Enhancing Dual-Target Cross-Domain Recommendation with Federated Privacy-Preserving Learning

Zhenghong Lin[1], **Wei Huang**[1], **Hengyu Zhang**[1], **Jiayu Xu**[1], **Weiming Liu**[2], **Xinting Liao**[2], **Fan Wang**[2], **Shiping Wang**[1] and **Yanchao Tan**[1] *

[1]College of Computer and Data Science, Fuzhou University, Fuzhou, China
[2]College of Computer Science and Technology, Zhejiang University, Hangzhou, China
hongzhenglin970323@gmail.com, huangweifujian@126.com,
{hengyuzhang07,wudijiayu666}@gmail.com, {21831010,xintingliao,fanwang97}@zju.edu.cn,
shipingwangphd@163.com, yctan@fzu.edu.cn

Abstract

Recently, dual-target cross-domain recommendation (DTCDR) has been proposed to alleviate the data sparsity problem by sharing the common knowledge across domains simultaneously. However, existing methods often assume that personal data containing abundant identifiable information can be directly accessed, which results in a controversial privacy leakage problem of DTCDR. To this end, we introduce the P^{2}DTR framework, a novel approach in DTCDR while protecting private user information. Specifically, we first design a novel inter-client knowledge extraction mechanism, which exploits the private set intersection algorithm and prototype-based federated learning to enable collaboratively modeling among multiple users and a server. Furthermore, to improve the recommendation performance based on the extracted common knowledge across domains, we proposed an intra-client enhanced recommendation, consisting of a constrained dominant set (CDS) propagation mechanism and dual-recommendation module. Extensive experiments on real-world datasets validate that our proposed P^{2}DTR framework achieves superior utility under a privacy-preserving guarantee on both domains.

1 Introduction

Targeting the existing problem of data sparsity in the real-world scenarios, dual-target cross-domain recommendation (DTCDR) has been widely employed in a myriad of real-life applications [Zhang *et al.*, 2023]. Different from the so-called single-target CDR exploiting abundant information from a relatively richer domain to improve recommendation performance on a sparser domain [Guo *et al.*, 2021], DTCDR aims to improve the recommendation accuracies on both sparse domains simultaneously by making good use of the knowledge from both domains, shown in Fig. 1(a).

However, most existing DTCRD methods often assume that the personal data of shared users, serving as the bridge for knowledge transferring, can be directly accessed or available in every situation [Zhu *et al.*, 2021a]. This is unrealistic and may raise trust concerns of users about privacy leakage problems. For example, any user is unwilling to share his or her sensitive data when two company attempt to collaborate on a promotion campaign based on these shared users. Besides, many law regulations [Du *et al.*, 2021; Liu *et al.*, 2023a] (e.g., GDPR and CCPA) are adopted to limit the transportation and exploitation of personal data, resulting in the prohibition of collecting user data. Since public awareness of privacy protection results in a controversial view of DTCDR, a nature question is raised: *How can we design a novel DTCDR while protecting the user privacy?*

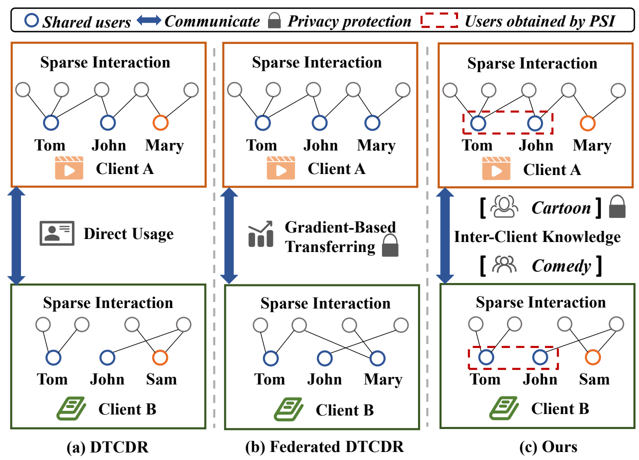

Figure 1: A toy example of dual-target cross-domain recommendation (DTCDR) with user privacy protection. (a) illustrates the limitation of the existing DTCDR method; (b) shows the traditional federated DTCDR; (c) represents our proposed P^{2}DTR.

To solve this problem, we need to focus on two central challenges. **Challenge I:** ***what to transfer*** aims at mining valuable transferable knowledge from different domains under a privacy-preserving scenario; **Challenge II:** ***how to recommend*** is dedicated to designing appropriate DTCDR paradigm based on the protected transferable knowledge. For the first challenge, a straightforward idea is to exploit federated learning (FL) to collaboratively learn inter-client knowl-

*Yanchao Tan is the corresponding author.

edge across a variety of clients without sharing private data. Nevertheless, most of these methods depend on gradient-based aggregation, resulting in heavy reliance on homogeneous local models but also expose clients' models, which further raise privacy concerns [Wang *et al.*, 2023]. For the second challenge, existing DTCDR methods perform the recommendation based on direct usage of the knowledge from the auxiliary domain. When transferred data is protected, most of the DTCDR models may fail or obtain rather inaccurate representations [Yang *et al.*, 2022]. Besides, most federated DTCDR often assumes a high ratio of shared users (even completely overlapping) between domains and the ID of shared users can be obtained as prior knowledge, shown in Fig 1(b), which is not so practical under the federated scenarios. Hence, how to recommend the items based on the protected knowledge under the privacy-preserving settings is still an open problem.

To alleviate the above challenges, in this paper, we introduce the P^2DTR framework, a novel approach in **D**ual-**T**arget cross-domain **R**ecommendation with federated **P**rivacy-**P**reserving Learning, which consists of two pivotal technical components. For **Challenge I**, we design a novel inter-client knowledge extraction mechanism under a privacy-preserving scenario. That is, we exploit the prototypes of user preferences to solely share class representatives as common knowledge, e.g. the users who have cartoon taste may also like the comedy theme, while maintaining the privacy of clients' models shown in Fig 1(c). Specifically, we first perform the private set intersection (PSI) to find out the same users between different domains as the bridge to exchange the inter-domain knowledge. Then, we enable the users in both domains and a server to collaboratively learn the privacy-preserved common knowledge through federated prototype-based learning. For **Challenge II**, we propose intra-client enhanced recommendation to improve the recommendation performance based on the extracted common knowledge across domains. Specifically, the novel constrained dominant set (CDS) propagation mechanism is designed to enhance the DTCDR based on the extracted common knowledge. And dual recommendation is proposed to inject the collaborative relations into recommendation.

Finally, we evaluate the proposed P^2DTR with extensive experiments on four real-world benchmark datasets for federated DTCDR. Extensive experimental results show that the proposed P^2DTR is able to significantly improve the recommendation performance under privacy-preserving scenarios over all baselines (e.g., with up to 18.32% improvements in NDCG@10 on the cloth dataset over the best baseline).

Our overall contributions are summarized as follows:

- *Formulation of federated DTCDR*: We propose a privacy-preserving setting tailored for dual-target cross-domain recommendation that considers a more general federated scenario across local clients.
- *Effective model designs*: We propose an effective framework P^2DTR to perform dual-target cross-domain recommendation while protecting the user privacy, through inter-client knowledge extraction mechanism and intra-client enhanced recommendation module.
- *Extensive experiments on real-world datasets*: Extensive experiments show the superiority of our proposed method in terms of test performance under a privacy-preserving guarantee in several benchmark datasets.

2 Related Work

2.1 Cross-Domain Recommendation

Cross-domain recommendation (CDR) is widely employed to overcome the issue of data sparsity in recommendation systems. Traditional methods, like single-target CDR, leverage the richness of information from the source domain to improve recommendations in sparser target domains. For example, NCF [He *et al.*, 2017] employs multi-layer perceptrons to learn the user-item interaction arbitrary function, replacing the inner product. DCDCSR [Zhu *et al.*, 2018] combines matrix factorization models and addresses challenges in cross-domain and cross-system recommendations. In recent years, the introduction of dual-target CDR seeks to enhance recommendation performance in both domains concurrently. For example,VDEA [Liu *et al.*, 2022] utilizes dual variational autoencoders with both local and global embedding alignment to exploit domain-invariant user embeddings. CPKSPA [Liu *et al.*, 2023f] introduces a cross-domain recommendation framework with three modules, which demonstrates superior performance compared to the state-of-the-art models. IESRec [Liu *et al.*, 2023e] incorporates an internal multi-interest exploration module and an external domain alignment module.

The aforementioned methods are having significant risks to user's privacy security, where every piece of content they use is closely associated with the user themselves. Different from these approaches, our proposed framework is designed with considerations for a federated scenario to ensure the protection of user privacy.

2.2 Federated Recommendation

Federated Learning (FL) is widely applied in various applications, enabling collaborative learning across diverse clients without the need to share private data. Traditional federated learning methods rely on gradient-based aggregation. In FedAVG [McMahan *et al.*, 2017], local devices upload their model parameters to the server, which computes the global average parameters and broadcasts them back to all devices. This process iterates until convergence. PFedRec [Zhang *et al.*, 2023] was proposed to effectively learn fine-grained personalization on both users and items. To address the high communication costs in gradient aggregation and the heavy reliance on homogeneous local models, a prototype-based federated learning approach has been proposed. For example, FedProto [Tan *et al.*, 2022a] aggregates local prototypes and maintains proximity to the global prototype to regularize the training of local models, minimizing classification errors, which achieved desired performance with limited users. FPPDM [Liu *et al.*, 2023b] integrates local domain modeling, global server aggregation, and the compact co-clustering strategy from FPPDM++ to enhance the extraction of semantic neighbor information among the whole overlapping users.

Unlike the aforementioned methods assuming a high ratio of shared users (even completely overlapping) between domains and the ID of shared users can be obtained as prior knowledge, our method considers DTCDR with a few unknown shared users.

3 Methodology

3.1 Problem Statement and Overall Architecture

Our goal of P^{2}DTR aims to perform dual-target cross-domain recommendation while protecting user privacy. Formally, there exist two domains (clients), e.g., client A and client B. We use $\mathcal{D}_A = (\mathcal{U}_A, \mathcal{V}_A, \mathcal{E}_A)$ and $\mathcal{D}_B = (\mathcal{U}_B, \mathcal{V}_B, \mathcal{E}_B)$ to represent the data included in two clients, where $\mathcal{U}, \mathcal{V}$ and $\mathcal{E}$ are the user set, item set and edge set in each client, respectively. Here, we define $\mathcal{U}_A = \{\mathcal{U}_a, \mathcal{U}_s\}$ and $\mathcal{U}_B = \{\mathcal{U}_b, \mathcal{U}_s\}$, where $\mathcal{U}_s = \mathcal{U}_A \cap \mathcal{U}_B$ is the shared user across two clients and $\mathcal{U}_a, \mathcal{U}_b$ are the users belonging to the specific client. Besides, we introduce $\boldsymbol{R}_A \in \mathbb{R}^{|\mathcal{U}_A| \times |\mathcal{V}_A|}$ and $\boldsymbol{R}_B \in \mathbb{R}^{|\mathcal{U}_B| \times |\mathcal{V}_B|}$ to represent their user-item interactions in the clients A and B. The value of $\boldsymbol{R}_{ij}$ is set to 1 if the $i-$th user $\boldsymbol{u}_i \in \mathcal{U}$ has interacted with the $j-$th item $\boldsymbol{v}_j \in \mathcal{V}$. Otherwise, $\boldsymbol{R}_{ij} = 0$. The inputs of our proposed P^{2}DTR are user-item interactions $\boldsymbol{R}_A$ and $\boldsymbol{R}_B$ on two clients. The outputs are the predicted probability matrices $\hat{\boldsymbol{R}}_A$ and $\hat{\boldsymbol{R}}_B$, where the value of $\hat{\boldsymbol{R}}_{ij}$ represents the probability that the j-th item is recommended to the i-th user in each client. Scenarios with multiple clients can be easily extended from this scenario.

We summarize the main steps of the P^{2}DTR framework in Fig. 2 and provide an overview. Our proposed model has two main steps. *Step 1:* We peform inter-client knowledge extraction under privacy-preserving scenarios. Specifically, we first initialize the shared users between different domains by PSI algorithm. Then, to enable the users in both domains and a server to collaboratively capture the common knowledge, we propose a federated mechanism based on prototype learning. *Step 2:* To enhance the DTCDR based on the extracted common knowledge, we design a novel Intra-client Enhanced Recommendation, CDS propagation mechanism and dual-recommendation module.

3.2 Inter-client Knowledge Extraction

Private Set Intersection (Client-Client). To employ abundant information from both domains to improve dual-target recommendation performance, the first step is to find out the same users between different domains as the bridge to exchange the shared inter-domain knowledge. However, due to the privacy policies, the ID of the shared user can not be directly obtained. Therefore, we exploit the private set intersection (PSI) based on RSA encryption/decryption algorithm and hashing algorithm [Huang *et al.*, 2023]. Specifically, client A first generates the public key: (n, b) and private key: (n, d) by the RSA algorithm, and passes the public key to client B. Then, client B encrypts the user ID x and returns encrypted Y_B to client A, which can be formulated as $Y_B = \{{r_i}^b\%n * Hash(x)\}$. Here, $Hash(x)$ is the hash function equivalent to encryption and r_i is a generated random number. After receiving Y_B, client A decrypts Y_B with the key d to get $\hat{Y}_B = \{r_i * (Hash(x))^d\%n\}$, where the key b and d corresponding to r_i are canceled, simultaneously. Then, client A makes one more hash with private key d as the index to get $\hat{Y}_A = \{Hash(Hash(x))^d\%n \mid x \in clientA\}$. Here, client A returns $\hat{Y}_A$ and $\hat{Y}_B$ together to the client B. The random noise in $\hat{Y}_B$ can be eliminated and client B can perform one more hash to generate the user set $\tilde{Y}_B$. Finally, we get the intersection of $\hat{Y}_A$ and $\tilde{Y}_B$ to obtain the shared user set $\mathcal{U}_s$. The process is formulated as

$$\begin{aligned} &\tilde{Y}_B = \{Hash(r_i * (H(x))^d / r_i = Hash(Hash(x))^d)\}, \\ &where\ r_i * (Hash(x))^d \in \hat{Y}_B\ and\ \mathcal{U}_s = \hat{Y}_A \cap \tilde{Y}_B. \end{aligned} \tag{1}$$

Prototype Learning (Client-Server). To enable the users in both domains and a server to collaboratively train models and help them supervise each other, we design a federated mechanism based on prototype learning. Specifically, we first extract the domain-specific by graph neural networks (GNNs) on each client. We first adopt a trainable lookup table to transfer the user and item one-hot coding and combine them as $\boldsymbol{X}_A \in \mathbb{R}^{(|\mathcal{U}_A|+|\mathcal{V}_A|)\times d} = [\boldsymbol{X}_A^{\mathcal{U}}; \boldsymbol{X}_A^{\mathcal{V}}]$, $\boldsymbol{X}_B \in \mathbb{R}^{(|\mathcal{U}_T|+|\mathcal{V}_B|)\times d} = [\boldsymbol{X}_B^{\mathcal{U}}; \boldsymbol{X}_B^{\mathcal{V}}]$, where $\boldsymbol{X}_A^{\mathcal{U}}$, $\boldsymbol{X}_B^{\mathcal{U}}$ are the user embeddings and $\boldsymbol{X}_A^{\mathcal{V}}$, $\boldsymbol{X}_B^{\mathcal{V}}$ are the item embeddings in client A and B. Then, we define the adjacency matrix $\boldsymbol{A}_k \in \mathbb{R}^{(|\mathcal{U}_k|+|\mathcal{V}_k|)\times(|\mathcal{U}_k|+|\mathcal{V}_k|)}$ by combination of user-item ranking matrix $\boldsymbol{R}_k$, formulated as $\boldsymbol{A}_k = \begin{bmatrix} \boldsymbol{R}^k & 0 \\ 0 & \boldsymbol{R}^{k^T} \end{bmatrix}$, and $k \in \{A, B\}$ means the k-th client. In consequence, the graph convolution can be formed:

$$\boldsymbol{X}_k^{l+1} = \tilde{\boldsymbol{D}}^{-\frac{1}{2}} \tilde{\boldsymbol{A}}_k \tilde{\boldsymbol{D}}^{-\frac{1}{2}} \boldsymbol{X}_k^l \boldsymbol{W}_{\mu,k}^l, \tag{2}$$

where $\tilde{\boldsymbol{D}}$ is the degree matrix of $\tilde{\boldsymbol{A}}_k$ and $\tilde{\boldsymbol{A}}_k = \boldsymbol{A}_k + \boldsymbol{I}_N$ and $\boldsymbol{I}_N$ is the degree matrix to add the self loop. We use $\boldsymbol{W}_{\sigma,k}^l$ and $\boldsymbol{W}_{\mu,k}^l$ to represent the weights of graph convolution networks in l-th layers.

Since user behavior data contain abundant personal identifiable information, we use the prototypes (the group features of user preference) as the common knowledge to be aggregated on the server. Specifically, we assume two clients reach a protocol: the shared users have K common preferences. Then, we initialize the user prototype indicator matrix $\boldsymbol{H}_k \in \mathbb{R}^{|\mathcal{U}_s|\times K}$ in k-th client, where $|\mathcal{U}_s|$ is the number of shared users. Then, the prototypes $\boldsymbol{C}_k \in \mathbb{R}^{K\times d}$ can be calculated by $\boldsymbol{C}_k = \boldsymbol{H}_k^T \boldsymbol{X}_{k,s}^{\mathcal{U}}$, where $\boldsymbol{X}_{k,s}^{\mathcal{U}} \in \mathbb{R}^{|\mathcal{U}_s|\times d}$ is the shared user embedding caculated by shared user set in Equation 1 and graph convolution in Equation 2. To further protect user privacy, we exploit the differential privacy (DP) [Li *et al.*, 2016] to protect the prototype through data perturbation, which is defined as

Definition 1 ($\epsilon-$Differential Privacy). *Given two neighboring datasets $\mathcal{D}$ and $\mathcal{D}'$, a random algorithm $\mathcal{P}$ satisfies $\epsilon-DP$ if its all output $\mathcal{O} \in Range(\mathcal{P})$ satisfies*

$$Pr(\mathcal{P}(\mathcal{D}) = \mathcal{O}) \leq e^{\epsilon} Pr(\mathcal{P}(\mathcal{D}') = \mathcal{O}). \tag{3}$$

To start with, we first generate a random projection matrix $\boldsymbol{P} \in \mathbb{R}^{d\times d}$ from the normal distribution according to [Liu *et al.*, 2023d]. Then, we further generate a noise matrix $\Delta \in \mathbb{R}^{K\times d}$. Therefore, We can transform the source prototype $\boldsymbol{C}_k$

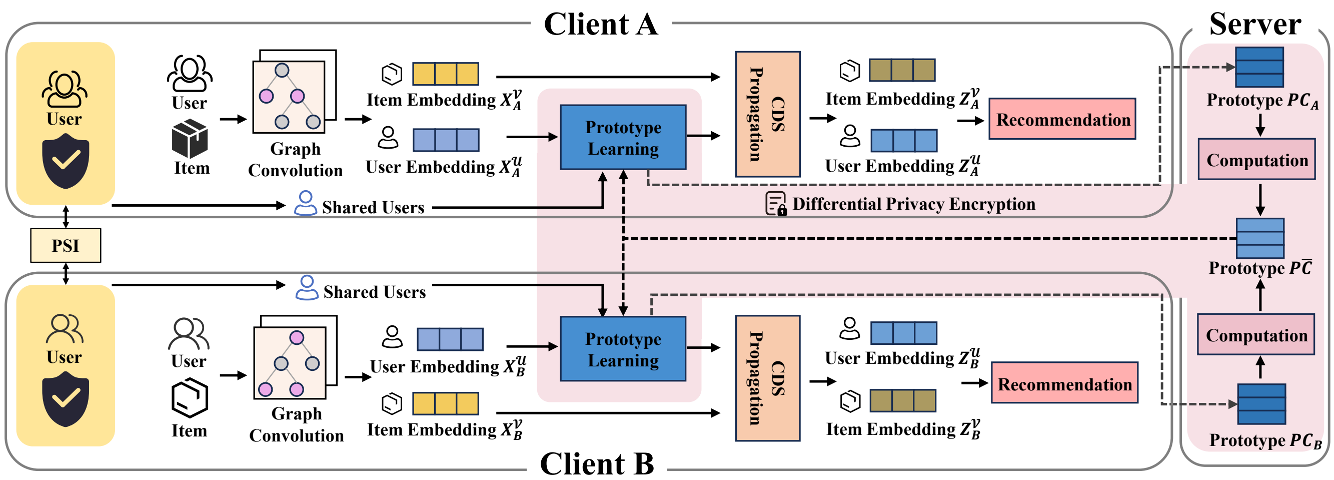

Figure 2: The overall architecture of P[2]DTR. Firstly, the shared users are initialized by PSI algorithm (client-client). Then, the shared user embeddings are fed to the prototype learning under federated scenarios to capture the common knowledge (client-server). Based on extracted common knowledge, CDS propagation is exploited to enhance the recommendation.

into $\boldsymbol{PC}_k = \boldsymbol{C}_k\boldsymbol{P} + \Delta$. Therefore, we upload the encrypted prototype $\boldsymbol{PC}_k$ from k-th client to the server for aggregation. The aggregation formula of the prototype is shown as

$$\boldsymbol{P\bar{C}} = Avg(\sum\nolimits_k \boldsymbol{PC}_k), \tag{4}$$

where $Avg(\cdot)$ is the average function of all prototypes uploaded to the server. Finally, to maintain inter-client consistency for common knowledge, the average prototype $\boldsymbol{P\bar{C}}$ is downloaded to the local clients and we propose a regularization term to reduce the distance among the local and global prototypes. The loss function of above process can be formed in k-th client:

$$\mathcal{L}_k^f = \left\|\boldsymbol{P\bar{C}} - \boldsymbol{PC}_k\right\|_F^2. \tag{5}$$

3.3 Intra-client Enhanced Recommendation

Constrained Dominant Set Propagation. To enhance the DTCDR based on the extracted common knowledge, we design the novel constrained dominant set (CDS) propagation mechanism and dual-recommendation module. We first calculate the enhanced shared user representations $\boldsymbol{Z}_{k,s}^{\mathcal{U}} = \boldsymbol{H}_k(\boldsymbol{P\bar{C}})$ based on the average prototype $\boldsymbol{P\bar{C}}$. Then, following the theory of deep constrained dominant set [Alemu *et al.*, 2019] to constrain that each cluster should contain the shared users, we exploit the CDS clustering to update the whole local user embeddings with shared features. Since the process of constrained clustering can be seen as finding constrained dominant sets under global similarity, we first need to construct the global similarity matrix $\hat{\boldsymbol{A}}_k = \boldsymbol{Z}_k^{\mathcal{U}}(\boldsymbol{Z}_k^{\mathcal{U}})^T$ in k-th client and select the constrained dominant sets P_k for graph $G_k = (\mathcal{U}_k, \mathcal{V}_k, \mathcal{E}_k)$. To alleviate computational costs, we adopt the mini-batch technique to sample M shared users and M unshared users randomly. We can combine them and define the sampled global similarity matrix as $\hat{\boldsymbol{A}}_k^m \in \mathbb{R}^{2M\times 2M}$. Considering the constrained sets $P_k^m \subseteq \mathcal{U}_s \subseteq \mathcal{U}_k$, where $\mathcal{U}_s$ is the shared user, we set the diagonal elements corresponding to the subset $\mathcal{U}_k \backslash P_k^m$ to parameter α, where $\mathcal{U}_k \backslash P_k^m$ means the the difference between set $\mathcal{U}_k$ and set P_k^m. Besides, the diagonal elements corresponding to the constraint sets P_k^m is set as zero. Then, we can obtain the final modification of the similarity matrix $\boldsymbol{B}_k^m$ Next, the modified adjacency matrix $\boldsymbol{B}_k^m$ is fed to the Replicator dynamics [Weibull, 1997] to ensure that all the users in the mini-batch are assigned equal membership probability to be part of the cluster. According to the optimization for constrained dominant sets [Zemene and Pelillo, 2016], finding a constrained cluster can be defined:

$$\text{maximize} \quad f_{P_k^m}^{\alpha}(\boldsymbol{h}^T\boldsymbol{B}_k^m\boldsymbol{h}) \quad \text{s.t. } \boldsymbol{h} \in \Delta, \tag{6}$$

where we define $\Delta = \{\boldsymbol{h} \in \mathbb{R}^{2M} : \sum_{i=1}^{2M}\boldsymbol{h}_i = 1, \text{and } \boldsymbol{h}_i \geq 0 \text{ for all } i = 1, ..., 2M\}$ and $\boldsymbol{B}_k^m = \boldsymbol{A}_k^m - \alpha\hat{\boldsymbol{I}}_{P_k^m}$. The elements of diagonal matrix $\hat{\boldsymbol{I}}_{P_k^m} \in \mathbb{R}^{2M\times 2M}$ are set to 0 in correspondence to the constrained dominant sets P_k^m and to 1 otherwise. From well-studied evolutionary game theory [Skoulakis *et al.*, 2021], the straightforward continuous optimization technique of Equation 6 are as follows:

$$\boldsymbol{h}_i(t+1) = \boldsymbol{h}_i(t)\frac{\boldsymbol{A}_k^m\boldsymbol{h}(t)_i}{\boldsymbol{h}(t)^T\boldsymbol{A}_k^m\boldsymbol{h}(t)}. \tag{7}$$

In consequence, we can obtain the optimal k-th domain solution $\boldsymbol{h}_{k,i}{}^* \in \mathbb{R}^{2M}$ and we select the solution corresponding to M shared users as the final clustering results, written as $\hat{\boldsymbol{H}}_k^m \in \mathbb{R}^{M\times 2M} = [\boldsymbol{h}_{k,1}; \ldots; \boldsymbol{h}_{k,M}]$. After obtaining the similarity between shared and global users, we exploit shared user representation to enhance the whole embedding as $\boldsymbol{Z}_k^{\mathcal{U},m} = (\hat{\boldsymbol{H}}_k^m)^T\boldsymbol{Z}_{k,s}^{\mathcal{U},m}$ where $\boldsymbol{Z}_{k,s}^{\mathcal{U},m}$ is the shared user representation in the minibatch of k-th client.

Dual-target Cross Domain Recommendation. Obtaining the enchanted user embeddings, we exploit the paradigm of collaborative filtering (CF), which is often adopted in recommender systems. The final user embedding $\boldsymbol{\Psi}_k^{\mathcal{U}}$ and item embedding $\boldsymbol{\Psi}_k^{\mathcal{V}}$ can be obtained by the graph-based CF message aggregation mechanism:

$$\boldsymbol{\Psi}_k^{\mathcal{V}} = {\boldsymbol{D}^V}^{-1} {\boldsymbol{R}_k}^T \boldsymbol{Z}_k^{\mathcal{U}}, \quad \boldsymbol{\Psi}_k^{\mathcal{U}} = {\boldsymbol{D}^U}^{-1} \boldsymbol{R}_k \boldsymbol{\Psi}_k^{\mathcal{V}}. \tag{8}$$

Here, $\boldsymbol{D}^V \in \mathbb{R}^{|\mathcal{V}_k| \times |\mathcal{V}_k|}$ and $\boldsymbol{D}^U \in \mathbb{R}^{|\mathcal{U}_k| \times |\mathcal{U}_k|}$ are the diagonal degree matrices of user-item and item-user interaction matrices $\boldsymbol{R}_k^T \in \mathbb{R}^{|\mathcal{V}_k| \times |\mathcal{U}_k|}$ and $\boldsymbol{R}_k \in \mathbb{R}^{|\mathcal{U}_k| \times |\mathcal{V}_k|}$. Then, the preference score $\hat{\boldsymbol{R}}_k$ can be predicted by $\hat{\boldsymbol{R}}_k = \boldsymbol{\Psi}_k^{\mathcal{U}} (\boldsymbol{\Psi}_k^{\mathcal{V}})^T$ and the value $\hat{\boldsymbol{r}}_{ij}$ in $\hat{\boldsymbol{R}}_k$ means the probability of item j recommended to user i in k-th client. We adopt the BPR loss, which is a common loss function in recommendation tasks:

$$\mathcal{L}_{BPR} = \sum_{(i,j_p,j_n)}^{|\mathcal{E}|} -log(\sigma(\hat{\boldsymbol{r}}_{ij_p} - \hat{\boldsymbol{r}}_{ij_n})), \tag{9}$$

where σ is the activation function. j_p and j_n denote the positive and negative samples for cold-start user i. Finally, We train our recommender systems with the combination loss to jointly optimize P^{2}DTR:

$$\mathcal{L} = \mathcal{L}_{BPR} + \lambda(\mathcal{L}_A^f + \mathcal{L}_B^f), \tag{10}$$

where λ is the hyperparameter to control the strength of gradients. The loss functions $\mathcal{L}_A^f$ and $\mathcal{L}_B^f$ are the consistency loss calculated by Equation 5.

Note that, we only illustrate the federated DTCRD with two clients ($K = 2$). The multi-client scenario can be easily extended by adding the different clients to prototype-based federated learning, where each client can get the intersections of shared user ID in this domain with other domains, and then just merge these intersections to a union set to construct the multi-client PSI algorithm.

3.4 Convergence Analysis

In this part, we will demonstrate the theoretical analysis of our proposed P^{2}DTR and illustrate the convergence guarantees under the specific hyperparameters. Firstly, to better represent the process of local model update, additional variables are introduced and we can rewrite the loss function of k-th client (domain) in Equation 10 as the formulation:

$$\begin{aligned} \mathcal{L}\left(\boldsymbol{\phi}_k, \boldsymbol{v}_k; \boldsymbol{x}, \boldsymbol{y}\right) &= \mathcal{L}_S\left(\mathcal{F}_i\left(\boldsymbol{\phi}_k, \boldsymbol{v}_k; \boldsymbol{x}\right), \boldsymbol{y}\right) \\ &+ \lambda \left\| f_k\left(\boldsymbol{\phi}_k; \boldsymbol{x}\right) - \boldsymbol{P}\bar{\boldsymbol{C}}_j \right\|_2^2, \end{aligned} \tag{11}$$

where $\mathcal{L}_S(\cdot)$ is the loss function about the local client (domain) and $\lambda \left\| f_k\left(\boldsymbol{\phi}_k; \boldsymbol{x}\right) - \boldsymbol{P}\bar{\boldsymbol{C}}_j \right\|_2^2$ means the loss function corresponding to the global server after j-th prototype aggregation. we define $f_k\left(\boldsymbol{\phi}_k\right) : \mathbb{R}^{d_x} \rightarrow \mathbb{R}^{d_c}$ to be the embedding function of the k-th client, where d_x and d_c represent the dimension of the input x and the prototype c. The function $g_k\left(\boldsymbol{v}_k\right) : \mathbb{R}^{d_c} \rightarrow \mathbb{R}^{d_y}$ means the prediction layer in the federated partial recommendation for all clients, in which d_y represents the dimension of output $\boldsymbol{y}$. In consequence, the whole federated DTCDR can be written as $\mathcal{F}_i\left(\boldsymbol{\phi}_k, \boldsymbol{v}_k\right) = g_k\left(\boldsymbol{v}_k\right) \circ f_k\left(\boldsymbol{\phi}_k\right)$, where $\boldsymbol{\phi}_k$ and $\boldsymbol{v}_k$ are the learnable weights in networks. Furthermore, we make the following assumption, similar to existing general frameworks [Tan *et al.*, 2022b]: (1) Lipschitz Smooth; (2) Unbiased Gradient and Bounded Variance; (3) Bounded Expectation of Euclidean Norm of Stochastic Gradients; (4) Lipschitz Continuity. More details about assumptions could be referred to **Appendix** due to space limitations.

Scenarios	User	Item	Training	#Shared User	#ratio	Density
Game	25,025	12,319	142588	1963	7.84%	0.05%
Video	19,457	8,751	141107		10.09%	1.70%
Cloth	41,829	17,943	154278	8847	21.15%	0.02%
Sport	27,328	12,655	123927		32.37%	0.03%

Table 1. Statistics of two federated DTCDR scenarios. (#Shared User denotes the number of shared users in the training set, #ratio is the proportion of shared users).

Based on the above assumptions, we analyze the theoretical results under non-convex conditions. The expected decrease per round is given in Theorem 1. We denote $e \in \{1, 2, ..., E\}$ as the local iteration, and $t \in \{1, 2, ..., T\}$ as the global communication round. Moreover, we use $1/2$ as the intermediate value to distinguish operations between clients and the central server. Specifically, tE represents the time step before prototype aggregation (clients complete iterations), and $tE + 1/2$ represents the time step between prototype aggregation and the first iteration of the current round. More proof details can be referred to the **Appendix**.

Theorem 1. (Non-convex convergence rate of P^{2}DTR) *When the learning rate satisfies* $\eta < \frac{2(\delta - \lambda L_2 G)}{L_1(\delta + \sigma^2)}$, *and the hyperparameter satisfies* $\lambda < \frac{\delta}{L_2 G}$, *given any* $\delta > 0$ *for an arbitrary client, we have*

$$\begin{aligned} \frac{1}{TE} \sum_{t=0}^{T-1} \sum_{e=1/2}^{E-1} \mathbb{E}\left[\left\|\nabla \mathcal{L}_{tE+e}\right\|_2^2\right] &\leqslant \frac{L_1 \eta \sigma^2 + 2\lambda L_2 G}{2 - L_1 \eta} \\ &+ \frac{\frac{2}{TE} \sum_{t=0}^{T-1} \left(\mathcal{L}_{tE+1/2} - \mathbb{E}\left[\mathcal{L}_{(t+1)E+1/2}\right]\right)}{\eta(2 - L_1 \eta)}. \end{aligned} \tag{12}$$

Corollary 1. *Let* $\eta = O(1/\sqrt{T})$ *with the upper bound of* $2\left(\delta - \lambda L_2 G\right)/L_1\left(\delta + \sigma^2\right)$, *and let* $\lambda = O(1/\sqrt{T})$ *with the upper bound of* $\delta/L_2 G$, *the proposed P^{2}DTR achieves a convergence rate of* $O(1/\sqrt{T})$.

4 Experiment

In this section, we start with a brief description of conducted datasets on four real-world datasets and experimental settings. Then, we evaluate our proposed P^{2}DTR framework focusing on the following research questions :

RQ1: How does P^{2}DTR perform in comparison with other state-of-the-art models for federated DTCDR?

RQ2: How does each component devised in the P^{2}DTR contribute to performance improvement?

RQ3: How do the hyperparameters affect the prediction performance and how to choose optimal values?

4.1 Experimental Settings

Dataset. On the basis of the previous works, we build our scenarios using the chosen cross-domain recommendation datasets [Zhu *et al.*, 2022], and the preprocessing settings with two domains ($K = 2$). In particular, we carry out experiments on the large-scale public Amazon datasets. To evaluate

Methods	Game-domain recommendation						Video-domain recommendation					
	MRR	NDCG		HR			MRR	NDCG		HR		
		@5	@10	@1	@5	@10		@5	@10	@1	@5	@10
PMLAM	2.96±0.05	1.99±0.08	2.33±0.08	0.76±0.02	2.89±0.12	6.04±0.09	1.52±0.06	1.34±0.15	1.67±0.12	0.46±0.11	2.64±0.09	4.37±0.10
LightGCN	3.06±0.03	2.07±0.06	2.51±0.14	0.83±0.04	2.95±0.10	6.31±0.08	1.67±0.13	1.39±0.11	1.76±0.06	0.51±0.07	2.71±0.10	4.61±0.12
CGCL	3.20±0.06	2.22±0.04	2.63±0.14	0.99±0.05	3.12±0.09	6.60±0.09	1.87±0.13	1.59±0.12	1.97±0.07	0.53±0.09	2.97±0.14	4.81±0.14
CoNet	3.16±0.11	2.24±0.16	2.85±0.03	0.86±0.06	3.24±0.12	6.60±0.10	1.83±0.11	1.63±0.09	2.03±0.08	0.54±0.13	3.01±0.10	4.96±0.04
ETL	3.32±0.08	2.42±0.07	3.21±0.09	1.02±0.02	3.44±0.09	6.73±0.07	1.98±0.06	1.78±0.12	2.15±0.03	0.59±0.12	3.16±0.13	5.15±0.11
CDRIB	3.50±0.12	2.50±0.15	3.44±0.10	1.12±0.08	3.69±0.04	7.06±0.13	2.28±0.11	1.94±0.08	2.52±0.11	0.65±0.13	3.37±0.12	5.52±0.07
FedGNN	3.48±0.09	2.46±0.13	3.34±0.09	1.09±0.09	3.36±0.05	6.89±0.15	2.05±0.08	1.86±0.15	2.40±0.08	0.60±0.11	3.30±0.10	5.26±0.13
PriCDR	3.62±0.09	2.55±0.09	4.14±0.13	1.15±0.04	4.16±0.16	8.43±0.10	3.14±0.07	2.52±0.06	3.44±0.12	1.08±0.08	4.22±0.08	7.50±0.06
FedCDR	3.66±0.13	2.67±0.06	4.16±0.05	1.20±0.03	4.28±0.06	8.64±0.04	3.30±0.03	2.64±0.10	3.62±0.07	1.13±0.02	4.36±0.12	7.72±0.11
P2FCDR	4.02±0.05	2.75±0.04	4.22±0.03	1.28±0.02	4.64±0.07	8.97±0.08	3.77±0.04	3.20±0.08	4.13±0.03	1.25±0.06	5.03±0.08	8.75±0.06
FPPDM	4.10±0.04	2.80±0.07	4.30±0.05	1.30±0.01	4.68±0.08	9.05±0.05	3.83±0.06	3.29±0.07	4.17±0.05	1.26±0.08	5.23±0.09	8.85±0.07
Ours	**4.30±0.06***	**3.10±0.12***	**4.62±0.06***	**1.38±0.03***	**4.97±0.08***	**9.32±0.03***	**4.48±0.11***	**3.64±0.08***	**4.73±0.03***	**1.47±0.06***	**5.80±0.04***	**9.66±0.14***
Improv.	4.88%	10.71%	7.44%	6.15%	6.20%	2.98%	16.97%	10.64%	13.43%	16.67%	10.90%	9.15%

Methods	Cloth-domain recommendation						Sport-domain recommendation					
	MRR	NDCG		HR			MRR	NDCG		HR		
		@5	@10	@1	@5	@10		@5	@10	@1	@5	@10
PMLAM	2.25±0.12	1.68±0.05	2.13±0.08	0.59±0.11	2.83±0.10	4.73±0.04	2.63±0.06	1.96±0.04	2.95±0.05	0.72±0.13	3.26±0.05	7.06±0.07
LightGCN	2.36±0.08	1.75±0.04	2.29±0.12	0.65±0.05	2.97±0.07	4.84±0.13	2.72±0.03	2.07±0.06	3.02±0.07	0.78±0.16	3.39±0.15	7.20±0.05
CGCL	2.47±0.03	1.83±0.08	2.40±0.14	0.68±0.09	3.11±0.13	5.05±0.07	2.84±0.07	2.16±0.10	3.15±0.16	0.81±0.09	3.54±0.04	7.31±0.10
CoNet	2.41±0.08	1.81±0.09	2.35±0.15	0.67±0.06	2.95±0.12	5.13±0.14	2.96±0.06	2.12±0.11	3.20±0.12	0.81±0.13	3.47±0.12	7.21±0.16
ETL	2.55±0.07	1.90±0.11	2.49±0.06	0.70±0.13	3.01±0.08	5.28±0.09	3.04±0.04	2.16±0.09	3.26±0.11	0.84±0.08	3.51±0.10	7.27±0.05
CDRIB	2.94±0.03	2.06±0.12	2.83±0.10	0.91±0.10	3.25±0.11	5.81±0.07	3.37±0.11	2.36±0.12	3.53±0.06	0.97±0.09	3.71±0.13	7.51±0.03
FedGNN	2.45±0.08	1.86±0.05	2.36±0.12	0.70±0.13	3.15±0.13	5.18±0.08	2.90±0.10	2.47±0.14	3.28±0.13	0.84±0.09	4.30±0.12	6.70±0.09
PriCDR	2.62±0.13	1.95±0.07	2.56±0.13	0.73±0.04	3.31±0.16	5.39±0.06	3.03±0.09	2.63±0.08	3.36±0.14	0.86±0.15	4.44±0.09	6.81±0.10
FedCDR	2.69±0.09	2.06±0.06	2.72±0.03	0.78±0.05	3.39±0.06	5.56±0.09	3.14±0.06	2.67±0.07	3.49±0.05	0.90±0.08	4.47±0.08	7.18±0.03
P2FCDR	2.99±0.11	2.36±0.10	3.08±0.12	0.98±0.02	3.82±0.02	6.26±0.12	3.52±0.02	2.75±0.03	3.70±0.03	1.00±0.04	4.50±0.02	7.36±0.07
FPPDM	3.03±0.11	2.41±0.09	3.11±0.13	0.99±0.03	3.84±0.04	6.36±0.14	3.54±0.03	2.78±0.05	3.74±0.02	1.16±0.03	4.53±0.03	7.40±0.10
Ours	**3.54±0.12***	**2.71±0.05***	**3.68±0.04***	**1.14±0.07***	**4.37±0.06***	**7.32±0.11***	**3.64±0.11***	**2.88±0.05***	**3.85±0.04***	**1.22±0.06***	**4.66±0.06***	**7.66±0.05***
Improv.	16.83%	12.45%	18.33%	15.15%	13.80%	15.09%	2.82%	3.60%	2.94%	5.17%	2.87%	3.51%

Table 2. Experimental results (%) on the bi-directional Game-Video and Cloth-Sport federated DTCDR scenario. The best performance is bold-faced and the runner-up is underlined in terms of the corresponding metric, where $*$ denotes a significant improvement according to the wilcoxon signed-rank test.

Methods	Game-domain recommendation			Video-domain recommendation		
	MRR	NDCG@5	HR@5	MRR	NDCG@5	HR@5
PriCDR	2.53	2.08	2.80	3.41	2.53	3.93
FedCDR	2.56	2.18	2.88	3.59	2.65	4.07
P2FCDR	2.81	2.25	3.12	4.10	3.21	4.70
FPPDM	2.86	2.27	3.14	4.15	3.26	4.71
Ours	**3.01**	**2.53**	**3.34**	**4.87**	**3.65**	**5.41**
Improv.	5.24%	11.45%	6.37%	17.35%	11.96%	14.86%

Table 3. Experimental results (%) on the bi-directional Game-Video federated DTCDR scenario for cold-start users. The best performance is bold-faced in terms of the corresponding metric.

DTCDR models for the federated bi-directional CDR scenarios, we choose two pairs of domains from Amazon datasets: there are Game-Video and Cloth-Sport (four datasets). Note that, to validate the superiority of our proposed framework, we recommend items in both domains for the whole users and cold-start users. Specifically, in the data preprocessing, we filter out the items that have fewer than 10 interactions and the users that have fewer than 5 interactions in their domains as the previous works [Cao *et al.*, 2022]. For each user, we use the first 40% of data as the training set, 30% data as the validation set, and 30% data as the testing set. Besides, we filter the users that have fewer than 3 interactions in the training data as the cold-start users. The concrete statistics of federated DTCDR scenarios are summarized in Table 1. Note that, we also conduct experiments under the multi-domain scenarios on Douban datasets with ($K = 3$), which follows [Liu *et al.*, 2023c]. More details about the multi-domain results could be referred to **Appendix** due to space limitations.

Evaluation Protocol. On the basis of the previous works [Kang *et al.*, 2019], the leave-one-out evaluation method is widely used [Zhu *et al.*, 2021b]. To illustrate the effectiveness of methods, we adopted leave-one-out evaluation as well. Specifically, we calculate 1000 records (1 positive and 999 negative samples) and the three adopted metrics under federated DTCDR are MRR, NDCG@5,10 and HR@1,5,10, similar to [Cao *et al.*, 2022; Liu *et al.*, 2023c].

Compared Methods. To illustrate the effectiveness of our proposed framework, we compare P^{2}DTR with the following SOTA baselines which can be divided into three branches. (1) Single-domain recommendation: PMLAM [Ma *et al.*, 2020], LightGCN [He *et al.*, 2020] and CGCL [He *et al.*, 2023]; (2) Dual-target cross-domain recommendation: CoNet [Hu *et al.*, 2018], ETL [Chen *et al.*, 2023b] and CDRIB [Cao *et al.*, 2022]; (3) Federated dual-target cross-domain recommendation: FedGNN [Meihan *et al.*, 2022], PriCDR [Chen *et al.*, 2022], FedCDR [Wu *et al.*, 2022], P2FCDR [Chen *et al.*, 2023a] and FPPDM [Liu *et al.*, 2023c].

Parameter Settings. In our experiments, we use official implementations of other baselines. For the common hyperparameters in the baselines, we adopt the same value for all the methods, such as the embedding dimension d to 128, the batch size to 1024 and the minibatch size to 128 or 256. For the specific hyperparameters in the baselines, what we adopt are the values which have been reported in their original literature. For our proposed model P^{2}DTR, we tune the hyperparameter λ in $\{10^2, 10, 1, 1e^{-1}, 1e^{-2}\}$, the number of prototypes in $\{16, 32, 64, 128\}$ and the number of graph encoder layer in $\{1, 2, 3, 4\}$. In our model, we use Adam optimizer and the decay learning rate. For all these methods, we run each experiment with a random seed for five times and select the best result according to the highest MRR performance on the validation set, tuned by grid search.

Datasets	Game-domain recommendation			Video-domain recommendation		
	MRR	NDCG@5	HR@5	MRR	NDCG@5	HR@5
Base	3.06	2.07	2.95	1.67	1.39	2.71
+Inter	3.55	2.46	3.31	2.51	2.27	4.18
+Intra	4.30	3.10	4.97	4.48	3.64	5.80

Table 4. Ablation study results (%) of the main components of P^2DTR on the two dual-target cross-domain datasets.

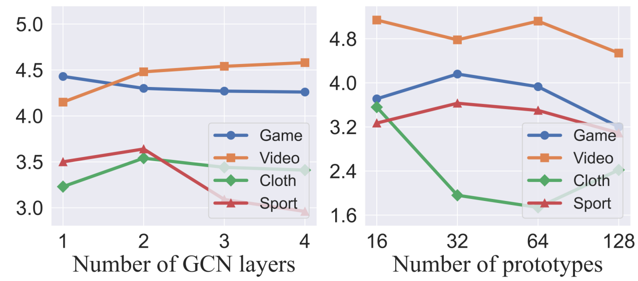

Figure 3: Performance of hyperparameter study regarding MRR with varying hyperparameters on Game-domain, Video-domain, Cloth-domain and Sport-domain datasets.

4.2 Overall Performance Comparison (RQ1)

To verify the effectiveness of our proposed model, we consider limited user transferring for the federated DTCDR. We compare the experimental results of our proposal P^2DTR with other SOTA baselines, shown in Table 2, and we can have the following observations.

In general, our P^2DTR outperforms all baselines across all evaluation metrics on all real-world datasets, which answers **RQ1** with an effective framework. Note that, limited by the federated experimental settings, the privacy data from different domains are prohibited from transmitting data directly. Compared with the second-best performance, the performance gains of P^2DTR range from reasonably large (2.83% achieved with HR@5 on sport) to significant large (16.82% achieved with MRR on video).

In particular, we compare the single-domain methods of collaborative filtering without auxiliary cross-domain contents with our P^2DTR. The results by P^2DTR outperform the three baselines across all evaluation metrics on all datasets, which illustrates the DTCDR is an effective way to alleviate data sparsity. Besides, by considering both DTCDR and privacy protection, P^2DTR performs better than cross-domain baselines. Although existing cross-domain methods can jointly capture knowledge from both domains, it fails to transfer the knowledge when the user data user data cannot be directly accessed. In this way, P^2DTR can outperform CDRIB by up to 34.3% in NDCG@10 on game dataset. Moreover, compared with the federated DTCDR models, although FPPDM can achieve the second-best performance via server aggregation to combine user characteristics across domains, our proposed P^2DTR can still gain improvements by enhancing the local user embeddings via intra-client enhanced recommendation.

Furthermore, to provide a more comprehensive demonstration of our model in capturing the auxiliary information from both domains, we also present the experimental results for cold-start users with other SOTA federated DTCDR methods. From the Table 3, we can observe the performance gains of P^2DTR in terms of FPPDM range from reasonably large (5.34% achieved with MRR on game) to significant large (17.31% achieved with MRR on video). The experimental results demonstrate the effectiveness of our proposed P^2DTR in enhancing the federated DTCDR based on the transferred knowledge across domains.

4.3 Ablation Experiment (RQ2)

In order to comprehensively evaluate the performance of our method, we conducted ablation experiments on our framework by incrementally adding components to answer **RQ2**. We adopted the widely used model, LightGCN, as our base model. Subsequently, we introduced Inter-client Knowledge Extraction (+Inter) followed by Intra-client Enhanced Recommendation (+Intra). The conclusions can be drawn by taking insights into Table 4.

Compared with the base model, Base+Inter implementation achieved an increase in model capability from 12.2% (achieved in HR@5 on Game) to 63.3% (achieved in NDCG@5 on Game). The experimental results demonstrated superior performance, highly indicating the effectiveness of the inter-client knowledge extraction. In addition, the increase from Base+Inter+Intra (our proposed P^2DTR) over Base+Inter within the range of 21.1% (achieved in MRR on Game) to 78.5% (achieved in MRR on Video). While the Base+Inter has already shown significant improvements, our P^2DTR can further enhance the performance through a well-designed intra-client enhanced recommendation.

4.4 Hyperparameter Study (RQ3)

Our proposed P^2DTR framework mainly introduces two hyperparameters, i.e., the number of prototypes K and graph layers L, respectively. Here we show how these two hyperparameters impact the performance, which answers the **RQ3**. From Figure 3, we have the following observations: (1) L is the number of graph neural network layers, where we found that the optimal values are about 2, 3 and 4 layers, which is sensitive to the hyperparameter. We set $L = 3$, which seems to be the rule-of-thumb. (2) K is the number of prototypes, where we found the optimal values are $16, 32$ and 128. In consequence, our P^2DTR is reasonably sensitive to the prototype number K and the optimal parameters can be obtained by slight tuning.

5 Conclusion

In this paper, we propose a novel framework named P^2DTR to perform DTCDR while protecting the user privacy. Specifically, we devise inter-client knowledge extraction to capture the inter-client knowledge under a privacy-preserving scenario. Furthermore, we design an intra-client enhanced recommendation to perform federated DTCDR based on the extracted common knowledge. Finally, we conduct extensive experiments to show the effectiveness of our proposed P^2DTR framework under a privacy-preserving guarantee on both domains.

Acknowledgments

This work is in part supported by the National Natural Science Foundation of China under Grants 6230071268, U21A20472 and 62276065; the National Key Research and Development Plan of China under Grant 2021YFB3600503; the Fujian Provincial Youth Education and Scientific Research Project under Grant JAT220811.

References

[Alemu *et al.*, 2019] Leulseged Tesfaye Alemu, Mubarak Shah, and Marcello Pelillo. Deep constrained dominant sets for person re-identification. In *2019 IEEE/CVF International Conference on Computer Vision, ICCV 2019*, pages 9854–9863, 2019.

[Cao *et al.*, 2022] Jiangxia Cao, Jiawei Sheng, Xin Cong, Tingwen Liu, and Bin Wang. Cross-domain recommendation to cold-start users via variational information bottleneck. In *2022 IEEE 38th International Conference on Data Engineering (ICDE)*, pages 2209–2223. IEEE, 2022.

[Chen *et al.*, 2022] Chaochao Chen, Huiwen Wu, Jiajie Su, Lingjuan Lyu, Xiaolin Zheng, and Li Wang. Differential private knowledge transfer for privacy-preserving cross-domain recommendation. In *WWW '22: The ACM Web Conference 2022*, pages 1455–1465, 2022.

[Chen *et al.*, 2023a] Gaode Chen, Xinghua Zhang, Yijun Su, Yantong Lai, Ji Xiang, Junbo Zhang, and Yu Zheng. Win-win: A privacy-preserving federated framework for dual-target cross-domain recommendation. In *Thirty-Seventh AAAI Conference on Artificial Intelligence*, pages 4149–4156, 2023.

[Chen *et al.*, 2023b] Xu Chen, Ya Zhang, Ivor W Tsang, Yuangang Pan, and Jingchao Su. Toward equivalent transformation of user preferences in cross domain recommendation. *ACM Transactions on Information Systems*, 41(1):1–31, 2023.

[Du *et al.*, 2021] Yongjie Du, Deyun Zhou, Yu Xie, Jiao Shi, and Maoguo Gong. Federated matrix factorization for privacy-preserving recommender systems. *Applied Soft Computing*, 111:107700, 2021.

[Guo *et al.*, 2021] Lei Guo, Li Tang, Tong Chen, Lei Zhu, Quoc Viet Hung Nguyen, and Hongzhi Yin. DA-GCN: A domain-aware attentive graph convolution network for shared-account cross-domain sequential recommendation. In *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence, IJCAI 2021, Virtual Event / Montreal, Canada, 19-27 August 2021*, pages 2483–2489, 2021.

[He *et al.*, 2017] Xiangnan He, Lizi Liao, Hanwang Zhang, Liqiang Nie, Xia Hu, and Tat-Seng Chua. Neural collaborative filtering. In *Proceedings of the 26th International Conference on World Wide Web*, pages 173–182, 2017.

[He *et al.*, 2020] Xiangnan He, Kuan Deng, Xiang Wang, Yan Li, Yongdong Zhang, and Meng Wang. Lightgcn: Simplifying and powering graph convolution network for recommendation. In *Proceedings of the 43rd International ACM SIGIR conference on research and development in Information Retrieval*, pages 639–648, 2020.

[He *et al.*, 2023] Wei He, Guohao Sun, Jinhu Lu, and Xiu Susie Fang. Candidate-aware graph contrastive learning for recommendation. In *Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 1670–1679, 2023.

[Hu *et al.*, 2018] Guangneng Hu, Yu Zhang, and Qiang Yang. Conet: Collaborative cross networks for cross-domain recommendation. In *Proceedings of the 27th ACM international conference on information and knowledge management*, pages 667–676, 2018.

[Huang *et al.*, 2023] Wei Huang, Jia Liu, Tianrui Li, Shenggong Ji, Dexian Wang, and Tianqiang Huang. Fedcke: Cross-domain knowledge graph embedding in federated learning. *IEEE Trans. Big Data*, 9(3):792–804, 2023.

[Kang *et al.*, 2019] SeongKu Kang, Junyoung Hwang, Dongha Lee, and Hwanjo Yu. Semi-supervised learning for cross-domain recommendation to cold-start users. In *Proceedings of the 28th ACM International Conference on Information and Knowledge Management*, pages 1563–1572, 2019.

[Li *et al.*, 2016] Ninghui Li, Min Lyu, Dong Su, and Weining Yang. *Differential Privacy: From Theory to Practice*. Synthesis Lectures on Information Security, Privacy, & Trust. 2016.

[Liu *et al.*, 2022] Weiming Liu, Xiaolin Zheng, Jiajie Su, Mengling Hu, Yanchao Tan, and Chaochao Chen. Exploiting variational domain-invariant user embedding for partially overlapped cross domain recommendation. In *Proceedings of the 45th International ACM SIGIR conference on research and development in information retrieval*, pages 312–321, 2022.

[Liu *et al.*, 2023a] Ruixuan Liu, Yang Cao, Yanlin Wang, Lingjuan Lyu, Yun Chen, and Hong Chen. Privaterec: Differentially private model training and online serving for federated news recommendation. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, KDD 2023, Long Beach, CA, USA, August 6-10, 2023*, pages 4539–4548, 2023.

[Liu *et al.*, 2023b] W. Liu, C. Chen, X. Liao, and M. Hu. Federated probabilistic preference distribution modelling with compactness co-clustering for privacy-preserving multi-domain recommendation. In *Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence (IJCAI-23)*, pages 2206–2214, 2023.

[Liu *et al.*, 2023c] Weiming Liu, Chaochao Chen, Xinting Liao, Mengling Hu, Jianwei Yin, Yanchao Tan, and Longfei Zheng. Federated probabilistic preference distribution modelling with compactness co-clustering for privacy-preserving multi-domain recommendation. In *Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence, IJCAI 2023, 19th-25th August 2023, Macao, SAR, China*, pages 2206–2214, 2023.

[Liu *et al.*, 2023d] Weiming Liu, Xiaolin Zheng, Chaochao Chen, Mengling Hu, Xinting Liao, Fan Wang, Yanchao Tan, Dan Meng, and Jun Wang. Differentially private sparse mapping for privacy-preserving cross domain recommendation. In *Proceedings of the 31st ACM International Conference on Multimedia, MM 2023, Ottawa, ON, Canada, 29 October 2023- 3 November 2023*, pages 6243–6252, 2023.

[Liu *et al.*, 2023e] Weiming Liu, Xiaolin Zheng, Chaochao Chen, Jiajie Su, Xinting Liao, Mengling Hu, and Yanchao Tan. Joint internal multi-interest exploration and external domain alignment for cross domain sequential recommendation. In *Proceedings of the ACM Web Conference 2023*, pages 383–394, 2023.

[Liu *et al.*, 2023f] Weiming Liu, Xiaolin Zheng, Jiajie Su, Longfei Zheng, Chaochao Chen, and Mengling Hu. Contrastive proxy kernel stein path alignment for cross-domain cold-start recommendation. *IEEE Transactions on Knowledge and Data Engineering*, 2023.

[Ma *et al.*, 2020] Chen Ma, Liheng Ma, Yingxue Zhang, Ruiming Tang, Xue Liu, and Mark Coates. Probabilistic metric learning with adaptive margin for top-k recommendation. In *KDD '20: The 26th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, Virtual Event*, pages 1036–1044, 2020.

[McMahan *et al.*, 2017] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, pages 1273–1282, 2017.

[Meihan *et al.*, 2022] 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 *Proceedings of the 31st ACM International Conference on Information & Knowledge Management*, pages 2179–2188, 2022.

[Skoulakis *et al.*, 2021] Stratis Skoulakis, Tanner Fiez, Ryann Sim, Georgios Piliouras, and Lillian J. Ratliff. Evolutionary game theory squared: Evolving agents in endogenously evolving zero-sum games. In *Thirty-Fifth AAAI Conference on Artificial Intelligence*, pages 11343–11351, 2021.

[Tan *et al.*, 2022a] Y. Tan, G. Long, L. Liu, T. Zhou, Q. Lu, J. Jiang, and C. Zhang. Fedproto: Federated prototype learning across heterogeneous clients. *Proceedings of the AAAI Conference on Artificial Intelligence*, 36(8):8432–8440, 2022.

[Tan *et al.*, 2022b] Yue Tan, Guodong Long, Lu Liu, Tianyi Zhou, Qinghua Lu, Jing Jiang, and Chengqi Zhang. Fedproto: Federated prototype learning across heterogeneous clients. In *Thirty-Sixth AAAI Conference on Artificial Intelligence*, pages 8432–8440, 2022.

[Wang *et al.*, 2023] Lianyu Wang, Meng Wang, Daoqiang Zhang, and Huazhu Fu. Model barrier: A compact untransferable isolation domain for model intellectual property protection. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 20475–20484, 2023.

[Weibull, 1997] Jörgen W Weibull. *Evolutionary game theory*. MIT press, 1997.

[Wu *et al.*, 2022] Meihan Wu, Li Li, Chang Tao, Eric Rigall, Xiaodong Wang, and Cheng-Zhong Xu. Fedcdr: Federated cross-domain recommendation for privacy-preserving rating prediction. In *Proceedings of the 31st ACM International Conference on Information & Knowledge Management*, pages 2179–2188. ACM, 2022.

[Yang *et al.*, 2022] Liu Yang, Junxue Zhang, Di Chai, Leye Wang, Kun Guo, Kai Chen, and Qiang Yang. Practical and secure federated recommendation with personalized mask. In *Trustworthy Federated Learning - First International Workshop, FL 2022, Held in Conjunction with IJCAI 2022, Vienna, Austria, July 23, 2022, Revised Selected Papers*, volume 13448, pages 33–45, 2022.

[Zemene and Pelillo, 2016] Eyasu Zemene and Marcello Pelillo. Interactive image segmentation using constrained dominant sets. In *Computer Vision - ECCV 2016 - 14th European Conference*, volume 9912, pages 278–294. Springer, 2016.

[Zhang *et al.*, 2023] Chunxu Zhang, Guodong Long, Tianyi Zhou, Peng Yan, Zijian Zhang, Chengqi Zhang, and Bo Yang. Dual personalization on federated recommendation. In *Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence, IJCAI 2023, 19th-25th August 2023, Macao, SAR, China*, pages 4558–4566, 2023.

[Zhu *et al.*, 2018] Feng Zhu, Yan Wang, Chaochao Chen, Guanfeng Liu, Mehmet Orgun, and Jia Wu. A deep framework for cross-domain and cross-system recommendations. In *IJCAI*, pages 3711–3717, 2018.

[Zhu *et al.*, 2021a] Feng Zhu, Yan Wang, Chaochao Chen, Jun Zhou, Longfei Li, and Guanfeng Liu. Cross-domain recommendation: Challenges, progress, and prospects. In *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence, IJCAI 2021, Virtual Event / Montreal, Canada, 19-27 August 2021*, pages 4721–4728, 2021.

[Zhu *et al.*, 2021b] Yongchun Zhu, Kaikai Ge, Fuzhen Zhuang, Ruobing Xie, Dongbo Xi, Xu Zhang, Leyu Lin, and Qing He. Transfer-meta framework for cross-domain recommendation to cold-start users. In *Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 1813–1817, 2021.

[Zhu *et al.*, 2022] Yongchun Zhu, Zhenwei Tang, Yudan Liu, Fuzhen Zhuang, Ruobing Xie, Xu Zhang, Leyu Lin, and Qing He. Personalized transfer of user preferences for cross-domain recommendation. In *Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining*, pages 1507–1515, 2022.