NEURAL INFORMATION PROCESSING SYSTEMS

Federated Graph Learning for Cross-Domain Recommendation

Ziqi Yang[1,2], Zhaopeng Peng[1,2], Zihui Wang[1,2], Jianzhong Qi[3], Chaochao Chen[4],Weike Pan[5], Chenglu Wen[1,2], Cheng Wang[1,2], Xiaoliang Fan[1,2*]

[1]Fujian Key Laboratory of Sensing and Computing for Smart Cities,Xiamen University, China.

[2]Key Laboratory of Multimedia Trusted Perception and Efficient Computing,Ministry of Education of China, Xiamen University, China.

[3]University of Melbourne

[4]College of Computer Science and Technology, Zhejiang University Hangzhou, China

[5]College of Computer Science and Software Engineering, Shenzhen University Shenzhen, China

Contact: Ziqi Yang, Xiaoliang Fan*

yangziqi@stu.xmu.edu.cn fanxiaoliang@xmu.edu.cn

Background: Cross-Domain Recommendation

Traditional recommendation systems are faced with two long-standing obstacles, namely data sparsity and cold-start problems, which promote the emergence and development of Cross-Domain Recommendation (CDR). The core idea of CDR is to leverage information collected from other domains to alleviate the two problems in one domain[1].

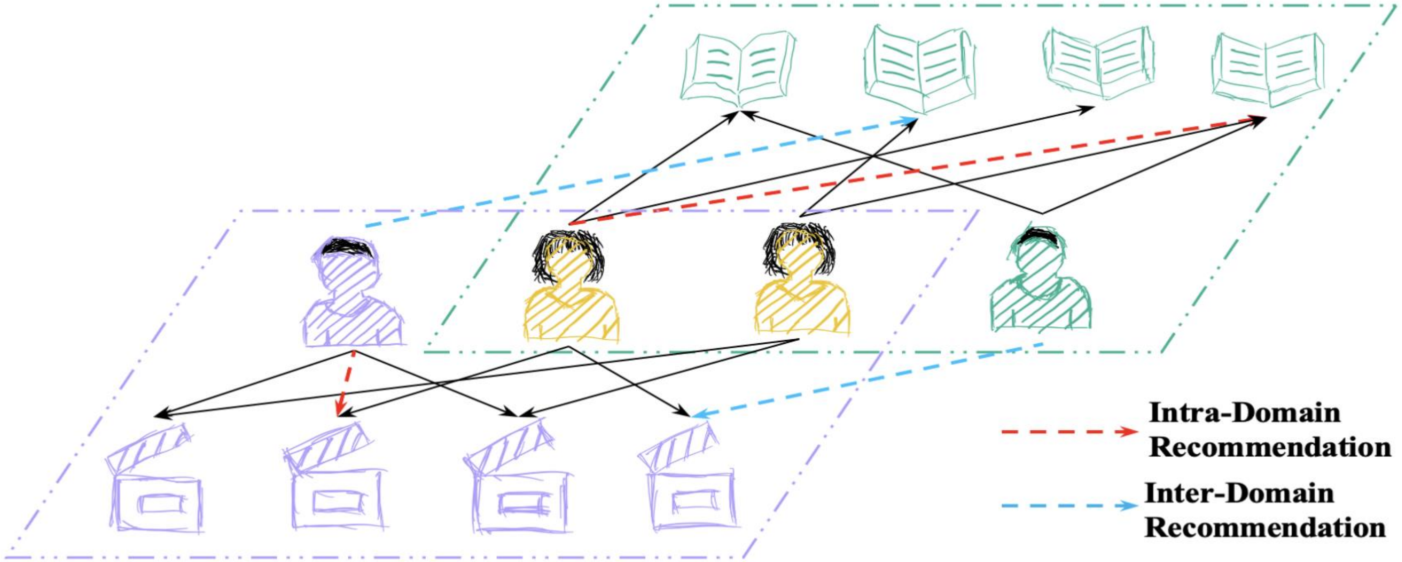
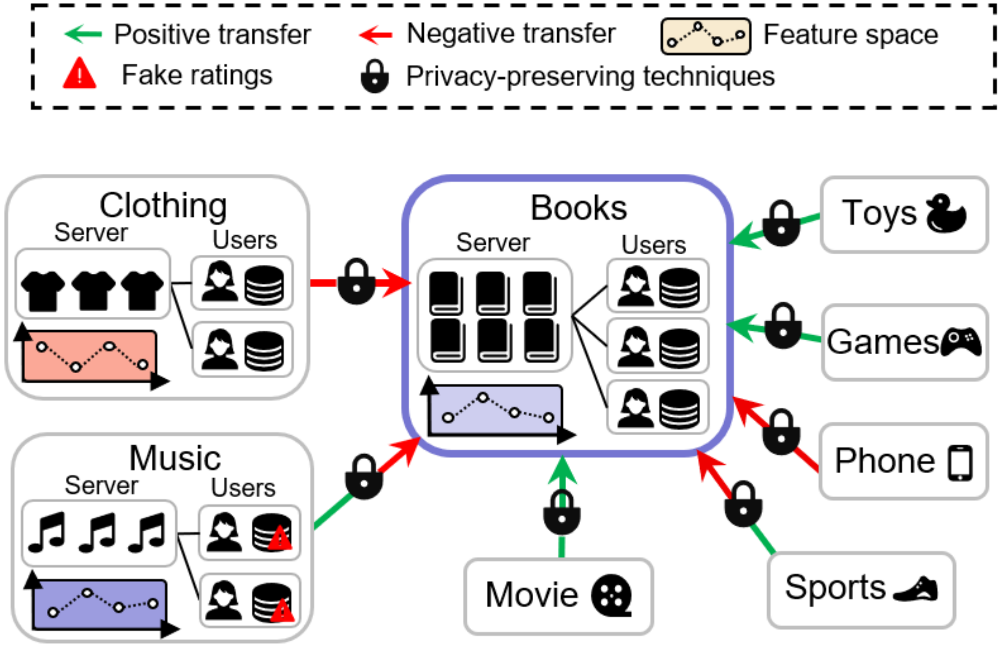


Figure 1. Illustration of cross-domain recommendation[2]

Motivation: Privacy and Negative Transfer

In order to distinguish our work from previous efforts, we focused a more generic scenario of Broader-Source Cross-Domain Recommendation (BS-CDR), which integrates knowledge from more than two source domains.



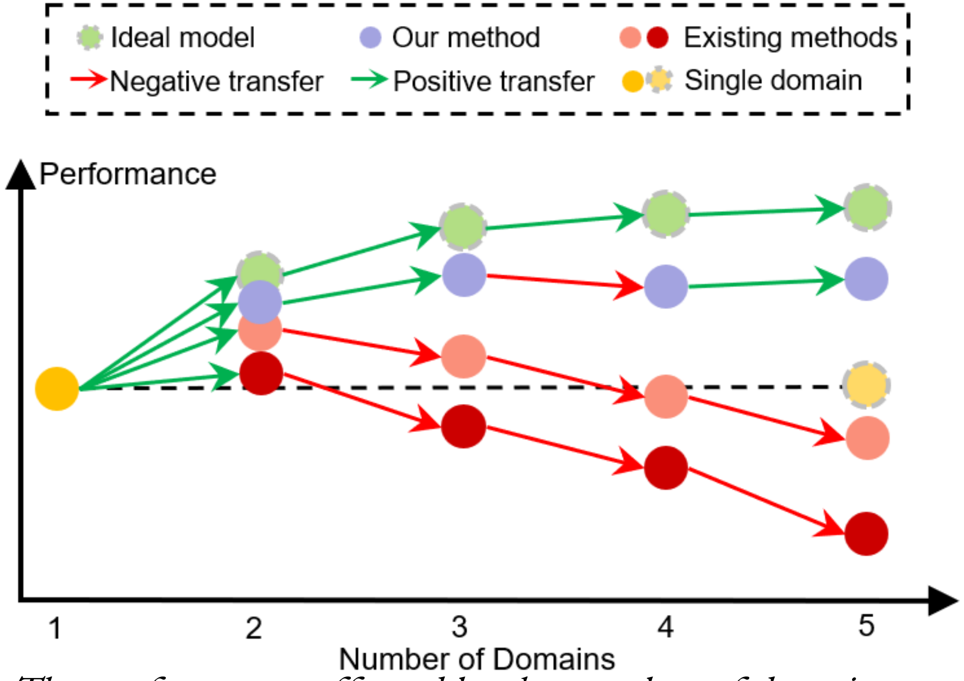


Figure 2. (a) The BS-CDR scenario. (b) The performance affected by the number of domains

In this specific scenario, we face two prominent challenges :

1. Inadequate privacy preservation. Both intra- and inter-domain privacy must be carefully considered in BS-CDR.
2. Accumulative negative transfer. The impact of negative transfer can inevitably intensify with an increasing number of source domains and the performance of CDR models can decline to levels lower than those of single-domain model.

空间感知与计算实验室
spAtial Sensing & Computing Lab

Method (1/4): Overall Architecture

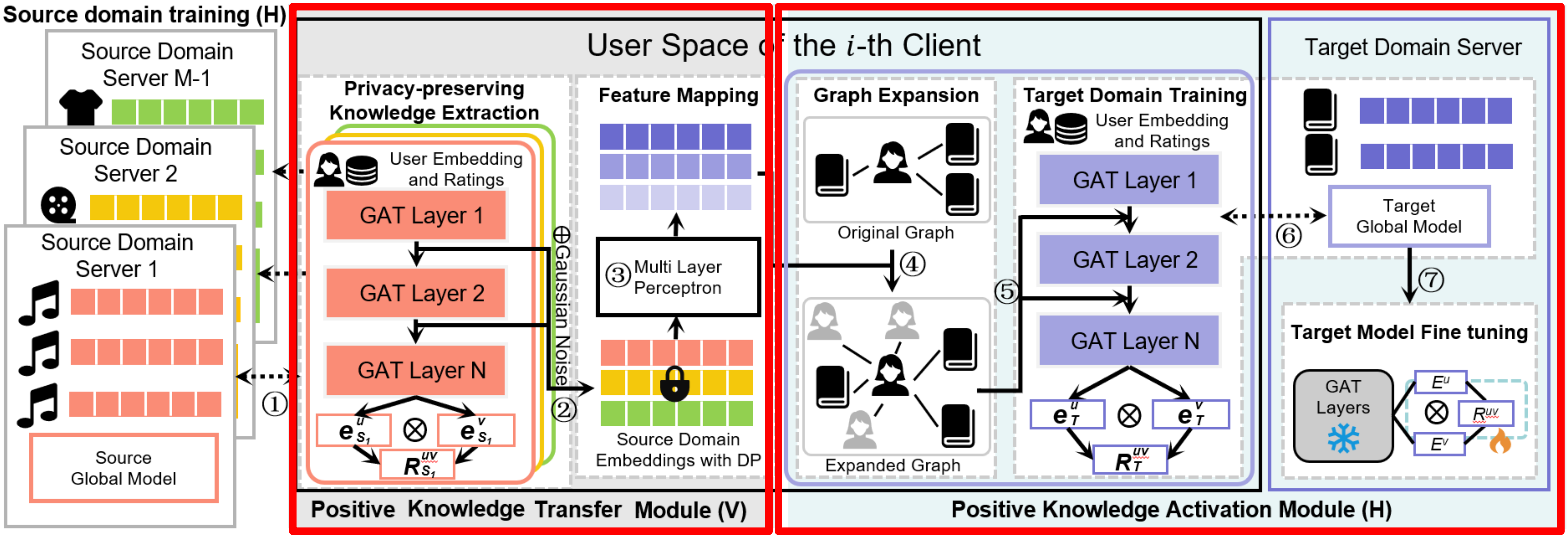


Figure 3. An overview of FedGCDR.

FedGCDR proposes two modules : Positive Knowledge Transfer Module and Positive Knowledge Activation Module to address these challenges.

空间感知与计算实验室 spAtial Sensing & Computing Lab

Method (2/4): Positive Knowledge Transfer Module (Module 1)

First, privacy-preserving knowledge extraction

In a GNN-based approach, direct transfers are subject to privacy attacks. Each message propagation layer can be viewed as a function with user and item embeddings as input. An attacker can easily obtain the private rating matrix based on these embeddings. We apply DP to the source domain embeddings to safeguard inter-domain privacy.

Second, feature mapping

User features could represent personal preferences and are influenced by domain features. The discrepancy of domains leads to the heterogeneity of feature space between domains which means that source domain embeddings cannot be utilized directly by the target domain. We adopt a series of MLP to explore mapping functions for each source domain. To learn more effective mapping function, we adopt a mapping loss term:

$$l_m = \sum_{i=1}^{M-1} \sum_{l=1}^{L} \left\| x_T^l - MLP_i\left(\hat{x}_{S_{M-1}}^l\right) \right\|^2$$

空间感知与计算实验室
spAtial Sensing & Computing Lab

Method (3/3): Positive Knowledge Activation Module (Module 2)

First, graph expansion and target domain training

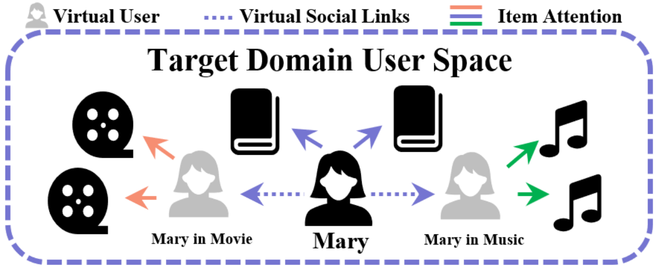


Figure 4. Illustration of graph expansion.

We construct virtual users by embeddings from the source domains. Based on their correlated preference (they actually are the same person), we build social links between them and the real target user to generate attention coefficients (which can be regarded as domain attention).

Beside, we introduce a social regularization term[3] to strengthen the virtual social links:

$$ls = \sum_{l=1}^{L} \left\| x_T^l - \frac{\sum_{i=1}^{M-1} Sim(x_T^l, \hat{x}_{S_i}^l) \times \hat{x}_{S_i}^l}{\sum_{i=1}^{M-1} Sim(x_T^l, \hat{x}_{S_i}^l)} \right\|$$

Considering the feature mapping and virtual social links, the objective function of the target domain is:

$$L_{GAT} = BCELoss\left(\hat{R}_{uv}^T, R_{uv}^T\right) + \frac{\alpha}{2} l_m + \frac{\beta}{2} l_s$$

Second, target model fine-tuning

To further filter external noise, we adopt an additional fine-tuning stage: First, we freeze the message propagation layer of GAT to isolate the influence of source domains preventing Gaussian noise from permeating through the transfer process. Second, we directly train the well-informed embeddings generated by the target domain GAT. These steps adapt the learned external knowledge for predicting the target domain ratings.

空间感知与计算实验室
spAtial Sensing & Computing Lab

Experiments (1/4): Setting

Datasets

We study the effectiveness of FedGCDR with 16 popular domains on a real-world dataset Amazon[4]. To study the impact of the number of domains on model performance, we divide these domains into three subsets containing 4, 8, and 16 domains respectively and denote them as Amazon-4, Amazon-8, and Amazon-16 respectively.

Dataset	$\|U\|$	$\|U_d\|$	$\|I_d\|$	$\|R_d\|$	avg (sparsity)
Amazon-4	55,518	6,632 - 12,626 - 27,402	53,082 - 134,438 - 501,153	623,420 - 646,266 - 5,481,801	0.0802%
Amazon-8	99,506	6,632 - 13,978 - 27,402	53,082 - 106,985 - 501,153	186,016 - 618,539 - 5,481,801	0.0399%
Amazon-16	117,672	1,036 - 9,038 - 27,402	17,209 - 64,624 - 501,153	41,427 - 379,657 - 5,481,801	0.0928%
Amazon-Dual	2,500	2,500 - 2,500 - 2,500	17,889 - 28,649 - 39,510	106,741 - 128,601 - 150,461	0.1955%

Table 1. Statistics on the datasets.

Baselines

- **FedGNN[5]:** an attempt to adopt FL graph learning to recommender systems.
- **EMCDR[6]:** a conventional embedding-mapping CDR framework.
- **PriCDR[7]:** a privacy-preserving CDR framework based on DP.
- **FedCT[8] :** a VAE-based federated framework.
- **FedCDR [9] :** a dual-target federated CDR framework.

Experiments (2/4): Recommendation Performance

Model	Amazon-4@Books				Amazon-8@Books				Amazon-16@Books			
	HR@5	NDCG@5	HR@10	NDCG@10	HR@5	NDCG@5	HR@10	NDCG@10	HR@5	NDCG@5	HR@10	NDCG@10
Single Domain	0.4693	0.3188	0.6067	0.3634	0.4693	0.3188	0.6067	0.3634	0.4693	0.3188	0.6067	0.3634
EMCDR	0.4633	0.3075	0.6179	0.3191	0.4678	0.3268	0.5990	0.3518	0.3140	0.2184	0.4207	0.2348
PriCDR	0.4061	0.3159	0.5275	0.3550	0.4409	0.3196	0.5913	0.3681	0.3699	0.2650	0.4914	0.3042
FedCT	0.2911	0.2044	0.4276	0.2482	0.4665	0.3516	0.6002	0.3939	0.2779	0.2335	0.3580	0.2593
FedCDR	0.4115	0.3153	0.5415	0.3570	0.4791	0.3538	0.6182	0.3967	0.3926	0.2907	0.5626	0.3403
FedGCDR-DP	0.4903	0.3417	0.6717	0.3733	0.5224	0.3608	0.6727	0.3973	0.4928	0.3509	0.6510	0.3742
FedGCDR	**0.4941**	**0.3592**	**0.6732**	**0.3920**	**0.5300**	**0.3686**	**0.6752**	**0.3985**	**0.5016**	**0.3600**	**0.6516**	**0.3854**

Table 2. The recommendation performance on Amazon@Books.

Model	Amazon-4@CDs				Amazon-8@CDs				Amazon-16@CDs			
	HR@5	NDCG@5	HR@10	NDCG@10	HR@5	NDCG@5	HR@10	NDCG@10	HR@5	NDCG@5	HR@10	NDCG@10
Single Domain	0.4119	0.2751	0.5031	0.3040	0.4119	0.2751	0.5031	0.3040	0.4119	0.2751	0.5031	0.3040
EMCDR	0.4074	0.2651	0.5591	0.2972	0.2882	0.1828	0.4361	0.2199	0.4704	0.3683	0.5740	0.3937
PriCDR	0.3987	0.2838	0.5114	0.3202	0.2946	0.1988	0.4229	0.2400	0.4405	0.3689	0.5399	0.4011
FedCT	0.2681	0.1603	0.3774	0.1956	0.1801	0.1282	0.3001	0.1681	0.3522	0.2963	0.4326	0.3219
FedCDR	0.4299	0.2949	0.5636	0.3381	0.3088	0.2109	0.4620	0.2600	0.4823	0.3983	0.5808	0.4297
FedGCDR-DP	0.4359	0.2960	0.5779	0.3520	0.4122	0.2983	0.5064	0.3106	0.4963	0.4061	0.6135	0.4453
FedGCDR	**0.4588**	**0.3282**	**0.5819**	**0.3679**	**0.4276**	**0.3142**	**0.5270**	**0.3464**	**0.5267**	**0.4382**	**0.6208**	**0.4684**

Table 3. The recommendation performance on Amazon@CDs.

Our method targets two domains with different data quality and achieves the best results on all three sub-datasets.

Experiments (3/4): Dual-domain Scenario

We randomly selected 2500 overlapping users in the Books domain and CDs domain to construct the dataset Amazon-Dual

Model	Books → CDs HR@10	Books → CDs NDCG@10	Books ← CDs HR@10	Books ← CDs NDCG@10
Single Domain	0.2713	0.1429	0.2594	0.1524
EMCDR	0.2816	0.1409	0.2596	0.1540
PriCDR	0.2903	0.1446	0.2662	0.1583
FedCT	0.2384	0.1239	0.2570	0.1551
FedCDR	0.2566	0.1376	0.2657	0.1554
FedGCDR-DP	<u>0.3076</u>	<u>0.1552</u>	<u>0.2749</u>	<u>0.1602</u>
FedGCDR	**0.3323**	**0.1838**	**0.2958**	**0.1797**

Table 4. The recommendation performance on Amazon@CDs.

Table 4 shows that our approach is also suitable for dual-domain scenarios where users full-overlap and have only a single source domain and a single target domain.

Experiments (4/4): Ablation Study and Privacy Budget Study

We studied the effects of two modules and privacy budget in FedGCDR.

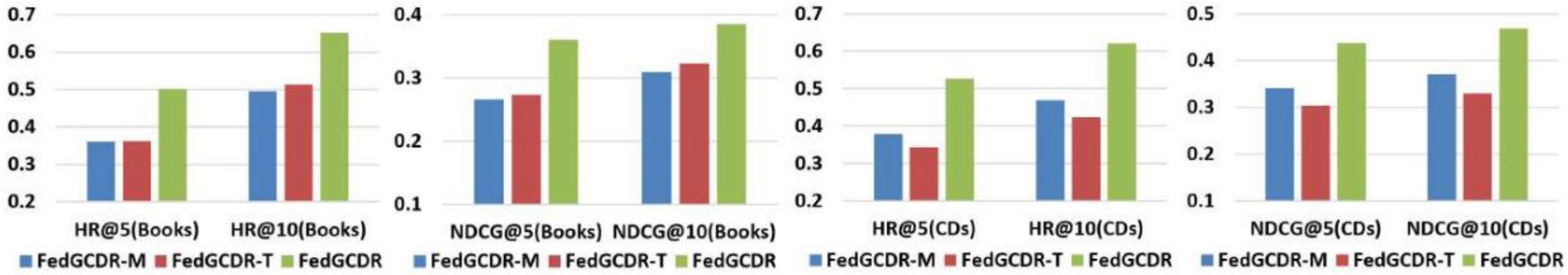


Figure 5. Ablation study on Amazon-16@CDs and Amazon-16@Books.

From the Figure 4, we can observe:

1) The two variants perform differently on different target domains. On the Books domain, FedGCDR-T performs better than FedGCDR-M, which indicates that for domains with higher data quality, preventing the transfer of negative knowledge from other domains is more important than mapping this knowledge better. The opposite results on the CDs domain indicates that for domains that are deficient in information, mapping knowledge correctly is more important.
2) Compared to FedGCDR, the absence of either module can cause a significant drop in performance.

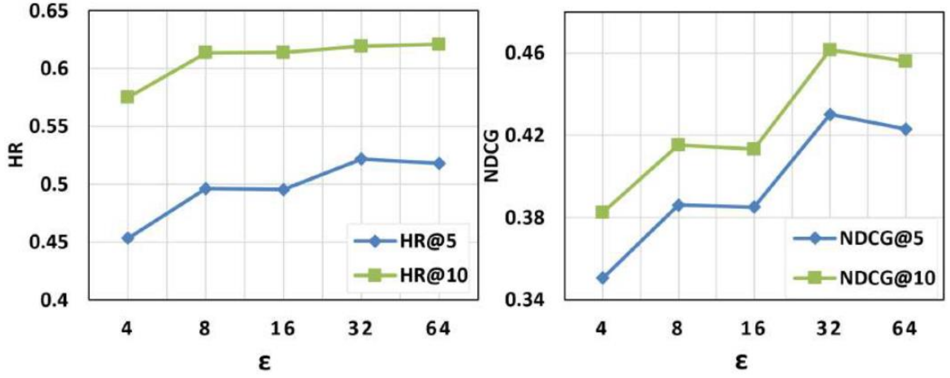


Figure 6. The effect of ϵ in DP on model performance.

To study the effects of privacy budget ϵ on the model performance. From Figure 6 we can observe that the model's performance decreases as ϵ decreases. The degradation in model performance suggests that our approach struggles to counteract the effects of high-intensity noise in a large number of domains, but the model performance is not completely destroyed by Gaussian noise.

空间感知与计算实验室
spAtial Sensing & Computing Lab

Reference

[1] Zang T, Zhu Y, Liu H, et al. A survey on cross-domain recommendation: taxonomies, methods, and future directions[J]. ACM Transactions on Information Systems, 2022, 41(2): 1-39.
[2] Jiangxia Cao, Shaoshuai Li, Bowen Yu, et al. 2023. Towards Universal Cross-Domain Recommendation. In Proceedings of the Sixteenth ACM International Conference on Web Search and Data Mining (WSDM '23). Association for Computing Machinery, New York, NY, USA, 78 – 86.
[3] Hao Ma, Dengyong Zhou, Chao Liu, Michael R Lyu, and Irwin King. Recommender systemswith social regularization. In Proceedings of the fourth ACM International Conference on WebSearch and Data Mining, pages 287 – 296, 2011.
[4] Jianmo Ni, Jiacheng Li, and Julian McAuley. Justifying recommendations using distantly-labeled reviews and fine-grained aspects. In Proceedings of the 2019 conference on empiricalmethods in natural language processing and the 9th International Joint Conference on NaturalLanguage Processing (EMNLP-IJCNLP), pages 188 – 197, 2019.
[5] Chuhan Wu, Fangzhao Wu, Yang Cao, Yongfeng Huang, and Xing Xie. Fedgnn: Federatedgraph neural network for privacy-preserving recommendation. arXiv preprint arXiv:2102.04925,2021.
[6] Tong Man, Huawei Shen, Xiaolong Jin, and Xueqi Cheng. Cross-domain recommendation: Anembedding and mapping approach. In IJCAI, volume 17, pages 2464 – 2470, 2017.
[7] Chaochao Chen, Huiwen Wu, Jiajie Su, Lingjuan Lyu, Xiaolin Zheng, and Li Wang. Differ-ential private knowledge transfer for privacy-preserving cross-domain recommendation. InProceedings of the ACM Web Conference 2022, pages 1455 – 1465, 2022.
[8] Shuchang Liu, Shuyuan Xu, Wenhui Yu, Zuohui Fu, Yongfeng Zhang, and Amelie Marian.Fedct: Federated collaborative transfer for recommendation. In Proceedings of the 44thInternational ACM SIGIR Conference on Research and Development in Information Retrieval,pages 716 – 725, 2021.
[9] Wu Meihan, Li Li, Chang Tao, Eric Rigall, Wang Xiaodong, and Xu Cheng-Zhong. Fedcdr:federated cross-domain recommendation for privacy-preserving rating prediction. In Proceed-ings of the 31st ACM International Conference on Information & Knowledge Management,pages 2179 – 2188, 2022.

Thanks For Watching!

Ziqi Yang, Xiaoliang Fan*
School of Informatics, Xiamen University, China
yangziqi@stu.xmu.edu.cn   fanxiaoliang@xmu.edu.cn

Paper and code: fanxlxmu.github.io