A Robust Collaborative Recommendation Algorithm Incorporating Trustworthy Neighborhood Model

Dongyan Jia, Fuzhi Zhang
School of Information Science and Engineering, Yanshan University, Qinhuangdao, China
The Key Laboratory for Computer Virtual Technology and System Integration of Hebei Province, Qinhuangdao, China
Email: jdy_1983@163.com, xjzfz@ysu.edu.cn

Abstract—**The conventional collaborative recommendation algorithms are quite vulnerable to user profile injection attacks. To solve this problem, in this paper we propose a robust collaborative recommendation algorithm incorporating trustworthy neighborhood model. Firstly, we present a method to calculate the users' degree of suspicion based on the user-item ratings data using the theory of entropy and the idea of density-based local outlier factor. Based on it, we measure the user's trust attributes from different angles by introducing the source credibility theory and propose a multidimensional trust model incorporating users' degree of suspicion. Then we propose a trustworthy neighborhood model by combining the baseline estimate approach with the multidimensional trust model. Finally, we devise a robust collaborative recommendation algorithm to provide more accurate recommendation for the target user by integrating the M-estimator based matrix factorization approach and the trustworthy neighborhood model. Experimental results on the MovieLens dataset show that the proposed algorithm has better robustness in comparison with the existing collaborative recommendation algorithms.**

Index Terms—**robust collaborative recommendation, trustworthy neighborhood model, multidimensional trust model, matrix factorization, recommender systems**

I. Introduction

Recommender systems, as a kind of information filtering technology, have provided an effective way to solve the information overload problem [1]. Specially, collaborative filtering [2, 3] is one of the most successful recommendation technologies used in recommender systems. Due to the openness of recommender systems, however, malicious users deliberately manipulate the recommendation output by mounting shilling attacks [4, 5]. Therefore, the robustness of recommender systems based on collaborative filtering is poor.

To solve this problem, some robust collaborative recommendation approaches have been proposed. A recommendation algorithm based on association rule mining is presented in Ref. [6]. This algorithm can get better robustness, but such robustness is acquired at the cost of lowering recommendation coverage. Cheng et al.[7] examined the performance of the least squares based matrix factorization (MF) and its extension methods such as the Bias MF [8], Neighborhood MF [9] and Temporal MF [10]. These methods can not generate reliable recommendations when the system's rating database is contaminated with some portion of attack profiles. To address this problem, Cheng et al.[7] proposed a least trimmed squares based matrix factorization to improve the robustness of recommender systems. But it may discard some rating information of genuine users. Mehta et al. [11] proposed a recommendation algorithm based on the singular value decomposition, which using M-estimators to reduce the influence of malicious ratings. But this algorithm shows poor robustness with the attack size increasing gradually. Li et al. [12] proposed a metadata-enhanced variational Bayesian matrix factorization model for robust recommendation. But this method has poor robustness in the presence of bandwagon attack.

Massa et al. [13] proposed that the quality of recommendation can be improved by incorporating trust information among users in the process of recommendation. In order to measure the degree of trust among users, various computational models of trust have been proposed. O'Donovan et al. [14] proposed the profile- and item-level computational model of trust and drew a conclusion that the latter performs better than the former by conducting experiments. Similarly, Lathia et al. [15] proposed an improved computational model of trust, which computed the degree of trust of target user to the recommender user based on the error of predicted rating. When there are attack profiles in the system, however, both of the models have the disadvantage of inaccurate computation of degree of trust . Aiming at the limitations of traditional collaborative filtering recommendation algorithms in selecting neighbors, Kwon et al. [16] proposed a multidimensional credibility model. However, it only takes into account the heterogeneous of ratings of users and still has the vulnerability when there are attack profiles in the system. Maida et al. [17] proposed a multidimensional model of trust, which was studied from the knowledge-based trustworthiness and inferred trustworthiness in theory. But the authors did not give the

Corresponding author: Fuzhi Zhang, xjzfz@ysu.edu.cn

doi:10.4304/jcp.9.10.2328-2334

calculation method of trust and experimental results.

To improve the robustness of recommender systems, we propose a robust collaborative recommendation algorithm incorporating trustworthy neighborhood model (RCRA). Our contributions mainly include:

(1) Introducing the idea of density-based local outlier factor and the source credibility theory, we propose a multidimensional trust model incorporating users' degree of suspicion. To reduce the probability of attackers to be neighbors of target user, we propose a trustworthy neighborhood model by combining the baseline estimate approach with the multidimensional trust model.

(2) To reduce the influence of shilling attacks on recommendation results, we devise a robust collaborative recommendation algorithm by combining the M-estimator based matrix factorization approach with the trustworthy neighborhood model.

(3) We conduct experiments on the MovieLens dataset and compare the performance of our algorithm with others to demonstrate the effectiveness of the proposed algorithm.

II. Trustworthy Neighborhood Model

The most common collaborative filtering approach is based on the neighborhood models. However, it is unreliable to select neighbors according to the similarity between users due to shilling attacks. To ensure the trustworthiness of neighbors, we incorporate degree of trust in the process of neighbor selection.

In this section, we describe a multidimensional trust model incorporating users' degree of suspicion, and combine the multidimensional trust model with the baseline estimate approach to construct a trustworthy neighborhood model.

A. Computation of Users'Degree of Suspicion

Suppose the rating database includes a set of m users, $U=\{u_1, u_2, \dots, u_m\}$, and a set of n items, $I=\{i_1, i_2, \dots, i_n\}$, so the user-item rating matrix can be described as a $m\times n$ matrix $\boldsymbol{R}$. $R_{i,j}(1\le i\le m, 1\le j\le n)$ is the rating of user u_i on item i_j. If user u_i hasn't rated the item i_j, we represent that as $R_{i,j}=\phi$.

For item i_j, let its ratings R_j be random variable and the range of value be described as $\{e_1, e_2, \dots, e_t\}$, P_x be the probability of e_x, so the item entropy of i_j is defined as follows:

$$E(R_j)=-\sum_{x=1}^{t}P_x\log_2 P_x. \tag{1}$$

Definition 1 (Zero-Efficiency Item Set). For item i_j, if its rating set $R(i_j)=\varnothing$, then the item i_j is called as zero-efficiency item. So the zero-efficiency item set can be described as $ZEI=\{i_j|\ i_j\in I,\ R(i_j)=\varnothing\}$.

Definition 2 (Outlier Item Set). For every item $i_j\in\overline{ZEI}$, if its item entropy $E(i_j)\ge\overline{E}$, then the i_j is called as an outlier item. So the outlier item set can be represented as $OI=\{i_j|\ i_j\in I,\ E(i_j)\ge\overline{E}\}$, where $\overline{E}$ is calculated as follows:

$$\overline{E}=\frac{1}{|\tilde{I}|}\times\sum_{i_j\in\tilde{I}}E(i_j). \tag{2}$$

Definition 3 (Weighted Manhattan Distance). For user $u_a\in U$ and user $u_b\in U$, let $R(u_a)$ and $R(u_b)$ be the rating set of u_a and u_b respectively, and the $I(u_a, u_b)$ be the co-rated item set of user u_a and u_b, then the weighted manhattan distance between user u_a and user u_b is defined as follows:

$$d(u_a,u_b)=\begin{cases}(|R(u_a)|+|R(u_b)|)\times \\ \sum_{s=1}^{n}w_s\,|R_{a,s}-R_{b,s}|, & R(u_a)\bigcap R(u_b)=\varnothing \\ \dfrac{(|R(u_a)|+|R(u_b)|)}{|I(u_a,u_b)|}\times \\ \sum_{s=1}^{n}w_s\,|R_{a,s}-R_{b,s}|, & R(u_a)\bigcap R(u_b)\neq\varnothing\end{cases} \tag{3}$$

where w_s is computed as follows:

$$w_s=\begin{cases}\delta, & \delta>1, i_s\in OI, i_s\notin ZEI \\ 1, & i_s\notin OI, i_s\notin ZEI \\ 0, & i_s\notin OI, i_s\in ZEI\end{cases} \tag{4}$$

Definition 4 (User's Degree of Suspicion). For user $u_a\in U$, its degree of suspicion $S(u_a)$ is defined as follows:

$$S(u_a)=\begin{cases}\left(\dfrac{LOF_k(u_a)}{10}\right)^3, & LOF_k(u_a)\le\zeta \\ 1-\mathrm{e}^{-\frac{LOF_k(u_a)}{5}}, & LOF_k(u_a)>\zeta\end{cases} \tag{5}$$

where $LOF_k(u_a)$ is local outlier factor of user u_a. From the Definition 4 we can see that, the larger local outlier factor a user has, the larger degree of suspicion is, in other words, the more likely it is regarded as an attacker. $LOF_k(u_a)$ is calculated as follows [18]:

$$LOF_k(u_a)=\frac{\sum\limits_{u_b\in N_{k\text{-}distance(u_a)}(u_a)}\dfrac{lrd_k(u_b)}{lrd_k(u_a)}}{|N_{k\text{-}distance(u_a)}(u_a)|} \tag{6}$$

where $N_{k\text{-}distance(u_a)}(u_a)$ is k-distance neighborhood of user u_a, which contains every user whose distance from user u_a is not greater than the k-distance, $lrd_k(u_a)$ and $lrd_k(u_b)$ are local reachability density of user u_a and user u_b respectively, which are computed by (7) [18].

$$lrd_k(u_a)=\left(\frac{|N_{k\text{-}distance(u_a)}(u_a)|}{\sum\limits_{u_b\in N_{k\text{-}distance(u_a)}(u_a)}reach\text{-}dist_k(u_a,u_b)}\right) \tag{7}$$

where $reach\text{-}dist_k(u_a,u_b)$ is the reachable distance of u_a with respect to user u_b, which is calculated as follows

$$reach\text{-}dist_k(u_a,u_b)=\max\{k\text{-}distance(u_b),d(u_a,u_b)\}. \quad (8)$$

The parameter $d(u_a, u_b)$ is weighted manhattan distance between user u_a and user u_b, k-$distance(u_b)$ is k-distance of user u_b, which is defined as the distance $d(u_b, u_c)$ between user u_b and user $u_c \in U$ such that [18]:

(1) for at least k users $u_d \in U/\{u_b\}$, it holds that $d(u_b,u_d) \le d(u_b,u_c)$;

(2) for at most k-1 users $u_d \in U/\{u_b\}$, it holds that $d(u_b,u_d) < d(u_b,u_c)$.

Based on the definitions above, for user $u_a \in U$, the steps of computing its degree of suspicion are as follows:

(1) According to the user-item ratings data, select zero-efficiency item set and outlier item set.

(2) Compute the weighted manhattan distance between user u_a and others, and select k-distance neighborhood of user u_a.

(3) Compute the local reachability density of user u_a and every user in k-distance neighborhood of user u_a.

(4) Compute the local outlier factor of user u_a, and based on that, compute its degree of suspicion.

B. Multidimensional Trust Model Incorporating Users' Degree of Suspicion

According to the source credibility theory [19], we analyze and measure the degree of trust users from three aspects: expertise, similarity and trustworthiness. Based on that, we propose a multidimensional trust model incorporating users' degree of suspicion.

Definition 5 (Expertise). For user $u_b \in U$, let $I(u_b)=\{i_j \mid R_{b,j} \ne \phi, i_j \in I\}$ be its rating item set, then its expertise is defined as follows:

$$E(u_b)=\frac{\sum_{i_j\in I(u_b)} R_{u_b}^{i_j}}{|I(u_b)|}\times(1-S(u_b)) \quad (9)$$

where $S(u_b)$ is the degree of suspicion of user u_b, $R_{u_b}^{i_j}$ is the user u_b's reliability of recommendation for item i_j and its calculation method can be found in [20].

Definition 6 (Similarity). For user $u_a \in U$ and user $u_b \in U$, let $S(u_a, u_b)$ be the rating similarity between user u_a and user u_b, which is defined as follows:

$$S(u_a,u_b)=sim(u_a,u_b)\times\frac{1}{1+e^{-\frac{|I(u_a,u_b)|}{l}}}\times(1-S(u_b)) \quad (10)$$

where $S(u_b)$ is the degree of suspicion of user u_b, $|I(u_a,u_b)|$ is the number of items co-rated by user u_a and user u_b, $sim(u_a, u_b)$ is Pearson correlation coefficient, l is a constant and we set l=3 according to the sparsity of user-item rating matrix.

Definition 7 (Trustworthiness). For user $u_b \in U$, let $T(u_b)$ be its trustworthiness, which is defined as follows:

$$T(u_b)=\left(\frac{2\sum_{i_j\in I(u_b),i_t\in I(u_b)} t_{j,t}^{b}}{|I(u_b)|(|I(u_b)|-1)}\right)\times(1-S(u_b)) \quad (11)$$

where $S(u_b)$ is the degree of suspicion of user u_b, $I(u_b)$ is the item set rated by user u_b, $t_{j,t}^{b}$ is the trustworthiness of u_b for item pair (i_j, i_t) and its calculation method can be found in Ref. [20].

Based on the analysis above, for user $u_a \in U$ and user $u_b \in U$, we can compute the degree of trust of user u_a to user u_b as follows:

$$trust_{a,b}=\alpha E(u_b)+\beta S(u_a,u_b)+\gamma T(u_b) \quad (12)$$

where α, β and γ are the importance weights of each attribute, the method of setting their values can be found in Ref. [20].

C. Multidimensional Trust-based Trustworthy Neighborhood Model

Koren et al. [9] pointed out that the rating data in collaborative filtering recommender system exhibits large user and item effects. In other words, some users have the tendency to give higher ratings than others, and some items have the tendency to receive higher ratings than others, which is accounted by baseline estimate as follows:

$$b_{ui}=\mu+b_u+b_i \quad (13)$$

where b_{ui} is the estimated value of the unknown rating $r_{u,i}$, μ is the overall average rating, b_u and b_i indicate the observed deviations of user u and item i, respectively.

Considering the influence of ratings of trusted neighbors on recommendation results, by incorporating the above multidimensional trust model, we can improve (13) as follows:

$$P_{u,i}=\mu+b_u+b_i+|U(u)|^{-\frac{1}{2}}\sum_{v\in U(u)}(R_{v,i}-\bar{R}_v)*trust_{u,v} \quad (14)$$

where $P_{u,i}$ and $R_{v,i}$ are the predicted rating and actual rating for user u and user v on item i, respectively, U is the trusted neighbors set of user u, $\bar{R}_v$ is the average rating of user v, $trust_{u,v}$ is the degree of trust of user u to user v.

III. Proposed Algorithm

To improve the robustness of recommender systems, we propose a robust collaborative recommendation algorithm, called RCRA, by integrating the trustworthy neighborhood model with M-estimator based matrix factorization approach.

Basic matrix factorization model can reveal the characteristics of users and items hidden from ratings data, which are denoted by user factor matrix P and item factor matrix Q. Let $\hat{R}$ be the matrix of predicted ratings, n be the total number of items and m be the total number of users, then the basic matrix factorization model is defined as follows:

$$\hat{\boldsymbol{R}} = \boldsymbol{Q}^T \boldsymbol{P} \tag{15}$$

where $\boldsymbol{P} = (\boldsymbol{p}_1, \boldsymbol{p}_2, ..., \boldsymbol{p}_m)$ is an $f \times m$ (f<m) matrix, and $\boldsymbol{p_u}$ is the f-dimensional user factors vector for user u, $\boldsymbol{Q} = (\boldsymbol{q}_1, \boldsymbol{q}_2, ..., \boldsymbol{q}_n)$ is an $f \times n$ (f<n) matrix, and $\boldsymbol{q_i}$ is the f-dimensional item factors vector for item i.

On the basis of matrix factorization model and the proposed trustworthy neighborhood model, we introduce M-estimator, which is described as follows:

$$\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{b} = \arg\min \sum_{r_{u,i} \neq \phi} w(e_{u,i}) e_{u,i}^2 \tag{16}$$

where $w(e_{u,i})$ is a weight function. It can be defined as follows:

$$w(e_{u,i}) = \begin{cases} 1, & e_{u,i} \leq L \\ \dfrac{L}{|e_{u,i}|}, & e_{u,i} > L \end{cases} \tag{17}$$

where $e_{u,i}$ is the residual between actual rating and predicted rating, L is a constant. For the case of the MovieLens dataset used in this paper, all ratings are on a scale from 1 to 5, so K is set to 1.345 in our experiments. The residual $e_{u,i}$ is computed as follows:

$$e_{u,i} = R_{u,i} - P_{u,i} \tag{18}$$

$$P_{u,i} = \mu + b_u + b_i + \boldsymbol{q_i}^T \boldsymbol{p_u} + |U(u)|^{-\frac{1}{2}} \sum_{v \in U(u)} (R_{v,i} - \bar{R}_v) * trust_{u,v} \tag{19}$$

where $\boldsymbol{p_u}$ is the latent factor vector of user u, $\boldsymbol{q_i}$ is the latent factor vector of item i.

Equation (16) can be solved by stochastic gradient descent. The steps are defined as:

$$\boldsymbol{q_i} \leftarrow \boldsymbol{q_i} + \gamma w(e_{u,i}) e_{u,i} \boldsymbol{p_u} \tag{20}$$

$$\boldsymbol{p_u} \leftarrow \boldsymbol{p_u} + \gamma w(e_{u,i}) e_{u,i} \boldsymbol{q_i} \tag{21}$$

$$b_u \leftarrow b_u + \gamma w(e_{u,i}) e_{u,i} \tag{22}$$

$$b_i \leftarrow b_i + \gamma w(e_{u,i}) e_{u,i} \tag{23}$$

Based on the ideas above, RCRA algorithm is described as follows.

```
Algorithm: RCRA
Input: the user-item rating matrix $R$
Output: the predicted rating $P_{a,j}$ for target user $u_a$ on target item $i_j$
Begin
(1) for count=1,…, Iterations do
(2)   for u=1,…, m do
(3)     for i =1,…, n do
(4)       if $R_{u,i} \neq \phi$ then
(5)         compute the residual $e_{v,i}$ by (18);
(6)         update $q_i$, $p_u$, $b_u$, $b_i$ by (20)~(23);
(7)       end if
(8)     end for
(9)   end for
(10) end for
(11) compute the predicted rating $P_{a,j}$ by (19);
(12) return $P_{a,j}$
End
```

This algorithm consists of two parts. The first part, from lines 1 to 14, is to train the model and get optimal value for every variable. The second part, from lines 15 to 16, is to compute the predicted rating $P_{a,j}$ for user u_a on item i_j based on the trained model.

IV. Experimental Evaluation

To evaluate the performance of the proposed RCRA algorithm, we have carried out experiments with algorithms as follows:

(1) MMF: M-estimator based matrix factorization approach proposed by Mehta et al [11].

(2) LTSMF: LTS-based matrix factorization approach proposed by Cheng et al [7].

(3) basicMF: the basic matrix factorization approach.

A. Experimental Data

In our experiments we use the publicly available dataset provided by MovieLens site[1], which contains 100,000 ratings on 1682 movies by 943 users. All ratings are integer values between 1 and 5, where 1 is the lowest (disliked) and 5 is the highest (most liked). We divide the dataset into two groups, 80% are used as the training set and the remaining 20% are used as the test set.

B. Evaluation Metrics

We use MAE metric to evaluate the recommendation precision of algorithm, which is computed by measuring the deviation between the predicted rating and the actual rating. Obviously, the smaller MAE is, the higher the precision of algorithm is. MAE can be computed as follows [21]:

$$\text{MAE} = \frac{\sum_{j=1}^{n} \left| P_j - R_j \right|}{n} \tag{24}$$

where P_j is the predicted rating given to target user on target item i_j, R_j is the actual rating of target user on target item i_j, n is the number of prediction.

We use prediction shift to evaluate the robustness of algorithm. The prediction shift measures the deviation of prediction on the attacked item (before and after attack) of the recommendation algorithm. The smaller the prediction shift is, the better robustness the algorithm has. The prediction shift is computed as follows [22]:

$$\text{PS} = \frac{1}{n} \sum_{i=1}^{n} \left(\hat{P}(u_i, i_j) - P(u_i, i_j) \right) \tag{25}$$

[1] http://movielens.umn.edu/

where $P(u_i, i_j)$ and $\widehat{P}(u_i, i_j)$ are the predicted ratings of user u_i on item i_j before and after the item i_j is attacked respectively, n is the number of predictions.

C. Experimental Results and Analysis

To evaluate the robustness of algorithms RCRA, basicMF, MMF and LTSMF, we inject attack profiles which are generated by average attack and bandwagon attack with filler sizes of 3% and 5% across attack sizes of 1%, 2%, 5%, and 10% into the training set, respectively. Tables I to IV show the comparison of recommendation precision for four algorithms.

TABLE I.
COMPARISONS OF RECOMMENDATION PRECISION FOR FOUR ALGORITHMS UNDER AVERAGE ATTACK WITH 3% FILLER SIZE

Attack size	basic MF	MMF	LTSMF	RCRA
1%	0.7594	0.7647	0.7597	0.7532
2%	0.7593	0.7644	0.7598	0.7532
5%	0.7597	0.7638	0.7607	0.7539
10%	0.7597	0.7654	0.7599	0.7553

TABLE II.
COMPARISONS OF RECOMMENDATION PRECISION FOR FOUR ALGORITHMS UNDER AVERAGE ATTACK WITH 5% FILLER SIZE

Attack size	basic MF	MMF	LTSMF	RCRA
1%	0.7595	0.7650	0.7602	0.7515
2%	0.7602	0.7655	0.7593	0.7542
5%	0.7585	0.7643	0.7590	0.7522
10%	0.7600	0.7647	0.7597	0.7539

TABLE III.
COMPARISONS OF RECOMMENDATION PRECISION FOR FOUR ALGORITHMS UNDER BANDWAGON ATTACK WITH 3% FILLER SIZE

Attack size	basic MF	MMF	LTSMF	RCRA
1%	0.7598	0.7645	0.7602	0.7534
2%	0.7596	0.7642	0.7598	0.7527
5%	0.7602	0.7652	0.7603	0.7529
10%	0.7598	0.7645	0.7602	0.7514

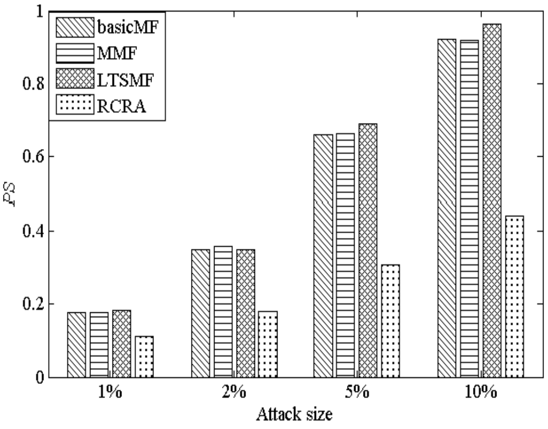
TABLE IV.

COMPARISONS OF RECOMMENDATION PRECISION FOR FOUR ALGORITHMS UNDER BANDWAGON ATTACK WITH 5% FILLER SIZE

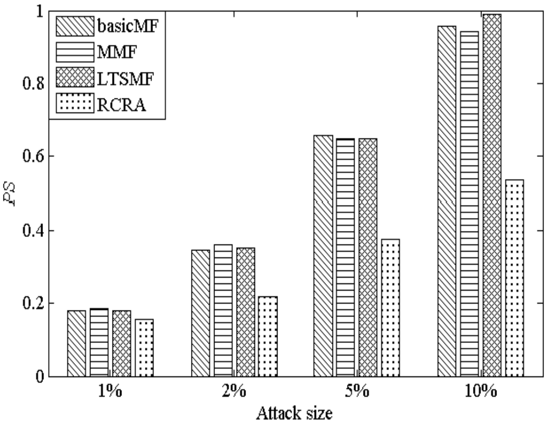
Attack size	basic MF	MMF	LTSMF	RCRA
1%	0.7600	0.7651	0.7594	0.7532
2%	0.7598	0.7648	0.7594	0.7523
5%	0.7606	0.7654	0.7599	0.7515
10%	0.7615	0.7657	0.7615	0.7509

As shown in Tables I to IV, whether average attack or bandwagon attack, the RCRA algorithm outperforms basic MF, MMF and LTSMF in term of precision under the same attack size and filler size. The reason is that RCRA incorporates the trustworthy neighborhood model which can reduce the influence of shilling attacks on the recommendation accuracy.

The comparisons of prediction shift for four algorithms with various attack types at various filler sizes across various attack sizes is depicted in Fig. 1 and Fig. 2.

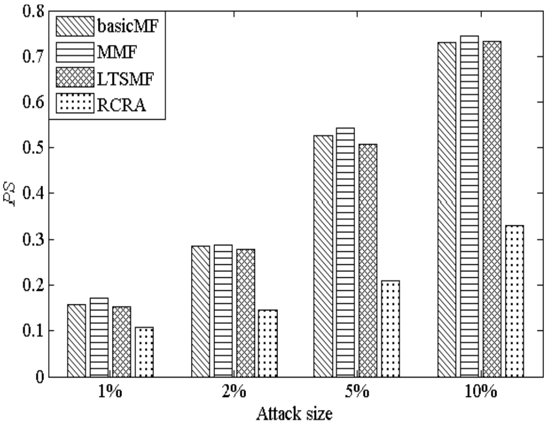


(a) 3% filler size

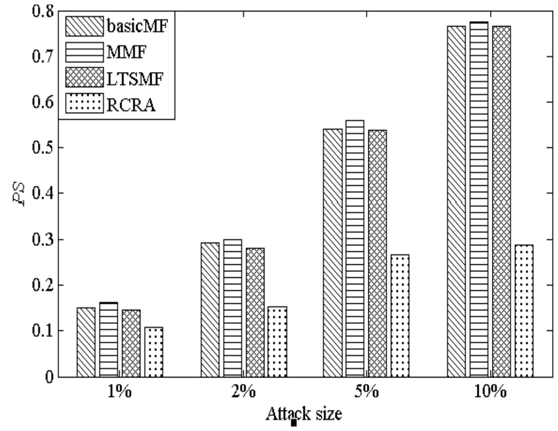


(b) 5% filler size

Figure 1 Comparisons of prediction shift for four algorithms under average attack with different filler size



(a) 3% filler size



(b) 5% filler size

Figure 2 Comparisons of prediction shift for four algorithms under bandwagon attack with different filler size

As shown in Fig. 1 and Fig. 2, under the same filler size, with the attack size increasing gradually, the prediction shift of all algorithms increases. So the more attackers there are in the system, the poorer the quality of recommendation is. Furthermore, under the same filler size and attack size, RCRA outperforms the basic MF, MMF and LTSMF in terms of prediction shift. Let us take the comparisons of prediction shift for four algorithms under average attack with different 5% size for an example, compared with basic MF, MMF and LTSMF, the robustness of RCRA improves by 34.46%, 35.09%, 34.83%, respectively. Therefore, RCRA algorithm has better robustness. The major reason is that RCRA algorithm incorporates the trustworthy neighborhood model which reduces the influence of shilling attacks on the recommendation.

V. Concluding Remarks

With the wide application of recommender systems in e-commerce websites, how to ensure the quality of recommendation has become more and more important. In this paper we propose a robust collaborative recommendation algorithm incorporating trustworthy neighborhood model. According to the source credibility theory and the idea of density-based local outlier factor, a multidimensional trust model incorporating users' degree of suspicion is presented. Based on the degree of trust between users, a trustworthy neighborhood model is proposed to reduce the risk of attackers to be neighbors. By incorporating the trustworthy neighborhood model with M-estimator based matrix factorization approach, we can make reliable recommendations for the target user. Compared with other algorithms, the proposed algorithm has better robustness. How to combine collaborative filtering with attack detection and devise more robust recommendation algorithm will be our future work.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (No.61379116), the Natural Science Foundation of Hebei Province, China (No.F2013203124), and the Key Program of Research on Science and Technology of Higher Education Institutions of Hebei Province, China (No.ZH2012028).

References

[1] Li Hui, Zhang Shu, Wang Xia. "A personalization recommendation algorithm for e-commerce". *Journal of Software*, 2013, 8(1): 176-183.

[2] Lü L, Medo M, Yeung C H, et al. "Recommender Systems". *Physics Reports*, 2012, 519(1): 1-50.

[3] Bobadilla J, Ortega F, Hernando A, et al. "Recommender Systems Survey". *Knowledge-Based Systems*, 2013, 46:109-132.

[4] Hurley N J, O'Mahony M P, Silvestre G C M. "Attacking recommender systems: a cost-benefit analysis". *IEEE Intelligent Systems*, 2007, 22(3): 64-68.

[5] Mobasher B, Burke R, Bhaumik R, et al. "Attacks and remedies in collaborative recommendation". *IEEE Intelligent Systems*, 2007, 22(3):56-63.

[6] Sandvig J, Mobasher B, Burke R. "Robustness of collaborative recommendation based on association rule mining". *Proceedings of the 2007 ACM Conference on Recommender systems*. ACM, 2007: 105-112.

[7] Cheng Zun-Ping, Hurley N. "Robust collaborative recommendation by least trimmed squares matrix factorization". *Proceedings of the 22nd IEEE International Conference on Tools with Artificial Intelligence*. IEEE, 2010: 105-112.

[8] Koren K, Bell R, Volinsky C. "Matrix factorization techniques for recommender systems". *IEEE Computer Society*. 2009, 42(8): 30-37.

[9] Koren Y. "Factorization meets the neighborhood: a multifaceted collaborative filtering model". *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 2008: 426-434.

[10] Koren Y. "Collaborative filtering with temporal dynamics". *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 2009: 447–456.

[11] Mehta B, Hofmann T, Nejdl W. "Robust collaborative filtering". *Proceedings of the 2007 ACM Conference on Recommender systems*. ACM, 2007: 49-56.

[12] Li Cong, Luo Zhigang. "A metadata-enhanced variational Bayesian matrix factorization model for robust collaborative recommendation". *ACTA AUTOMATICA SINICA*, 2011, 37(9): 1067-1076.

[13] Massa P, Bhattacharjee B. "Using trust in recommender systems: an experimental analysis". *Proceedings of 2nd International Conference on Trust Management*. Springer, 2004: 221-235.

[14] O'Donovan J, Smyth B. "Trust in Recommender Systems". *Proceedings of the 10th International Conference on Intelligent User Interfaces*. ACM, 2005: 167-174.

[15] Lathia N, Hailes S, Capra L. "Trust-based collaborative filtering". *Proceedings of Joint iTrust and PST Conference on Privacy, Trust Management and Security*. Springer, 2008: 119-134.

[16] Kwon K, Cho J, Park Y. "Multidimensional credibility model for neighbor selection in collaborative recommendation". *Expert Systems with Applications*, 2009, 36(3): 7114-7122.

[17] Maida M, Maier K, Obwegeser N, et al. "A multidimensional model of trust in recommender systems". *Proceedings of 13th International Conference on Electronic Commerce and Web Technologies*. Springer,

2012: 212-219.

[18] Breunig M, Kriegel H P, Ng R T, Sander J. “LOF: identifying density-based local outliers”. *Proceedings of the 2000 ACM SIGMOD International Conference on Management of data*. ACM, 2000: 93-104.

[19] Eisend M. “Source credibility dimensions in marketing communication – a generalized solution”. *Journal of Empirical Generalizations in Marketing*, 2006, 10(2): 1-33.

[20] Jia, Dongyan, Zhang, Fuzhi, Liu, Sai. “A robust collaborative filtering recommendation algorithm based on multidimensional trust model”. *Journal of software*, 2013: 8(1), 11-18.

[21] Ye Hongwu. “A personalized collaborative filtering recommendation using association rules mining and self-organizing map”. *Journal of Software*, 2011, 6(4):732-739.

[22] Mehta B, Nejdl W. “Attack resistant collaborative filtering”. *Proceedings of the 31st annual International ACM SIGIR Conference on Research and Development in Information Retrieval*. ACM, 2008: 75-82.

Jia Dongyan was born in 1983. Currently, she is a PhD candidate in school of information science and engineeringYanshan University, Qinhuangdao, China. Her main research interests include collaborative filtering, trusted computing and information security.

Fuzhi Zhang was born in 1964. Currently, he is a professor and PhD supervisor in school of information science and engineering, Yanshan University, Qinhuangdao, China. His research interests include intelligent information processing, network and information security, and service-oriented computing.