected methods, it outperforms baseline models such as FLAG and NextIP and performs comparable with GEAR; and compared with privacy-preserving methods like FedPerGNN and LP-GCN, it achieves more superior recommendation performance. On the JD dataset, SPCR's performance is slightly lower than GEAR, with $Rec@10=0.1981$ and $NDCG@10=0.1114$, representing improvements of approximately 10.86% and 9.42% respectively compared to the second-best baseline NextIP. On the UB dataset, SPCR outperforms GEAR on $Rec@10$, and its results ($Rec@10=0.0932$ and $NDCG@10=0.0604$) outperform the second-best baseline FLAG by approximately 4.48% and 7.67%, respectively. Moreover, the results of our SPCR and its centralized version SCR without privacy protection are completely consistent on $Rec@10$ and $NDCG@10$, verifying the losslessness of the privacy protection scheme. Our SPCR is the first method in FMBSR with accurate multi-behavior sequential modeling, privacy security, lossless performance, and strong interpretability, achieving an effective balance between privacy protection, recommendation performance, and interpretability.

Keywords federated recommendation; multi-behavior sequential recommendation; collaborative recommendation; user similarity; privacy protection

1 引言

随着互联网的飞速发展与大数据时代的到来,推荐系统在电子商务^[1]、社交媒体^[2]和短视频平台^[3]等众多领域发挥着不可替代的作用。面对信息过载的难题,推荐系统可以有效地帮助用户筛选出他们真正感兴趣的信息,显著提升用户体验。

在实际应用中,用户的历史交互数据具有多行为性和序列性等特征。以电子商务领域为例,用户通常会通过浏览、收藏、添加购物车和购买等多种行为与物品产生交互。相较于只考虑单一行为类型的方法,融合多种行为类型的方法能更加全面地理解用户偏好,从而提供更贴合用户兴趣的个性化推荐。此外,用户偏好也并非一成不变,而是随时间动态变化并呈现出序列性特征。近年来,多行为序列推荐(Multi-Behavior Sequential Recommendation, MB-SR)已然成为一个热门的研究方向,其核心是利用用户历史交互的序列信息,预测用户下一时刻可能会交互的物品。

协同过滤^[4]是推荐领域的经典方法,与深度学习方法相比,其核心优势在于更强的可解释性——通过计算用户或物品间的相似度即可实现个性化推荐,逻辑直观且结果可追溯。在相似度度量中,杰卡德指数是常用的指标。传统的协同过滤方法仅基于一种行为类型来计算相似度,且未考虑序列信息。Zeng 等人^[5]提出的基于双向物品相似度的协同过滤推荐方法(Bidirectional Item Similarity, BIS),通过双向物品相似度捕捉序列模式,适用于单行为序列推荐场景。但在多行为序列推荐领域,目前仍缺乏能有效捕捉多行为序列信息的协同过滤方法。

随着我国的《中华人民共和国个人信息保护法》^[6]和欧盟的《通用数据保护条例》(General Data Protection Regulation, GDPR)等隐私保护法规的出台^[7-8],用户的隐私意识日益增强。传统的多行为序列推荐在用户隐私保护方面存在明显不足,无法满足这些法规的要求。联邦学习作为一种分布式机器学习框架,允许参与方在本地保留数据,仅通过参数交互完成模型训练,为隐私保护推荐系统提供了新的解决方案。然而,现有的联邦推荐方法大多侧重单行为推荐或通用推荐场景,缺乏对多行为序列中“辅助行为-目标行为”的语义关联及时序递进关系的针对性处理。因此,能够在保护用户隐私的同时有效挖掘多行为序列信息的联邦多行为序列推荐

(Federated MBSR, FMBSR),正逐渐成为推荐系统领域一个重要的新兴研究方向。

联邦多行为序列推荐面临两大挑战:第一个挑战是行为序列信息与多行为信息建模难题。一方面,辅助行为(浏览、收藏等)与购买行为间的“偏好探索-最终决策”递进关系隐含于交互序列中,传统方法缺乏有效的结构化划分手段以精准刻画这一关联,且难以量化用户兴趣的时间衰减特性,导致用户行为模式捕捉存在偏差;另一方面,传统协同过滤仅基于相同行为类型的物品计算用户相似度,忽略了“浏览-购买”等跨行为关联对用户偏好的影响,无法捕捉多行为场景下用户相似度的语义差异;此外,传统评分预测采用静态相似度加权方式,针对同一对邻居与不同目标物品的场景,仍累加相同的相似度,无法适配用户购买不同目标物品前的行为模式差异,制约推荐性能提升。综上,如何实现行为序列特性与多行为信息的协同建模是精准捕捉用户偏好、提升推荐精度的关键。第二个挑战是隐私保护与推荐性能的平衡难题。在隐私保护方面,需确保用户历史交互序列的安全性,在相似度计算、预测评分等全过程通信中严格避免隐私泄露,防止用户数据被服务器或其他客户端获取;在性能方面,需保证引入隐私保护机制后,推荐性能没有显著下降,与非联邦的集中式推荐方法相当。传统方法往往难以兼顾二者,要么隐私保护措施不完善导致数据泄露风险,要么过度强调隐私保护而牺牲推荐性能,如何实现隐私安全与性能无损的有效平衡,成为联邦推荐场景落地的主要障碍。

随着深度学习技术的快速发展,推荐系统领域的研究多以该技术为核心支撑。这类方法虽能建模复杂的行为关联,却普遍存在可解释性弱的问题,不利于实际场景落地。而协同过滤作为经典推荐范式,与深度学习方法相比具有更强的可解释性,其相似度计算逻辑直观、结果可追溯。因此,为在解决上述联邦多行为序列推荐两大挑战的同时兼顾这一强可解释性优势,本文提出了一种联邦多行为序列推荐方法,即基于子序列的隐私保护协同推荐方法(Subsequence-based Privacy-preserving Collaborative Recommendation, SPCR)。该方法包含了三个主要模块:密钥初始化、计算相似度和预测评分。具体而言,针对第一个挑战,在计算相似度前,本文先基于购买行为将用户原始序列划分成若干子序列,参考遗忘曲线^[9-10]设计双层时间衰减函数,量化序列中物品所表征的偏好与用户当前偏好的关联程

度,并通过归一化消除序列长度差异的影响;随后改进杰卡德指数所构建的用户相似度公式,融合同行为与跨行为的关联信息,提高用户相似度计算的准确性;最终在预测阶段引入动态调整机制,结合目标物品动态调整用户相似度。针对第二个挑战,本文以密钥初始化为基础,采用对称与非对称加密技术^[11-14]相结合的方案,实现从密钥初始化到预测评分的全过程无损隐私保护,有效防止用户数据向服务器及其他客户端泄露,同时确保推荐性能与非联邦的集中式方法相当,实现隐私安全与推荐性能的平衡。

本文的主要贡献如下:

(1)提出了 FMBSR 领域第一个实现多行为序列精准建模、隐私安全、性能无损与可解释性强的方法。该方法在保护隐私安全的同时,推荐性能优于或接近非联邦集中式的多行为序列推荐方法。

(2)提出了兼具序列信息与多行为信息感知的相似度度量及动态预测机制,将多行为序列信息融入用户相似度度量。预测评分阶段引入近期行为模式一致性模块,捕捉用户购买不同目标物品前的行为模式差异,动态调节邻居相似度对预测结果的影响,提升推荐精度。

(3)通过对称与非对称加密相结合的方式,在密钥初始化阶段保证共享密钥的安全;同时,在保证计算相似度、预测评分等主要模块顺畅推进的前提下,有效避免用户隐私敏感信息泄露,最终实现全过程无损的隐私保护。

(4)通过理论分析证明了 SPCR 隐私保护的安全性,并从理论与实验两方面验证了其无损性。在 JD 和 UB 数据集上的实验结果表明,SPCR 的推荐性能优于现有绝大多数基线模型,平均性能提升显著,实现了隐私保护、推荐性能与可解释性的有效平衡。

2 相关工作

2.1 单行为序列推荐

单行为序列推荐是序列建模的基础,致力于挖掘单一交互行为(如购买)的序列特征,核心目标在于平衡用户长期偏好与短期动态需求。早期研究多以马尔可夫链为核心技术框架,重点捕捉序列中物品间的依赖关系。Rendle 等人^[15]提出个性化马尔可夫链分解模型(Factorized Personalized Markov Chains, FPMC),通过分解个性化转移矩阵,将矩阵

分解与一阶马尔可夫链结合,实现下一个购物篮推荐。He 等人^[16]则在此基础上进一步提出基于相似度与高阶马尔可夫链融合的模型(Factorized Sequential Prediction with Item Similarity Models, Fossil),通过融合基于相似度的基础模型与高阶马尔可夫链,并引入个性化权重学习机制,增强对稀疏数据的适应性,从而更全面地捕捉用户长期偏好与短期动态。

随着深度学习技术的快速发展,基于神经网络的建模方法逐渐成为该领域的主流。Tang 等人^[17]提出卷积序列嵌入推荐模型(Convolutional Sequence Embedding Recommendation Model, Caser),将用户近期交互行为建模为时间与潜在空间交织的图像结构,利用水平与垂直卷积滤波器来学习丰富的序列模式,从而捕捉用户兴趣。Hidasi 等人^[18]提出基于门控循环单元的会话推荐模型(Gated Recurrent Unit for Recommendation, GRU4Rec),采用门控循环单元(GRU)来获取用户表示,同时利用会话并行小批量来加速训练。针对长序列依赖与计算效率问题,Kang 等人^[19]提出自注意力序列推荐模型(Self-Attentive Sequential Recommendation, SASRec),引入自注意力机制,自适应为历史行为分配权重,兼顾长期偏好捕捉与并行计算效率,成为长序列推荐的核心基准。

然而,上述单行为序列推荐方法均仅聚焦单一交互行为建模,无法有效刻画用户从“浏览探索”到“购买决策”的多行为递进过程,难以满足复杂场景的偏好刻画需求。

2.2 多行为序列推荐

为解决单行为序列推荐无法充分捕捉用户多行为序列信息的核心问题,多行为序列推荐应运而生,成为序列推荐领域的重要发展方向。其存在两大核心挑战:一是“行为异质性”,即浏览、收藏、购买等不同行为存在显著语义差异;二是“时序递进性”,需有效捕捉从辅助行为到目标行为的关联。

围绕这两大核心挑战,研究者们展开了一系列技术创新。Li 等人^[20]提出行为密集型神经网络模型(Behavior-Intensive Neural Network, BINN),构建双路径框架:一方面通过会话行为学习精准建模用户短期动机,另一方面借助双向偏好行为学习深度捕捉长期偏好,最终实现长短周期用户偏好的有效融合。Zhou 等人^[21]在行为粒度刻画上进一步深化,提出基于微行为的推荐模型(Recommendation Framework from the Micro Behavior Perspective,

RIB)。该模型围绕停留时间、点击来源等细粒度微行为,将物品嵌入、行为类型嵌入与停留时间嵌入拼接后输入门控循环单元,同时引入注意力机制区分不同微行为的重要性权重,显著提升了用户偏好建模的精准度。

为更精准地处理行为异质性与时序动态的耦合问题,Liu 等人^[22]提出递归对数双线性模型(Recurrent Log-Bilinear Model, RLBL),该模型结合递归结构与对数双线性模型,通过行为特定转移矩阵区分不同行为的语义差异,同时利用位置特定矩阵捕捉短期上下文信息,大幅增强了对时序动态的适应性。He 等人^[23]提出反馈感知的局部和全局模型(Feedback-aware Local and Global Model, FLAG),借助自注意力机制,设计反馈感知自注意力块、位置注意力层和反馈感知注意力层,分别捕捉局部偏好、全局偏好和当前意图,再通过门控机制实现多维度偏好的融合,其整体效率显著优于传统推荐方法。此外,针对多行为数据普遍存在的稀疏性问题,Luo 等人^[24]提出基于双任务学习的多行为序列推荐模型(Next-item and Purchase Prediction Framework, NextIP)。该模型采用双任务学习框架:通过目标行为感知上下文聚合器引导多行为子序列间的知识转移,同时利用行为感知自注意力提取负样本信息,强化购买偏好的学习。

然而,上述多行为序列推荐方法均基于集中式架构设计,需收集用户完整交互序列,存在隐私泄露风险,难以适配《中华人民共和国个人信息保护法》和《通用数据保护条例》等隐私保护法规要求。

2.3 联邦推荐

多行为序列推荐等集中式方法存在隐私泄露^[25]问题,联邦推荐^[26-27]的发展较好地解决了推荐系统领域隐私保护问题。联邦推荐在确保用户数据始终留存本地、不对外传输的前提下,通过分布式节点协同完成全局推荐模型的训练。当前研究主要围绕传统推荐模型的联邦化改造与“隐私保护-推荐性能”的平衡优化两大方向展开,为多行为序列推荐的隐私保护需求提供了基础技术支撑。

针对显式反馈任务,Lin 等人^[28]提出基于虚拟评分填充的联邦推荐框架(Federated Recommendation with Explicit Feedback, FedRec),通过用户平均和混合填充策略为未评分物品分配虚拟评分,在避免真实评分行为与数值泄露的同时,解决数据稀疏性问题。在此基础上,Liang 等人^[29]进一步提出引入去噪客户端的联邦推荐框架(Lossless Fed-

erated Recommendation with Explicit Feedback, FedRec++),通过匿名噪声的分布式发送与聚合,有效消除虚拟评分带来的噪声干扰,最终实现推荐性能无损伤并降低跨节点通信成本。

针对隐式反馈任务,Lin 等人^[30]聚焦隐私保护范围的扩展,提出基于虚假标记与秘密共享的通用联邦推荐框架(Federated Recommendation via Fake Marks and Secret Sharing, FR-FMSS),借助虚假标记(fake marks)与秘密共享(secret sharing)技术,将隐私保护维度从基础交互行为延伸至评分值、序列位置等关键标识符,实现多个推荐任务兼容且性能无损。Wu 等人^[31]针对图卷积推荐的隐私痛点,提出无损隐私保护图卷积网络(Lossless and Privacy-Preserving Graph Convolution Network for Federated Item Recommendation, LP-GCN),通过混合加密物品 ID 与虚拟物品策略,解决图卷积推荐中子图扩展引发的隐私泄露问题,同时设计嵌入同步机制确保图卷积信息的无损传播,最终使模型性能与集中式图卷积推荐方法相当。而针对多行为场景下用户数据的异质性问题,Li 等人^[32]提出基于加性个性化的联邦推荐方法(Federated Recommendation with Additive Personalization, FedRAP),通过引入加性个性化算法管理多样化用户行为的数据异质性,同时兼顾物品的独特属性与共享特征,进一步提升模型适配性与推荐性能。

然而,现有联邦推荐方法大多侧重单行为为推荐或通用推荐场景,缺乏对多行为序列中“辅助行为-目标行为”的语义关联及时序递进关系的针对性处理。少数尝试兼容多行为的方法,又难以在严格保护用户历史交互序列隐私的前提下,确保推荐性能无损耗,最终无法兼顾多行为序列精准建模、隐私安全与性能无损。这一现状凸显了设计新方法的迫切性——该方法需同时实现多行为序列模式的精准捕捉、用户交互序列的严格隐私保护和推荐性能的无损保障,以及强可解释性的有效兼顾。而这正是本文提出基于子序列的隐私保护协同推荐方法(SPCR)的核心动机。

2.4 基于加密技术的隐私保护推荐

相较于其他联邦推荐方法,基于加密技术的隐私保护推荐具有隐私保护更全面彻底、推荐性能无损的优势。Kim 等人^[33]提出基于全同态加密的隐私保护矩阵分解推荐框架(Efficient Privacy-Preserving Matrix Factorization via FHE, EPPMF-FHE),融合全同态加密、新型向量拼接与聚合数据结构及安

全二方计算技术,将隐私保护维度从基础用户评分延伸至用户、物品嵌入及推荐系统调优参数,最终实现矩阵分解完整迭代收敛,且推荐准确性无损。

常见的加密技术主要分为对称加密与非对称加密两类,二者在密钥使用逻辑、性能及安全性上各具特点。对称加密使用相同的密钥对数据进行加密和解密,发送方与接收方需共同持有该密钥才可完成正常通信。其具有运算速度快、效率高的特点,适用于处理大量数据。但短板也十分突出,密钥需在双方间共享,密钥的安全分发与管理面临较大挑战,容易成为隐私泄露的风险点。与对称加密不同,非对称加密采用“公钥加密-私钥解密”的密钥分离机制,公钥可公开共享,私钥则由接收方单独保管,这一特性从根源上解决了对称加密的密钥分配难题,安全性更具保障。但受限于复杂的加密算法,非对称加密存在计算量庞大、运算速度较慢的问题,不适用于大规模推荐场景。现存基于加密技术的隐私保护推荐方法多数依赖单一加密技术,难以兼顾推荐效率与隐私保护。

基于上述两类加密技术的特点,使用对称与非对称加密技术相结合的方式可以有效规避单一技术的局限性,实现优势互补。具体而言,先通过非对称加密技术对对称加密的共享密钥进行加密保护,并分发到各个通信方,确保共享密钥在传输过程中不被泄露;在后续通信中,发送方利用共享密钥对敏感信息进行加密,实现机密通信。该融合方案既充分发挥了对称加密运算速度快、适配海量数据的优势,又借助非对称加密解决了对称加密的密钥安全问

题,兼顾了推荐服务的高效性与隐私保护。

3 方 法

3.1 问题定义

在联邦多行为序列推荐(Federated Multi-Behavior Sequential Recommendation, FMBSR)中,每个用户 $u \in \mathcal{U}$ 都有一条历史交互序列 $S_u = \{(i_u^1, b_u^1), \dots, (i_u^L, b_u^L)\}$, 其中, i_u^l 是用户 u 在 l 时刻交互的物品,对应的行为类型为 b_u^l , $\mathcal{U}$ 是全部用户集合。用户对物品的行为类型可以用 e, c, f 和 p 表示,分别代表浏览、添加购物车、收藏和购买(为了方便说明本方法,本文使用电商领域作为例子。此外,本方法还可以应用到其他多行为领域)。这些行为与对应物品的时序交互构成历史交互序列 S_u , 其不仅表示用户的交互历史,还隐含了个人的行为模式(如消费能力、兴趣变化等)。因此,该问题需要保护的隐私是每个用户对应的历史交互序列。本文的目标是在保护用户隐私的前提下,设计一种联邦多行为序列推荐方法,预测每一个用户在 $L+1$ 时刻最有可能购买的物品(L 为序列长度)。需要注意的是,推荐物品是从用户未购买过的物品 $j \in \mathcal{J} \setminus \mathcal{J}_u^p$ 中选取的,其中 $\mathcal{J}$ 是全部物品集合, $\mathcal{J}_u^p$ 是被用户 u 购买过的全部物品的集合。

3.2 方法概述

本文提出的方法——基于子序列的隐私保护协同推荐方法(SPCR)是一种联邦多行为序列推荐方法。如图1所示,这种基于相似度的方法包括三个

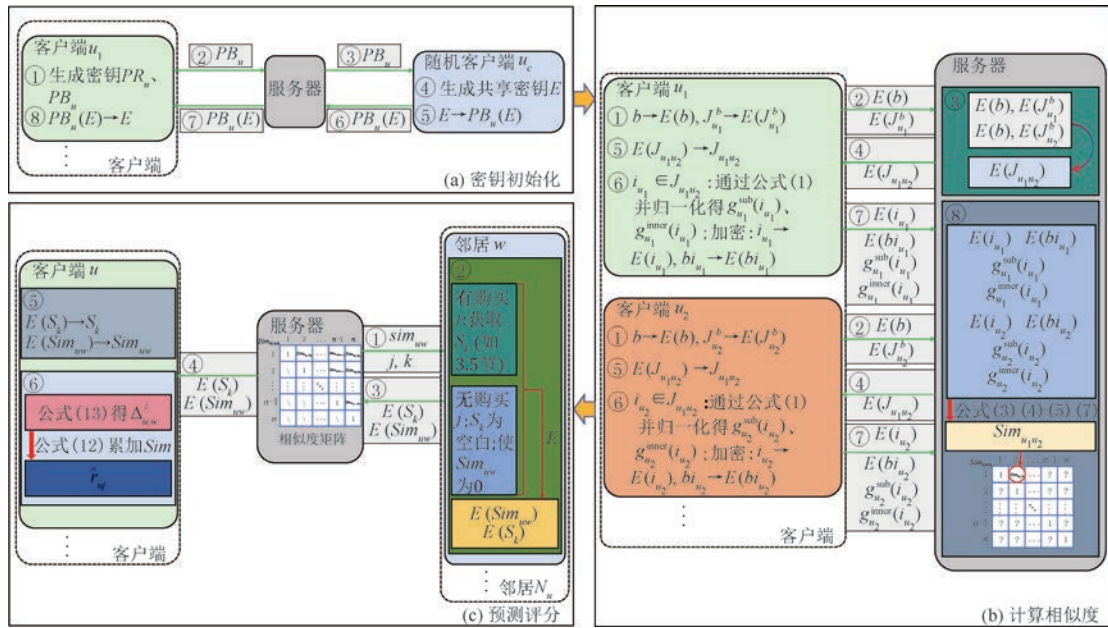


图1 SPCR流程图

主要模块:密钥初始化、计算相似度和预测评分。在密钥初始化阶段,随机选择的客户端 u_c 生成共享密钥 E , 该密钥用于加密后续通信过程的隐私敏感内容。在计算相似度的阶段,本方法首先对原始序列进行子序列划分,其次设计时间衰减函数及其归一化来量化序列中物品所表征的偏好与用户当前偏好的关联程度,最后改进传统杰卡德指数,将跨行为类型的关联信息纳入用户相似度度量,实现相似度的计算。在预测评分阶段,本方法所设计的近期行为模式一致性模块可以动态调节邻居相似度,捕捉用户购买不同目标物品前的行为模式差异,提高推荐性能。值得注意的是,在计算相似度和预测评分这两个阶段,服务器和客户端之间通信涉及的隐私敏感信息均通过共享密钥 E 加密,且服务器不会向信息接收方透露信息来源,可以有效避免隐私泄露。

下文将从密钥初始化、计算相似度和预测评分三个模块来介绍本方法。

3.3 密钥初始化

为了避免用户的历史交互序列 S_u 泄露给服务器或其他客户端,相似度以及预测评分的计算过程需要结合对称加密和非对称加密的技术来实现隐私保护。遵循推荐系统与联邦学习领域的主流安全假设,本文假设服务器是诚实且好奇的^[7],它对其接收到的信息所涉及的隐私怀有好奇之心,但是它会严格遵循本方法的策略。为保障整个通信与计算过程的隐私性,本方法要求所有客户端共同持有一个通过对称加密生成的通用共享密钥 E , 且服务器无法获取该密钥。具体来说,每个客户端 u 会利用非对称加密技术生成一对密钥,包括一个私有密钥 PR_u 和一个公有密钥 PB_u , 然后将公有密钥 PB_u 发送到服务器。随后,服务器收集所有客户端的公有密钥($PB_u: u \in \mathcal{U}$)并将其发送给一个随机选择的客户端 u_c 。客户端 u_c 利用对称加密生成共享密钥 E , 并用从服务器接收到的所有公有密钥加密 E , 生成密文 $PB_u(E): u \in \mathcal{U}$, 然后将这些密文发送到服务器。服务器接收到这些密文后,将每个 $PB_u(E)$ 分发给相应的客户端 u 。每个客户端 u 随后使用其私有密钥 PR_u 解密 $PB_u(E)$, 从而得到共享密钥 E 。

算法 1. SPCR 中密钥初始化过程

输入:客户端集合 $\mathcal{U}$

输出:所有客户端共享的对称加密密钥 E

1. FOR 客户端 $u \in \mathcal{U}$ DO
2. 生成私有密钥 PR_u 和公有密钥 PB_u
3. 将公有密钥 PB_u 发送给服务器

4. END FOR
5. 随机选择一个客户端 $u_c: u_c \in \mathcal{U}$, 服务器向其发送所有公有密钥 $PB_u: u \in \mathcal{U}$
6. 客户端 u_c :
7. 利用对称加密生成共享密钥 E
8. 利用公有密钥 PB_u 生成密文 $PB_u(E): u \in \mathcal{U}$
9. 将 $PB_u(E): u \in \mathcal{U}$, 发送给服务器
10. 服务器:
11. 将每个 $PB_u(E)$ 转发给相应的客户端
12. FOR 客户端 $u \in \mathcal{U}$ DO
13. 使用私有密钥 PR_u 解密, 得到共享密钥 E
14. END FOR

在后续客户端之间的通信中,发送方利用共享密钥 E 对内容进行加密,经服务器转发给接收方,接收方再使用共享密钥 E 进行解密,得到真正的内容,从而防止服务器得到真实的历史交互记录。

3.4 用户相似度

在每个客户端得到共享密钥 E 后,SPCR 需要每个用户对自己的交互序列进行划分得到子序列。本文的目标是预测用户在 $L+1$ 时刻最有可能购买的物品,因而购买行为可以视作目标行为,其他行为可以视作辅助行为。这些辅助行为、购买行为及其交互的物品共同构成了用户在一定时间范围内的短期偏好。具体来说,某一时间范围内的辅助行为及其交互物品反映了用户在对应时间范围内的偏好探索,而购买行为及其交互的物品反映了用户在对应时间范围内的最终决策。为此,某一时间范围内的辅助行为及其交互的物品与购买行为及其交互的物品存在从偏好探索到最终决策的递进关系,构成了用户在一定时间范围内的短期偏好。基于以上分析,将用户原始的交互序列划分成若干个体现用户某个时间范围内偏好的子序列,此举不仅利于更精确地捕捉用户在不同时间范围偏好的变化,还充分考虑了某一时间范围内用户不同行为类型及其交互的物品之间的递进关系。因为购买行为及其交互的物品反映了用户在某一时间范围内的最终决策,标志着短期偏好周期的结束,所以本方法依据购买行为将用户原始序列划分成若干个子序列。值得注意的是,为清晰阐释本文方法每一步的计算过程,本文以电商领域为示例,依据购买行为将用户原始序列划分成若干个子序列。针对无购买行为的场景,可将待预测行为视作目标行为,其余行为视作辅助行为,并以目标行为作为节点划分子序列,即可适配本文的方法。

如图 2 所示,该图是对原始序列进行划分的示

意图(黄色代表浏览,橙色代表添加购物车,蓝色代表收藏,绿色代表购买)。需要说明的是,除非原始序列最后一个物品上的行为类型不是购买,原始序列未被划分的物品作为最后一个子序列,否则每个子序列一般都以购买行为结束。对此,本文将结合图 2 的示例加以详细说明。上述的划分方式,具体可表示为

$$S_u = \{(i_u^1, b_u^1), \dots, (i_u^l, b_u^l), \dots, (i_u^L, b_u^L)\} \\ = \{s^1, s^2, \dots, s^q\}.$$

经过划分后,序列被分为 q 个子序列 $s^1, s^2, \dots, s^q$ 。在实际情况下,划分出来的子序列可能会出现三种情况:(1)以辅助行为对应的物品开始,以购买行为对应的物品结束:这是最常见的一种情况,如图 2 中的 s^1 子序列;(2)以购买行为对应的物品开始,以购买行为对应的物品结束:一般出现在原始序列中存在两个或者以上连续的购买行为的情况,如图 2 中的 s^4 子序列;(3)以辅助行为对应的物品开始,以辅助行为对应的物品结束:一般出现在原始序列中最后一个物品对应的行为类型不是购买的情况,如图 2 中的 s^5 子序列。

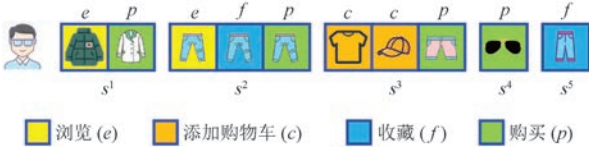


图 2 原始序列划分成子序列示意图

为了直观地解释本方法,本节会用一个实际例子来说明方法的整个流程,例子如图 3 所示。其中,为了方便表示,序列中的数字代表物品 ID。

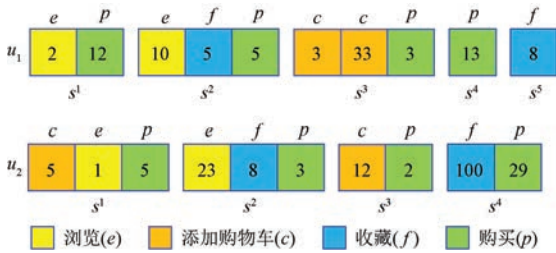


图 3 用户历史交互记录示意图

在用户原始行为序列中,物品位置与当前位置的距离,与该物品对用户当前偏好的表征能力通常呈正相关——越靠近当前位置的物品,往往越能反映用户当下的即时偏好。例如,若用户最近一次行为是浏览裤子,其下一步大概率会购买裤子或同类服饰;反之,时间越久远的物品,所反映的用户偏好与当前偏好的偏差可能会比较大。

在原始序列划分成若干个子序列后,本文可清

晰界定序列中每个物品的两个位置属性,分别为子序列位置 $p_u^{\text{sub}}(i)$ 和子序列内物品的位置 $p_u^{\text{inner}}(i)$ 。具体来说,用 $p_u^{\text{sub}}(i)$ 来表示在用户 u 序列中,物品 i 所在子序列的位置,满足: $p_u^{\text{sub}}(i) \in \{0, 1, 2, \dots, q-1\}$, q 为子序列的数量。 $p_u^{\text{sub}}(i)$ 越小表示物品 i 所在子序列的位置越靠近当前位置,也就是说最靠近当前位置的子序列内的所有物品对应的 p_u^{sub} 都为 0。因此, $p_u^{\text{sub}}(i)$ 也代表了物品 i 所在子序列所承载的短期偏好与用户当前位置偏好的差异程度。类似的,在用户 u 序列中,物品 i 在其对应的子序列内的位置可以用 $p_u^{\text{inner}}(i)$ 来表示,满足: $p_u^{\text{inner}}(i) \in \{0, 1, 2, \dots, |s^k|-1\}$, $|s^k|$ 是对应的子序列的长度。因为子序列内最后的物品对应的 p_u^{inner} 为 0, 所以 $p_u^{\text{inner}}(i)$ 也反映了物品 i (偏好探索)对最终购买物品(最终决策)递进关系的强弱。对于图 3, 用户 u_1 的序列中物品 8 对应的 $p_{u_1}^{\text{sub}}(8)$ 和 $p_{u_1}^{\text{inner}}(8)$ 都为 0, 而物品 2 对应的 $p_{u_1}^{\text{sub}}(2)$ 和 $p_{u_1}^{\text{inner}}(2)$ 为 4 和 1。

此外,本文还需要设计一种机制,借助 $p_u^{\text{sub}}(i)$ 和 $p_u^{\text{inner}}(i)$ 量化物品 i 所表征的偏好与用户当前偏好的关联程度。心理学中的遗忘曲线理论^[9-10]表明,人类对事件的记忆强度随时间呈指数衰减。用户的兴趣偏好本质上是短期记忆的体现,近期的行为序列对当前决策的影响显著高于历史行为。因此,本方法引入时间衰减函数来建模这种特性。时间衰减函数为

$$f(p) = e^{-ap} \quad (1)$$

其中, $a \in [0, 1]$ 为衰减参数, a 越大,衰减越快,当 $p=0$ 时, $f(p)$ 取最大值 1, 如图 4 所示。 $f(p)$ 作为一个单调递减的函数,可用于调节不同位置的重要性,其符合越靠近当前位置(p 越小)越重要($f(p)$ 越大)的要求。此外, $f(p)$ 的衰减速率是逐步放缓的,与衰减速率逐步增加相比, p 较大(远期物品)时,“衰减速率逐步增加”会使得远期物品的值骤降,基本归零;而 $f(p)$ 可以更好地避免近期偏好完全覆盖远期偏好的情况。

基于这个函数,每个用户原始序列中的每个物品都有其对应的 $p_u^{\text{sub}}(i)$ 和 $p_u^{\text{inner}}(i)$, 将 $p_u^{\text{sub}}(i)$ 和 $p_u^{\text{inner}}(i)$ 分别代入这个时间衰减函数,可以得到子序列权重 $f_u^{\text{sub}}(i) = f(p_u^{\text{sub}}(i))$ 和物品权重 $f_u^{\text{inner}}(i) = f(p_u^{\text{inner}}(i))$ 。对于图 3, 假设 a_{sub} 和 a_{inner} 都取 0.5, 用户 u_1 的序列中物品 8 对应的 $f_{u_1}^{\text{sub}}(8)$ 和 $f_{u_1}^{\text{inner}}(8)$ 都为 1, 而物品 2 对应的 $f_{u_1}^{\text{sub}}(2)$ 和 $f_{u_1}^{\text{inner}}(2)$ 为 0.1353 和 0.6065。

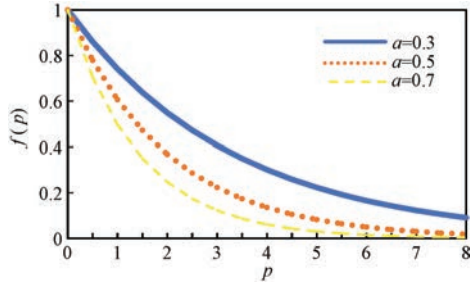


图4 时间衰减函数示意图

然而,不同用户原始序列的长度或者子序列的长度差异较大,为了消除这种因序列长度差异导致的权重计算偏差,确保不同用户或子序列之间的权重具有可比性,需要对子序列权重 $f_u^{\text{sub}}(i)$ 和物品权重 $f_u^{\text{inner}}(i)$ 进行归一化处理,得到归一化子序列权重 $g_u^{\text{sub}}(i)$ 和归一化物品权重 $g_u^{\text{inner}}(i)$ 。具体公式如下:

$$g(p) = \frac{f(p)}{\sum_{x=0}^{X-1} f(x)} \quad (2)$$

其中,当计算 $g_u^{\text{sub}}(i)$ 时, X 取 q ; 而当计算 $g_u^{\text{inner}}(i)$ 时, X 取 $|s^k|$ 。对于图 2 中的用户 u_1 序列,假设 α_{sub} 取 0.5, 则 s^5, s^4, s^3, s^2 和 s^1 子序列中物品的归一化子序列权重分别为 0.4287、0.2600、0.1577、0.0956 和 0.0580, 累加等于 1。而对于图 2 中的用户 u_2 序列,假设 α_{inner} 取 0.5, 则 s^2 子序列中所有物品的归一化物品权重分别为 0.5065、0.3072 和 0.1863, 累加等于 1。

每个客户端对原始序列划分完成后,根据以上公式(1)和公式(2),序列中每个物品都有对应的 $p_u^{\text{sub}}(i)$ 和 $p_u^{\text{inner}}(i)$, 将 $p_u^{\text{sub}}(i)$ 和 $p_u^{\text{inner}}(i)$ 分别代入时间衰减函数,可以得到子序列权重 $f_u^{\text{sub}}(i)$ 和物品权重 $f_u^{\text{inner}}(i)$ 。接着对其进行归一化,从而得到归一化子序列权重 $g_u^{\text{sub}}(i)$ 和归一化物品权重 $g_u^{\text{inner}}(i)$ 。

为了减少不必要的通信,客户端首先按行为类型分类,将交互过的物品集合 $\mathcal{J}_u$ 依据行为类型 b 分成若干个集合 $\mathcal{J}_u^b$ ($\mathcal{J}_u^b$ 即是用户 u 在行为类型 b 下交互的物品集合)。然后客户端利用共享密钥 E 对每种行为类型 b 及其对应的物品集合 $\mathcal{J}_u^b$ 进行加密,得到每种行为类型的 $E(b)$ 和 $E(\mathcal{J}_u^b)$, 并发送给服务器。服务器在接收所有用户的 $E(b)$ 和 $E(\mathcal{J}_u^b)$ 后,在不解密的情况下,可以通过每个客户端发来的每种行为类型的 $E(b)$ 和 $E(\mathcal{J}_u^b)$ 来判断不同用户之间是否有共同交互的物品,若某两个用户没有共同交互的物品,则这两个用户的相似度直接置为 0, 后续不需要再进行计算。

算法 2. SPCR 中相似度计算前的通信过程

输入:客户端集合 $\mathcal{U}$, 共享密钥 E , 每个客户端 $u \in \mathcal{U}$ 的原始交互序列

输出:任意两个客户端 $u_1, u_2 \in \mathcal{U}$ 共同交互的物品集合对应的密文 $E(\mathcal{J}_{u_1 u_2})$

1. FOR 客户端 $u \in \mathcal{U}$ DO
2. 使用共享密钥 E 加密每种行为类型及其对应的物品集合: $b \rightarrow E(b), \mathcal{J}_u^b \rightarrow E(\mathcal{J}_u^b)$
3. 将每种行为类型的 $E(b)$ 和 $E(\mathcal{J}_u^b)$ 发送给服务器
4. END FOR
5. 服务器:
6. 对任意两个客户端 u_1 和 u_2 :
7. 通过每种行为类型的 $E(\mathcal{J}_{u_1}^b)$ 和 $E(\mathcal{J}_{u_2}^b)$ 判断 u_1 和 u_2 是否有共同交互的物品:
8. 若没有共同交互的物品,则 $\text{Sim}(u_1, u_2) = 0$ (无需参与后续计算)
9. 若有共同交互的物品,则可以得到两个客户端共同交互的物品集合对应的密文 $E(\mathcal{J}_{u_1 u_2})$ 和 $\sum_{b \in B} |\mathcal{J}_{u_1}^b \cup \mathcal{J}_{u_2}^b|$

每一个子序列代表用户某个时间范围内的偏好,利用好这些序列信息可以有效地提高推荐性能。在现实当中,用户的偏好并非一成不变,不同时间范围内用户的需求一般是不相同的,例如,一般来说,冬天的时候用户对羽绒服的需求会增大,体现了这个时间范围用户对羽绒服的偏好较高。但可能由于居住地点,个人耐寒能力等因素的不同,不同用户对羽绒服的偏好也会不同,这个不同可能体现在不同用户购买羽绒服的时间,或不同用户对羽绒服的行为类型(即某个用户因为冬天到了,收藏了羽绒服,但是因为天气突变,他最后却选择购买了一件风衣而不是羽绒服)等。所以,两个用户的历史交互记录中,对同一物品的交互时间和行为类型蕴含了两个用户各自的特征(例如居住地点,个人耐寒能力等)。基于以上分析,可以设计一些公式来量化出两个用户的相似度。

对于交互时间的差异,主要通过归一化子序列权重 $g_u^{\text{sub}}(i)$ 和归一化物品权重 $g_u^{\text{inner}}(i)$ 来量化。本文受欧几里得距离^[34-35]思想的启发,设计了公式(3),将归一化子序列权重和归一化物品权重的差异融合在一起,进而量化两个用户的相似度:

$$d(u_1, u_2, i) = 1 - \sqrt{\frac{d_{\text{sub}}^2 + d_{\text{inner}}^2}{2}} \quad (3)$$

$$d_{\text{sub}} = |g_{u_1}^{\text{sub}}(i) - g_{u_2}^{\text{sub}}(i)| \quad (4)$$

$$d_{\text{inner}} = |g_{u_1}^{\text{inner}}(i) - g_{u_2}^{\text{inner}}(i)| \quad (5)$$

其中, u_1 和 u_2 是用户, i 是物品。显然, $d(u_1, u_2,$

i) 的范围是 $(0, 1]$, 当 u_1 和 u_2 为同一个用户(序列)时, d 取最大值 1。对于图 3, 假设 a_{sub} 和 a_{inner} 都取 0.5, 则用户 u_1 和用户 u_2 对于物品 8 有 $d(u_1, u_2, 8) = 0.4764$, 对物品 2 有 $d(u_1, u_2, 2) = 0.7681$ 。

本方法是一种基于相似度的联邦多行为序列推荐方法, 杰卡德指数是一种经典的相似度度量。基于此, 本文在杰卡德指数的基础上构建自己的相似度公式:

$$\text{Sim}(u, w) = \frac{\sum_{b \in \mathcal{B}} \sum_{i \in \mathcal{J}_u^b \cap \mathcal{J}_w^b} d(u, w, i)}{\sum_{b \in \mathcal{B}} |\mathcal{J}_u^b \cup \mathcal{J}_w^b|} \quad (6)$$

其中, $\mathcal{B}$ 是所有行为类型的集合, $\mathcal{J}_u^b$ 和 $\mathcal{J}_w^b$ 分别表示用户 u 和 w 行为类型为 b 的物品集合。至此, 公式(6)只是考虑了两条序列中物品和行为类型都相同的情况。而在实际的场景中, 对于两条序列中的相同物品, 它们对应的行为类型不同的情况往往比行为类型相同的情况要更加普遍。为此, 挖掘这类情况隐含的用户偏好差异, 能够为相似度计算补充更丰富的行为关联信息, 有利于更加准确地量化两个用户的相似度。对公式(6)进行扩展, 详细的公式如下:

$$\text{Sim}(u, w) = \frac{\lambda * d_s + (1 - \lambda) * d_d}{\lambda * n_s + (1 - \lambda) * n_d} \quad (7)$$

$$d_s = \sum_{b \in \mathcal{B}} \sum_{i \in \mathcal{J}_u^b \cap \mathcal{J}_w^b} d(u, w, i) \quad (8)$$

$$d_d = \sum_{b_1 \in \mathcal{B}, b_2 \in \mathcal{B}, b_2 \neq b_1} \sum_{j \in \mathcal{J}_u^{b_1} \cap \mathcal{J}_w^{b_2}} d(u, w, j) \quad (9)$$

$$n_s = \sum_{b \in \mathcal{B}} |\mathcal{J}_u^b \cup \mathcal{J}_w^b| \quad (10)$$

$$n_d = \sum_{b_1 \in \mathcal{B}, b_2 \in \mathcal{B}, b_2 \neq b_1} |\mathcal{J}_u^{b_1} \cap \mathcal{J}_w^{b_2}| \quad (11)$$

其中, 分子新增的第二项 d_d 是用于量化同一物品在两条序列中行为类型不同时的偏好关联。为了方便调节“相同行为类型”和“不同行为类型”的影响程度引入了可调节权重 λ , λ 的取值范围是 $[0, 1]$ 。同时为了使 $\text{Sim}(u, w)$ 的取值范围是 $[0, 1]$, 分母上也新增了第二项以及和分子上一样的权重 λ 。

值得注意的是, 分母新增的第二项“ $|\mathcal{J}_u^{b_1} \cap \mathcal{J}_w^{b_2}|$ ”采用交集运算, 与第一项的并集运算有所不同, 但这样的设计是合理的。原因是: (1) 不同行为类型下, 采用交集运算能精准捕捉跨行为但物品重叠的部分, 让这部分计算聚焦在有实际物品交集的跨行为场景中, 保证公式合理性; (2) 如果分母的第二项设计成与第一项相同——都为并集运算, 那么在跨行为场景下, 分母会包含大量无物品交集的组合, 例如

用户 u 行为 b_1 的物品集合和用户 w 行为 b_2 的物品集合即使完全没有重叠, 但通过并集运算仍然会计算两者的数量, 让分母不合理地虚大, 导致相似度最终计算的值得偏小, 无法较好地捕捉跨行为场景的信息。(3) 采用交集运算还可以保证 $\text{Sim}(u, w)$ 的取值范围为 $[0, 1]$, 当 $u = w$ 时, $\text{Sim}(u, w)$ 取最大值 1。相反, 采用并集运算是无法保证这一点的。

当服务器需要某两个用户的相似度时, 例如现在需要计算用户 u_1 和用户 u_2 的相似度, 服务器可根据 $E(b)$ 和 $E(\mathcal{J}_u^b)$ 得到两个客户端的 $\sum_{b \in \mathcal{B}} |\mathcal{J}_{u_1}^b \cup \mathcal{J}_{u_2}^b|$ (即公式(7)中分母的第一项)。同时, 还可以得到两个用户共同交互的物品集合 $\mathcal{J}_{u_1 u_2}$ 对应的密文 $E(\mathcal{J}_{u_1 u_2})$, 服务器将 $E(\mathcal{J}_{u_1 u_2})$ 分别发送给两个客户端。两个客户端在接收密文后, 使用共享密钥 E 对密文进行解密, 从而得到共同交互的物品。然后, 两个客户端分别使用共享密钥 E 对共同交互的物品 $i \in \mathcal{J}_{u_1 u_2}$ 及对应的行为类型 $b_i \in \mathcal{B}$ 一一进行加密。最后, 客户端向服务器逐一发送每个共同交互物品 $i \in \mathcal{J}_{u_1 u_2}$ 对应的物品 ID 的密文 $E(i)$ 、行为类型的密文 $E(b_i)$ 、归一化子序列权重 $g_u^{\text{sub}}(i)$ 和归一化物品权重 $g_u^{\text{inner}}(i)$ 。服务器在接收用户 u_1 和用户 u_2 发送的所有信息后, 根据公式(7)计算两个用户的相似度 $\text{Sim}(u_1, u_2)$ 。

算法 3. SPCR 中计算用户相似度矩阵的通信过程
输入: 客户端集合 $\mathcal{U}$, 共享密钥 E , 每个客户端对 (u_1, u_2) 共同交互的物品集合对应的密文 $E(\mathcal{J}_{u_1 u_2})$, 每个客户端 $u \in \mathcal{U}$ 的归一化子序列权重 $g_u^{\text{sub}}(i)$ 和归一化物品权重 $g_u^{\text{inner}}(i)$ (i 为客户端 u 交互过的物品)
输出: 完整的用户相似度矩阵

1. FOR 客户端 $u_1 \in \mathcal{U}$ DO
2. FOR 客户端 $u_2 \in \mathcal{U}$ DO
3. 服务器向客户端 u_1 和客户端 u_2 发送 $E(\mathcal{J}_{u_1 u_2})$
4. 两个客户端使用共享密钥 E 解密得到 $\mathcal{J}_{u_1 u_2}$
5. 两个客户端使用共享密钥 E 对共同交互的物品 $i \in \mathcal{J}_{u_1 u_2}$ 及对应的行为类型 b_i 逐一加密, 得到 $E(i)$ 和 $E(b_i)$
6. 两个客户端向服务器发送共同交互的每个物品的 $E(i)$ 、 $E(b_i)$ 、归一化子序列权重 $g_u^{\text{sub}}(i)$ 和归一化物品权重 $g_u^{\text{inner}}(i)$
7. 服务器接收两个客户端发送的所有信息后, 根据公式(7)计算两个用户的相似度 $\text{Sim}(u_1, u_2)$
8. END FOR
9. END FOR

3.5 预测评分

对于每一对用户, 在服务器中, 重复计算公式

(7)即可得到 $n \times n$ 的相似度矩阵。根据相似度矩阵,对任意一个用户 u 都可以得到其对应的邻居 $\mathcal{N}_u$ 。至此,下一步是计算预测评分,具体公式如下:

$$\hat{r}_{uj} = \sum_{w \in \mathcal{N}_u \cap \mathcal{U}_j} \text{Sim}(u, w) * (1 + \Delta_{u,w}^j) \quad (12)$$

其中, $\mathcal{U}_j$ 是购买过物品 j 的用户集合。公式(12)中 $\Delta_{u,w}^j$ 用于衡量两个用户在购买目标物品 j 前的行为模式相似性。在具体计算前需要先定义两个物品集合:(1) $\mathcal{J}_{w,j}^k$: 在用户 w 的序列中,以购买物品 j 这一行为所在的子序列为起点,向前回溯 k 个子序列(包含物品 j 所在的子序列),进而得到这些子序列中所有物品组成的集合,然后去除该集合中的物品 j ,余下的物品组成的集合即是 $\mathcal{J}_{w,j}^k$; (2) $\mathcal{J}_{u,j}^k$: 与 $\mathcal{J}_{w,j}^k$ 有所不同, $\hat{r}_{uj}$ 的本质是预测物品 j 会出现在用户 u 序列中最新的一个物品的概率,故 $\mathcal{J}_{u,j}^k$ 代表用户 u 序列中最新 k 个子序列的物品集合。如图 5,假设 k 取 2 且用户 w 是用户 u 的邻居,下面需要计算用户 u 对于物品 2 的预测评分。首先,在用户 w 的序列中,找到购买物品 2 这一行为所在的子序列(即 S^3),然后向前回溯 2 个子序列(假设 k 取 2),即子序列 S^3 和 S^2 。这两个子序列中所有物品组成的集合为 $\{2, 12, 3, 8, 23\}$,然后去除集合中的物品 2,得到 $\mathcal{J}_{w,2}^2 = \{12, 3, 8, 23\}$ 。其次,在用户 u 的序列中,找到最新的 2 个子序列(即 S^5 和 S^4),这两个子序列中所有物品组成的集合为 $\{8, 13\}$,即 $\mathcal{J}_{u,2}^2 = \{8, 13\}$ 。最后,通过公式(13)计算得到 $\Delta_{u,w}^j$:

$$\Delta_{u,w}^j = 1 - \frac{\sum_{j_k \in \mathcal{J}_{u,j}^k \cap \mathcal{J}_{w,j}^k} d_{\text{sub}}(u, w, j_k)}{|\mathcal{J}_{u,j}^k \cap \mathcal{J}_{w,j}^k|} \quad (13)$$

其中, $\Delta_{u,w}^j$ 的取值范围为 $[0, 1]$, 当 $u=w$ 时,取最大值 1。分母部分是计算 $\mathcal{J}_{u,j}^k$ 和 $\mathcal{J}_{w,j}^k$ 的交集大小,目的是对“共同交互物品数量”进行归一化。分子部分再次运用了 $d_{\text{sub}}(u, w, j_k)$, 即公式(4),通过子序列距离来捕捉两个用户在购买目标物品前行为模式的微小差异。具体来说,若不考虑 $\Delta_{u,w}^j$, 在计算用户 u 对不同物品的预测评分时,会比较“死板”地对所有目标物品无差别累加两个用户的相似度,无法区分两个用户交互不同目标物品前行为模式的差异。相反,考虑 $\Delta_{u,w}^j$ 时,根据目标物品的不同,计算得到不同的 $\Delta_{u,w}^j$, 进而实现累加的是两个用户动态调整后的相似度,可以比较灵敏地提取出两个用户在购买目标物品前行为偏好的差异,得到更加准确的预测评分,提高推荐性能。

假设现在需要预测用户 u 对物品 j 的评分。服

务器需要向用户 u 的邻居 $w \in \mathcal{N}_u$ 发送用户 u 与其(w)的用户相似度、物品 j 的 ID 和参数 k 。每个邻居在接收到来自服务器的信息后,判断自己是否购买过物品 j , 如果购买过物品 j , 则 $\text{Sim}(u, w)$ 不作任何处理,保持原值不变。与此同时,每个邻居从自己的历史交互序列中找到购买物品 j 所在子序列的位置,并对该位置最近的 k 个子序列进行加密。例如图 5 中的用户 w , k 取 2 且物品 j 为 2 时,有 $S_2 = \{s^2, s^3\}$, 加密后得 $E(S_2)$ 。随后,将 $E(\text{Sim}(u, w))$ 和 $E(S_k)$ 发送服务器。如果该邻居没有购买过物品 j , 则 $\text{Sim}(u, w)$ 置 0, S_k 为空白,并使用共享密钥 E 加密后,将 $E(\text{Sim}(u, w))$ 和 $E(S_k)$ 发送给服务器。值得注意的是,为了不暴露邻居是否购买过物品 j 这一隐私,虽然此时 S_k 为空白,但仍要向服务器发送 $E(S_k)$ 。

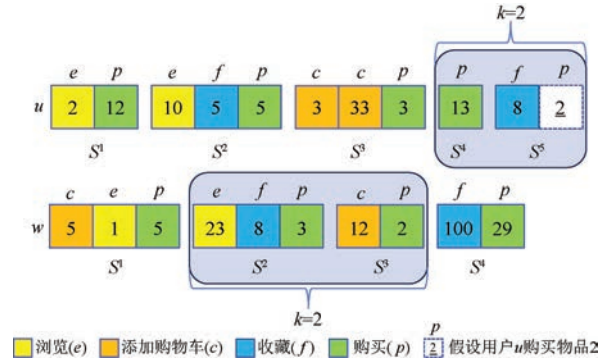


图 5 用户近期交互记录示意图

算法 4. SPCR 中计算预测评分的通信过程

输入: 客户端集合 $\mathcal{U}$, 共享密钥 E , 用户相似度矩阵, 每个客户端 $u \in \mathcal{U}$ 的原始交互序列, 参数 k

输出: 每个客户端 $u \in \mathcal{U}$ 的物品推荐列表

1. FOR 客户端 $u \in \mathcal{U}$ DO
2. 服务器根据相似度矩阵得到 u 的邻居 $\mathcal{N}_u$
3. FOR 候选物品 $j \in \mathcal{J} \setminus \mathcal{J}_u^k$ DO
4. 服务器向每个邻居 $w \in \mathcal{N}_u$ 发送 $\text{Sim}(u, w)$ 、目标物品 j 和参数 k
5. FOR 邻居 $w \in \mathcal{N}_u$ DO
6. 判断自身是否购买目标物品 j :
7. 若有购买, 则提取购买物品 j 所在的子序列及其之前的 $k-1$ 个子序列(即 $S_k = \{s^{l-k+1}, s^{l-k+2}, \dots, s^{l-1}, s^l\}$), 并通过加密得 $E(\text{Sim}(u, w))$ 和 $E(S_k)$ 。最后, 将 $E(\text{Sim}(u, w))$ 和 $E(S_k)$ 发送服务器
8. 若没有购买, 则使 $\text{Sim}(u, w) = 0$, 再重新加密得到 $E(\text{Sim}(u, w))$ 。 S_k 为空白。最后, 将 $E(\text{Sim}(u, w))$ 和 $E(S_k)$ 发送服务器
9. END FOR
10. 服务器将来自邻居的信息转发给客户端 u

11. 客户端 u 接收所有邻居的 $E(\text{Sim}(u, w))$ 和 $E(S_k)$ 后, 对其进行解密, 根据公式(12)和公式(13)计算得到用户 u 对物品 j 的预测评分 $\hat{r}_{uj}$
12. END FOR
13. 生成客户端 u 的物品推荐列表
14. END FOR

服务器接收到邻居发来的 $E(\text{Sim}(u, w))$ 和 $E(S_k)$ 后, 会转发给用户 u 。用户 u 接收到所有邻居的 $E(\text{Sim}(u, w))$ 和 $E(S_k)$ 后, 通过解密得到每个邻居对应的 $\text{Sim}(u, w)$ 和 S_k 。随后, 用户 u 在客户端本地根据公式(12)和公式(13)计算得到用户 u 对物品 j 的预测评分 $\hat{r}_{uj}$ 。重复以上步骤, 即可得到用户 u 对所有候选物品的预测评分, 进而在客户端本地生成物品推荐列表。

4 分析与讨论

本节主要从三个方面进行分析和讨论: 一是无损性分析, 通过理论验证 SPCR 的无损性。二是隐私分析, 探讨 SPCR 如何防御参数重构攻击、成员推理攻击和属性推理攻击, 以确保用户历史交互序列等隐私不泄露给服务器或其他客户端; 三是通信成本分析, 分为密钥初始化、计算相似度前、计算相似度矩阵和计算预测评分四个阶段, 评估 SPCR 的总通信量及各阶段通信成本。

4.1 无损性分析

本方法是一种无损的推荐方法, 下面将理论分析整个过程的无损性(实验分析可见 5.3 节)。在算法 2 中, 服务器接收所有用户每种行为类型的 $E(b)$ 和 $E(\mathcal{J}_u^b)$, 在不解密的情况下, 仅通过任意两个用户每种行为类型的 $E(b)$ 和 $E(\mathcal{J}_u^b)$ 即可知道这两个用户的 $\sum_{b \in \mathcal{B}} |\mathcal{J}_{u_1}^b \cup \mathcal{J}_{u_2}^b|$ (即公式(7)中分母的第一项)。值得注意的是, 该过程中是否知道物品真实 ID 不影响最终结果与中心化场景的一致性。在算法 3 计算用户相似度时, 客户端向服务器逐一发送每个共同交互物品对应的物品 ID 的密文 $E(i)$ 、行为类型的密文 $E(b_i)$ 、归一化子序列权重 $g_u^{\text{sub}}(i)$ 和归一化物品权重 $g_u^{\text{inner}}(i)$ 。服务器在不解密的情况下, 将加密后的物品 ID 以及对应的行为类型作为标识参与匹配。匹配成功后, 根据公式(3)计算得到 $d(u_1, u_2, i)$, 参与该过程计算的归一化子序列权重和归一化物品权重无需加密, 因此 $d(u_1, u_2, i)$ 的结果和中心化场景一致。最后, 将所有前面计算得到的 $d(u_1, u_2, i)$ 累加即可得到用户相似度的分子

项。结合以上分析可知, 通过该方法计算得到的用户相似度和中心化场景的结果一致。在算法 4 计算预测评分时, 与中心化场景相比, 虽然多了使用共享密钥 E 加密和解密的过程, 但最终在客户端参与计算预测评分的数据(如 $\text{Sim}(u, w)$ 、 S_k)与原始数据一致, 因此本方法计算得到的预测评分与中心化场景的结果也是一致的。综上所述, 本方法是一个具有无损性的联邦多行为序列推荐方法。

4.2 隐私分析

在本小节中, 分析 SPCR 是否有效保护用户的隐私, 其中 SPCR 整个算法过程如算法 5 所示。遵循推荐系统与联邦学习领域的主流安全假设, 本文假设客户端和服务端是诚实且好奇的^[7], 这意味着它们会遵守 SPCR 的算法流程, 但是它们会对接收到的数据感到好奇并试图推断出其他客户的隐私。下面将分析 SPCR 如何防御一些常见的攻击, 包括参数重构攻击、成员推理攻击和属性推理攻击。

对于参数重构攻击, 攻击者(例如服务器或任意一个客户端)试图从接收到的数据中重构任何其他客户端的原始数据(即用户的交互序列)。第一次通信: 客户端向服务器发送每种行为类型 b 及其对应的物品集合 $\mathcal{J}_u^b$ 的密文。虽然服务器可以通过所有客户端发送来的密文来推断某些客户端之间具有共同交互的物品, 但是服务器没有共享密钥 E , 无法解密, 即无法得知密文对应的物品 ID。第二次通信: 服务器向客户端(假设为 u_1)发送其与其他客户端(假设为 u_2)共同交互物品的密文。虽然客户端 u_1 拥有共享密钥 E , 可以通过解密得到其与客户端 u_2 共同交互物品的 ID, 但是服务器并不会将客户端 u_2 的真实用户 ID 告知客户端 u_1 。故客户端无法得知其他客户端交互过的物品。第三次通信: 计算客户端 u_1 和客户端 u_2 的相似度时, 两个客户端向服务器逐一发送每个共同交互物品 $i \in \mathcal{J}_{u_1 u_2}$ 对应的物品 ID 的密文 $E(i)$ 、行为类型的密文 $E(b_i)$ 、归一化子序列权重 $g_u^{\text{sub}}(i)$ 和归一化物品权重 $g_u^{\text{inner}}(i)$ 。服务器因为没有共享密钥 E , 无法得知两个客户端实际交互的物品及其行为类型。第四次通信: 服务器将目标用户(假设为 u)与邻居(假设为 w)的相似度、目标物品 j 的 ID 和参数 k 分别发送给每个对应的邻居, 此过程中服务器不会将目标用户的真实 ID 告知邻居, 因此不存在用户隐私泄露问题。第五次通信: 每个邻居将 $E(\text{Sim}(u, w))$ 和 $E(S_k)$ 发送给服务器。因为服务器没有共享密钥 E , 无法得知

$Sim(u, w)$ 为 0 还是为原值,也无法得知 S_k 是否为空白,因而无法判断邻居是否购买过目标物品 j ,从而保护了邻居的隐私。第六次通信:服务器将所有邻居发送来的 $E(Sim(u, w))$ 和 $E(S_k)$ 转发给目标用户。因为服务器不会将邻居的用户 ID 告知目标用户,目标用户无法得知 $Sim(u, w)$ 和 S_k 对应的用户 ID。因此,整个过程中客户端的历史交互序列不会泄露给服务器和其他客户端。

对于成员推理攻击,攻击者试图从模型中推断特定数据是否在训练集中。由于预测评分的过程在目标客户端本地进行,服务器和其他客户端无法获得目标客户端对特定物品的预测评分,更无法得知是否和某个物品有交互记录。

对于属性推理攻击,攻击者试图推断用户的私有属性,其必须获取用户的行为、社会成员信息或转移的知识,然后从上述信息中推断属性。在本方法中,所有传输的信息都是经过加密的,尽管客户端具有密钥进行解密,但是服务器在传输的过程中不会告知接收的客户端加密信息的来源,因此攻击者很难获取上述信息。

算法 5. SPCR 算法过程

输入:每个客户端 $u \in \mathcal{U}$ 的原始交互序列,参数 a_{sub} 、 a_{inner} 、 λ 、 k 和 a_k

输出:每个客户端 $u \in \mathcal{U}$ 的物品推荐列表

1. 调用算法 1:SPCR 中密钥初始化(完成客户端公钥和私钥生成、共享密钥 S 的分发与解密)
2. 调用算法 2:SPCR 中相似度计算前的通信过程(完成客户端交互物品集合加密传输、服务器判断用户间共同交互物品)
3. 调用算法 3:SPCR 中计算用户相似度矩阵的通信过程(完成用户对共同交互物品信息加密传输、服务器计算用户相似度矩阵)
4. 调用算法 4:SPCR 中计算预测评分的通信过程(完成基于相似度矩阵的邻居筛选、预测评分计算及推荐列表生成)

4.3 通信成本分析

本小节将分析 SPCR 的通信成本,值得注意的是,以下分析均默认密文长度与明文一致^[7]。假设有 n 个用户和 m 个物品,分 4 个阶段来分析:

密钥初始化的通信过程:非对称公钥 PB_u 的大小为 $L_{pb}=256$ 字节,对称共享密钥 E 的大小为 $L_s=16$ 字节。这个过程中每个用户发送 1 次非对称公钥,接收 1 次加密的共享密钥 E 。而候选客户端额外接收 n 个公钥并发送 n 个加密的共享密钥 E 。故总通信量为: $2n \times (L_{pb} + L_s) = 544n$ 字节。

计算用户相似度前的通信过程:假设单个用户

交互的物品总数为 $|\mathcal{J}_u|$,平均为 $\overline{|\mathcal{J}_u|}$,行为类型的数目为 4,物品 ID 加密后大小为 $L_{id}=4$ 字节,行为类型的密文占 $L_b=1$ 字节。该过程中,客户端向服务器发送交互物品集合的密文。故总通信量为: $n \times (\overline{|\mathcal{J}_u|} \times L_{id} + 4) = 4n(\overline{|\mathcal{J}_u|} + 1)$ 字节。

计算用户相似度矩阵的通信过程:在算法 2 中提到,没有共同交互物品的用户对,其相似度直接置 0,无需参与后续的计算。在实际应用中,拥有共同交互物品的用户对占总用户对的比例是很低的。因此,总用户对的数量为 $n(n-1)/2$,而实际参与通信和计算的用户对数量为 $p \ll n(n-1)/2$ 。假设每个用户对共同交互物品数为 $|\mathcal{J}_{u_1 u_2}|$,平均为 $\overline{|\mathcal{J}_{u_1 u_2}|}$ 。服务器向两个客户端发送共同交互物品集合的密文的通信成本是: $2 \times \overline{|\mathcal{J}_{u_1 u_2}|} \times L_{id}$ 。随后,客户端向服务器发送单个共同物品的加密数据:物品 ID 的密文占 L_{id} 字节、对应行为类型的密文占 $L_b=1$ 字节和两个归一化权重分别占 $L_w=8$ 字节,共 $2 \times L_w$ 字节。因此,这个过程总通信量为: $p \times [(2 \times \overline{|\mathcal{J}_{u_1 u_2}|} \times L_{id}) + 2 \times \overline{|\mathcal{J}_{u_1 u_2}|} \times (L_{id} + L_b + 2L_w)] = p \times (2L_{id} + L_b + 2L_w) = 25p \ll 12.5n(n-1)$ 字节。

计算预测评分的通信过程:本文固定单个用户的邻居数为 50,假设每个子序列所含物品的平均数为 $\overline{|\mathcal{T}|}$ 。首先,服务器向每个邻居发送相似度(占 L_{sim} 字节)、目标物品 ID(占 L_{id} 字节)和参数 k (占 1 字节),则单个邻居通信量为 $L_{sim} + L_{id} + 1$ 。然后,邻居向服务器返回相似度的密文(占 $L_{sim}=8$ 字节)、加密的子序列(占 $k \times \overline{|\mathcal{T}|} \times L_{id}$ 字节),则单个邻居通信量为 $L_{sim} + k \times \overline{|\mathcal{T}|} \times L_{id}$ 。最后,服务器将来自邻居的信息转发给目标用户,则有 $L_{sim} + k \times \overline{|\mathcal{T}|} \times L_{id}$ 。总的来说,单个目标用户对单个目标物品整个过程的总通信量为: $50 \times [(L_{sim} + L_{id} + 1) + 2 \times (L_{sim} + k \times \overline{|\mathcal{T}|} \times L_{id})]$ 字节。

为适配百万用户级大规模场景并进一步降低通信代价,本文对算法 4 进行优化,如算法 6 所示。算法 6 的核心优化逻辑为:若客户端 u 发现其大部分邻居未购买过候选物品 j ,则直接将预测评分 $\hat{r}_{uj}$ 置 0,无需进行后续的通信和计算。在实际场景中,用户-物品交互矩阵具有明显的稀疏性,客户端 u 的邻居购买过的物品仅占总物品集的极小比例,这意味着绝大多数候选物品 j 的 $\hat{r}_{uj}$ 直接置 0,每个用户实际需要参与完整计算流程的目标物品数量远小于总物品数(即 $m_u \ll m$)。因此,对于 n 个用户和 m_u

个物品,整个过程的总通信量为: $50 \times n \times m_u \times [(L_{sim} + L_{id} + 1) + 2 \times (L_{sim} + k \lceil T \rceil L_{id})] = 50nm_u (29 + 8k \lceil T \rceil) \ll 50nm (29 + 8k \lceil T \rceil)$ 字节。

算法 6. 计算预测评分的通信过程优化

输入:客户端集合 $\mathcal{U}$, 共享密钥 E , 用户相似度矩阵, 每个客户端 $u \in \mathcal{U}$ 的原始交互序列, 参数 k

输出:每个客户端 $u \in \mathcal{U}$ 的物品推荐列表

1. FOR 客户端 $u \in \mathcal{U}$ DO
2. 服务器根据相似度矩阵得到 u 的邻居 N_u
3. FOR 候选物品 $j \in \mathcal{J} \setminus \mathcal{J}_u^p$ DO
4. (与算法 4 的第 4 至 9 行一致)
5. 服务器将邻居的 $E(S_k)$ 转发给客户端 u
6. 客户端 u 接收 $E(S_k)$ 后, 对其解密, 若 S_k 为空白, 则该 S_k 的信息源(即对应的邻居)没有购买过 j 。
7. 若客户端 u 发现大部分邻居没有购买过候选物品 j , 则直接将 $\hat{r}_{uj}$ 置 0, 不需要进行后续的通信和计算。
8. 反之, 服务器将来自邻居的 $E(\text{Sim}(u, w))$ 发送给客户端 u , 客户端 u 对其解密, 根据公式(12)和公式(13)计算得到用户 u 对物品 j 的预测评分 $\hat{r}_{uj}$
9. END FOR
10. 生成客户端 u 的物品推荐列表
11. END FOR

通过以上分析,SPCR 的总通信成本为 $544n + 4n(\lceil \mathcal{J}_u \rceil + 1) + 25p + 50nm_u (29 + 8k \lceil T \rceil) \ll 12.5n^2 + n[535.5 + 4\lceil \mathcal{J}_u \rceil + 50m(29 + 8k \lceil T \rceil)]$ 字节。其中, k 是超参数, 其取值范围是 $\{1, 2, 3\}$ 。在实际场景中, 用户-物品交互矩阵具有明显的稀疏性, 使得每个用户交互物品数的平均值 $\lceil \mathcal{J}_u \rceil$ 与每个子序列所含物品的平均值 $\lceil T \rceil$ 均较小。因此, SPCR 的总通信成本处于可接受范围。

5 实验与结果分析

为了评估 SPCR 的有效性, 在两个真实数据集上进行多组实验。本节将重点讨论以下四个研究问题(RQ):

RQ1: SPCR 结合隐私保护技术后推荐性能是否无损?

RQ2: 与现有的基准方法相比, SPCR 的性能表现如何?

RQ3: SPCR 中的超参数如何影响性能?

RQ4: SPCR 各部分如何影响性能?

5.1 数据集和评估指标

本实验使用了两个面向用户隐式反馈的公共数

据集, 包括 Jdata 2019(JD)和 User Behavior (UB)。JD 包含来自 1608707 名用户和 378457 个物品的 5 种行为类型的历史交互记录, 其中浏览、添加购物车、收藏、评论和购买行为的数量分别为 33151074、600979、441966、826761 和 2193489。而 UB 则包含来自 987994 名用户和 4162024 个物品的 4 种行为类型的历史交互记录, 其中浏览、添加购物车、收藏和购买行为的数量分别为 89716264、5530446、2888258 和 2015839。

本实验通过以下步骤处理每个数据集:(1)针对某个物品, 若其被购买次数在 JD 数据集少于 20 次或者在 UB 数据集少于 10 次, 则删除该物品的全部相关记录。(2)对于某条序列, 若存在针对同一物品、相同行为类型的多次交互记录, 仅留存时间最早的那条。(3)对于某条序列, 若其中购买行为数量在 JD 或者 UB 数据集中少于 5 次, 就删除该序列。(4)按照时间戳对数据集中的所有序列进行排序, 取时间轴前 80% 内的记录作为训练集, 取时间轴 80%~90% 内的记录作为验证集, 取时间轴 90%~100% 内的记录作为测试集。(5)测试集只保留购买行为, 删除其他行为类型及其交互的物品。(6)删除验证集和测试集中有交互记录, 但是没有在训练集购买过物品的用户所对应的整条序列。(7)删除验证集和测试集中的冷启动物品。冷启动物品是指在所有用户的训练数据中都没有出现过的物品。(8)在验证时, 只使用验证集中购买行为的首个记录, 用作调参。在测试时, 保留验证集中的所有物品, 并将训练集和验证集的数据拼接在一起, 共同参与计算。最后, 将测试集中购买行为的首个记录用作测试。

经过预处理之后, 数据集的详细信息如表 1 所示。

表 1 JD 和 UB 数据集预处理后的记录数量

数据集		浏览	添加购物车	收藏	评论	购买
JD	训练集	217977	0	7380	24662	60967
	验证集	18851	1690	852	3785	5160
	测试集	/	/	/	/	1296
UB	训练集	511020	68207	22270	/	107489
	验证集	59750	8143	2727	/	12925
	测试集	/	/	/	/	6125

对于每种方法的性能评估, 本实验使用两个常用的指标, 即召回率($Rec@K$)和归一化折损累积增益($NDCG@K$)。 $Rec@K$ 衡量推荐列表的前 K 个物品中成功命中用户真实交互物品的比例。 $NDCG@K$ 不仅关注是否命中, 还衡量命中物品在推荐列表中的排序是否靠前。为了统一标准, 本文所有实验

都采取如下方式,在生成目标用户推荐列表时,先将目标用户历史购买过的物品(在验证时,即是训练集中购买过的物品;在测试时,即是训练集和测试集中购买过的物品)从数据集所有物品中去除,然后剩下的所有物品作为候选物品,用于生成目标用户推荐列表。

以下是 $Rec@K$ 和 $NDCG@K$ 的计算公式:

$$Rec@K = \frac{1}{|U^{te}|} \sum_{u \in U^{te}} \frac{1}{|J_u^{te}|} \sum_{l=1}^K \delta(i(l) \in J_u^{te}) \quad (14)$$

$$NDCG@K = \frac{1}{|U^{te}|} \sum_{u \in U^{te}} \frac{DCG_u@K}{IDCG_u@K} \quad (15)$$

$$DCG_u@K = \sum_{l=1}^K \frac{2^{\delta(i(l) \in J_u^{te})} - 1}{\log_2(l+1)} \quad (16)$$

其中, U^{te} 表示测试集中的用户集合, $\delta(i(l) \in J_u^{te})$ 表示在物品推荐列表中,排列在位置 l 的物品是否在当前用户的真实交互列表中,若在,则该表达式的值为 1,否则为 0; $IDCG_u@K$ 则表示理想状态下的 $DCG_u@K$ 值,即当前用户的真实交互列表 J_u^{te} 中的物品恰好排在推荐列表 J_u^{te} 开头的情况。

5.2 基线模型和参数设置

为了充分验证 SPCR 的有效性,本文选取了一些常见的单行为推荐方法、单行为序列推荐方法和多行为序列推荐方法作为基线模型。

(1)UCF^[36]:一种基于杰卡德指数的协同过滤推荐方法。通过杰卡德指数量化用户相似性,是传统相似性度量的根基。

(2)BPRMF^[37]:一种基于矩阵分解的贝叶斯个性化排序推荐方法。以矩阵分解为基础,通过贝叶斯框架优化排序,专注用户偏好建模。

(3)BIS^[5]:一种基于双向物品相似度的协同过滤推荐方法。通过双向物品相似度捕捉序列模式,既考虑物品间的正向关联,又关注用户近期交互的物品,适用于单行为序列推荐场景。

(4)SASRec^[19]:一种基于自注意力机制的序列推荐模型。凭借物品交互序列,通过自注意力机制精准捕捉长期偏好关系,以简洁架构实现高效推荐,为注意力机制在序列推荐中的应用奠定了基础。

(5)FLAG^[23]:一种基于感知局部-全局偏好的多行为序列推荐模型。利用位置注意力层获取全局偏好;借助反馈感知自注意力块提取局部偏好。最终通过物品相似性门控机制,平衡融合局部与全局偏好,结合意图特征实现精准推荐。

(6)NextIP^[24]:一种双任务的多行为序列推荐框架,将问题分解为下一物品预测与购买预测:前者利用目标行为感知上下文聚合器,通过行为序列填充聚合多行为特征;后者通过行为感知自注意力提取行为兴趣作负样本,结合对比学习强化购买导向,提升推荐效果。

(7)FedMF^[38]:一种面向联邦学习的安全矩阵分解模型。用户本地计算梯度并上传,针对梯度泄露问题引入同态加密,无需第三方参与。

(8)FedPerGNN^[39]:一种面向隐私保护的个性化联邦图神经网络框架。结合本地差分隐私与虚拟物品采样保障模型更新安全,通过图扩展协议挖掘高阶信息,全面保护评分与交互历史。

(9)LP-GCN^[31]:一种面向联邦物品推荐的无损隐私保护图卷积网络。采用混合加密与虚拟物品策略,实现嵌入同步和无损卷积,在保护隐私的同时达到集中式模型推荐性能。

(10)GEAR^[40]:一种基于广义交替回归器的多行为序列推荐模型。通过交替编码整合多个要素,结合时间偏差模块化注意力与分层融合,通过自回归的方式实现预测和推荐,并以轻量化架构平衡精度与效率。

本实验借助 TensorFlow 和 Pytorch 框架完成各类深度学习方法的实现,且所有实验均部署于 Linux 操作系统环境。其中,SASRec 方法严格依据对应论文的技术细节自主实现,其他方法则使用了开源代码实现。对于参数设置,固定所有模型的物品嵌入维度 d 为 50、序列长度 L 为 50,学习率为 0.001,批量大小为 128, $Rec@K$ 和 $NDCG@K$ 中的 K 为 10。其他关键参数根据各个推荐方法论文中的建议设置。对于各个方法的超参数,根据其在验证集上 $Rec@10$ 的表现来选取。超参数选取后,各个方法在测试集上的表现即作为实验结果。

对于本文方法 SPCR,固定邻居的数量为 50。可以调节的参数及其范围有:两个衰减参数 a_{sub} 和 a_{inner} , 范围是 $\{0.3, 0.5, 0.7\}$; 权重 λ , 其范围是 $\{0.3, 0.5, 0.7\}$; 衰减参数 a_k , 其范围是 $\{0.1, 0.2, 0.3\}$; k 的范围是 $\{1, 2, 3\}$ 。

5.3 隐私保护技术无损性实验

本实验重点在于验证结合隐私保护技术后,SPCR 性能的无损性,可通过比较中心化方法和结合隐私保护技术的方法 $Rec@10$ 和 $NDCG@10$ 是否一致来验证。

本文在表 2 中报告了实验结果,其中,SCR 和

SPCR 分别表示未结合隐私保护技术的中心化方法和结合隐私保护技术的方法。在实验中,SCR 和 SPCR 的参数选取完全一致。

表 2 隐私保护技术无损性实验结果

数据集	方法	$Rec@10$	$NDCG@10$
JD	SCR	0.1981	0.1114
	SPCR	0.1981	0.1114
UB	SCR	0.0932	0.0604
	SPCR	0.0932	0.0604

与 4.1 节中的无损性理论分析一致,从表 2 实验结果可以看出,在 JD 和 UB 两个数据集中 SCR 和 SPCR 的 $Rec@10$ 和 $NDCG@10$ 结果完全一致,通过实验再次验证了 SPCR 的无损性。

5.4 推荐性能的实验结果与分析

各个方法在两个数据集上的 $Rec@10$ 和 $NDCG@10$ 结果如表 3 所示,其中最佳结果用粗体标记,次优结果用下划线标记。需要注意的是,SASRec(union)是多行为序列版本的 SASRec,两者的不同在于 SASRec(union)训练时会区分不同的行为类型,而 SASRec 不会区分行为类型,默认所有行为类型都为购买行为。类似的,对于其他单行为推荐方法和单行为序列推荐方法,如 UCF、BPRMF、BIS、FedMF、FedPerGNN 和 LP-GCN 采用与 SASRec 相同的处理。此外,SPCR 的结果是通过验证集调参得到的最佳结果。具体参数设置为(详细分析可见 5.6 节):在 JD 数据集上, a_{sub} 和 a_{inner} 分别取 0.5 和 0.3, λ 取 0.5, a_k 取 0.2, k 取 2。在 UB 数据集上, a_{sub} 和 a_{inner} 分别取 0.3 和 0.5, λ 取 0.3, a_k 取 0.2, k 取 1。

从表 3 可以看出,单行为推荐、单行为序列推荐和联邦单行为推荐方法的性能较差,主要原因是这些方法没有捕捉多行为序列信息。对于多行为序列推荐方法,GEAR 在 JD 和 UB 数据集上表现优于 SASRec(union)、FLAG 和 NextIP,主要原因在于其更贴合多行为序列的真实交互规律:通过交替编码将“行为-物品”交织为统一序列,结合低层解耦、高层融合的设计,解决了其他方法中多行为与物品语义割裂的问题;引入时间偏差项精准量化偏好的时序衰减,弥补了同类方法忽略真实时间间隔影响的不足;采用自回归双预测机制,先推进行为意图再预测物品,契合用户决策逻辑。而 SPCR 与 GEAR 在 JD、UB 数据集上的性能,主要源于方法特性与数据集特性的适配度差异。JD 数据集具有购买行为频繁、用户兴趣更新快、子序列独立性强、辅助行为

与购买行为关联较弱等特征。GEAR 凭借交替编码与时间偏差项,精准捕捉行为间的连续时序变化,快速响应用户高频切换的即时兴趣,比较适配这类场景;而 SPCR 的跨行为模块依赖行为间有效关联挖掘信息,在辅助行为与购买行为关联较弱的场景不利于提取有用信息,最终性能略低于 GEAR。UB 数据集则呈现跨行为交互密集、用户兴趣变化慢、数据相对稀疏等特点。SPCR 通过其相似度公式挖掘跨行为语义关联,再通过动态调节相似度适配稳定的行为模式;而 GEAR 的自回归建模依赖长序列,稀疏数据下易受噪声影响,对跨行为语义关联建模缺乏针对性,难以利用 UB 的跨行为密集特性,因此 SPCR 性能更优。

表 3 SPCR 和基线方法在 JD 和 UB 上的推荐性能

数据集	JD		UB		
	方法	$Rec@10$	$NDCG@10$	$Rec@10$	$NDCG@10$
数据集	UCF	0.1311	0.0694	0.0157	0.0083
	BPRMF	0.1156	0.0332	0.0130	0.0068
	BIS	0.1311	0.0694	0.0157	0.0083
	SASRec	0.1503	0.0754	0.0657	0.0504
	SASRec (union)	0.1525	0.0770	0.0675	0.0504
	FLAG	0.1699	0.0784	0.0892	0.0561
	NextIP	0.1787	0.1018	0.0587	0.0411
	GEAR	0.2059	0.1126	<u>0.0921</u>	0.0655
	FedMF	0.1295	0.0675	0.0108	0.0056
	FedPerGNN	0.1403	0.0714	0.0137	0.0066
	LP-GCN	0.1372	0.0742	0.0170	0.0083
	SPCR	0.1981	0.1114	0.0932	0.0604

此外,与 SASRec(union)、FLAG、NextIP 相比,SPCR 在两个数据集上两个评估指标都有所提升。SPCR 通过子序列划分,利用用户之间对同一物品的交互时间和行为类型的差异来构建用户相似度,并在预测评分时根据目标物品的不同,动态调整用户相似度。具体来说,公式(12)和公式(13)量化了两个用户在购买目标物品前行为偏好的差异,并根据这个差异灵活调节用户相似度,可更细致地挖掘用户近期行为中的一致性特征,弥补传统方法对动态行为模式刻画和不足,从而提高推荐性能。而 SASRec(union)可能仅依赖一般的序列编码方式,无法充分挖掘这种细粒度的行为特征。FLAG 虽设计了反馈感知自注意力块,但在行为序列划分和权重利用的针对性上可能不如 SPCR。NextIP 在处理行为序列时,重点在于双任务学习,对序列内行为的权重分配可能不够细致。

为了分析 SPCR 的推荐性能比 SASRec(union)、

FLAG 和 NextIP 的推荐性能更佳的原因,同时体现其具有强可解释性的优势,下面通过图 6 的例子来说明 SPCR 可以捕捉 SASRec(union)、FLAG 和 NextIP 无法捕捉的信息,进而得到更好的推荐性能。

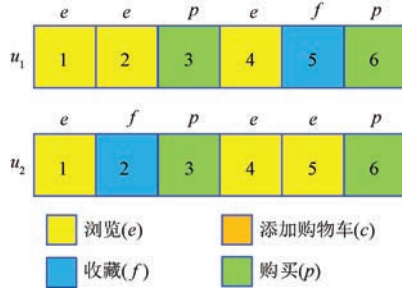


图 6 用户交互序列示意图

结合图 6 分析, SASRec(union) 将所有行为等同处理, 通过自注意力捕捉序列关联, 但未区分不同行为类型的权重, 无法捕捉不同行为类型之间的差异。而在 SPCR 的公式(7)中, 分子的第一项对应用户 u_1 和用户 u_2 的相同行为类型(如用户 u_1 和用户 u_2 均购买物品 6)的关联程度, 第二项对应不同行为类型(如用户 u_1 浏览物品 2 和用户 u_2 收藏物品 2)的关联程度, 并通过权重 λ 灵活调节两类关联的影响占比, 让行为关联的计算逻辑更清晰。对于 FLAG: 它虽能通过反馈感知自注意力区分为行为类型, 进而建模单一用户的局部或全局偏好, 但并未考虑用户间的协同相似性。具体来说, FLAG 能识别用户 u_1 对于物品 3 和物品 6 是购买行为, 权重最大, 但是它无法利用到用户 u_1 和用户 u_2 在购买物品 3 后都浏览了物品 4, 并后续购买了物品 6 这个信息, 因此难以通过用户 u_2 的序列(后续浏览了物品 5)来帮助判断用户 u_1 中收藏物品 5 对于购买物品 6 的影响, 这会影响其推荐性能。而 SPCR 通过近期行为模式一致性模块, 识别用户 u_1 和用户 u_2 在购买物品 6 前的交互共性, 动态调节相似度。NextIP 通过双任务学习和行为感知自注意力处理行为变化, 但对子序列结构的利用不足。用户 u_1 和用户 u_2 的序列都可以划分为两条子序列(根据购买行为划分), 子序列内的行为对后续购买的影响权重随位置衰减。NextIP 虽能聚合行为为特定子序列, 但未明确区分以购买物品 3 为子序列的边界, 导致无法精准计算用户 u_1 中收藏物品 5 的衰减权重, 进而很难准确表示收藏物品 5 对购买物品 6 的关联。而 SPCR 则以购买行为为子序列边界, 借助时间衰减函数, 能明确计算出子序列内收藏物品 5 对购买物品 6 的影响程度, 让子序列中的行为关联更清晰可溯。

综上, 相较于无隐私保护的方法, SPCR 既优于 FLAG、NextIP 等基线模型, 又与 GEAR 在不同数据集上展现出差异化表现; 而与 FedPerGNN、LP-GCN 等隐私保护方法相比, 其推荐性能同样更具优势, 充分彰显了 SPCR 兼顾推荐性能与隐私保护的优点。

5.5 参数敏感性实验

本小节将研究每个参数对 SPCR 性能的影响。其中, 可以调节的参数及其范围有: 两个衰减参数 a_{sub} 和 a_{inner} , 其范围都是 $\{0.3, 0.5, 0.7\}$; 权重 λ , 其范围是 $\{0.3, 0.5, 0.7\}$; 衰减参数 a_k , 其范围是 $\{0.1, 0.2, 0.3\}$; k 的范围是 $\{1, 2, 3\}$ 。

首先, 需要对参数 a_{sub} 和 a_{inner} 进行实验, 从而得到在两个数据集上 a_{sub} 和 a_{inner} 的最佳组合。其中, 最佳结果用粗体标记。

通过表 4 的结果可以看出在 JD 数据集上, a_{sub} 和 a_{inner} 取 0.5 和 0.3 时, 推荐性能最好。而在 UB 数据集上, a_{sub} 和 a_{inner} 取 0.3 和 0.5 时, 推荐性能最好。

表 4 不同衰减参数在 JD 和 UB 上的推荐性能

数据集	a_{sub}	a_{inner}	$Rec@10$	$NDCG@10$
JD	0.3	0.3	0.1904	0.1067
	0.3	0.5	0.1897	0.1068
	0.3	0.7	0.1889	0.1071
	0.5	0.3	0.1904	0.1071
	0.5	0.5	0.1897	0.1067
	0.5	0.7	0.1889	0.1066
	0.7	0.3	0.1881	0.1072
	0.7	0.5	0.1874	0.1069
	0.7	0.7	0.1881	0.1071
UB	0.3	0.3	0.0722	0.0451
	0.3	0.5	0.0726	0.0451
	0.3	0.7	0.0710	0.0444
	0.5	0.3	0.0718	0.0448
	0.5	0.5	0.0718	0.0448
	0.5	0.7	0.0708	0.0443
	0.7	0.3	0.0715	0.0441
	0.7	0.5	0.0713	0.0440
	0.7	0.7	0.0710	0.0440

分析时间衰减函数, 可知 a_{sub} 越大, 子序列权重随时间快速衰减, 意味着更关注最近的子序列, 适用于用户兴趣变化频繁的场景; a_{sub} 越小, 衰减越平缓, 历史子序列仍保留较高权重, 适用于用户兴趣较稳定、长期偏好显著的场景。对于 a_{inner} , 较大的 a_{inner} 使子序列内早期物品权重快速下降, 强调近期交互物品的影响, 适用于短期兴趣波动较大的场景。较小的 a_{inner} 使子序列内物品权重差异更小, 更均衡地考虑整个子序列内的物品, 适用于兴趣连贯性较

强的场景。两个数据集上使性能最优的 a_{sub} 和 a_{inner} 取值存在差异,原因可能是 JD 数据集购买行为频繁,兴趣更新快,因而子序列间独立性较强,不同子序列可能对应完全不同的需求,同时子序列内物品的关联性也相对较弱。而对于 UB 数据集,其交互行为连贯性较强,兴趣变化较慢,子序列间存在长期偏好的延续性,可捕捉长期兴趣。

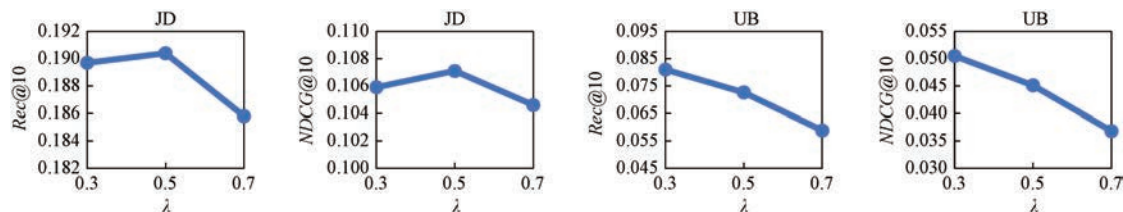


图7 不同权重参数在 JD 和 UB 上的推荐性能

接下来,探讨衰减参数 a_k 和 k 对推荐性能的影响。在 JD 数据集上 a_{sub} 、 a_{inner} 和 λ 设置为 0.5、0.3 和 0.5,在 UB 数据集上 a_{sub} 、 a_{inner} 和 λ 设置为 0.3、0.5 和 0.3。

表5 不同衰减参数和子序列窗口数
在 JD 和 UB 上的推荐性能

数据集	a_k	k	Rec@10	NDCG@10
JD	0.1	1	0.1935	0.1121
	0.1	2	0.1974	0.1105
	0.1	3	0.1928	0.1083
	0.2	1	0.1935	0.1121
	0.2	2	0.1981	0.1114
	0.2	3	0.1928	0.1086
	0.3	1	0.1935	0.1121
	0.3	2	0.1974	0.1109
	0.3	3	0.1904	0.1080
	0.3	3	0.1904	0.1080
UB	0.1	1	0.0932	0.0604
	0.1	2	0.0911	0.0584
	0.1	3	0.0890	0.0560
	0.2	1	0.0932	0.0604
	0.2	2	0.0913	0.0585
	0.2	3	0.0893	0.0563
	0.3	1	0.0932	0.0604
	0.3	2	0.0906	0.0583
	0.3	3	0.0899	0.0565
	0.3	3	0.0899	0.0565

通过表5的结果可以看出在 JD 和 UB 数据集上, a_k 取 0.2 时,推荐性能最好,而 k 则分别取 2 和 1 时,推荐性能最佳。与 a_{sub} 不同, a_k 对应的子序列数量由 k 控制, k 在大多数情况下显著小于一条完整序列的子序列数,所以 a_k 取一个较小的值是合理的,其有利于平缓相近 k 个子序列的衰减速度,强调相近 k 个子序列偏好的传递性和相似性。

5.6 消融实验

本小节主要研究 SPCR 的三个模块(三个模块

下面探讨权重 λ 对推荐性能的影响。实验过程中,在 JD 数据集上 a_{sub} 和 a_{inner} 设置为 0.5 和 0.3,在 UB 数据集上 a_{sub} 和 a_{inner} 设置为 0.3 和 0.5。

通过图7的结果可以看出,在 JD 数据集上, λ 取 0.5 时,推荐性能最好,而在 UB 数据集上, λ 取 0.3 时,推荐性能最好。说明 UB 数据集与 JD 数据集相比,跨行为能更好地表示用户的偏好。

的具体含义会在本小节中详细说明)对推荐性能的影响。在两个数据集上进行消融实验,实验结果如表6所示。

表6 不同子组件对推荐性能的影响

数据集	方法	Rec@10	NDCG@10
JD	w/o DD	0.1951(−1.5%)	0.1078(−3.2%)
	w/o λ	0.1981(0)	0.1114(0)
	w/o $\Delta_{u,w}^j$	0.1904(−4.0%)	0.1071(−3.9%)
	SPCR	0.1981	0.1114
UB	w/o DD	0.0442(−52.6%)	0.0272(−55.0%)
	w/o λ	0.0826(−11.4%)	0.0536(−11.3%)
	w/o $\Delta_{u,w}^j$	0.0810(−13.1%)	0.0505(−16.4%)
	SPCR	0.0932	0.0604

w/o DD 表示去除跨行为交互模块,即相似度公式从公式(6)退回公式(5),剔除不同行为类型的贡献项。从表6可知,其推荐性能与 SPCR 相比在 JD 和 UB 数据集上都有下降。其中,在 UB 数据集上,w/o DD 与另外两组消融方法(w/o λ 和 w/o $\Delta_{u,w}^j$)相比,下降幅度最大。这可能是因为 UB 数据集跨行为交互更密集,占相似性计算的比例较高,即在公式(6)中分子的第二项比第一项对相似度计算的贡献程度更大。故删去跨行为交互模块后,会丢失大量跨行为关联信息,导致推荐性能下降。JD 数据集跨行为交互较少(占比较低),辅助行为与购买行为的关联较弱,因而 w/o DD 下降幅度较小。

w/o λ 表示不考虑相同行为类型的贡献和不同行为类型的贡献的权重关系,将两者的权重都固定为 1,即公式(6)中分子和分母两项的权重都为 1。从实验结果可以看出,与 SPCR 相比,在 JD 数据集上,w/o λ 推荐性能没有下降;而在 UB 数据集上,存在性能下降。因为在 JD 数据集上,SPCR 的 λ 取

0.5,即公式(6)中分子和分母两项的权重都为0.5,相当于第一项和第二项的权重相等,与 $w/o\lambda$ 的情况是一致的,所以性能不变是合理的。在UB数据集上, $w/o\lambda$ 存在性能下降,验证了权重调节对提升性能的有效性。从UB数据集本身的特点分析,如上一段文字所述,该数据集跨行为交互更密集,公式(6)中分子的第二项比第一项对相似度计算的贡献程度更大。而SPCR变成 $w/o\lambda$,即第二项的权重从0.7下降到0.5,第一项的权重从0.3上升到0.5,不仅降低了跨行为交互对相似度计算的贡献程度,还提高了同行为交互对相似度计算的贡献程度,相当于降低了更能代表用户偏好的信息的权重,导致性能下降。

$w/o\Delta_{u,w}^j$ 表示去除近期行为模式一致性模块,即预测公式中 $\Delta_{u,w}^j$ 固定为0,推荐性能有所下降,证明了近期行为模式一致性模块的有效性。其中, $w/o\Delta_{u,w}^j$ 在UB数据集的降幅大于JD数据集,其原因是:JD数据集具有购买行为频繁、用户兴趣更新快的特点,不同用户购买相同物品前的行为模式差异较大,近期行为模式一致性模块的动态调节作用在此场景下发挥受限,因此去除后对推荐性能的影响较小,下降幅度较小;而UB数据集中用户兴趣更新较慢,不同用户购买相同物品前的行为模式比较相似,有利于发挥近期行为模式一致性模块的调节作用,去除后损失关键信息,降幅较大。

6 结 论

针对联邦多行为序列推荐(FMBSR)问题的核心痛点——难以同时实现多行为序列精准建模、用户隐私严格保护与推荐性能无损,本文提出了基于子序列的隐私保护协同推荐方法(SPCR)。该方法以强可解释性的协同过滤作为核心框架,包含三个模块和阶段:密钥初始化阶段由随机选择的客户端 u_c 生成共享密钥 E ,用于加密后续敏感信息;相似度计算阶段先划分原始序列为子序列,通过含归一化的时间衰减函数量化偏好关联,再设计融入跨行为信息的相似度公式;预测评分阶段通过近期行为模式一致性模块动态调节邻居相似度,适配目标物品差异。

本文通过理论分析证明了SPCR可防御参数重构、成员推理与属性推理等常见攻击,充分保障用户数据安全。在JD和UB两个真实数据集上的实验结果表明,SPCR兼具推荐性能与隐私保护优势:相

较于无隐私保护的方法,它优于FLAG、NextIP等基线模型,与GEAR相当;相较于FedPerGNN、LP-GCN等隐私保护类方法,它在推荐性能上具有显著优势。此外,SPCR与未结合隐私保护的中心化方法(SCR)的实验结果完全一致,充分验证了其隐私保护无损化的优势。

综上,SPCR是FMBSR场景中,同时满足多行为序列精准建模、用户隐私严格保护与推荐性能无损的有效方法,为FMBSR的实际落地提供了兼具安全性、实用性与可解释性的技术方案。

最后,基于本文的研究,关于未来工作方向,SPCR后续可以从两个方向进行拓展:结合多模态与去噪机制优化用户偏好建模^[41],探索SPCR在多模态敏感信息场景中的优化;结合联邦跨域框架^[42],将SPCR拓展至多平台、跨领域的场景。

参 考 文 献

- [1] Cen Y, Zhang J, Wang G, Qian Y, Meng C, Dai Z, Yang H, Tang J. Trust relationship prediction in Alibaba e-commerce platform. *IEEE Transactions on Knowledge and Data Engineering*, 2019,32(5):1024-1035
- [2] Sharma K, Lee Y C, Nambi S, Salian A, Shah S, Kim S W, Kumar S. A survey of graph neural networks for social recommender systems. *ACM Computing Surveys*, 2024,56(10):1-34
- [3] Gong X, Feng Q, Zhang Y, Qin J, Ding W, Li B, Jiang P, Gai K. Real-time short video recommendation on mobile devices//*Proceedings of the 31st ACM International Conference on Information & Knowledge Management*. Atlanta, USA, 2022:3103-3112
- [4] Zhao X, Zhang W, Wang J. Interactive collaborative filtering//*Proceedings of the 22nd ACM International Conference on Information & Knowledge Management*. San Francisco, USA, 2013:1411-1420
- [5] Zeng Z, Lin J, Li L, Pan W, Ming Z. Next-item recommendation via collaborative filtering with bidirectional item similarity. *ACM Transactions on Information Systems*, 2019,38(1):1-22
- [6] Zhao Jing-Xin, Yue Xing-Hui, Feng Chong-Peng, et al. A survey on data privacy and security based on general data protection regulation. *Journal of Computer Research and Development*, 2022,59(10):2130-2163(in Chinese)
(赵景欣,岳星辉,冯崇朋等.基于通用数据保护条例的数据隐私安全综述. *计算机研究与发展*, 2022,59(10):2130-2163)
- [7] Yang Q, Liu Y, Chen T, Tong Y. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, 2019,10(2):1-19
- [8] Tang Xiang-Yun, Wang Wei, Weng Yu, et al. A survey on privacy security and algorithm efficiency in federated unlearning. *Chinese Journal of Computers*, 2025,48(9):2064-2093

- (in Chinese)
(唐湘云,王伟,翁或等.联邦遗忘学习隐私安全与算法效率研究综述.计算机学报,2025,48(9):2064-2093)
- [9] Xie W, Lu Y, Li D, Li Y. Ebbinghaus-curve guided low-rank component-induced attention for multisource remote sensing classification. *IEEE Transactions on Geoscience and Remote Sensing*, 2024,62: 1-12
- [10] Cui Z, Sun X, Chen H, Pan L, Cui L, Liu S, Xu G. Dynamic recommendation based on graph diffusion and ebbinghaus curve. *IEEE Transactions on Computational Social Systems*, 2023,11(2):2755-2764
- [11] Kamara S, Papamanthou C, Roeder T. Dynamic searchable symmetric encryption//*Proceedings of the 2012 ACM Conference on Computer and Communications Security*. Raleigh, USA, 2012:965-976
- [12] Abd Elminaam D S, Abdual-Kader H M, Hadhoud M M. Evaluating the performance of symmetric encryption algorithms. *International Journal of Network Security*, 2010,10(3):216-222
- [13] Meng Yang, Liu Ke-Long, Qing Si-Han. A scalable multi-level secure conference key distribution system. *Chinese Journal of Computers*, 2000,23(8):793-798(in Chinese)
(蒙杨,刘克龙,卿斯汉.可扩展的多级安全会议密钥分发体制.计算机学报,2000,23(8):793-798)
- [14] Simmons G J. Symmetric and asymmetric encryption. *ACM Computing Surveys*, 1979,11(4):305-330
- [15] Rendle S, Freudenthaler C, Schmidt-Thieme L. Factorizing personalized markov chains for next-basket recommendation//*Proceedings of the 19th International Conference on World Wide Web*. Raleigh, USA, 2010:811-820
- [16] He R, McAuley J. Fusing similarity models with markov chains for sparse sequential recommendation//*Proceedings of the IEEE 16th International Conference on Data Mining*. Barcelona, Spain, 2016:191-200
- [17] Tang J, Wang K. Personalized top-n sequential recommendation via convolutional sequence embedding//*Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining*. Marina Del Rey, USA, 2018:565-573
- [18] Hidasi B, Karatzoglou A. Recurrent neural networks with top-k gains for session-based recommendations//*Proceedings of the 27th ACM International Conference on Information and Knowledge Management*. Torino, Italy, 2018:843-852
- [19] Kang W C, McAuley J. Self-attentive sequential recommendation//*Proceedings of the 2018 IEEE International Conference on Data Mining*. Singapore, 2018:197-206
- [20] Li Z, Zhao H, Liu Q, Huang Z, Mei T, Chen E. Learning from history and present: Next-item recommendation via discriminatively exploiting user behaviors//*Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*. London, UK, 2018:1734-1743
- [21] Zhou M, Ding Z, Tang J, Yin D. Micro behaviors: A new perspective in e-commerce recommender systems//*Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining*. Los Angeles, USA, 2018:727-735
- [22] Liu Q, Wu S, Wang L. Multi-behavioral sequential prediction with recurrent log-bilinear model. *IEEE Transactions on Knowledge and Data Engineering*, 2017,29(6):1254-1267
- [23] He M, Lin J, Luo J, Pan W, Ming Z. FLAG: A feedback-aware local and global model for heterogeneous sequential recommendation. *ACM Transactions on Intelligent Systems and Technology*, 2022,14(1):1-22
- [24] Luo J, He M, Lin X, Pan W, Ming Z. Dual-task learning for multi-behavior sequential recommendation//*Proceedings of the 31st ACM International Conference on Information & Knowledge Management*. Atlanta, USA, 2022:1379-1388
- [25] Wang Kun, Wang Yong, Zhang Zhi-Qiang, et al. A privacy-preserving graph neural network framework for recommendation. *Chinese Journal of Computers*, 2025,48(5):1116-1133 (in Chinese)
(王锬,王永,张智强等.一种面向推荐系统的隐私保护图神经网络.计算机学报,2025,48(5):1116-1133)
- [26] Yang En-Yue, Pan Wei-Ke, Yang Qiang, Ming Zhong. Federated learning and recommender systems. *Communications of the China Computer Federation*, 2022,18(9):19-27 (in Chinese)
(羊恩跃,潘微科,杨强等.联邦学习和推荐系统.中国计算机学会通讯,2022,18(9):19-27)
- [27] Liang Feng, Yang En-Yue, Pan Wei-Ke, Yang Qiang, Ming Zhong. A Survey on Recommender Systems Based on Federated Learning. *SCIENTIA SINICA Informationis*, 2022,52(5):713-741(in Chinese)
(梁锋,羊恩跃,潘微科等.基于联邦学习的推荐系统综述.中国科学:信息科学,2022,52(5):713-741)
- [28] Lin G, Liang F, Pan W, Ming Z. FedRec: Federated recommendation with explicit feedback. *IEEE Intelligent Systems*, 2020,36(5):21-30
- [29] Liang F, Pan W, Ming Z. FedRec++: Lossless federated recommendation with explicit feedback//*Proceedings of the AAAI Conference on Artificial Intelligence*. Virtual, 2021: 4224-4231
- [30] Lin Z, Pan W, Yang Q, Ming Z. A generic federated recommendation framework via fake marks and secret sharing. *ACM Transactions on Information Systems*, 2022,41(2): 1-37
- [31] Wu G, Pan W, Yang Q, Ming Z. Lossless and privacy-preserving graph convolution network for federated item recommendation. *arXiv preprint arXiv: 2412.01141*, 2024
- [32] Li Z, Long G, Zhou T. Federated recommendation with additive personalization. *arXiv preprint arXiv: 2301.09109*, 2023
- [33] Kim J, Koo D, Kim Y, Yoon H, Shin J, Kim S. Efficient privacy-preserving matrix factorization for recommendation via fully homomorphic encryption. *ACM Transactions on Privacy and Security*, 2018,21(4):1-30
- [34] Khoshneshin M, Street W N. Collaborative filtering via euclidean embedding//*Proceedings of the 4th ACM Conference on Recommender Systems*. Barcelona, Spain, 2010:87-94
- [35] Wang L, Zhang Y, Feng J. On the euclidean distance of images. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2005,27(8):1334-1339
- [36] Pan R, Zhou Y, Cao B, Liu N N, Lukose R, Scholz M, Yang Q. One-class collaborative filtering//*Proceedings of the 8th IEEE International Conference on Data Mining*. Pisa, Italy, 2008:502-511
- [37] Rendle S, Freudenthaler C, Gantner Z, Schmidt-Thieme L.

- BPR: Bayesian personalized ranking from implicit feedback//
Proceedings of the 25th Conference on Uncertainty in Artificial Intelligence. Montreal, Canada, 2009:452-461
- [38] Chai D, Wang L, Chen K, Yang Q. Secure federated matrix factorization. *IEEE Intelligent Systems*, 2020,36(5):11-20
- [39] Wu C, Wu F, Lyu L, Qi T, Huang Y, Xie X. A federated graph neural network framework for privacy-preserving personalization. *Nature Communications*, 2022,13(1):3091
- [40] Jiang J, Zhang K, Kang J, Luo Y, Gao M. GEAR: Generalized alternating regressor for multi-behavior sequential recommendation//Proceedings of the 48th International ACM SIGIR Conference on Research and Development in Information Retrieval. Manila, Philippines, 2025:2870-2874
- [41] Cui X, Lu W, Tong Y, Li Y, Zhao Z. Multi-modal multi-behavior sequential recommendation with conditional diffusion-based feature denoising//Proceedings of the 48th International ACM SIGIR Conference on Research and Development in Information Retrieval. Manila, Philippines, 2025:1593-1602
- [42] Zheng D, Zhang H, Zhai J, Zhong L, Wang L, Feng J, Liao X, Tian Y, Xiao N, Liao Q. FedCSR: A federated framework for multi-platform cross-domain sequential recommendation with dual contrastive learning//Proceedings of the 31st International Conference on Computational Linguistics. Bangkok, Thailand, 2025:8699-8713



GUAN Hao-Rong, M. S. candidate. His research interests include recommender systems and federated learning.

PAN Wei-Ke, Ph. D., professor. His research interests include recommender systems, deep learning, transfer

learning and federated learning.

MING Zhong, Ph. D., professor. His research interests include software engineering and artificial intelligence.

Background

With the rapid development of the Internet, recommender systems play an increasingly important role in various fields such as e-commerce. Traditional multi-behavior sequential recommendation (MBSR) requires the centralized collection of complete user interaction sequences, posing a risk of privacy leakage. Although federated multi-behavior sequential recommendation (FMBSR) avoids the privacy issues associated with centralized data storage, existing studies have obvious limitations: federated recommendation methods can ensure privacy but often fail to capture multi-behavior sequential characteristics, while centralized multi-behavior recommendation models can effectively capture users' dynamic multi-behavior preferences but have risks of privacy leakage. Currently, there is no method in the FMBSR field that can simultaneously achieve accurate multi-behavior sequential modeling, privacy security, and lossless performance.

To address the above issues, this paper proposes a subsequence-based privacy-preserving collaborative recommendation method (SPCR), which takes collaborative filtering with strong interpretability as its core framework and is implemented with three components and stages: (i) in the key initialization stage, a randomly selected client generates a shared key for encrypting subsequent sensitive information; (ii) in the similarity calculation stage, the original sequence is first divided into subsequences, a temporal decay function with normalization is used to quantify the preference correlation, and then a similarity formula integrating cross-behavior information is designed; and (iii) in the prediction scoring stage, a recent behavior pattern consistency module dynam-

cally adjusts neighbor similarity to adapt to differences among target items.

Experiments on two real-world datasets, i. e., JD and UB, demonstrate that SPCR possesses the advantage of balancing recommendation performance and privacy protection: compared with privacy-unprotected methods, it outperforms baseline models such as FLAG and NextIP and performs comparable with GEAR; while compared with privacy-preserving methods like FedPerGNN and LP-GCN, it achieves more superior recommendation performance. On the JD dataset, SPCR's performance is slightly lower than that of GEAR, with Rec@10 reaching 0.1981 and NDCG@10 reaching 0.1114, representing increases of approximately 10.86% and 9.42% respectively compared to the second-best baseline NextIP. On the UB dataset, SPCR outperforms GEAR on Rec@10, and its results (Rec@10 = 0.0932 and NDCG@10 = 0.0604) outperform the second-best baseline FLAG by approximately 4.48% and 7.67%, respectively. Furthermore, the results of our SPCR and its centralized version SCR without privacy protection are completely consistent on Rec@10 and NDCG@10, verifying the losslessness of the privacy protection scheme. Our SPCR is the first method in FMBSR with accurate multi-behavior sequential modeling, privacy security, lossless performance, and strong interpretability, achieving an effective balance between privacy protection, recommendation performance, and interpretability.

This work was supported by the National Natural Science Foundation of China (62461160311,62272315).