International Journal of Security and Its Applications
Vol. 9, No. 3 (2015), pp. 13-24
http://dx.doi.org/10.14257/ijsia.2015.9.3.03

Robust Analysis of Network based Recommendation Algorithms against Shilling Attacks

Fuguo Zhang[1,2]

[1](School of Information and Technology, Jiangxi University of Finance and Economics, Nanchang, China)
[2](Jiangxi Key Laboratory of Data and Knowledge Engineering, Jiangxi University of Finance and Economics, Nanchang, China)
redbird_mail@163.com

Abstract

Despite their great adoption in e-commerce sites, recommender systems are still vulnerable to unscrupulous producers who try to promote their products by shilling the systems. In the past decade, network based recommendation approaches have been demonstrated to be both more efficient and of lower computational complexity than collaborative filtering methods, however as far as we know, there is rare research on the robustness of network based recommendation approaches. In this paper, we conducted a serious of experiments to examine the robustness of five typical network based recommendation algorithms. The empirical results obtained from the movielens dataset show that all the two limited knowledge shilling attacks are successful against the network based algorithms, and the bandwagon attack affects very strongly against most network based recommendation algorithms, especially the algorithms considering the preferential diffusion at the last step. One way to relieve the attack impact is to assign the algorithm a heterogeneous initial resource configuration.

Keywords: *recommender system, shilling attack, network based algorithm, hit ratio*

1. Introduction

The ongoing rapid expansion of the world-wide-web and e-commerce has led to a serious problem of information overload: the customers are difficult to choose the right product without wasting too much time. Recommender systems have emerged in response to this problem [1]. Many electronic commerce sites already benefit from novel opportunities of personalized marketing leverage offered by these information systems [2, 3]. For example, Amazon asserted 35% of the sales were from the system recommendation [4], and Netflix claimed about 60% of the rental business was from the recommender system [5].

Thus far, a great many recommendation algorithms have been proposed such as collaborative filtering (CF) [6–9], content-based analysis [10-13], matrix factorization [14, 15] and so on. In recent years, the bipartite networks have catched lots of attentions [16]. Zhang, *et al.*, have successfully applied the classical physical processes, such as the heat conduction and mass diffusion, to deal with the personalized recommendation problem [17-19]. Network based recommendation approaches have been demonstrated to be both more efficient and of lower computational complexity than collaborative filtering methods [20].

ISSN: 1738-9976 IJSIA

However, with recommender systems, there is a natural motivation for producers of items (manufacturers, authors, *etc.*,) to want one's own products to be recommended more often than those of a competitor. Unscrupulous producers may opt to insert fake profiles into the user-item matrices so that they can affect the predicted ratings on behalf of their advantages [17]. For instance, in 2002 Amazon.com Inc. received many complaints from the online customers that the website often recommended a spiritual guide by well-known Christian televangelist Pat Robertson as well as a sex manual book. Later Amazon conducted an investigation and found these recommendation results were made by unscrupulous vendors. In fact, there weren't hundreds of genuine customers going to the same items while they were shopping on the site [21].

For the robustness of recommendation algorithms, in the past decade, there have been a number of significant works paying attention to examine the robustness of collaborative filtering algorithms in the face of profile injected attacks [17, 22-27]. Furthermore, many detection methods such as Statistical techniques [28, 29], Classification [30, 31], Unsupervised clustering [32, 33], and Other detection techniques [34, 35] have been proposed. However, as far as we know, rare work is about the robustness of network based recommendation.

This paper reports the empirical analysis on the well-known Movielens dataset to evaluate the effect of the limited knowledge shilling attacks against network based recommendation algorithms. Our main findings are threefold: (i) All the attack models employed in the experiments are effective in attacking the network based recommender algorithms. (ii)Most of the network algorithms response very strongly to the bandwagon attack.(iii)The algorithms considering the preferential diffusion at the first step can relieve the attack impact of the bandwagon attack.

Remaining parts of this paper are organized as follows. Section 2 briefly describes the network based recommendation algorithms used in the experiments. Section 3 is an analysis of the shilling attack models against network based algorithms. Section 4 presents our experimental work including details of our data set, evaluation metrics, results of different experiments. Finally, in Section 5 we provide some conclusion.

2. Network based Recommendation Algorithms

Up to now, there exists many network based Recommendation algorithms. Most of them are based on the original resource-allocation process (Probability Spreading, refer to as Probs) or heat-conduction analogous process (Heat Spreading, refer to as Heats) on a bipartite network. Generally, a recommender system could be demonstrated by a bipartite network, in which there are two kinds of nodes: users U and objects O. Supposing there are m objects O = $\{o_1,o_2, \ldots ,o_m\}$ and n users U =$\{u_1,u_2, \ldots ,u_n\}$, the system can be fully described by an adjacency matrix A =$\{ a_{i\alpha} \}_{m,n}$, where the element $a_{i\alpha}$ =1 if a user i has collected an item α, and $a_{i\alpha}$ = 0 otherwise. The result of network based algorithms can be seen as a three-step random walk process starting from the target user. At first, for a target user u_i, an initial resource $f_i = \{ f_{i1}, f_{i2}, \ldots, f_{i\alpha}, \ldots, f_{in} \}$ is assigned on those objects already collected by u_i. In the later two steps, the resource is distributed to its neighbors according to the different method. For ProbS, the method is to distribute evenly the resource to its neighbors; while in HeatS, the resource is redistributed via an averaging procedure, with users receiving a level of resource equal to the mean amount possessed by their neighboring objects, and objects then receiving back the mean of their neighboring users' resource levels [36]. The resource

reallocation process for each user in the network-based recommendation algorithms can be expressed using the following equation:

$$f' = Wf^{i}, \quad (1)$$

where W is is the resource reallocation matrix, and $f = \{f_1, f_2, ..., f_\alpha, ..., f_n\}$ is the final resource configuration on objects.

In this paper, we select five typical network based recommendation algorithms including MD algorithm, Hybrid algorithm, MF algorithm, BHC algorithm and PD algorithm. These algorithms are briefly described below.

(1)MD: The massive diffusion (MD) algorithm [18] starts by assigning one unit of resource to each item collected by the target user i. That is to say, If an object is collected by the user i, its initial resource is assigned to be 1, otherwise, to be 0. The transformation matrix in MD is
which is a column-normalized probability matrix representing the diffusion process,

$$W_{\alpha\beta} = \frac{1}{k_\beta}\sum_{i=1}^{N}\frac{a_{i\alpha}a_{i\beta}}{k_i}, \quad (2)$$

and where k_β is the degree of o_β and k_i is the degree of u_i. This method has been demonstrated to be more accurate than the classical CF algorithm, with lower computational complexity. However, it has difficulty in generating diverse recommendations. Figure 1 is an example of the resource reallocation process on the bipartite user-object network. Figure 1(a) and Figure 1(b) is for ProbS and Heats, respectively. In Figure 1(a), at first, one unit of resource is assigned to the object No. 1 and No. 5, which have been collected by the target user with the shaded circle. Secondly, after one step diffusion from object side to user side according to evenly redistributed rule, the three users respectively obtain 1, 1/2, and 1/2 units of resource. The last step is the diffusion from user side to object side, and the five objects are assigned 3/4,1/6,1/6,1/4,2/3 units of resource, respectively. For HeatS in Figure 1(b), so is the same with Probs at first step. The later two steps are to redistribute the resource via an averaging procedure. Finally, the five objects are assigned 3/4,1/3,1/3,1/2,2/3 units of resource, respectively.

(2)Hybrid: In order to solve the apparent accuracy–diversity dilemma of recommender systems, a hybrid algorithm by integrating MD and HC [19] was proposed in [18], which combines these two algorithms as follows:

$$W_{\alpha\beta} = \frac{1}{k_\alpha^{1-\lambda}k_\beta^{\lambda}}\sum_{i=1}^{N}\frac{a_{i\alpha}a_{i\beta}}{k_i}, \quad (3)$$

where λ is a tunable parameter to control the relative weight between the two algorithms. When λ increases from 0 to 1, the Hybrid algorithm changes gradually from HC to MD. The numerical results of such hybrid algorithm indicate that both of the accuracy and diversity could be increased at the optimal case. Since the pure mass diffusion algorithm enjoys high recommendation accuracy while the heat conduction algorithm is very outstanding in recommendation diversity. Fusing these two algorithms can gain high performance in both aspects.

(3)MF: One way to improve the recommendation accuracy of MD recommendation algorithm is to assign a heterogeneity initial resource configuration. The correspondence algorithm (MF) is proposed by Zhou, *et al.*, [37]. The initial resource of object α in a MF algorithm is $a_{i\alpha}k_\alpha^{\theta}$, where θ is a negative parameter.

(4)BHC: The biased heat conduction algorithm (BHC) [38] could greatly improve the accuracy of the standard HC algorithm by decreasing the temperatures of small degree objects. In this case, the resource transfer matrix reads

$$W_{\alpha\beta} = \frac{1}{k_\alpha^\lambda} \sum_{i=1}^{n} \frac{a_{i\alpha} a_{i\beta}}{k_i}. \quad (4)$$

(5)PD: In order to enhance the algorithm's ability to find unpopular and niche objects, a preferential diffusion (PD) method is proposed in [28]. The resource transfer matrix in the algorithm is

$$W_{\alpha\beta} = \frac{1}{k_\beta \; k_\alpha^{-\varepsilon}} \sum_{l=1}^{n} \frac{a_{l\alpha} a_{l\beta}}{M}, \quad (5)$$

where $M = \sum_{r=1}^{m} a_{lr} k_r^{\varepsilon}$ denotes the mean value of over all the objects having been collected by user u_l.

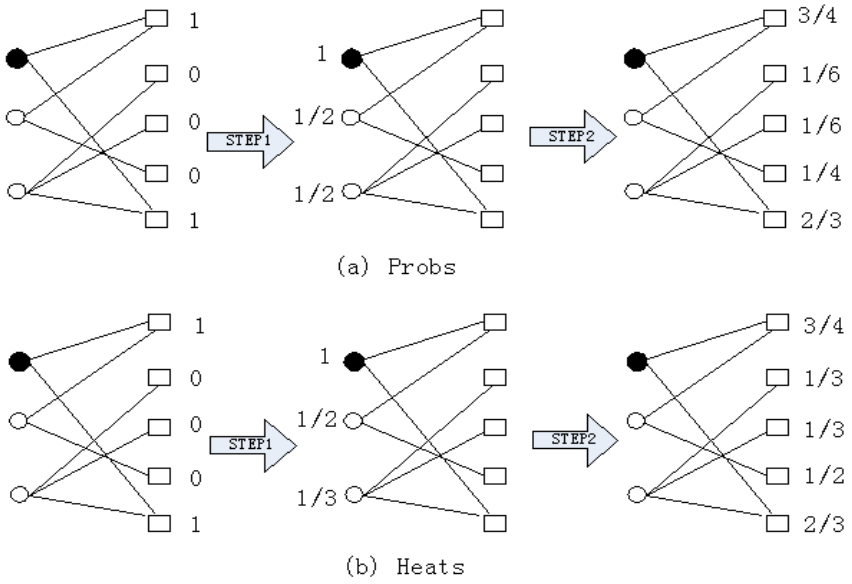

Figure 1. An Illustration of the Resource Reallocation Process on the Bipartite User-object Network, (a) for the MD Method, and (b) for the HC Method, Users are shown as Circles, Objects are Squares, The Target User is Indicated by the Shaded Circle

3. Attack Models

An attack against a collaborative filtering recommender system consists of a set of attack profiles, each contained biased rating data associated with a fictitious user identity, and including a target item, the item that the attacker wishes the system to recommend more highly (a push attack), or wishes to prevent the system from recommending (a nuke attack) [39].

An attack model is an approach to constructing attack profiles based on knowledge of the recommender system, its rating database, its products, and/or its users [38]. Shilling attacks can be classified as push and nuke attacks according to their intent. Push attacks try to make one or more target items recommended to more users, while nuke attacks

try to cause them less likely to be recommended. Shilling attacks can be classified as push and nuke attacks according to their intent. Push attacks try to make one or more target items recommended to more users, while nuke attacks try to cause them less likely to be recommended. An attack against a recommender system consists of a set of attack profiles. An attack profile consists of an m-dimensional vector of ratings, where m is the total number of items in the system. It is partitioned in three parts. Firstly, the unrated items partitions are those items with no ratings in the profile. Secondly, the target items will be given a rating designed to bias its recommendations, generally they will be either the maximum (push attack) or minimum (nuke attack) rating depending on the attack type. Finally, the set of filler items represent a group of selected items in the database which are assigned ratings within the attack profile, they will be given a rating according to the attack strategy [40].

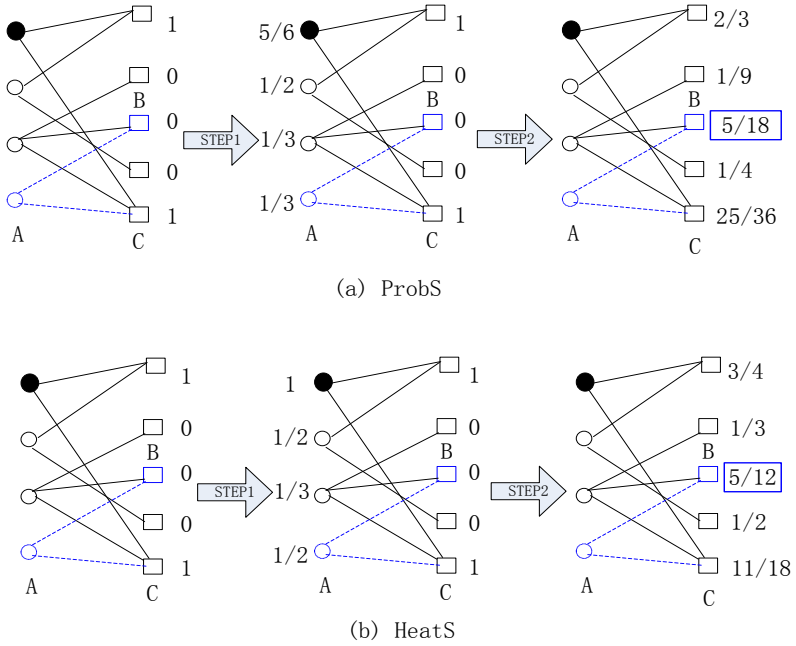

Figure 2. An Illustration of the Resource Reallocation Process on the Bipartite User-object Network after an Attack Profile has been Injected. Users are Shown as Circles; Objects are Squares. The Target User is Indicated by the Shaded Circle. The Attack user A is Denoted by the Dashed Circle. Object B is the Target Item, and Object C is a Popular Item.

Many attack types such as random attack, average attack, bandwagon attack, probe attack, segmented attack, love/hate attack, reverse bandwagon attack *etc.*, has been identified in recent years [22]. Different attack may require different level of knowledge about the items. In this paper, we select the following two types of attack models which are easy to execute because of minimum knowledge.

(1)Random attack: Lam, *et al.*, [17] originally introduced an attack model in which the filler items are assigned values generated randomly within the rating scale with a distribution centered on the mean for overall ratings. The knowledge required to mount such an attack is quite minimal, but the attack is not particularly effective.

(2)Bandwagon attack [41]: The bandwagon attack takes advantage of the Zipf's law distribution of popularity in consumer markets to build attack profiles, which contain those items that have high visibility. This information is easy to obtain and not system-dependent. Such profiles will have a good probability of being similar to a large number of users, since the high visibility items are those that many users have rated.

Figure 2 is an example of the resource reallocation process on the bipartite user-object network after an attack profile was injected. Suppose object B and object C are the target item and the popular item, respectively. User A is a forged user. For the bandwagon attack, he has collected object B and object C. Thus, as shown in Figure 2, after two step diffusion from object side to user side and from user side to object side, the final resources have changed after the attack profile injected. Table 1 and Table 2 are the comparison of the rank of the target item before and after one attack profile injected for Probs and Heats, respectively. Table 1 tells us clearly that the rank of the target item changes from No. 4 to No. 3 after one attack profile was injected. Although the rank of the target item in Table 2 doesn't change after one attack profile was injected, the predict score increases by 1/6.Therefore, injecting the attack profiles into network based recommender system can influence the recommendation results.

Table 1. Comparison of the Rank of the Target Item Before and after One Attack Profile Injected for ProbS

Item No.	The final resource before the attack profile injected	Ranks before the attack profile injected	The final resource after the attack profile injected	Ranks after the attack profile injected
1	3/4	1	2/3	2
2	1/6	4	1/9	5
3(the target item B)	1/6	4	5/18(↑ 1/6)	3(↑ 1)
4	1/4	3	1/4	4
5	2/3	2	25/36	1

Table 2. Comparison of the Rank of the Target Item Before and After One Attack Profile Injected for HeatS

Item No.	The final resource before the attack profile injected	Ranks before the attack profile injected	The final resource after the attack profile injected	Ranks after the attack profile injected
1	3/4	1	3/4	2
2	1/3	4	1/3	5
3(the target item B)	1/3	4	5/12(↑ 1/6)	4(↑ 0)
4	1/2	3	1/2	3
5	2/3	2	11/18	1

4. Experimental Evaluation

4.1. Dataset and Metrics

In our experiments we have used the publicly-available Movie Lens (http://www.grouplens.org/) 100K dataset. This dataset consists of 100,000 ratings on 1682 movies by 943 users. Ratings are discrete-valued between 1 and 5. Profile sizes vary from 18 to 706 with an average size 105.

In order to examine how effective an attack is in accomplishing its goal, we use the hit ratio [42] metric to measure the number of times that a target item appears in top-N recommended lists. A customer is only interested in top N recommendations, so not all prediction shifts are of equal importance in effect. For instance, on a 5-point rating scale, causing a prediction to change from 2 to 3 is far less meaningful than moving it from 4 to 5. Therefore, hit ratio is defined as the sum of the occurrence number of all target items in a top-N recommendation list across all test users divided by the number of pushed items. Therefore, the hit ratio for a pushed item i over all the test users, $HitRatio_i$, can be computed as:

$$HitRatio_i = \sum_{u \in U_t} H_{ui} / |U_t| , \quad (6)$$

where H_{ui} denotes the value of a recommendation hit on item i for user u. $H_{ui} = 1$ if $i \in R_u$, and $H_{ui} = 0$ otherwise. U_t denotes the set of the test users. The hit ratio of the recommender system is defined as follows:

$$HitRatio = \sum_{i \in I_t} HitRatio_i / |I_t| , \quad (7)$$

where I_t is the set of the target items.

4.2. Attack Experimental Design

This paper focuses on empirical analysis of the robustness of the random and bandwagon attack against the five network based recommendation algorithms including MD, BHC, Hybrid, MF and PD (the preferential diffusion algorithm at third step). The full dataset is divided into training and test sets. The test set contains a sample of 50 user profiles that mirror the overall distribution of users in terms of number of movies seen and ratings provided. We argued that unscrupulous producers were more willing to promote those items that have been liked by some users, therefore, 30 items among the movies which degree is more than 60 were selected manually for the target items set; this selection of items represents range of popularity (number of ratings) and likability (mean rating).The remainder of user profiles after removing the test set is designated as the training set.

We set the filler size (the number of filler ratings given to a specific attack profile measured as a percentage of the total number of movies) =25%. To evaluate the sensitivity of attack size and top-N value, we have tested 5%, 10%, 15%, 20%, 25%,30% attack size and 10, 20, 30, 40,50 top-N value on each attack type. The parameters for the parameter-dependent algorithms are set as the ones corresponding to the lowest ranking scores [for Hybrid, λopt = 0.20; for BHC, λopt = 0.85; for PD, εopt=-0.85; for MF, θopt = -0.8].

For the bandwagon attack, we selected the top n greatest degree items as the popular items, and use the number of popular items to denote filler size.

4.3. Results and Discussion

The efficiency of the random attack and the bandwagon attack against the five network based algorithms were examined in the beginning. Figure 3 presents the hit ratios of the random attack in different attack size at 15% filler size(the recommendation list L = 30), and Figure 4 presents the hit ratios of the bandwagon attack in different attack size with 20 popular items. Clearly, both the two attack types can affect the recommendation result at different degree, and the bandwagon attack has a stronger attacking effect than the random attack. When attack size varies from 0 to

30%, the hit ratio of the random attack against all the five algorithm is smaller than 0.2, but the biggest hit ratio of the bandwagon attack against PD algorithm and HBC algorithm are more than 0.6. Another phenomenon is the biggest hit ratio of the bandwagon attack against MF is smaller than 0.1. MF algorithm is taking into account the object degree effect in the first diffusion step. It help the target user distributes more resource to those who co-collected unpopular objects than co-collected popular objects. However, both PD algorithm and HBC algorithm directly punish the popular object by assigning more resource to the low-degree objects at the last diffusion step. This will enhance the rank of the target items by decreasing the rank of the popular items.

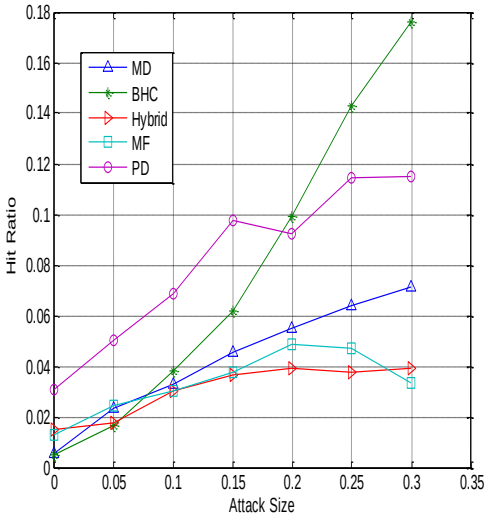

Figure 3. Hit Ratio for the Random Attack at Different Attack Size and 15% Filler Size

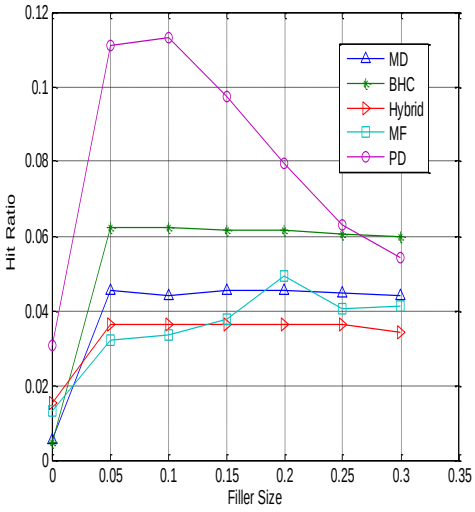

Figure 5. Hit Ratio for Random Attack at Different Filler Size and 15% Attack Size

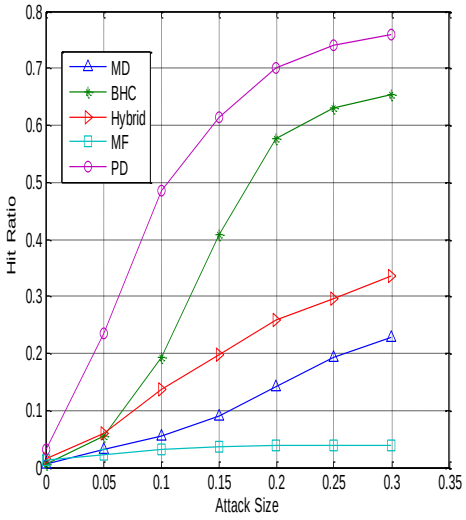

Figure 4. Hit Ratio for the Bandwagon Attack at Different Attack Size and 20 Popular Items Filler Size

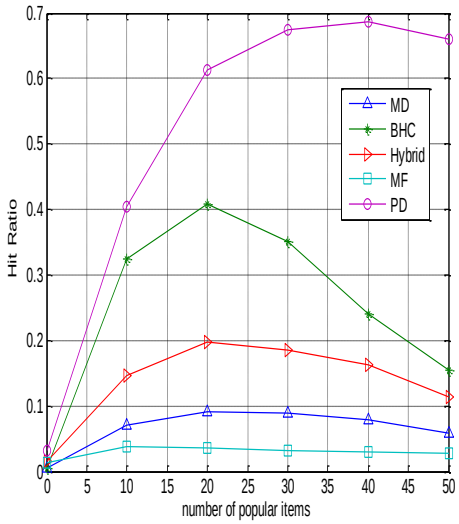

Figure 6. Hit Ratio for Bandwagon Attack in Different Filler Number of Popular Items

The next aspect we examine is the impact on hit ratio with different filler size value. Figure 5 and Figure 6 present the hit ratios of the random attack and the bandwagon attack in different filler size at 15% attack size respectively. We can find that the hit ratios of the random attack become big when the filler size is small, then they are not sensitive to the filler size. For the bandwagon attack, the hit ratio becomes smaller after it reaches the top value when popular items size varies from 10 to 50.

5. Conclusion and Future Work

Significant vulnerabilities have been identified in recommender systems. In this paper, we have conducted a serious of experiments to examine the robustness of network based recommendation algorithms. The two attack models, including a limited knowledge bandwagon attack that requires only that the attacker identify a small number of very popular items and the random attack being implemented very easily, were employed in the experiments to attack the five network based recommendation algorithms: the massd diffusion algorithm, the biased heat conduction algorithm, the hybrid algorithm by integrating MD and HC, the preferential diffusion algorithm at first step and the preferential diffusion algorithm at third step.

Our experiments have shown that these two attack models can be successful against network based recommendation algorithms, but the bandwagon attack has a very stronger effect against the network based algorithms than the random attack. Among the five network based recommendation algorithms, the two algorithms taking into account the object degree effect in the third diffusion step respond very stronger than the standard diffusion algorithm; On the contrary, MF algorithm can relieve the attack effect according to considering the object degree effect in the first diffusion step, therefore, we can use this method to improve the ability of network based algorithms to decrease the efficiency of the bandwagon attack.

Considering the overall performance in accuracy and robustness, future work will focus on how to detect the shilling attack, especially the bandwagon attack, in a network based recommender system.

Acknowledgment

This work is supported by the Foundation of Jiangxi Provincial Department of Education (GJJ. 12744) and National Natural Science Foundation of China under Grant Nos. 71361012 and 71363022.

References

[1] G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions", IEEE Trans KnowlData Eng, vol. 17, **(2005)**, pp. 734-749.
[2] B. Xiao and I. Benbasat, "E-commerce product recommendation agents: use, characteristics, and impact", MIS Quarterly, vol. 31, no. 1, **(2007)**, pp. 137-209.
[3] L. Y. Lü, M. Medo, C. H. Yeung, Y. C. Zhang, Z. K. Zhang and T. Zhou, "Recommender System", Physics Reports, vol. 519, no. 1, **(2012)**, pp. 1- 49.
[4] M. Marshall, "Aggregate Knowledge raises $5M from Kleiner, on a roll", **(2006)**, http://venturebeat.com/2006/12/10/aggregate-knowledge-raises-5m-from-kleiner-on-a-roll.
[5] "Netflix 2006 annual report", [OL], [2009-1-1], **(2009)**, http://ir.netflix.com/annuals.cfm.
[6] D. Goldberg, D. Nichols, B. M. Oki and D. Terry, "Using collaborative filtering to weave an information tapestry", Commun ACM, vol. 35, **(1992)**, pp. 61-70.
[7] J. B. Schafer, D. Frankowski, J. Herlocker and S. Sen, "Collaborative filtering recommender systems", In: The adaptive web, Springer, **(2007)**, pp. 291-324.
[8] J. S. Breese, D. Heckerman and C. Kadie, "Empirical analysis of predictive algorithms for collaborative filtering", Proceedings of the 14th Conference on Uncertainty in artificial intelligence, Morgan Kaufmann Publishers Inc., **(1998)**, pp. 43-52.
[9] B. Sarwar, G. Karypis, J. Konstan and J. Riedl J,"Item-based collaborative filtering recommendation algorithms", Proceedings of the 10th International World Wide Web Conference, **(2001)**.
[10] M. J. Pazzan and D. Billsus,"Content-based recommendation systems", The adaptive web, Springer, **(2007)**, pp. 325-341.
[11] M. Lipczak, Y. Hu, Y. Kollet and E. Milios, "Tag sources for recommendation in collaborative tagging systems", Proceedings ECML/PKDD Discovery Challenge, **(2009)**, pp. 157-172.
[12] Cantador, D. Vallet and J. M. Jose, "Measuring vertex centrality in cooccurrence graphs for online social tag recommendation", Proceedings ECML/PKDD Discovery Challenge, **(2009)**, pp. 17-33.
[13] S. Ju and K. B. Hwang, "A weighting scheme for tag recommendation in social bookmarking systems", Proceedings ECML/PKDD Discovery Challenge, **(2009)**, pp. 109–118.
[14] Y. Koren, R. Bell and C. Volinsky," Matrix factorization techniques for recommender systems", Computer, vol. 42, **(2009)**, pp. 30-37.
[15] M. Jamali and M. Ester, "A matrix factorization technique with trust propagation for recommendation in social networks", Proc of the 4th ACM RecSys Conference, **(2010)**, pp. 135-142.
[16] Z. Huang, D. Zeng and H. Chen, "Analyzing consumer product graphs: Empirical findings and applications in recommender systems," Management Science, vol. 53, no. 7, **(2007)**, pp. 1146-1164.
[17] S. Lam and J. Reidl, "Shilling recommender systems for fun and profit", Proceedings of the 13th International WWW Conference, New York, May, **(2004)**.
[18] T. Zhou, J. Ren, M. Medo and Y. C. Zhang, "Bipartite network projection and personal recommendation," Physical Review E, vol. 76, **(2007)**, pp. 046115.
[19] Y. C. Zhang, M. Blattner and Y. K. Yu, "Heat conduction process on community networks as a recommendation model," Phys. Rev. Lett., vol. 99, **(2007)**, pp. 154301.
[20] T. Zhou, Z. Kuscsik, J.-G. Liu, M. Medo, J. R. Wakeling and Y.-C. Zhang, "Solving the apparent diversity-accuracy dilemma of recommender systems", Proceedings of the National Academy of Sciences of the United States of America, vol. 107, no. 10,**(2010)**, pp. 4511-4515.
[21] "Amazon blushes over sex link gaffe", **(2006)**, http://news.cnet.com/2100-1023-976435.html.
[22] Gunes, C. Kaleli, A. Bilge and H. Polat, "Shilling attacks against recommender systems: A comprehensive survey", Artificial Intelligence Review, vol. 11, **(2012)**, pp. 1-33.
[23] B. Mobasher, R. Burke, C. Williams and R. Bhaumik, "Analysis and detection of segment-focused attacks against collaborative recommendation", Proceedings of the 2005 WebKDD Workshop, **(2006)**.
[24] B. Mehta, T. Hoffman and P. Fankhauser. "Lies and propaganda: detecting spam users in collaborative filtering", Proceedings of IUI'07, **(2007)**.
[25] P. A. Chirita, W. Nejdl and C. Zamfir, "Preventing shilling attacks in online recommender systems", In WIDM 05, **(2005)**, pp. 67-74.
[26] B. Mobasher, R. D. Burke, R. Bhaumik and J. J. Sandvig, "Attacks and remedies in collaborative recommendation", IEEE Intell Syst, vol. 22, no. 3, **(2007)**, pp. 56-63.

[27] R. Bhaumik, B. Mobasher, R. D. Burke, "A clustering approach to unsupervised attack detection in collaborative recommender systems", Proceedings of the 7th IEEE international conference on data mining, Las Vegas, NV, USA, **(2011)**, pp. 181-187.
[28] R. Bhaumik, C. A. Williams, B. Mobasher and R. D. Burke, "Securing collaborative filtering against malicious attacks through anomaly detection," Proceedings of the 4th workshop on intelligent techniques for web personalization, Boston, MA, **(2006)**.
[29] N. J. Hurley, Z. Cheng and M. Zhang, "Statistical attack detection", Proceedings of the 3rdACMinternational conference on recommender systems, New York, NY, USA, **(2009)**, pp. 149-156.
[30] R. D. Burke, B. Mobasher, C. A. Williams and R. Bhaumik, "Detecting profile injection attacks in collaborative recommender systems", Proceedings of the 8th IEEE conference on e-commerce technology, San Francisco, CA, USA, **(2006)**, pp. 23-30.
[31] C. A. Williams," Profile injection attack detection for securing collaborative recommender systems," Masters thesis, DePaul University, **(2006)**.
[32] M. P. O'Mahony, N. J. Hurley and G. C. M. Silvestre," Collaborative filtering-safe and sound", Lect Notes Comput Sci, vol. 2871, **(2003)**, pp. 506-510.
[33] R. D. Burke, M. P. O'Mahony and N. J. Hurley, "Robust collaborative recommendation", Recommender systems handbook. Springer, New York, **(2011)**, pp. 805-835.
[34] C. Y. Chung, P. Y. Hsu and S. H. Huang, "A novel approach to filter out malicious rating profiles from recommender systems", Decision Support Systems, vol. 55, no. 1, **(2013)**, pp. 314-325.
[35] F. G. Zhang, "Preventing recommendation attack in trust-based recommender systems", Journal of Computer Science and Technology, vol. 26, no. 5, **(2011)**, pp. 823-828.
[36] L. Lu and W. Liu, "Information filtering via preferential diffusion", Phys. Rev. E, vol. 83, **(2011)**, pp. 066119.
[37] T. Zhou, L.-L. Jiang, R.-Q. Su and Y.-C. Zhang, "Effect of initial configuration on network-based recommendation", EPL (Europhys. Lett.), vol. 81, **(2008)**, pp. 58004.
[38] J. G. Liu, T. Zhou and Q. Guo, "Information filtering via biased heat conduction", PHYSICAL REVIEW E, vol. 84, **(2011)**, pp. 037101.
[39] B. Mobasher, R. Burke, R. Bhaumik and C. Williams, "Towards trustworthy recommender systems: An analysis of attack models and algorithm robustness", ACM Transactions on Internet Technology, vol. 7, no. 4, **(2007)**, pp. 23-60 .
[40] R. Burke, B. Mobasher, C. Williams and R. Bhaumik, "Classification features for attack detection in collaborative recommender systems", Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, New York, USA: ACM Press, **(2006)**, pp. 542- 547.
[41] R. Burke, B. Mobasher, R. Zabicki and R. Bhaumik, "Identifying attack models for secure recommendation", Beyond Personalization Workshop at the International Conference on Intelligent User Interfaces, **(2005)**, pp. 347-361.
[42] B. Mobasher, R. Burke, C. Williams and R. Bhaumik. "Analysis and detection of segment-focused attacks against collaborative recommendation", Proceedings of the 2005 WebKDD Workshop, **(2006)**.

Authors

Fu-Guo Zhang, is an associate professor in the school of information and technology at Jiangxi University of Finance and Economics, Nanchang, China. He received Ph. D. degree from Jiangxi University of Finance and Economics, Nanchang. His research interests include recommender system and social network trust.

