Applied Mechanics and Materials Vol. 610 (2014) pp 717-721
Online available since 2014/Aug/11 at www.scientific.net

doi:10.4028/www.scientific.net/AMM.610.717

Robust Analysis on a Privacy Preserving Recommendation Algorithm under the KNN Attack

Yan Gao, Jingbo Xia*, Jingjing Ji, Ling Ma

College of Science, Huazhong Agricultural University, Wuhan, China. P. R.

*xiajingbo.math@gmail.com

Keywords: Privacy-Preserving, Collaborative Filtering (CF), A KNN Attack, Accuracy, Recommendation System.

Abstract: Among algorithms in recommendation system, Collaborative Filtering (CF) is a popular one. However, the CF methods can't guarantee the safety of the user rating data which cause private preserving issue. In general, there are four kinds of methods to solve private preserving: Perturbation, randomization, swapping and encryption. In this paper, we mimic algorithms which attack the privacy-preserving methods with randomized perturbation techniques. After leaking part of rating history of a customer, we can infer this customer's other rating history. At the end, we propose an algorithm to enhance the system so as to avoid being attacked.

Introduction

Recently, with the rapid development of science and computer technology, recommender systems are ubiquitous on e-commerce websites. People can get great convenience in sharing information and resources. In the meanwhile, it's easy to be stuck in the information overload. The research on personalized recommendation is coming into being in time.

Typically, the recommender system is based on the recommender algorithm. There are four major types of algorithms: content-based recommendation, collaborative filtering (CF) recommendation, recommendation based on network structure and graph theory and hybrid recommendation [1], CF is the earliest and most successful technology applied to the recommendation system. It can be further categorized into the neighborhood-based methods and model-based methods [2]. On the paper, we mainly discuss the first one. Moreover, the neighborhood-based methods are generally performed by the k nearest neighbor rule (KNN) [3].

The task of collaborative filtering recommendation system based on KNN can be abstractly described as follows [4]: Considering a matrix represents a user's revealed or stated preference for the whole items. Through the preference of the users, we can predict a user's preference on some items by means of his k nearest neighbors' preference, but it arise a series of security problems.

It has shown that continual observation of recommendation with some background information makes it possible to infer the individual's rating or even transaction history, especially for the neighbor-based methods [4]. This is usually called as a KNN attack, in which an adversary can infer the rating history of an active user by creating fake neighbors based on background information [3].

To overcome this challenge, researchers propose different privacy-preserving schemes to produce prediction without jeopardizing privacy [6]. Some mask users' confidential information data before submitting them to the data holder by disguising the rated items and the ratings [7]. In a certain sense, even it can improve scalability of user-item matrix, but when a user, a sunset of his transaction history is available to the attacker, an inference attack can be successful if it enables the attacker to learn items which are not part of the known items [4].

To resist KNN attack, the neighbor information in both stages should be preserved, we integrate Zhu's algorithm [2] to address the problem. In the stage of selecting k neighbors, we can employ the exponential mechanism ensuring little influence on the chosen probability for a particular item after deleting a user. Thus the attacker can't infer the rating history by creating fake ratings .

To copy with the sparsity of user-item matrix, in the study, we give the definition of content-based profiling (CBP) of user's ratings based on item categories, moreover, we can preserving the user's rating record, if we combine with the PNS, we can get better result.

Preliminaries

Description of the recommendation system. The recommendation system collects user's ratings and form user-item matrix n×m, representing ratings from n users on m items. For an active user (a), we can predict the rating for a target item (q) after sending her available ratings. The prediction consists of two steps:

(1) Select neighbors by computing similarities between user a and the rest of users;

(2) Predict a weighted prediction according to preferences of neighbors on q. Calculate the similarities between user a and any user u. Pearson's correlations coefficient (PCC) is given in

$$sim_{au} = \frac{\sum_{i-1}^{m'} (r_{ai} - \overline{r}_a)(r_{ui} - \overline{r}_u)}{\sqrt{\sum_{i-1}^{m'} (r_{ai} - \overline{r}_a)^2} \sqrt{\sum_{i-1}^{m'} (r_{ui} - \overline{r}_u)^2}},$$

where r_{ui} is the rating for item i from user u; r_u is the average rating of user u; m is the number of items which are co-rated by uses. After comparing similarities, choose the K closest neighbors based on similarities. P_{aq} means a prediction for a on q, namely,

$$p_{aq} = \overline{r}_a + \frac{\sum_{u=1}^{N} (r_{up} - \overline{r}_u) \times sim_{au}}{\sum_{u=1}^{N} sim_{au}}.$$

Related Work. To solve the sparsity of user-item matrix and improve scalability, Chen et al used orthogonal non-negative matrix tri-factorization [8]. Jeong et al offer a novel iterative semi-explicit rating method, which aggregates neighbor ratings and extrapolates unrated elements in a semi-supervised manner to obtain a dense preference matrix [5], and Russell and Yoon applied discrete wavelet transformation as an approach to enhance the scalability of memory-based collaborative filtering recommender systems, in which data size was reduced significantly to decrease time [9].

After overcoming the sparsity and scalability problems, the quality of predictions are taken into consideration. Kim et al propose a collaborative filtering method to provide an enhanced recommendation quality derived from user-created tags [10], and Lee et al propose a CF-based recommendation methodology based on both implicit ratings and less ambitious ordinal scales [11].

As the information overload becoming more and more serious, privacy-preserving grasping more and more interests. Kaleli and Polat propose a novel privacy-preserving scheme to produce SOM clustering-based recommendations on vertically distributed data among multiple parties [12]. Bilge and Polat build RPT onto discrete wavelet transform-based recommender systems to preserve individuals' privacy [13].In the paper of ALPER and Huseyin, they focus on privacy-preserving schemes applied on clustering-based recommendations to produce referrals without greatly jeopardizing users' privacy [5].

KNN Attack. Recently, Calandrino et al presented the KNN attack [4]. They claim that if the partial rating history is available to the attacker, they can infer user's remaining rating history.

Considering an attacker has known the user U's partial transaction history, i.e., he already know m items which user U has already rated ,his goal is to find out the remaining rated item that he does not know. The attacker initially creates k fake users as sybils, and arrange the sybils' rating history with the m items using the user U's rating history. With the KNN and CF method, there are high probability that k nearest neighbors of each sybils will consist of the other k-1 sybils and the user U, the attacker can scan the recommendation list which given by the recommendation system according to the similarities among all users. If any item not belong to the former m items occurs, it should be rated by the user U.

For traditional CF methods, a KNN attack can perform well due to the sparsity of a typical rating dataset, and $m=O(\log n)$ is dangerous for the user to be attacked, where n is the total number of users in the rating dataset. However, in the paper, the KNN attack are based on the masked data with privacy protection by randomized perturbation techniques

Experiment

Dataset. In order to illustrate the performance of our proposal, we carry out the experiment based on the MovieLens dataset (http://www.movielens.org/) which has been widely used in the CF methods. It consists of 1.000.209 ratings, which was assigned by 6040 users on 3952 movies. The data guarantees that each user give their preference on at least 20 movies, the rating scores vary from 0(bad) to 5(excellent).we employ part of the dataset to perform the experiment.

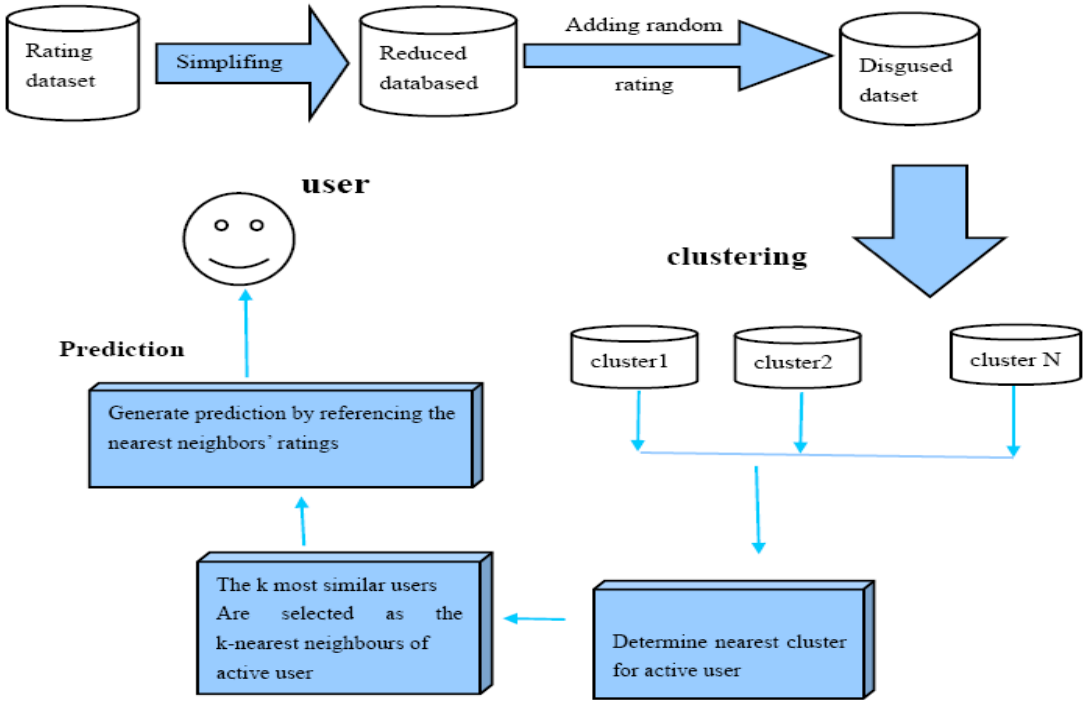
Experimental Setup. In order to simplify the process of the KNN attack algorithm, we present the recommendation system in Fig.1 (a).

To evaluate the KNN attack method, the steps are follows, which are showed in Fig.1 (b).

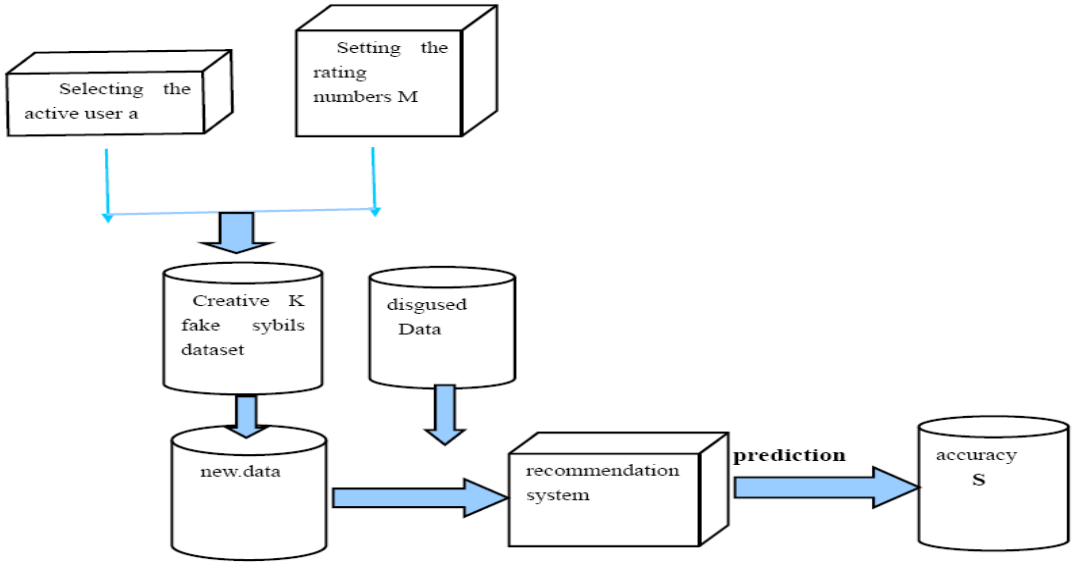
Select the active user a, the data are based on the MovieLens dataset; we can choose the active user from the 3952users randomly. Then, set the true rating number M, it assumes that the attacker has already known the k rating history of the active user a. Creat K fake sybils, they just have rated m movies which are based on the active user a, and the other ratings are put to zero. Afterwards, update the previous dataset, and add the k fake sybils to the former rating dataset. Given the recommendation to the sybils, we put the updated data into the recommendation system (the process are presented in Fig.1). For the sybils, every movies will have its own prediction, and we sort the prediction rating in decrease.

For the active user a, we denote the number which had been rated as N, and counting the number D which the movies occur in the rated dataset and are recommended to sybils (we just recommend the first N movies in the prediction dataset), so the accuracy S: is $S=(D-M)/(N-M)*100\%$.

The experiment is implemented by Matlab R 2012b and conducted on a PC. We carry out a series of K and M, they are compared in terms of the attack accuracy, in the following part, we will discuss the result in detail.



(a)



(b)

Fig. 1 Flowchart

Results and Conclusion

The Influence of K. In the experiment 1, we choose the 4169th user as the active user, and he has rated 2314 movies, we set the true rating number M as 600 and 800,and let the fake sybils K range from 500 to 1000, it has predicted that the attack accuracy S just makes little difference, as shown in Table1.

Table 1. Influence of K

M\K	500	600	700	800	900	1000
600	0.732	0.744	0.742	0.744	0.765	0.761
800	0.713	0.736	0.721	0.740	0.738	0.727

The Influence of *M*. In the experiment 2, we choose the 1010th user as the active user, and he has rated 1004 movies, we set the fake sybils K as 300 and 450, and let the true rating number M range from 500 to 1000, it has predicted that the attack accuracy S changed a lot, in a certain range, with the increase of M,S shows greater. But when M is larger than 400, the attack accuracy is becoming worse and worse as shown in Table 2.

Table 2. Influence of M

K\M	300	350	400	450	500	550	600
300	0.631	0.668	0.556	0.619	0.611	0.150	0.134
450	0.686	0.589	0.656	0.569	0.625	0.661	0.124

The influence of *N*. When we set the same *M* and *K*, we figure out that the attack accuracy S is greater while the user give more rating on the movie. Though for the 62th user, S is lower as 0.5, because the rating number is small, it is a small part of the movie dataset. But for the maximum rating user, the prediction is pretty good, S can reach at least 0.7, owing to the half of the rating movies, the user can be attacked easily.

Moreover, for the true rating number *M* and the fake sybils *M*, *M* is the vital factor. In the process of recommendation, clustering is the significant stage, it determines whether the *k* fake sybils can be clustered together, further it influences the prediction and the accuracy.

Conclusion

For the KNN collaborative filtering algorithm, though the privacy can be protected by adding random rating, it can be attacked partly, when the rating movie number increase, the threat to the

privacy of the user is serious. In the experiment in part V, it predict that the user's information can be access to 75% if the parameter is set right, with the increase of the rating movie, the accuracy of prediction can be higher.

To solve the problem of KNN and CF algorithm, we can adopt a private neighbor selection method. In a sense, it can prevent the adversary from inferring "who is the neighbor". Specifically, we choose a mechanism to perform private selection on the item similarity matrix to find k neighbors. The mechanism should guarantee there are high chance that the k nearest neighbor will be chosen, and deleting a user has little impact on the chosen probability, so it is unlikely to infer the rating history by creating faking neighbors of active user

Acknowledgement

This work is partly supported by Students Research Fund of Huazhong Agricultural University, the Fundamental Research Funds for the Central Universities of China (Project no. 2013PY120), and the National Natural Science Foundation of China (Grant no. 61202305).

References

[1] Yin, Chun-Xia, and Qin-Ke Peng. A careful assessment of recommendation algorithms related to dimension reduction techniques. *Knowledge-Based Systems* 27 (2012): 407-423.

[2] Zhu, Tianqing, et al. An effective privacy preserving algorithm for neighborhood-based collaborative filtering. *Future Generation Computer Systems* (2013).

[3] Ren Y, Li G, Zhang J, et al. The efficient imputation method for neighborhood-based collaborative filtering. *Proceedings of the 21st ACM international conference on Information and knowledge management. ACM*, 2012: 684-693.

[4] Calandrino J A, Kilzer A, Narayanan A, et al. " You Might Also Like:" Privacy Risks of Collaborative Filtering *Security and Privacy (SP), 2011 IEEE Symposium on. IEEE*, 2011: 231-246.

[5] Bilge A, Polat H. A comparison of clustering-based privacy-preserving collaborative filtering schemes. *Applied Soft Computing*, 2013, 13(5): 2478-2489.

[6] Canny J. Collaborative filtering with privacy, *IEEE Symposium on Security and Privacy*. IEEE, 2002: 45-57.

[7] Kaleli C, Polat H. Providing private recommendations using naive Bayesian classifier[M]//Advances in Intelligent Web Mastering. Springer Berlin Heidelberg, 2007: 168-173.

[8] Chen G, Wang F, Zhang C. Collaborative filtering using orthogonal nonnegative matrix tri-factorization. *Information Processing & Management,* 2009, 45(3): 368-379..

[9] Russell S, Yoon V. Applications of wavelet data reduction in a recommender system. *Expert Systems with Applications,* 2008, 34(4): 2316-2325.

[10]Kim H N, Ji A T, Ha I, et al. Collaborative filtering based on collaborative tagging for enhancing the quality of recommendation. *Electronic Commerce Research and Applications,* 2010, 9(1): 73-83.

[11]Lee S K, Cho Y H, Kim S H. Collaborative filtering with ordinal scale-based implicit ratings for mobile music recommendations. *Information Sciences,* 2010, 180(11): 2142-2155.

[12]Kaleli C, Polat H. SOM-based recommendations with privacy on multi-party vertically distributed data [J]. Journal of the Operational Research Society, 2012, 63(6): 826-838.

[13]Bilge A, Polat H. An improved privacy-preserving DWT-based collaborative filtering scheme. *Expert Systems with Applications*, 2012, 39(3): 3841-38.

Mechanics, Mechatronics, Intelligent System and Information Technology
10.4028/www.scientific.net/AMM.610

Robust Analysis on a Privacy Preserving Recommendation Algorithm under the KNN Attack
10.4028/www.scientific.net/AMM.610.717

DOI References
[5] Bilge A, Polat H. A comparison of clustering-based privacy-preserving collaborative filtering schemes. Applied Soft Computing, 2013, 13(5): 2478-2489.
http://dx.doi.org/10.1016/j.asoc.2012.11.046
[9] Russell S, Yoon V. Applications of wavelet data reduction in a recommender system. Expert Systems with Applications, 2008, 34(4): 2316-2325.
http://dx.doi.org/10.1016/j.eswa.2007.03.009
[10] Kim H N, Ji A T, Ha I, et al. Collaborative filtering based on collaborative tagging for enhancing the quality of recommendation. Electronic Commerce Research and Applications, 2010, 9(1): 73-83.
http://dx.doi.org/10.1016/j.elerap.2009.08.004
[11] Lee S K, Cho Y H, Kim S H. Collaborative filtering with ordinal scale-based implicit ratings for mobile music recommendations. Information Sciences, 2010, 180(11): 2142-2155.
http://dx.doi.org/10.1016/j.ins.2010.02.004
[13] Bilge A, Polat H. An improved privacy-preserving DWT-based collaborative filtering scheme. Expert Systems with Applications, 2012, 39(3): 3841-38.
http://dx.doi.org/10.1016/j.eswa.2011.09.094