Finding Shilling Attack in Recommender System based on Dynamic Feature Selection

Gaofeng Cao, Huan Zhang, Yuyou Fan, Li Kuang*
School of software
Central South University
Changsha, China
{caogaofeng, 3901140112, hatsune, kuangli} @csu.edu.cn

***Abstract*—Recommender system is widely used as an important tool in various fields for effectively dealing with information overload, and collaborative filtering algorithm plays a vital role in the system. However, such system is highly vulnerable to malicious attacks, especially shilling attack because of data openness and independence. Therefore, detecting shilling attack has become an important issue to ensure the security of recommender system. Most of existing methods for detecting shilling attack are based on rating classification features and their limitation is that they are easily to be interfered by obfuscation techniques. Moreover, traditional detection algorithms can not handle multiple types of shilling attack flexibly. In order to solve these problems, in this paper, we propose an outlier degree shilling attack detection algorithm based on dynamic feature selection. By considering the differences of user choosing items and taking user popularity as a detection metric, as well as using information entropy to select detection metrics dynamically, a variety of shilling attack models can be dealt with flexibly. Experiments show that the algorithm has stronger detection performance and interference immunity in shilling attack detection.**

Keyword-Recommender System; Malicious Attacks; Detection Algorithm; User Selection; Detection Metrics

I. INTRODUCTION

As an information filtering technology, recommender system plays a role with importance increasing and has become an effective way to deal with information overload. Typical recommendation approaches, including content-based recommendation [1], collaborative filtering recommendation [2], knowledge-based recommendation [3], hybrid recommendation [4], have been widely used in large e-commerce websites such as Taobao, Amazon, Google News, etc. A good recommender system can provide users with relevant interesting items and thus bring more economic benefits to merchants. Not only has now research on recommender system become a popular research field in academia, but also many companies, such as Netflix and Alibaba, have set up their own research teams in order to improve the accuracy of their own recommender system.

At present, recommender system is faced with many problems such as data sparse [7-8], poor scalability, cold-start [9], security [10], etc., and the security will be the focus of this paper. The openness can reflect user's preference through rating, which provides data foundation for recommendation. However, because of the openness some junk information could be inserted into the system by malicious users and thus influence system's behaviors, like, in recent years, popular network part-time jobs "brush credit" and "brush praise". This phenomenon is called aggression behavior of malicious user [11], profile injection attack [12] or shilling attack [13]. Facing with shilling attack, traditional collaborative filtering recommender system shows their vulnerability that is attackers can change the predictions of some target items when the system has no protection. The inserted junk information causes a decline in accuracy and reliability of the system.

Detecting shilling attack can be regarded as a binary classification problem between normal users and attackers. When it comes to classifying attackers, most current classification features are relative to user ratings, and the corresponding classification features, which can differentiate normal users and fake users, could be found by detecting how they rate certain items. However, there are some problems in classification features based on ratings: (1) Misjudging a user as an attacker easily; (2) When attacker's ratings are camouflaged and not the same as the normal shilling attack models, it will result in low detection accuracy, and the current detection metrics are useless for various changes of shilling attack models.

In order to solve above problem, this paper starts from dealing with the user's selection of rating items. Since normal user has certain needs to choose items -- item popularity is generally follow long tail effects, thus we can use the user's popularity [21] as a metric to detect the shilling attack. And by using information entropy effective detection metrics can be selected dynamically; the most effective metric helps to calculate user's outlier degree [22] and then we can detect attackers. Taking detection mistakes into account, we propose a new method which can get the intent and target items of shilling attack through analyzing suspected users, and remove abnormal users, users always give good reviews or bad reviews, based on the information we get.

The main contributions of this paper are as follows: (1) Combining user's popularity with conventional classification features based on ratings as detection metrics to improve the accuracy of shilling attack detection. (2) Using information entropy to dynamically select metrics to adapt a flexibility in

DOI reference number: 10.18293/SEKE2018-134

coping with various attack models. (3) Using metrics selected dynamically to calculate user's outlier degree and detect attacker.

The rest of this paper is structured as follows: In Section 2 we introduce the research background. In Section 3 we propose an outlier degree shilling attack algorithm based on dynamic feature selection, and then we introduce the experiment and analyze experimental results in Section 4. Finally we conclude with a summary and future work in Section 5.

II. BACKGROUND

Due to that the accuracy of collaborative filtering recommendation depend on a large amount of user data and the open nature of recommender system, so that attackers can inject fake profiles into the system with a little cost and maximize their interests by affecting the prediction results with the attack profiles, . Shilling attack contains two intents: (1) increase the recommendation frequency of target items, namely push attack; (2) reduce the recommendation frequency of target items, namely nuke attack.

The research on shilling attack mainly includes attack detection and robust recommendation algorithm of defense. This paper is to analyze algorithms of shilling attack detection, and there are two main categories: based on supervised learning and unsupervised learning.

Research on shilling attack detection has been fully developed. Chirita et al. [14] proposed using statistical metrics, such as the degree of similarity with top neighbors, rating deviation from mean agreement (RDMA), to distinguish genuine profiles and attack profiles. This method performs very well in the detection on the attack profiles of high density filling but not great in low density filling. Mehta et al. [15-16] believe that the information in recommender system mainly depends on genuine profiles and they used principal component analysis technology to filter attack profiles. Then, they proposed a PCA-Var Select detection that can effectively detect multiple attack types. Li Cong et al. [17] constructed a corresponding object function for genetic optimization through qualifying the group effect of attack profiles and combined it with Bayesian inference in the process of genetic optimization, which is an new unsupervised algorithm for detecting shilling attack — IBIGDA. To some extent, IBIGDA reduces the dependence on prior knowledge, but it still assumes that the number of attack profiles is less than genuine profiles and obtain higher precision with sacrificing recall. Chung et al. [18] proposed a detection algorithm based on Beta distribution, namely Beta-Protection, to detect attack profiles. Beta-Protection has better detection performance when it meets certain conditions: the number of ratings is extremely small, the rating value is extremely small or extremely large.

According to the existing researches, the existing unsupervised algorithms for detecting shilling attack only rely on one solid feature and take it as a detection metric of attack profiles. This kind of single detection metric is difficult to ensure the accuracy under different attack scenarios and its inflexibility causes problems when nre attack strategies appear. .

In order to improve accuracy and interference immunity of the detection algorithm, first we use rating metrics and popularity-based metrics in the literature [19,23] as a feature candidate set of detecting shilling attack; the second step uses information entropy to dynamically select five features; the third step is to use selected features to calculate user's outlier degree and find out suspected user; the fourth step is to judge the user regarded as a attacker by mistake, analyze suspected users and get the intent and target items of shilling attack. After these steps, we can remove users who do not meet the intent and target items from suspected users so as to determine real attacker. we will illustrate the feasibility and superiority of this algorithm through experimental results.

III. AN OUTLIER DEGREE SHILLING ATTACK DETECTION ALGORITHM BASED ON DYNAMIC FEATURE SELECTION

A. Definition

Item popularity: the rating frequency of item in the recommender system. d_i refers to the item popularity of item i.

User popularity vector: a vector of the item popularity and the item has been rated by user.

$$V_u = \left(d_1,\ d_2,\ \cdots,\ d_k\right) \tag{1}$$

Each element in user popularity vector is a user's item popularity, and k refers to item k rated by user.

Mean of user popularity degree(MUPD): the mean of elements in user popularity vector. The specific formula as follow:

$$MUPD_u = \frac{1}{n}\sum_{i=1}^{n} d_i \tag{2}$$

d_i refers to the popularity of item i in user popularity vector.

Range of user popularity degree(RUPD): the difference between the maximum and minumum of item popularity in user popularity vector. The specific formula as follow:

$$RUPD_u = d_{max} - d_{min} \tag{3}$$

d_{max} and d_{min} refer to the maximum of item popularity and the minimum of item popularity in user popularity vector.

Attack Profiles: In general, each attacker's rating vector consists of four parts: a set of selected items $I_S(I_S \subset I)$, a set of filler items $I_F(I_F \subset I)$, a set of target items $I_T\left(\{I_T\} \subset I\right)$ and a set of unrated items $I_\phi(I_\phi = I - (I_S \cup I_F \cup \{I_T\}))$.

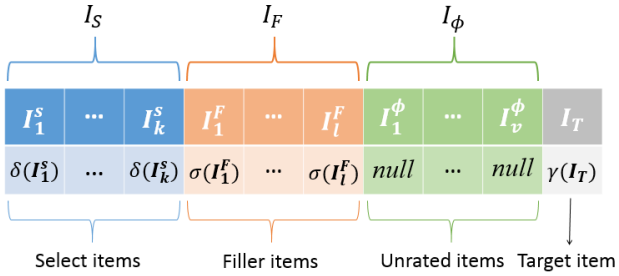

Figure 1. Attack profile vector structure

Attack size: the ratio of the number of attack profiles

injected into the system to the total number of user profiles.

Filler size: the ratio of the number of items reted by users to the total items in the system.

Attack model: $M = (\chi,\ \delta,\ \sigma,\ \gamma)$, χ refers to selection function,

$$\chi\left(I,\ U,\ \Phi,\ I_T\right) = < I_S,\ I_F,\ I_\phi,\ I_T >$$

The function has four parameters: item set(I), user set(U), target item set(I_T), and a set of other parameters(Φ).

Random attacks: rate a subset of items randomly around the overall mean vote.

Average attacks: rate a subset of items randomly around the mean vote of every item.

Bandwagon attacks: rate a subset of items randomly around the overall mean vote, and some highly popular items are rated with the maximum vote.

Segment attacks: rate target items highest (or lowest) score, the most relevant items with the target items highest (or lowest) score, and items filled lowest (or highest) score.

B. Construction of Detection Features of shilling Attacks

Based on the user popularity indicators introduced above, this paper cites the 10 user rating indicators defined in the literature [19,23], including RDMA(Rating Deviation from Mean Agreement)、WDA(Weighted Degree of Agreement)、WDMA(Weighted Deviation from Mean Agreement)、ADegSim(Average Degree of Similarity with Top Neighbors)、LengthVar(Length Variance)、FMTD(Filler Mean Target Difference)、FMV(FillerMeanVariance)、MeanVar(MeanVariance)、TMF(Target Model Focus)、SDUR (Standard Deviation in User 's Ratings)、DAOU (Degree of Agreement the Other Users).

The essence of the attack detection problem is a two-class problem, namely classifying normal users and attackers in the user dataset. However, the classifier with the machine learning method have poor flexibility, and they can only work on a particular attack type. And if all the feature attributes are selected to implement the training machine learning model, the classifier will be too complex, which will seriously affect the efficiency of the classifier.

Therefore, in order to improve the flexibility of classifier, especially in the case of dealing with unknown types of attack, this paper proposes a method to dynamically select a set of feature subsets according to the training set, and then perform the attack detection based on this set of feature subsets.

The main idea of the dynamic feature selection method based on information gain is: First, calculate the index values of each feature of each user. Then, calculate the information gain of each feature by dividing the normal user and the attack user in the training set. Finally select the feature with the greatest information gain.

The feature construction algorithm is as follows:

Input: Training Set D_t,

Output: Best classification feature subset F′

1：Calculate the popular features of each user u in the training set D_t：

$$F_1 = \{MUPD,\quad RUPD,\ QUPD\}$$

2: Calculate the 10 indicators proposed in the literature[19,23] of each user u in the training set D_t:

$$F_1 = \{f_1,\quad f_2,\ \ldots,\ f_{10}\}$$

3：Calculate the proportion of attacker feature values $p_{i,s}$, S is attack user set, U is all user set：

$$p_{i,s} = \frac{\sum_{k=1}^{|S|} \varphi_{f_i}(P_k)}{\sum_{j=1}^{|U|} \varphi_{f_i}(P_j)}$$

Here, P_u denotes the user profile of user u, and $\varphi_{f_i}(*)$ denotes calculate the feature value of f_i.

4: Calculate the proportion of normal user feature values $p_{i,r}$：

$$p_{i,r} = 1 - p_{i,s}$$

5: Calculate the information entropy H_i of the feature index f_i:

$$H_i = -p_{i,r} * log(p_{i,r}) - p_{i,s} * \log(p_{i,s})$$

6: Compute empirical entropy of Training Set D_t:

$$H(D_t) = -\frac{|S|}{|D_t|} log \frac{|S|}{|D_t|} - \frac{|N|}{|D_t|} log \frac{|N|}{|D_t|}$$

Here, N denotes normal user set

7: calculate empirical gain $H(D_t, f_i)$:

$$H(D_t, f_i) = H(D_t) - H_i$$

8: sort the features f_i in descending based on the values of information gain and select top-k features：$F_2 = \{f_1',\ \ldots,\ f_k'\}$:

9: Build a feature subset:

$$F' = F_1 + F_2$$

C. An Outlier Degree shilling Attack User Detection Algorithm Base on Feature Vector

we get a subset of features through dynamic feature selection algorithm based on information entropy. In order to detect the attack user, this paper proposes an outlier degree detection algorithm based on feature vectors. According to the subset of features, we can get the feature vector of each user. Moreover, the features in the feature vectors are the attributes that have high classification ability for the attackers in the dataset. There is a difference between the feature profiles of normal users and attackers.Therefore, we can use user's feature vectors to determine whether he is an attacker.In this paper we use the Euclidean distance to measure the outlier degrees of the user's feature vectors，then mark user with outlier degree as a suspected user.

When it comes to the detection of attacker, we can find out attacker who deviates from the normal user's profile by his outlier degree. The specific formula of calculating outlier degree is as follow :

$$d(u) = \sum_{v \in U, v \neq u} \left\| V_a - V_b \right\|$$

$$= \sum_{b\in U, b\neq a} \left(\sum_{i=1}^{n} (\mathrm{V}_{a,i} - \mathrm{V}_{b,i})^2\right)^{\frac{1}{2}} \quad (4)$$

V_a refers to the feature vector of user a, and V_b refers to the feature vector of user b. a user whose outlier degree exceeds a certain threshold can be marked as a suspected user.

Input: The dataset of user ratings
Output: The set of attackers

For a in all U do:
Cconstruct user's feature vector.
$\mathrm{V}_a = (\mathrm{V}_{a,1}, \mathrm{V}_{a,2}, \ldots, \mathrm{V}_{a,\mathrm{n}})$
end for
For a in all U do:
Calculate user's outlier degree:
$\mathrm{outlierD}_a = \sum_{b\in U, b\neq a} \left(\sum_{i=1}^{n} (\mathrm{V}_{a,i} - \mathrm{V}_{b,i})^2\right)^{\frac{1}{2}}$
End for
List users in descending order by their outlier degree;
Select 20% users with the highest outlier degree to form suspected user set S_h;

IV. EXPERIMENT

In this section, we introduce the dataset, the setup and objectives of the experiments, and analyze the experimental results.

A. Data description

We use the MovieLens 100K dataset in experiments, which is a popular dataset used by researchers and developers in the field of recommendation. The dataset contains ratings from 943 users on 1,682 movies. Furthermore, we write spider program to get the required data about the introduction information of movies (for item similarity) and the communication messages between users (for trust relationship). The dataset contains 19194 communication messages between 4932 users. The rating records are integers from 1 to 5.

In order to verify the accuracy of the recommendation algorithm, we use 5-fold cross validation. The attacking users in the experimental data set are generated through simulation experiments. According to the principle of the attacking attack model, artificially generated attacking user data is generated in the original data set.

B. Evaluation Metric

In our experiments, we first use the following evaluation indicators to determine the parameters of our methods, and then we use the indicators to analyze and compare our proposed methods with other two in literature.

In the experiment, two types of user profiles will be included, one is the real user profile and the other is the profile of attack user. Detect shilling attack users can be seen as a two-class problem. Therefore, the test results can be represented by the confusion matrix shown in Table 1. Negative represents the real user profile, and Positive represents the profile of the attacked user.

TABLE I. CONFUSION MATRIX TABLE OF CLASSIFICATION RESULTS OF SUPPORT ATTACK DETECTION

The actual situation	**The Predicted situation**	
	Real user	*Attack user*
Real user	True Negative(TN)	False Positive(FP)
Attack user	False Negative(FN)	True Positive(TP)

This paper, we use the accuracy to evaluate the performance of shilling attack detection algorithm and accuracy formula is defined as following:

$$\text{Accuracy} = \frac{TP + TN}{TN + FP + TP + FN}$$

C. Feasibility analysis based on item popularity characteristics

1) Analysis MUPD

MUPD can effectively partition the type of attack that there is no select item in the user attack profile vector, including the random attack model and the average attack model. Because the filled item is selected randomly in these two types of attacks, the probability of each item selected come to be equal, and the distribution of popularity of the item belongs to the long tail distribution. Therefore, the mean of user popularity vector will be very low in the general appearance of the attack users generated by the random attack model and the average attack model. As shown in Figure 2.

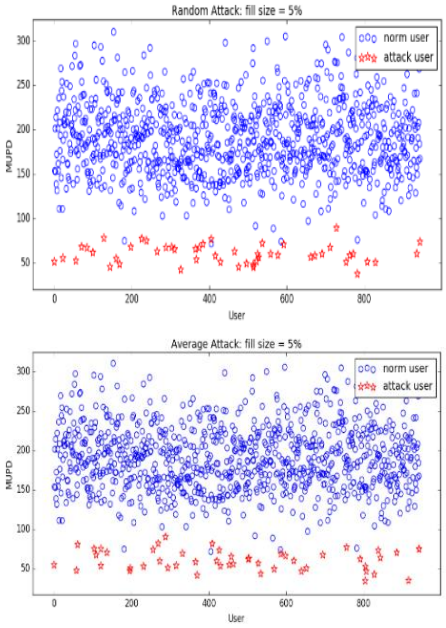

Figure 2. Distinguish the attack Model of Non-select items by MUPD

2) Analysis RUPD

RUPD can effectively distinguish the popular attack model. According to the principle of popular attack model, there exist one most popular items in the attack profile. Therefore, the popularity of the attack user profile will have a great range. In

this case, MUPD can distinguish the popular attack model Invalid, as shown in Figure 3 and Figure 4:

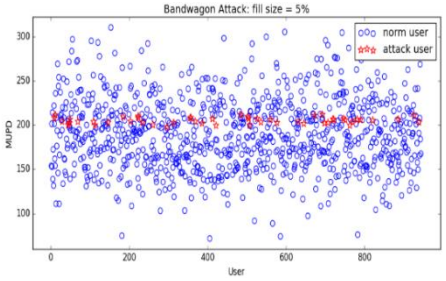

Figure 3. Identification of popular attack users using MUPD

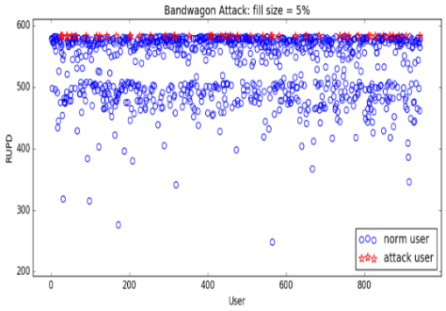

Figure 4. Identify popular attacking users using RUPD

D. *Experimental parameter settings*

TABLE II. PARAMETER SETTINGS

S_h	I_h	Filler size	Attack size	F′ size
20%	3	5%,10%,15%	3%,5%,10%	6

As shown in the table 2, the suspect attack user set is set to top 20%. Because of taking the cost of attack into account , the attack size won't exceed 20%. The suspect item set is set to 3, that is, the three items with the highest rating deviation are selected as the suspected attacked item set. Filler size is set to 5% or 10% or 15% respectively and Attack size is set to 3% or 5% or 10% respectively. size of Feature subset F′ is 6, because according to the existing shilling attack detection algorithm, selecting three appropriate rating-based metrics can provide good detection results, so here we choose three rating-based metrics that have best detect ability, and then combine three popularity-based metrics as the result of feature subset.

E. *Verification the Performance of shilling Attack Detection Algorithm Based on Dynamic Feature Selection and Outlier*

In order to verify the performance of our method, experiment compares with the classical feature-based select method PCA-VarSelect algorithm proposed by Mehta et al. In order to distinguish this algorithm from the comparison algorithm, our method named outlier-based method, and the detection algorithm proposed by Mehta is named pca-based method.

TABLE III. ACCURACY OF RANDOM ATTACKS DETECTION RESULTS

Attack size \ Filler size		Random attacks		
		5%	10%	15%
3%	outlier-Based	0.9802	0.9723	0.9910
	pca-Based	0.9246	0.9302	0.9372
5%	outlier-Based	0.9846	0.9819	0.9921
	pca-Based	0.9060	0.9390	0.9783
10%	outlier-Based	0.9967	0.9882	0.9977
	pca-Based	0.9811	0.9607	0.9513

TABLE IV. ACCURACY OF AVERAGE ATTACKS DETECTION RESULTS

Attack size \ Filler size		Average attacks		
		5%	10%	15%
3%	outlier-Based	0.9853	0.9936	0.9834
	pca-Based	0.9353	0.9464	0.9177
5%	outlier-Based	0.9909	0.9845	0.9857
	pca-Based	0.9372	0.9628	0.9699
10%	outlier-Based	0.9874	0.9748	0.9850
	pca-Based	0.9528	0.9659	0.9408

As shown in Table 2 and Table 3, the outlier-based method and the pca-based method have high accuracy in the detection results of the random attacks and the average attacks. And even if the filler size and attack size is small, both methods can identify the attack user and the accuracy rate is more than 90%.However, the accuracy of outlier-based method proposed in this paper has a slightly higher than the pca-based method. Considering the combination of any attack size and filler size, the average accuracy of pac-based method is 0.9456, while outlier-based method is 0.9864.Though there are a improvement in 5%, but when the filler size is fixed, outlier-based method become relatively stable as attack size increasing, while a accuracy increased in pac-based method. What causes this phenomenon is that pac-based method, when attacker size increases, can do better in identifying the feature between attackers and normal users, but outlier-based can identify the feature very well even if attacker size is small.

TABLE V. ACCURACY OF *BANDWAGON ATTACKS* DETECTION RESULTS

Attack size \ Filler size（selected size 5%）		*Bandwagon attacks*		
		5%	10%	15%
3%	outlier-Based	0.9937	0.9781	0.9970
	pca-Based	0.7033	0.7226	0.7759
5%	outlier-Based	0.9887	0.9758	0.9869
	pca-Based	0.8517	0.7639	0.8876
10%	outlier-Based	0.99546	0.9658	0.9841
	pca-Based	0.8446	0.8677	0.8701

As shown in Table 4, the pca-Based method has a lower accuracy when the attack size and filler size is smaller. Because the amount of positive and negative sample data in the data set, the effect of the pca-based method only using the user rating index is not good. For small-scale attack, outlier-based methods can be well identified. Moreover, outlier-based methods are significantly more efficient than pca-based methods for Bandwagon attack model and segmentation attack

models, which proves that the proposed attack detection method has a good efficiency. For combination of any attack size and filler size, the average accuracy of pac-based method is 0.9837 and outlier-based method is 0.8905, which there has a improvement in 22%. We conclude that when user popularity is added, outlier-based method can identify a more complex attack model, while pac-based method has no such good performance.

V. CONCLUSION AND FUTURE WORK

This paper combines traditional score-based attack detection indicators with user popularity-based attack detection indicators to build vectors based on user popularity and average indicators with utilizing feature subsets selected by PCA based on user's average indicators; Vectors are used to calculate the degree of user's outliers, and the degree helps us mark the outlier users as suspects. Considering odd-looking users in system, we can find out the real attacker by analyzing the score of suspects, judging the intent of attacker and removing the users who dissatisfy the intent.

Through comparing experiment results, we can see the outlier-based attack detection algorithm based on dynamic feature selection has high accuracy and can be adapted to the different attack models flexibly in the system.

In the future work we will: (1) Finding the attack detection features from other perspectives, (2) Integrating existing feature indicators more effectively to find out more feature indicators, (3) building the attack defense from two levels by combining the attack detection method and attack defense robustness algorithm

ACKNOWLEDGMENT

The research is supported by "National Natural Science Foundation of China" (No. 61772560) and the scientific research "Innovation Project for Graduate Students in Central South University" (No. 1053320170318).

REFERENCES

[1] Cerqueira, Thaciana, L. Marinho, and F. Ramalho. "A Content-Based Approach for Recommending UML Sequence Diagrams." SEKE 2016.

[2] J. Ben Schafer, Dan Frankowski, Jon Herlocker, et al. Collaborative Filtering Recommender Systems[J]. Acm Transactions on Information Systems, 2007, 22(1):5-53.

[3] Felfernig A, Gula B, Leitner G, et al. Persuasion in Knowledge-Based Recommendation[C]// International Conference on Persuasive Technology. Springer-Verlag, 2008:71-82.

[4] Zhang, Chi, G. Chen, and H. M. Wang. "Recommendation Model Based on Blending Recommendation Technology." Computer Engineering36.22(2010):248-250.

[5] Bartolini I, Zhang Z, Papadias D. Collaborative filtering with personalized skylines[J]. Knowledge and Data Engineering, IEEE Transactions on, 2011, 23(2): 190-203.

[6] Barragáns-Martínez B, Costa-Montenegro E, Juncal-Martínez J. Developing a recommender system in a consumer electronic device[J]. Expert Systems with Applications, 2015, 42(9):4216-4228.

[7] Yan, W. U., et al. "Algorithm for Sparse Problem in Collaborative Filtering." Application Research of Computers 24.6(2007):94-97.

[8] CHEN Zong-yan,Yan jun. "Collaborative Filtering Recommendation Algorithm Based on Sparse Data Pre-processing". The computer technology and development, 2016, 26(7):59-64.

[9] Yang, Yu, et al. "Cold-Start Developer Recommendation in Software Crowdsourcing: A Topic Sampling Approach." The, International Conference on Software Engineering and Knowledge Engineering2017:376-381.

[10] Zhang, Fu Guo, and X. U. Sheng-Hua. "Review of key security threats and countermeasures in recommender systems." Application Research of Computers 25.3(2008):656-659.

[11] Xiang, X. U. "Analysis of shilling attacks on SVD-based collaborative filtering algorithm." Computer Engineering & Applications 45.20(2009):92-95.

[12] Huang, Sheng, M. Shang, and S. Cai. "A Hybrid Decision Approach to Detect Profile Injection Attacks in Collaborative Recommender Systems." International Symposium on Methodologies for Intelligent SystemsSpringer, Berlin, Heidelberg, 2012:377-386.

[13] Zhi-Ang, W. U., et al. "Shilling Attack Detection Based on Feature Selection for Recommendation Systems." Acta Electronica Sinica40.8(2012):1687-1693.

[14] Chirita P A, Nejdl W, Zamfir C. Preventing Shilling Attacks in Online Recommender Systems[C]//Proceedings of the 7th Annual ACM International Workshop on Web Information and Data Management. New York: ACM, 2005: 67-74.

[15] Mehta B. Unsupervised Shilling Detection for Collaborative Filtering[C]//Proceedings of the 22nd National Conference on Artificial intelligence. Menlo Park, London: AAAI, 2007: 1402.

[16] Mehta B, Hofmann T, Fankhauser P. Lies and Propaganda: Detecting Spam Users in Collaborative Filtering[C]//Proceedings of the 12th International Conference on Intelligent User Interfaces. New York: ACM, 2007: 14-21.

[17] Li, Cong, Z. G. Luo, and J. L. Shi. "An Unsupervised Algorithm for Detecting Shilling Attacks on Recommender Systems." Acta Automatica Sinica 37.2(2011):160-167.

[18] Chung C Y, Hsu P Y, Huang S H. βP: A Novel Approach to Filter out Malicious Rating Profiles from Recommender Systems[J]. Decision Support Systems, 2013, 55(1): 314-325.

[19] Burke R, Mobasher B, Williams C, et al. Classification features for attack detection in collaborative recommender systems[C]// ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2006:542-547.

[20] Wang J K, JIANG Y C, Sun J S, SUN C H." Item-based Collaborative Filtering Algorithm Integrating User Activity and Item Popularity". Computer science. Vol. 43. No.12.pp. 158-162.

[21] Li, W. T., et al. "An shilling attack detection algorithm based on popularity degree features." Zidonghua Xuebao/acta Automatica Sinica41.9(2011):1563-1576.

[22] Chengshu, L. "SHILLING ATTACK DETECTION BASED ON FEATURE SELECTION AND SVM." Computer Applications & Software (2015).

[23] Williams C A, Research Advisor, Mobasher B. Thesis: Profile Injection Attack Detection for Securing Collaborative Recommender Systems[J]. Service Oriented Computing & Applications, 2012, 1(3):157-170.