Computing, Performance and Communication Systems (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/cpcs.2022.060107
ISSN 2371-8889 Vol. 6 Num. 1

# *Demand Response Recommendation Scheme with Privacy Protection for Users in Smart Grid*

**Shaomin Zhang[a,*], Xuechun Wang[b] and Baoyi Wang[c]**

*School of Control and Computer Engineering, North China Electric Power University, China*
*a. zhangshaomin@126.com, b. 935089528@qq.com, c. wangbaoyiqj@126.com*
**corresponding author*

***Keywords:*** smart grid,demand response,privacy protection,group recommender system

***Abstract:***In order to adapt to the randomness of new energy power generation, the diversity of residential electricity consumption behavior and the reform of the power trading system, it is necessary to improve the real-time demand response and the information interaction between the power grid and users. This paper firstly applies cluster analysis in the field of demand response to distinguish user groups with different electricity consumption characteristics, and then evaluates the potential of different user groups to participate in demand response, and uses group recommender system strategy to make corresponding recommendations. In addition, considering that a large amount of user historical data needs to be collected in the group recommender system to realize the recommendation for user groups, there may be the risk of leaking user privacy. This paper proposes a privacy protection demand response group based on implicit feedback. The recommendation model realizes the privacy protection of users in the group during the recommendation process.

## 1. Introduction

With the transition from traditional grid to smart grid, renewable energy is gradually emerging, and the power of advanced control and communication technologies is steadily growing. Demand response (DR), as an important part of the smart grid, plays a key role in reducing peak load and incorporating renewable energy into the grid by motivating users to adjust their power demand to supply availability[1].Existing demand response mechanism can usually be divided into price-based demand response and demand response based on incentive [2-3].In this paper, cluster analysis is applied in the field of demand response to distinguish user groups with different electricity consumption characteristics, distinguish user groups with different power characteristics, then evaluate the potential of different user groups to participate in demand response, and recommend the group recommender system strategy. However, considering the large amount of user history data collected in the group recommender system, these data may contain some sensitive information of the users, and in most cases the recommendation system is not credible and has the risk of leaking user privacy. Therefore, it is imperative to protect the privacy of users in the group during the recommendation process.

In recent years, many privacy approaches to conservation have been implemented based on protected user historical data. In the literature [4], a framework called PrivRank was proposed by Yang et al. In PrivRank, both user historical data and activity data are protected by confusion. In the literature [5], Xu et al. have proposed a privacy-preserving online medical service recommendation scheme in an electronic healthcare system. The scheme uses the Paillier encryption algorithm to match each patient's needs with the doctor's information, and can recommend an appropriate doctor to the patient without knowing the exact needs. Literature [6] proposes a MSNs privacy protection group recommender system based on influencing factor I F, which uses fuzzy matrix algorithm to protect the privacy of group users, and can realize the group recommender system with privacy protection even if not every person is online. Literature [7] proposed a personalized privacy protection framework based on trusted client and group sensitive preference protection method, it uses the similarity of user sensitive topics to find similar users, using the group of similar user score to target user score to protect user privacy, however, ignored the risk of privacy leakage in the process of data transmission. In addition, more research results at the present stage are also achieved by adding perturbations to the original group preferences. Literature [8] proposes to perturb the preference profile of users within the group, serialize the perturbbed data and then transmit it. Finally, the recommendation server obtains the available group preference data from the perturbative data according to the relevant data iteration algorithm. Literature [9] proposes a group-based privacy protection method, which protects group users as a middleware for group users. After group users aggregate their personal preference data through the aggregation strategy, they recommend them in a group way, effectively protecting the privacy data of group users.

## 2. Related technology

### 2.1. Group recommender system

Group recommender system emphasizes the aggregation of group member preferences. Due to the large differences between each member of a group, different preferences, and different expectations and desires, conflicts between group members often occur in the process of preference aggregation. During the group decision-making process, to reach agreement, each member accepts or rejects the preferred needs of other members to varying degrees. The final recommendation program needs to be able to minimize conflicts between group members and improve common acceptance among members. In addition, groups are dynamic and complex. Group members will change due to various factors, and users' preferences will also be affected by other group members, which need to dynamically capture real-time changes in groups. This makes making recommendations for groups more difficult.

### 2.2. Implicit feedback

In order to obtain more accurate and appropriate recommendation results, the recommendation system needs three basic components: user, project, and feedback. In terms of feedback, there are two main categories: explicit feedback and implicit feedback. Scoring is like the user to the project adhesive, both in explicit feedback and implicit feedback, score can be manually input by the user, but in the implicit feedback needs to calculate according to the user behavior, defined an implicit scoring function, its output is the calculated user to the demand response plan, can show whether the user i is interested in the demand response plan j. More specifically, it is possible to understand the positive degree of the user i to join the demand response plan j, so that the power companies can use the calculation results to find the demand response plan that the users are more likely to join and recommend to the user accordingly.

### 2.3. Localize Differential Privacy

Differential privacy method is a statistical query method for privacy protection based on statistical data. The aim is that even if all the records in the database change, the statistical results do not change much. However, one problem with centralized differential privacy is that a third party must be trusted. In fact, third parties are not necessarily trustworthy in reality. To address this problem, Local Differential Privacy (LDP) is proposed[10].In an LDP, data is processed locally by the user and then uploaded to the central server; therefore, it provides better privacy protection. The LDP is defined as follows:

Definition 1. A privacy mechanism M satisfies the$\varepsilon$ -localization differential privacy $(\varepsilon \geq 0)$ if, for any two different records $t, t' \in domain(M)$, for any output $t^* \in range(M)$,

$$Pr(M(t) = t^*) \leq e^{\varepsilon} Pr(M(t') = t^*) \quad (1)$$

Localized differential privacy has the same sequential combinability as differential privacy. Sequential composability means that a privacy budget can be allocated in different steps of the algorithm.

Property2.For n privacy protection algorithms$M_i$ ,$1 \leq i \leq n$, if the algorithmM$_i$satisfies$\varepsilon_i$-*LDP* (localized differential privacy), the algorithm $M = \{M_1, \cdots M_n\}$ satisfies$\varepsilon$-*LDP*, where $\varepsilon = \sum_{i=1}^{n} \varepsilon_i$

The common perturbation mechanism of localized differential privacy (LDP) is the stochastic response technique. In the LDP, each user disrupts their data and uploads it to the CPU. Therefore, the data of any two users cannot acquire each other's sensitive information, so there is no concept of global sensitivity. Localized differential privacy (LDP) is a more advanced concept that ensures that users can safely share private data.

## 3. Scheme Design

### 3.1. Demand Response Group Recommender System

$IR_{i,j}$This section describes the proposed demand response group recommender system model. We assume that there is a demand response recommender system consisting of m types of demand response strategy and n users, and we express the user *i* scoring demand response policy *j* as, if user *i* does not score demand response policy *j*,$IR_{i,j}$=*null*.The demand response recommendation system has many groups composed of different users, and this paper represents a typical group with g users as *G*.

In the demand response group recommender system , first to collect the historical data of the user implicit feedback score $IR_{i,j}$, to predict the demand response strategy without the user implicit feedback score $IR_i^*$, and then aggregate the implicit feedback score $IR_{i,j}^*$ of all users i for demand response strategy *j* in each group *G*, in order to further obtain the group preferences$GP_{i,j}$ for the demand response strategy $j$.

## 3.2. Privacy Protection Group Recommender System Model Based on Implicit Feedback

### 3.2.1. Implicit Feedback Score Calculation

For the smart grid demand response strategy release platform, The most important thing is that electricity users can really actively join in the demand response plan and have a high satisfaction, In this way, the power companies can realize the macro-control of the power load, Improve the operation stability and reliability of the power grid, At the same time, users can also get the corresponding revenue from it, Therefore, this paper selects the four behaviors of the user who are actually added to the demand response plan and have the greatest impact of satisfaction to analyze and set the corresponding weight, The specific analysis settings are described in the following Table1:

Table 1:Behavioral event weight setting.

| Behavioral events | Influence degree | weight |
|---|---|---|
| partake | highest | $w_1$=1.2 |
| collect | Times high | $w_2$=1 |
| communicate | secondary | $w_3$=0.8 |
| look over | lowest | $w_4$=0.6 |

Defining an implicit scoring function, whose output is a calculated implicit user score of the demand response plan, is able to show whether the user i is interested in the demand response plan j.More specifically, it can understand the positive of user i to join the demand response plan j, so that the power company can use the calculation results to find the demand response plan that users are more likely to join and thus recommend to the user. The implicit scoring function is as follows:

$$IR_{i,j} = (w_1 \times e_1) + (w_2 \times e_2) + \cdots + (w_n \times e_n) \qquad (2)$$

Among them, the user i implicitly scores $IR_{i,j}$the demand response plan $j$,$e_1, e_2 \cdots e_n$which refers to the number of behavioral events, and $w_1, w_2 \cdots w_n$is the weight set according to the previous analysis.

### 3.2.2. Privacy Protection Group Recommender System Algorithm Model

This paper designs a privacy protection group recommender system scheme. Figure 1 further illustrates our basic idea, which can be divided into two parts. Steps ①, ②, and ③ show the personalized recommendations section. Users interact with the recommendation server of the power company under the localized differential privacy, and train the personalized recommendation model through the matrix decomposition mechanism, which does not disclose the privacy, and then generate the personalized recommendation results. After the personalized recommendation section, each user gets their own preference. Steps ④ and ⑤ represent the preference aggregation part. When recommended to a group, the group performs the Privacy-preserving Preference

Aggregation(PPPA) algorithm. Personal preferences of each group member were passed perturbed within the group before being sent to the server. In this case, the true preferences of the group members are hidden during random transmission and are not exposed to others. After receiving the perturbation preferences of all members, the server uses the median aggregation strategy to obtain the final group preferences.

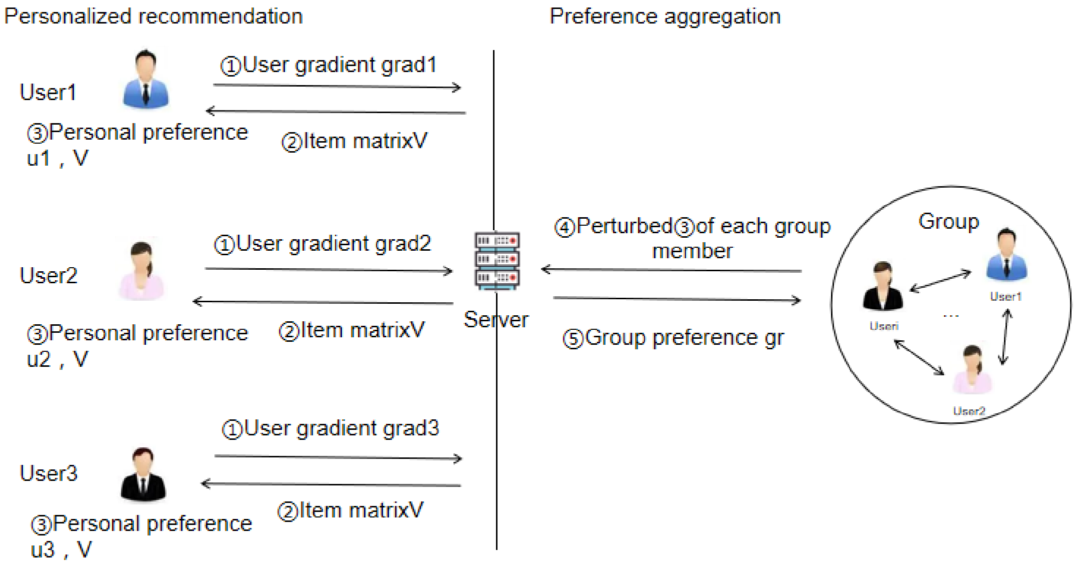

Figure 1:Framework diagram of the privacy protection group recommender system scheme.

## 4. Results and Discussion

The recommendation model and peaking demand response are combined to obtain potential users and recommend relevant information.As shown in Figure 2.It can be seen that the recommendation model can recommend alternative power consumption scheme for users to help users participate in demand response and achieve the purpose of peak reduction.

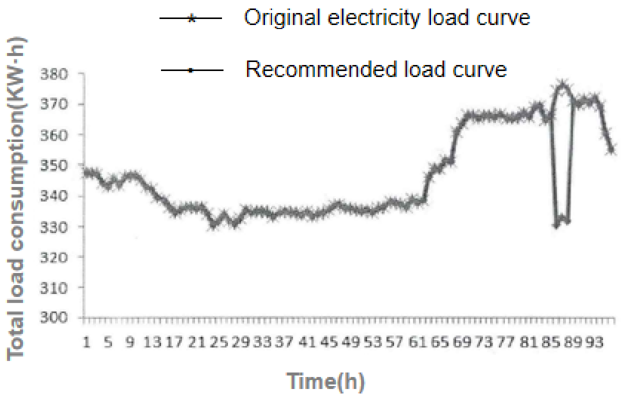

Figure 2: User original load curve and the load curve under the demand response model.

## 5. Conclusion

In order to adapt to the randomness of new energy power generation, the diversity of residential electricity consumption behavior and the reform of the power trading system, it is necessary to improve the real-time demand response and the information interaction between the power grid and users. This paper firstly applies cluster analysis in the field of demand response to distinguish user groups with different electricity consumption characteristics, and then evaluates the potential of different user groups to participate in demand response, and uses group recommender system strategy to make corresponding recommendations. In the recommendation system, a large amount of user historical data needs to be collected to realize the recommendation for user groups, and there is a risk of leaking user privacy. This paper proposes a privacy-preserving demand-response group recommender system model based on implicit feedback, which is implemented in the recommendation process. Privacy protection for users in the group.

## References

*[1]Bhattarai B P ,M Lévesque, Bak-Jensen B ,et al. Design and Co-simulation of Hierarchical Architecture for Demand Response Control and Coordination[J].IEEE Transactions on Industrial Informatics, 2017, 13(4):1806-1816.*

*[2]B.Sharma, N.Gupta, K.R.Niazi, A.Swarnkar and S.Vashisth. Demand Response in the Global Arena: Challenges and Future Trends[J].2019 8th International Conference on Power Systems (ICPS), 2019, pp.1-5.*

*[3]D Li, Sun H , Chiu W Y , et al.Multiobjective Optimization for Demand Side Management in Smart Grid[J].IEEE Transactions on Industrial Informatics, 2018:1-1.*

*[4]Dara S , Chowdary C R , Kumar C .A survey on group recommender systems[J].Journal of Intelligent Information Systems, 2019.*

*[5]Choudhary N,Bharadwaj K K .Preference-Oriented Group Recommender System: SIGMA 2018, Volume 1[M].2019.*

*[6]D.Yang, B.Qu, and P.Cudré-Mauroux. Privacy-preserving social media data publishing for personalized ranking-based recommendation[J].IEEE Transactions on Knowledge and Data Engineering, vol.31, no.3, pp.507-520, 2019.*

*[7]C.Xu, J.Wang, L.Zhu, C.Zhang, and K.Sharif. Ppmr: a privacy-preserving online medical service recommendation scheme in ehealthcare system[J]. IEEE Internet of Things Journal, vol.6, no.3, pp.5665-5673, 2019.*

*[8]He Y,Zhang K,Wang H,et al.Impact factor-based group recommender system scheme with privacy preservation in MSNs[C] IEEE International Conference on Communications ( ICC),2017:1-6.*

*[9]Wang Hai-yan,Lu Jin-xiang.Personalized privacy protection method for group recommendation[J].Journal on Communications, 2019,40-(9) :106-115.*

*[10]H.Shin, S.Kim, J.Shin, and X.Xiao. Privacy enhanced matrix factorization for recommendation with local differential privacy[J].IEEE Transactions on Knowledge and Data Engineering, vol.30, no.9, pp.1770-1782, 2018.*