Device-Cloud Collaborative Learning for Recommendation

Jiangchao Yao†, Feng Wang†, Kunyang Jia†, Bo Han‡, Jingren Zhou†, Hongxia Yang†
†DAMO Academy, Alibaba Group, Hangzhou, China; ‡Hong Kong Baptist University, Hong Kong, China;
†{jiangchao.yjc, wf135777, kunyang.jky, jingren.zhou, yang.yhx}@alibaba-inc.com, ‡bhanml@comp.hkbu.edu.hk

ABSTRACT

With the rapid development of storage and computing power on mobile devices, it becomes critical and popular to deploy models on devices to save onerous communication latencies and to capture real-time features. While quite a lot of works have explored to facilitate on-device learning and inference, most of them focus on dealing with response delay or privacy protection. Little has been done to model the collaboration between the device and the cloud modeling and benefit both sides jointly. To bridge this gap, we are among the first attempts to study the Device-Cloud Collaborative Learning (DCCL) framework. Specifically, we propose a novel Meta-Patch learning approach on the device side to efficiently achieve “thousands of people with thousands of models” given a centralized cloud model. Then, with billions of updated personalization device models, we propose a “model-over-models” distillation algorithm, namely MoMoDistill, to update the centralized cloud model. Our extensive experiments over a range of datasets with different settings demonstrate the effectiveness of such collaboration on both cloud and devices, especially its superiority to model long-tailed users.

CCS CONCEPTS

• Information systems → Recommender systems.

KEYWORDS

On-device Intelligence, Cloud Computing, Recommender Systems

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ACM Reference Format:
Jiangchao Yao†, Feng Wang†, Kunyang Jia†, Bo Han‡, Jingren Zhou†, Hongxia Yang†. 2021. Device-Cloud Collaborative Learning for Recommendation. In Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '21), August 14–18, 2021, Virtual Event, Singapore. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3447548.3467097

1 INTRODUCTION

Nascent applications for mobile computing and the Internet of Things (IoTs) are driving computing toward dispersion [38]. Specifically, the evolving capacity of mobile devices makes it possible to consider the intelligence services, e.g., online recommendation, from cloud to device modeling. Recently, several works in different perspectives like privacy [2, 22, 23], efficiency [4, 14], applications [8, 11, 42] have explored this pervasive computing advantages. Mobile recommender systems with the on-device engines e.g., TFLite† and CoreML‡ hence attract more and more attention.

Previous research in this area of recommender systems can be summarized into two lines, on-device inference and on-device learning given the centralized model. The former deploys the pretrained model to the devices, and executes the inference to save the onerous communication latencies and capture real-time features. This mainly solves the computational efficiency problem, yielding the exploration of the device-friendly model inference. For example, Sun et al. [41] proposed CpRec to shrink the sequential recommender system, which compress the size of input and output matrices as well as the parameters of middle layers via adaptive decomposition and parameter sharing. In a broader area, Cai et al. [3] introduced a generalized network pruning method, progressive shrinking, to reduce the model size across dimensions for efficient deployment. Gong et al. [11] explored a split deployment across cloud and device to reduce the inference cost of on-device components.

The latter line of works aggregate the temporal on-device training pieces into a centralized model to overcome the privacy constraint, namely Federated recommender systems [44]. The gradients of the local copy from the centralized deep model is first executed on plenty of devices, and then are collected to the server to update the model parameters by federated averaging (FedAvg) or its variants [22, 23, 29]. For example, Qi et al. [33] applied Federated Learning and differential privacy for news recommendation and achieved a balance between recommendation performance and privacy protection. Lin et al. [27] introduced a MetaMF to account for the storage, energy and communication bandwiths in mobile environments, which distributes the gradient computation across cloud and devices. Niu et al. [30] followed a similar split in gradient computation but designed a tunable privacy to the local submodel.

Different from the above two lines of works, we focus on how to leverage the advantages of the device modeling and the cloud modeling jointly to benefit both sides. The intuition behind this direction is two-fold: on the one hand, the centralized cloud model usually ignores or even sacrifices the experience of long-tailed samples, users or items, to maximize the global revenue. And long-tailed and non-i.i.d (independent and identically distributed) characteristics in recommendation samples inevitably induce the model bias to the minorities [31]. One possible solution is to personalize the cloud model with local data on each device. On the other hand, training samples on each device alone may be quite limited suffering from local optimization [10]. In contrast, the centralized cloud models
are updated with data from all devices and able to avoid this problem. This motivates us to propose a comprehensive Device-Cloud Collaborative Learning (DCCL) framework.

We summarize our contributions as follows:

- Compared to existing works that either only consider the cloud modeling, or on-device inference, or the aggregation of the temporal on-device training pieces to handle the privacy constraint, we formally propose a Device-Cloud Collaborative Learning framework (DCCL) to benefit both sides.
- We propose two novel methods MetaPatch and MoMoDistill to instantiate each side in DCCL, which consider the sparsity challenge for on-device personalization, and enhance the centralized cloud model via the "model-over-models" MoMoDistill distillation instead of the conventional "model-over-data" paradigm.
- Extensive experiments on a range of datasets demonstrate that DCCL outperforms the state-of-the-art methods, and especially, we provide a comprehensive analysis about its advantage to long-tailed users and the inter-loops between computing interactions of cloud and device.

2 RELATED WORKS

2.1 Recommender System

Recommender systems [36] have been widely studied in the last decade and become an indispensable infrastructure of web services in the era of cloud computing and big data. The related recommendation methods are gradually improved with the development of collaborative filtering, deep learning and sequential modeling. The early stage mainly focused on the user-based collaborative filtering [48], the item-based collaborative filtering [37] and matrix factorization [24, 34]. As deep learning achieved a great success in computer vision, several variants of collaborative filtering combined with deep neural networks were proposed [5–7, 12, 16, 45]. They leveraged the non-linear transformation of deep neural networks to activate high-level semantics for more accurate recommendation. Sequential modeling as another perspective to model the user interests has been successfully applied to recommender systems [39]. With the optimization in architectures, several methods based on GRU [19], Attention [21, 43, 47, 49] have achieved the remarkable performance in recommender systems.

2.2 On-device Inference

On-device inference as an important part of Edge AI [40] greatly reduces the onerous latency and incorporates rich features in recommendation. This line of works critically depend on the device capacity [1], efficient neural network architectures [15], the model compression technique [14] and some split deployment strategies. Recently, several hardware efficient architectures like MobileNets [18] were proposed, which made the model size and the computational budget for on-device inference lightweight. Another effective perspective is the model compression based on the network pruning or quantization [3, 14], which reduces the units, the channels or the value accuracy of the parameters. In recommender systems, CpRec [41] considered to construct a compressed counterpart of the sequential models by introducing a block-wise adaptive decomposition and parameter sharing scheme. Lee et al. [26] described how to leverage the mobile GPU to run deep neural network tasks, which considers the special limited computing power, thermal constraints, and energy consumption. Dai et al. [8] presented an app to demonstrate the potential usage of on-device inference for mobile health applications. Some other works [11] also explored the divide-and-conquer deployment to save the running time on devices, in which the computational prohibitive modules can be moved to the cloud. Nevertheless, all these works still share a centralized model.

2.3 On-device Learning

On-device learning is more time-consuming than on-device inference as it requires the extra computation regarding gradients [9]. Current methods are mainly for Federated Learning [23], a distributed learning framework to keep the data in the local and only communicate gradients or parameters. It is important as more and more users consider the privacy protection on the Internet as General Data Protection Regulation (GDPR)3 claims in Europe. In Federated Learning, on-device learning is used to compute the temporal training pieces and send to the cloud for averaging, and several
works applied Federated Learning to the recommender systems. Qi et al. [33] applied Federated Learning and differential privacy to News Recommendation, which achieved a promising trade-off between recommendation performance and privacy protection. Lin et al. [27] introduced a MetaMF to account for the storage, energy and communication bandwidth in mobile environments, which distributed the gradient computation of Federated Learning across cloud and devices. Niu et al. [30] followed a similar split in gradient computation and designed a tunable privacy to the local submodel. Nevertheless, we argue that privacy protection is an exemplar usage of conceivable on-device learning. How to explore the collaboration between the cloud modeling and the device modeling for mutual benefit of two sides is also meaningful in practice [25]. One previous work [28] has the similar intuition differs from our method in the way to handle the sparsity issue and their method has not considered the frequent checkpoint loading issue.

3 THE PROPOSED FRAMEWORK

3.1 Preliminary

Given a recommendation dataset \(\{(x_n, y_n)\}_{n=1,...,N}\), we target to learn a mapping function \(f : x_n \in \mathbb{R}^D \rightarrow y_n \in \mathbb{R}\) on the cloud side. Here, \(x_n\) is the input \(D\)-dimensional feature that concatenates all available candidate features and user context, \(y_n\) is the user implicit feedback (click or not) to the corresponding candidate and \(N\) is the sample number. On the device side, each device (indexed by \(m\)) has its own local dataset, \(\{(x_n^{(m)}, y_n^{(m)})\}_{n=1,...,N^{(m)}}\). We add a few parameter-efficient patches [46] to the cloud model \(f\) (freezing its parameters on the device side) for each device to construct a new function \(f^{(m)} : x_n^{(m)} \in \mathbb{R}^D \rightarrow y_n^{(m)} \in \mathbb{R}\). Note that, only the parameters related to patches are used for the model personalization and updated based on the local dataset.

As summarized in previous sections, the works regarding on-device inference and those related to on-device learning for the centralized model have been explored in an independent perspective by means of the pervasive computing advantages. There are few works that consider how to make the device modeling and the cloud modeling to benefit both sides jointly in the recommendation scenarios. However, this is critical and meaningful, since the conventional centralized cloud model follows the "model-over-data" paradigm and is prone to Matthew effect [32]. On the other side, personalized models updated with relatively limited samples on the device side suffers from the local optimum [10], which can be calibrated by the centralized cloud model. We introduce the DCCL to bridge the gap, which customizes the personalization on the device side and enhances the centralized model with the "model-over-models" distillation over billions of personalized device models. Figure 1 gives the general illustration of the DCCL framework, however, real-world challenges make it not straightforward for implementation. In the following, we will discuss the practical challenges and deployment of each side in DCCL.

3.2 MetaPatch for On-device Personalization

Although the device hardware has been greatly improved in the recent years, compared to the rich computing power, energy and storage in the cloud, it is still resource-constrained to learn a complete big model on the device. Considering the parameter scale of the centralized cloud model \(f\) and the storage of the intermediate activations, it is an impractical choice to adapt the whole network on the device side. Meanwhile, only finetuning last few layers is performance-limited due to the feature basis of the pretrained layers. Fortunately, some previous works have demonstrated that it is possible to achieve the comparable performance as the whole network finetuning via patch learning [4, 17, 46]. Inspired by these works, we insert the model patches on basis of the cloud model \(f\) for on-device personalization. Formally, the output of the \(l\)-th layer attached with one patch on the \(m\)-th device is expressed as

\[
\hat{y}_m = \Theta_l \ast \hat{y}^{(m)},
\]

Figure 2: The proposed MetaPatch to reduce the parameter space on the device side. It uses the global parameter basis \(\Theta_l\) with the metapatch parameter \(\hat{y}^{(m)}\) to generate all parameters \(\{\hat{y}^{(m)}\}\), and parameterize \(h^{(m)}(\cdot)\) correspondingly. The dimension of patch parameters is reduced to \(\hat{K}\) from \(\sum_i K_i\).
surrogate tunable parameter vector to generate each patch parameter $\hat{\theta}_m$ in the device-model $f(m)$. To facilitate the understanding, we term $\hat{\theta}_m$ as the metapatch parameter. In this paper, we keep $\sum \hat{K}_i \gg \hat{K}$ so that the metapatch parameters to be learned for personalization are greatly reduced. Figure 2 illustrates the idea of MetaPatch. Note that, regarding the pretraining of $\Theta_f$, we leave the discussion in the following section to avoid the clutter, since it is learned on the cloud side. According to Eq. (2), we implement the patch parameter generation via the metapatch parameter $\hat{\theta}_m$ instead of directly learning $\hat{\theta}_m$. To learn the metapatch parameter, we can leverage the local dataset to minimize the following loss.

$$\min_{\hat{\theta}_m} \ell(y, \hat{y}) \big|_{\hat{y} = f(m)(x)^*} \tag{3}$$

where $\ell$ is the pointwise cross-entropy loss, $f(m)(\cdot) = f_L(m)(\cdot) \circ \cdots \circ f_1(m)(\cdot)$ and $L$ is the number of total layers. After training the device specific parameter $\hat{\theta}_m$ by Eq.(3), we can use Eq. (2) to generate all patches, and then insert them into the cloud network $f$ via Eq.(1) to get the final personalized model $f(m)$, which will provide the on-device personalized recommendation.

### 3.3 MoMoDistill to Enhance the Cloud Modeling

The conventional incremental training of the centralized cloud model follows the “model-over-data” paradigm. That is, when the new training samples are collected from devices, we directly perform the incremental learning based on the model trained in the early sample collection. The objective function is formulated as

$$\min_{W_f} \ell(y, \hat{y}) \big|_{\hat{y} = f(x)} \tag{4}$$

where $W_f$ is the network parameter of the cloud model $f$ to be trained. This is an independent perspective without considering the device modeling. However, the on-device personalization actually can be more powerful than the centralized cloud model to handle the corresponding local samples. Thus, the guidance from the on-device models could be a meaningful prior to help the cloud modeling. Inspired by this, we propose a “model-over-models” paradigm to simultaneously learn from data and aggregate the knowledge from on-device models, to enhance the training of the centralized cloud model. Besides, considering that on-device learning in a long term suffers from local optimization [10], this step also helps calibrate the model. Besides, considering that on-device learning in a long term suffers from local optimization [10], this step also helps calibrate the model.

Formally, the objective with the distillation procedure on the samples from all devices is defined as,

$$\min_{W_f} \ell(y, \hat{y}) + \beta \text{KL}(\hat{y}, \tilde{y}) \big|_{\hat{y} = f(x), \tilde{y} = f(m)(x)^*} \tag{5}$$

where $\beta$ is the hyperparameter to balance the distillation and “model-over-data” learning. Note that, the feasibility of the distillation in Eq. (5) critically depends on the patch mechanism in the previous section, since it allows us to input the metapatch parameters like features with only loading the other model parameters of $f(m)$ in one time. Otherwise, we will suffer from the engineering issue of reloading numerous checkpoints frequently, which is almost impossible for current open source frameworks like Tensorflow.

In MetaPatch, we introduce the global parameter basis $\{\Theta_f\}$ (simplified by $\Theta$) to reduce the parameter space on the device. Regarding its training, we empirically find that coupled learning with $W_f$ easily falls into undesirable local optimal, since they play different roles in terms of their semantics. Therefore, we resort to a progressive optimization strategy, that is, first optimize $f$ based on Eq. (5), and then distill the knowledge for the parameter basis $\Theta$ with the learned $f$. For the second step, we design an auxiliary component by considering the heterogeneous characteristics of the metapatches from all devices and the cold-start issue at the beginning. Concretely, given the dataset $\{x, y, \hat{f}(x^i), \hat{\theta}_i \} \in \mathbb{R}^{K \times \mathbb{R}^{d_u}}$, where $I$ maps the sample index to the device index and $u \subset x$ is the user profile features (e.g., age, gender, purchase level, etc.) of the corresponding device, we define the following auxiliary encoder,

$$U(\hat{\theta}_u) = \mathbb{W}^{(1)} \text{tanh}(\mathbb{W}^{(2)} \hat{\theta} + \mathbb{W}^{(3)} u), \tag{6}$$

where $\mathbb{W}^{(1)} \in \mathbb{R}^{K_i \times \mathbb{R}^{d_u}}$, $\mathbb{W}^{(2)} \in \mathbb{R}^{K_i \times \mathbb{R}^{d_u}}$, $\mathbb{W}^{(3)} \in \mathbb{R}^{d_u \times d_u}$ are tunable projection matrices, $d_u$ is the dimension of user profile features. Here, we use $\mathbb{W}_e$ denotes the collection $\{\mathbb{W}^{(1)}, \mathbb{W}^{(2)}, \mathbb{W}^{(3)}\}$ for simplicity. To learn the global parameter basis, we replace $\hat{\theta}$ by $U(\hat{\theta}_u)$ to simulate Eq. (2) to generate the model patch, i.e., $\Theta = U(\hat{\theta}_u)$, since actually $\hat{\theta}$ is too heterogeneous to be directly used. Then, combining $\Theta = U(\hat{\theta}_u)$ with $f$ learned in the first distillation step, we can form a new proxy device model $\hat{f}(m)$ (different from $f(m)$ in the patch generation). Here, we leverage such a proxy $\hat{f}(m)$ to directly distill the knowledge from the true $f(m)$ from devices, which optimizes $\Theta$ and $\mathbb{W}_e$ of the auxiliary encoder as follows,

$$\min_{(\Theta, \mathbb{W}_e)} \ell(y, \hat{y}) + \beta \text{KL}(\hat{y}, \tilde{y}) \big|_{\hat{y} = f(m)(x), \tilde{y} = f(m)(x)^*} \tag{7}$$

![Figure 3: The proposed MoMoDistill to enhance the cloud modeling.](image-url)
Algorithm 1: Device-Cloud Collaborative Learning

Pretrain the cloud model \( f \), and then learn the global parameter basis \( \Theta \) based on Eq. (7) by setting \( \hat{\theta} \) as 0.

\[
\text{while lifecycle do}
\]

Send \( f \) and \( \Theta \) to devices.

\[
\text{Device}(f, \Theta) \rightarrow \text{MetaPatch}
\]

1. Accumulate the local data into batches
2. On-device personalization via Eq.(3)
3. If time \( > \) threshold: upload \( f^{(m)} \)
4. Else: return step 1)

Recycle all model patches \( \{\hat{f}^{(m)}\} \).

\[
\text{Cloud}(\hat{\theta}^{(m)})) \rightarrow \text{MoMoDistill}
\]

1. Optimize the cloud model \( f \) based on Eq.(5)
2. Learn the parameter basis \( \Theta \) by Eq.(7)

\[
\text{end}
\]

Eq. (5) and Eq. (7) progressively help learn the centralized cloud model and the global parameter basis. We specially term this progressive distillation mechanism as \text{MoMoDistill} to emphasize our “model-over-models” paradigm different from the conventional “model-over-data” incremental training on the cloud side, and gives the illustration in Figure 3. Finally, in Algorithm 1, we summarize the complete procedure of DCCL with \text{MetaPatch} and \text{MoMoDistill}.

4 EXPERIMENTS

In this section, we will conduct a range of recommendation experiments to demonstrate the effectiveness of the proposed framework. To be specific, we will answer the following questions about DCCL.

(1) \textbf{RQ1:} Whether learning through the proposed framework can achieve a better performance compared with the conventional centralized incremental training in the cloud? The challenges come into two folds. First, we need to train the personalized models for each device. The detailed results of this part will be analysed in RQ2. Second, it is challenging to aggregate the knowledge from plenty of weakly heterogeneous on-device model “experts”, which has never been explored before.

(2) \textbf{RQ2:} Whether on-device model personalization can achieve further improvement than the centralized cloud model? The sparse data flow on the local devices can be very challenging to learn and easy to overfit. To our best knowledge, this has never been investigated on the large-scale industrial recommendation datasets at device granularity.

(3) \textbf{RQ3:} How is the convergence property regarding the their inter-loops between two modules and is it capable to maintain a cyclical process which iterates and optimizes between the cloud and the devices? It is important to characterize the long-term performance of our method, as once deployed, this framework will continually maintain such a learning cycle, which is a novel trial in the area of recommender systems.

4.1 Experimental Setup

4.1.1 Datasets. Our experiments are implemented on three recommendation datasets Amazon, Movielens-1M and Taobao. The statistics of all the above datasets are shown in Table 1. Generally, all these three datasets are user interactive history in sequence format, and the last user interacted item is cut out as test sample. For each last interacted item, we randomly sample 100 items that didn’t appear in user’s history. Detailed description about the data generation process is given in Appendix section.

| Dataset   | Amazon | MovieLens-1M | Taobao |
|-----------|--------|--------------|--------|
| Users     | 360,828| 6,040        | 17,018,570 |
| Goods     | 68,000 | 3,900        | 20,000,000 |
| Categories| 257    | 21           | 14,641  |
| Samples   | 3,087,820 | 1,000,209 | ~9 billions |

4.1.2 Baselines & Our methods. We compare DCCL with some classical cloud models in different perspectives, namely, the conventional methods, deep learning-based methods and sequence-based methods.

- \textbf{Conventional methods:}
  - MF [24]: The matrix factorization approach to model user-item interactions, which decomposes the observation as the product of the user embedding and the item embedding.
  - FM [35]: Factorization Machines (FM) maps real-valued features into a low-dimensional latent space, and models all interactions between variables using factorized parameters.

- \textbf{Deep learning-based methods:}
  - NeuMF [16]: It generalizes the classical MF into a deep-learning counterpart. It uses multiple neural layers to build a more expressive distance measure instead of inner product to capture the non-linearity in the implicit feedbacks.
  - DeepFM [12]: A wide & deep architecture that incorporates the factorization machine to automatically extract the wide features instead of the previous hand-crafted effort.

- \textbf{Sequence-based methods:}
  - SASRec [21]: A self-attention based sequential model, which utilizes the attention mechanism to adaptively assign weights to previous items for the next-item prediction.
  - DIN [49]: A target-attention based user interest model, which takes the candidates as the query w.r.t. the user historical behaviors to learn a user representation for prediction.

For the whole experiments, we implement our model on the basis of DIN, where we insert the model patches in the last second fully-connected layer and the first two fully-connected layers after the feature embedding layer. In all comparisons, we term \text{MetaPatch} as DCCL-e and \text{MoMoDistill} as DCCL-m, since the whole framework resembles EM\(^4\) iterations. The default method to compare the baselines is named DCCL, which indicates that it goes through both on-device personalization and the "model-over-models" distillation.

\[^4\text{https://en.wikipedia.org/wiki/Expectation-maximization_algorithm} \]
Metric MF FM NeuMF DeepFM SASRec DIN DCCL Improv.

| Datasets   | HitRate@1 | HitRate@5 | HitRate@10 | NDCG@5 | NDCG@10 | HitRate@1 | HitRate@5 | HitRate@10 | NDCG@5 | NDCG@10 | HitRate@1 | HitRate@5 | HitRate@10 | NDCG@5 | NDCG@10 |
|------------|-----------|-----------|------------|--------|---------|-----------|-----------|------------|--------|---------|-----------|-----------|------------|--------|---------|
| Amazon     | 23.69     | 21.53     | 26.10      | 25.43  | 26.53   | 26.94     | 44.79     | 44.00      | 44.53  | 56.59   | 44.05     | 4.14%     |            | 3.31%   |
| MovieLens-1M| 14.60     | 14.90     | 16.45      | 15.41  | 34.85   | 37.45     | 38.69     | 61.25      | 71.97  | 68.65   | 59.77     | 1.91%     |            | 5.79%   |
| Taobao     | 24.88     | 25.29     | 29.11      | 33.28  | 35.19   | 52.17     | 55.71     | 60.13      | 68.12  | 70.31   | 65.49     | 4.27%     |            | 6.79%   |

4.1.3 Evaluation Metrics. The model performance in our experiments are measured by the widely used AUC and NDCG. They are respectively calculated by the following equations.

\[
\text{HitRate}_K = \frac{1}{|U|} \sum_{u \in U} \mathbb{1}(R_{u, g_u} \leq K),
\]

\[
\text{NDCG}_K = \frac{1}{|U|} \sum_{u \in U} \frac{\sum_{x_1 \in D_F^{(u)}} \sum_{x_0 \in D_F^{(u)}} \mathbb{1}[f(x_1) < f(x_0)]}{|D_F^{(u)}||D_F^{(u)}|},
\]

where \( U \) is the user set, \( \mathbb{1} (\cdot) \) is the indicator function, \( R_{u, g_u} \) is the rank generated by the model for the ground truth item \( g_u \) and user \( u \), \( f \) is the model to be evaluated and \( D_F^{(u)} \), \( D_F^{(u)} \) is the positive and negative sample sets in testing data.

4.2 Experiments and Results

4.2.1 RQ1. To demonstrate the effectiveness of DCCL, we conduct the experiments on Amazon, MovieLens and Taobao to compare to a range of baselines. Aligned with the popular experimental settings \([16, 49]\), the last interactive item of each user on three datasets is left for evaluation and all items before the last one are used for training. For DCCL, we split the training data into two parts on average according to the temporal order: one part is for the pretraining of the backbone (DIN) and the other part is for the training of DCCL. In the experiments, we conduct one-round DCCL-e and DCCL-m. Finally, the DCCL-m is compared with the six representative models, whose results are summarized in Table 2.

According to Table 2, we find that the deep learning based methods NeuMF and DeepFM usually outperform the conventional methods MF and FM, and the sequence-based methods SASRec and DIN consistently outperform previous non-sequence-based methods.

Our DCCL builds upon on the best baseline DIN and further improves its results. Specifically, DCCL shows about 2% or more improvements in terms of NDCG@10, and at least 1% improvements in terms of HitRate@10 on all three datasets. The performance on both small and large datasets confirms the superiority of DCCL.

4.2.2 RQ2. In this section, we target to demonstrate that how on-device personalization via MetaPatch (abbreviated as DCCl-e) can improve the recommendation performance from different levels of users compared with the centralized cloud model. Considering the data scale and the availability of the context information for visualization, only the Taobao dataset is used to conduct this experiment. To validate the performance of DCCL-e in the fine-grained granularity, we sort the users based on their sample numbers and then partition them into 20 groups on average along the sorted user axis (see the statistic of the sample number w.r.t. the user in the appendix). After on-device model personalization, we calculate the performance for each group based on the personalized models. Here, the macro-AUC is used, which equally treats the users in the group instead of the sample-number-aware group AUC \([49]\).

We use DIN as baseline in this experiment and pretrain it on the Taobao Dataset of the first 20 days. Then, we test the model in the data of the remaining 10 days. For DCCL-e, we first pretrain DIN on the Taobao Dataset of the first 10 days, and then insert the patches into the pretrained DIN same as previous settings. Finally, we perform the on-device personalization in the subsequent 10 days. Similarly, we test the DCCL-e on the data of the last 10 days. The evaluation is respectively conducted in the 20 groups and their results are plot in Figure 4. According to the results, we can find that with the increase of the group index number, the performance approximately decreases. This is because the users in the group of larger indices are more like the long-tailed users based on our group partition, and their patterns are easily ignored or even sacrificed by the centralized cloud model. In comparison, DCCL-e shows the consistent improvement over DIN on all groups, and especially achieve the large improvement in the long-tailed user groups.

Table 2: The top-K recommendation performance of DCCL and baselines on three datasets.

| Datasets    | HitRate@10 | HitRate@5 | HitRate@10 | NDCG@5 | NDCG@10 | HitRate@10 | HitRate@5 | HitRate@10 | NDCG@5 | NDCG@10 | HitRate@10 | HitRate@5 | HitRate@10 | NDCG@5 | NDCG@10 |
|-------------|-------------|-----------|------------|--------|---------|-------------|-----------|------------|--------|---------|-------------|-----------|------------|--------|---------|
| Amazon      | 23.69       | 21.53     | 26.10      | 25.43  | 26.53   | 26.94       | 44.79     | 44.00      | 44.53  | 56.59   | 44.05       | 4.14%     |            | 3.31%   |
| MovieLens-1M| 14.60       | 14.90     | 16.45      | 15.41  | 34.85   | 37.45       | 38.69     | 61.25      | 71.97  | 68.65   | 59.77       | 1.91%     |            | 5.79%   |
| Taobao      | 24.88       | 25.29     | 29.11      | 33.28  | 35.19   | 52.17       | 55.71     | 60.13      | 68.12  | 70.31   | 65.49       | 4.27%     |            | 6.79%   |
4.2.3 RQ3. To illustrate the convergence property of DCCL, we conduct the experiments on the Taobao dataset in different device-cloud interaction temporal intervals. Concretely, we specify every 2, 5, 10 days interactions between device and cloud, and respectively trace the performance of each round evaluated on the last click of each user. Figure 5 illustrates the convergence procedure of DCCL in different intervals. According to Figure 5, we observe that frequent interactions achieve much better performance than the infrequent counterparts. We speculate that, as MetaPatch and MoMoDistill could promote each other at every round, the advantages in performance have been continuously strengthened with more frequent interactions. However, the side effect is we have to frequently update the on-device models, which may introduce other uncertain crash risks. Thus, in the real-world scenarios, we still need to make a trade-off between performance and the interaction interval in the cold-start.

4.2.4 Ablation and Case Study. In this section, we present more analysis of DCCL about MoMoDistill and MetaPatch. Then, we will exhibit a case study to illustrate the difference of recommendation results between DCCL and DIN for the long-tailed users.

For the first study, we give the results of MetaPatch and MoMoDistill in one-round DCCL on the Taobao dataset and compare with DIN in Table 3. From the results, we can observe the progressive improvement after DCCL-e and DCCL-m, and DCCL-e acquires more benefit than DCCL-m in terms of the improvement. The revenue behind DCCL-e is MetaPatch customizes a personalized model for each user to improve their recommendation experience once new behavior logs are collected on device, without the delayed update from the centralized cloud server. Regarding DCCL-m, as stated before, the local samples could be scarce and noisy. Therefore, the lengthy on-device personalization will be easy to be trapped by the limited knowledge of each user and result in the local optimal for the recommendation model. The further improvements from DCCL-m confirm the necessity of MoMoDistill to re-calibrate the backbone and the parameter basis. However, if we conduct the experiments without our two modules, the model performance is as DIN, which is not better than both DCCL-e and DCCL-m.

For the second ablation study, we explore the effect of the model patches in different layer junctions. As claimed in previous sections, we insert two patches (1st Junction, 2nd Junction) in the two fully-connected layers respectively after the feature embedding layer.
and one patch (3rd Junction) to the layer before the last softmax transformation layer. In this experiment, we validate their effectiveness by only keep each of them in one-round DCCL. Their results on the Taobao dataset are summarized in Table 4. Compared with the full model in Table 3, we can find that removing the model patch would decrease the performance. And the results suggest that the model patches in the 1st and 2nd junctions are more effective than the higher layer (the 3rd junction). The intuition is that the model patches in low layers more easily adjust the item contributions, which highlights or downweights items according to the user interests, resulting in a more expressive personalization.

To visualize the metapatches learned from on-device personalization, we project their parameter vectors $\{\tilde{\theta}^{(m)}\}$ into the 2-D space via t-SNE as shown in Figure 7. For a better visualization, we assign each point with the color representing the most frequent level-1 category in the local samples to train the metapatch. Note that, it does not mean the true label but we conjecture that the optimization direction of the metapatch is possibly correlated with the sample categories. From Figure 7, we can find that the points belonging to the same color approximately form into a cluster. This might indicate they share similar on-device models to some extent, which inherently keeps the consistency with motivation of learning the global parameter basis $\Theta$ to reduce the parameter space.

To visualize the difference between the centralized cloud model and DCCL, we illustrate one case study based on DIN, DCCL-e and DCCL-m in Figure 6. Specifically, one long-tailed user is chosen to validate their effectiveness. As shown in Figure 6, although the user has clicked many items from the bed categories, DIN has not recommend the expected items related to his history. It is because the bed category is a minority compared to other daily supplies, and the centralized cloud model are optimized bias to this pattern, which is prone to recall other supplies. In comparison, DCCL-e that has adapted to the historical behaviors of this user recommends more relevant items of this category. Nevertheless, it is not perfect to ease the bias effect of the pretrained cloud model and also introduces some bad cases like the last sofa item. In comparison, DCCL-m that refines the global parameter basis further alleviates this issue and recommends all items to the user historical behaviors.

5 CONCLUSION

In this paper, we focus on the general mobile-cloud collaboration scenarios, and propose a Device-Cloud Collaborative Learning framework to explore mutual benefit of the mobile and the cloud modeling. Specifically, we introduce a novel MetaPatch approach to efficiently achieve the model personalization for each device, and simultaneously introduce a MoMoDistill enhance the cloud modeling via the knowledge distillation from the personalized on-device models. Extensive experiments on a range of datasets demonstrate the superiority of DCCL over state-of-the-art methods. However, as an initial exploration about the collaboration between the device and the cloud modeling, more works need to be contributed to on-device intelligence and solving the general challenges about the data sparsity, noise and other computational constraints.

6 ACKNOWLEDGMENTS

This work is supported by National Natural Science Foundation of China under Grant U20A20222.

REFERENCES

[1] Guneet Bedi, Ganesh Kumar Venayagamoorthy, Rajendra Singh, Richard R Brooks, and Kuang-Ching Wang. 2018. Review of Internet of Things (IoT) in
A REPRODUCIBILITY DETAILS

A.1 Dataset Generation

Amazon\(^6\) and Movielens-1M\(^7\) are public datasets containing user-item interactions. We collect Taobao dataset from Mobile Taobao App\(^8\), containing historical behaviors of randomly sampled users in one month. We show the line plot of sorted number of user behaviors in descending order in Figure 8. One can observe the long-tail effect of data distribution, which indicates the necessity of personalized model.

![Figure 8: The Taobao sample number w.r.t. the user index.](image)

We preprocess the datasets to guarantee that users and items have been interacted at least 8 times in Amazon dataset, 20 times in Movielens-1M dataset and 50 times in Taobao dataset.

To train one-round DCCL, each dataset is divided into three disjoint parts according to the log timestamps, including pre-training phase, device-cloud collaborative learning phase and test phase. Pre-training phase is used to learn the initial cloud model \(f\) and globally shared parameter basis \(\Theta\). Then, MetaPatch and MoMoDistill are performed successively on device-cloud collaborative learning phase. Finally the model is evaluated on the test phase dataset. For multi-round DCCL in RQ3, the device-cloud collaborative learning phase is further equally divided into multiple parts, each of which corresponding to one round.

A.2 Parameter Settings

Table 5 shows the hyper-parameter setting of DCCL method for three datasets.

| Dataset | Parameters | Setting |
|---------|------------|---------|
| Amazon | user embedding dimension | 15 |
| | item embedding dimension | 10 |
| | brand embedding dimension | 10 |
| | category embedding dimension | 10 |
| | learning rate | 1e-3 |
| | batch size | 512 |
| | num_attention_layers | 2 |
| | attention dimension(Q,K,V) | 32 |
| | feed_forward_layer_dimension | 32,16 |
| | patch dimension | 32,16,32 |
| | optimizer | Adam |
| | \(\beta\) | 0.01 |
| Movielens-1M | user embedding | 8 |
| | item embedding | 8 |
| | learning rate | 1e-3 |
| | optimizer | Adam |
| | batch size | 256 |
| | encoder layer | 2 |
| | encoder size | 32 |
| | attention dimension(Q,K,V) | 32 |
| | classifier dimension | 32 |
| | patch dimension | 32,16,32 |
| | User Profile Dimension | 8 |
| | \(\beta\) | 0.01 |
| Taobao | user embedding | 8 |
| | item embedding | 8 |
| | learning rate | 1e-3 |
| | optimizer | Adam |
| | batch size | 1024 |
| | encoder layer | 2 |
| | encoder size | 32 |
| | attention dimension(Q,K,V) | 32 |
| | classifier dimension | 32 |
| | patch dimension | 32,16,32 |
| | User Profile Dimension | 8 |
| | \(\beta\) | 0.01 |

\(^6\)https://nijianmo.github.io/amazon/
\(^7\)https://grouplens.org/datasets/movielens/1m/
\(^8\)https://market.m.taobao.com/app/fdilab/download-page/main/index.html

A.3 Experiment Environment

All experiments are conducted on workstations equipped with GPUs (Tesla V100). All baselines and DCCL method are implemented with TensorFlow. Software versions of Python and TensorFlow are 2.7 and 1.12 respectively.