
ISSN: 2321-2152
IJMECE
International Journal of modern
electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 12, Issue.2 May 2024

DETECTING GROUP SHILLING ATTACKS IN ONLINE RECOMMENDER SYSTEMS USING BISECTING K-MEANS CLUSTERING

[1]Minhaj Begum, [2]T sai pragna, [3]G. Sai Sushma

[1]Assistant professor in Department of Information Technology Bhoj Reddy Engineering College for Women

[2,3] UG Scholars in Department of Information Technology Bhoj Reddy Engineering College for Women

Abstract

Existing shilling attack detection approaches focus mainly on identifying individual attackers in online recommender systems and rarely address the detection of group shilling attacks in which a group of attackers colludes to bias the output of an online recommender system by injecting fake profiles. In this article, we propose a group shilling attack detection method based on the bisecting K-means clustering algorithm. First, we extract the rating track of each item and divide the rating tracks to generate candidate groups according to a fixed time interval. Second, we propose item attention degree and user activity to calculate the suspicious degrees of candidate groups. Finally, we employ the bisecting K-means algorithm to cluster the candidate groups according to their suspicious degrees and obtain the attack groups. The results of experiments on the Netflix and Amazon data sets indicate that the proposed method outperforms the baseline methods .

Keywords: Shilling Attacks, random attacks, traditional attacks.

INTRODUCTION

With the explosive growth of online information, the phenomenon of information overload becomes a key issue. Online recommender systems make recommendations for their users, which can alleviate the information overload problem to some extent. However, the online recommender systems are vulnerable to shilling attacks in which attackers inject a large number of attack profiles to bias the output of the recommender system, . Shilling attacks can be divided into push attacks and nuke attacks, which are used for promoting and demoting target items (e.g., movies or products) to be recommended, respectively. The well-studied shilling attacks include random attack, average attack, bandwagon attack, reverse bandwagon attack, average-target shift attack, average-noise injecting attack, and so on. In these attacks, attackers usually separately inject attack profiles into

recommender systems. In fact, a group of attackers might collude to make a tactical attack. Such shilling behaviors have been termed group shilling attacks, which are more threatening to the system than traditional shilling attacks. Therefore, how to effectively identify group shilling attacks has become a key issue needed to be addressed.

LITERATURE SURVEY

The internet is the home for huge volumes of useful data that is constantly being created making it difficult for users to find information relevant to them. Recommendation System is a special type of information filtering system adapted by online vendors to provide recommendations to their customers based on their requirements. Collaborative filtering is one of the most widely used recommendation systems; unfortunately, it is prone to shilling/profile injection attacks. Such attacks alter the recommendation process to promote or demote a particular product. Over the years, multiple attack models and detection techniques have been developed to mitigate the problem. This paper aims to be a comprehensive survey of the shilling attack models, detection attributes, and detection algorithms. Additionally, we unravel and classify the intrinsic traits of the injected profiles that are exploited by the detection algorithms, which have not been explored in previous works. We also briefly discuss recent works in the development of robust algorithms that alleviate the impact of shilling attacks, attacks on multi-criteria systems, and intrinsic feedback based collaborative filtering methods.

EXISTING SYSTEM

To protect recommender systems, various approaches have been presented to detect shilling attacks over the past decade. However, these approaches focus mainly on detecting individual attackers in recommender systems and rarely consider the collusive shilling behaviors among attackers.

Although some approaches have been proposed to detect shilling behaviors at the group level, they divide candidate groups and identify attack groups according to profile similarity. There are some group attack models that can generate attack profiles with great diversity. As a result, these approaches cannot fully detect attack groups, which cause poor precision and recall. Recently, some approaches have been presented to detect spammer groups in review websites. However, the group shilling attacks in recommender systems are different from the

spammer groups in review websites. Therefore, the spammer group detection approaches are not applicable to the detection of group shilling attacks.

PROPOSED SYSTEM

To overcome the abovementioned limitations, we propose a method to detect group shilling attacks in online recommender systems through bisecting K-means clustering. The proposed approach takes advantage of the time concentration characteristics of group shilling attacks, which has a better performance in detecting group attacks with collusive shilling behaviors.

The major contributions of this article are listed as follows

- We propose a candidate group division method, which first mines the rating tracks of items and then divides the users in the item rating tracks (IRTs) into multiple groups according to a certain length of time.
- Since the attackers in an attack group must rate the target item(s) within a certain period of time, the proposed candidate group division method is more likely to divide the attackers in an attack group together, which can lay a good foundation for the group shilling attack detection.

We propose metrics of item attention degree and user activity (UA) to analyze the candidate groups, making the judgment of attack groups more accurate.

Based on the divided candidate groups, the item attention degree and the UA for each candidate group are calculated, and the suspicious degrees of these groups are obtained. Based on this, the bisecting K-means algorithm is employed to cluster the candidate groups according to their suspicious degrees, and the attack groups are obtained.

To evaluate the performance of our method, we conduct experiments on the Netflix and Amazon data sets and compare the proposed method with four baseline methods.

Advantages of Proposed System

- Scalability
- Interpretability
- Adaptability
- Robustness to initialization.

IMPLEMENTATION

Group Shilling Attacks The concept of group shilling attacks was proposed by Su et al. They provided two scenarios for such attacks.

In scenario 1, besides giving biased ratings for the target item(s), the attackers also provide normal ratings for non target items to conceal their attack intentions.

In scenario 2, the gray organizations first collect different target items and send these items to the hired members, and thereafter, the group members select some target items for attacking.

Bisecting K-Means Clustering

Algorithm The core idea of the bisecting K-means clustering algorithm is to treat all data samples as a cluster at first and then divide this cluster into two clusters. Subsequently, the cluster that can minimize the clustering cost function (i.e., the sum of squared errors) is selected and divided into two clusters. This process continues until the number of clusters reaches the given number K. The main steps of the bisecting K-means algorithm are given as follows.

1) Use the basic K-means algorithm to divide all data samples into two clusters and add them to the set of clusters.

2) In the set of clusters, select the cluster that can reduce the sum of squared errors to the greatest extent and use the basic K-means clustering algorithm to divide it into two clusters, and, thereafter, add them to the set of clusters.

3) Repeat step 2) until there are K clusters in the set. Unlike the traditional K-means clustering, the bisecting K-means clustering can overcome the situation that the algorithm enters the local optimal state to some extent.

How Bisecting K-means Work

1. Set K to define the number of cluster
2. Set all data as a single cluster
3. Use K means with K=2 to split the cluster

They first utilized Borderline-SMOTE to relieve the unbalance classification situation and obtained a preliminary result via SVM. Then, they used a target item analysis method to identify attackers. Li et al. extracted some features from the item popularity degree and detected shilling attacks using the improved ID3 decision tree. This approach is not very effective when the filler size and attack size are small. The abovementioned approaches need to label sample data and train classification model, which are only applicable to detecting known types of shilling attacks. To overcome the limitations of supervised methods, some unsupervised methods have been proposed. Mehta and Nejdl analyzed the similarity structure in attack profiles and used principal component analysis (PCA) to identifythe attack profiles. Bryan et al. utilized H-score to sort users and obtained the target items on the basis of the sorted list of users. After the two steps, attack profiles were detected by the target item deviation. Unsupervised detection methods do not need to consider attack types or label training samples, but they need a priori knowledge of attacks (e.g., the attack size). The aforementioned methods focus mainly on detecting individual attackers in recommender systems. However, a group of attackers might collude to bias the output of recommender systems. Therefore, the detection of group shilling attacks has attracted attention in recent years. Zhou et al. improved the individual shilling attack detection metrics and proposed a two-step method to detect group shilling attacks.

ISSN2321-2152

www.ijmece .com

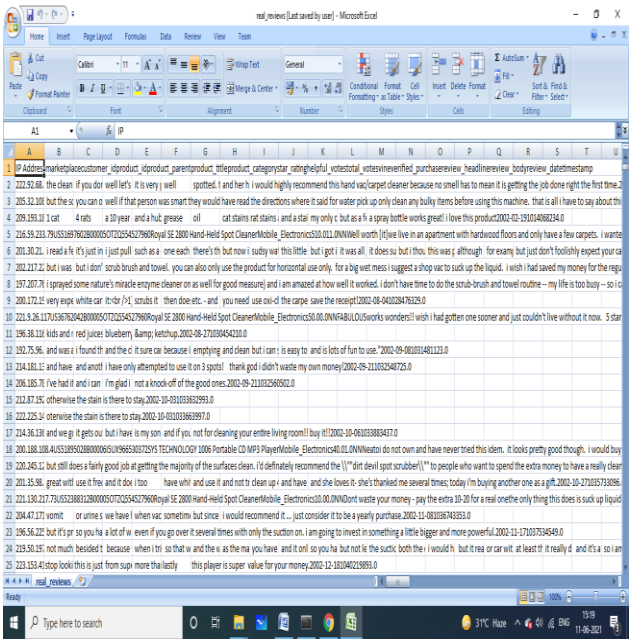
Vol 12, Issue.2 May 2024

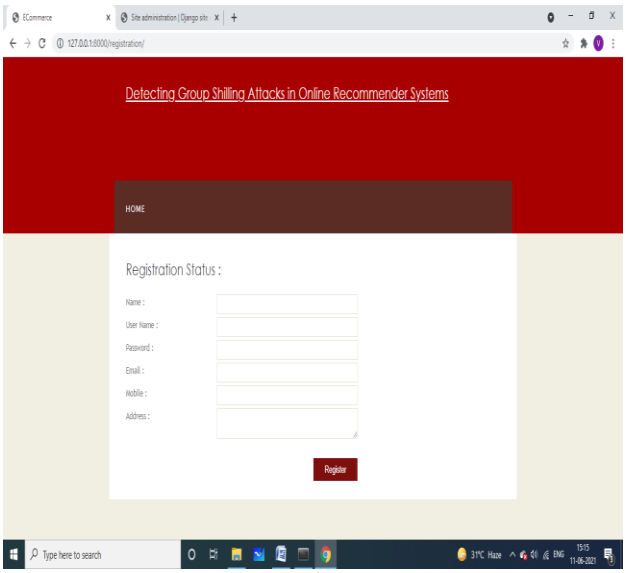
While this method is effective for detecting group attacks in synthetic data sets, it is not effective in detecting group attacks with a low similarity between attackers.

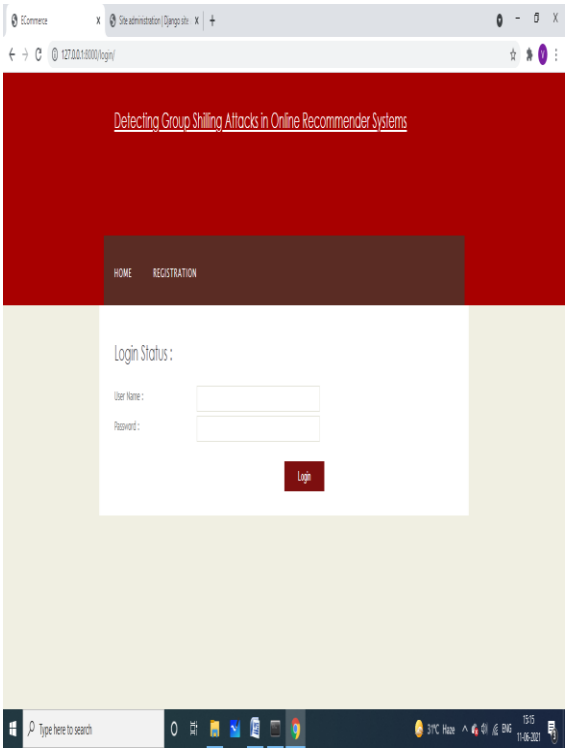
Wang et al. improved several traditional features and proposed a method for group attack detection based on these features. They first manually labeled candidate groups with high minimum support, and thereafter, they computed the group metrics and employed PCA to rank the candidate groups.

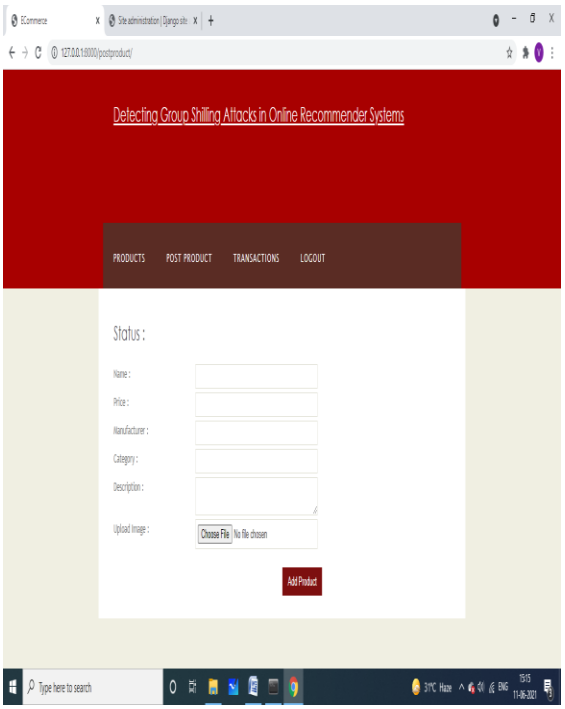
RESULTS

Input







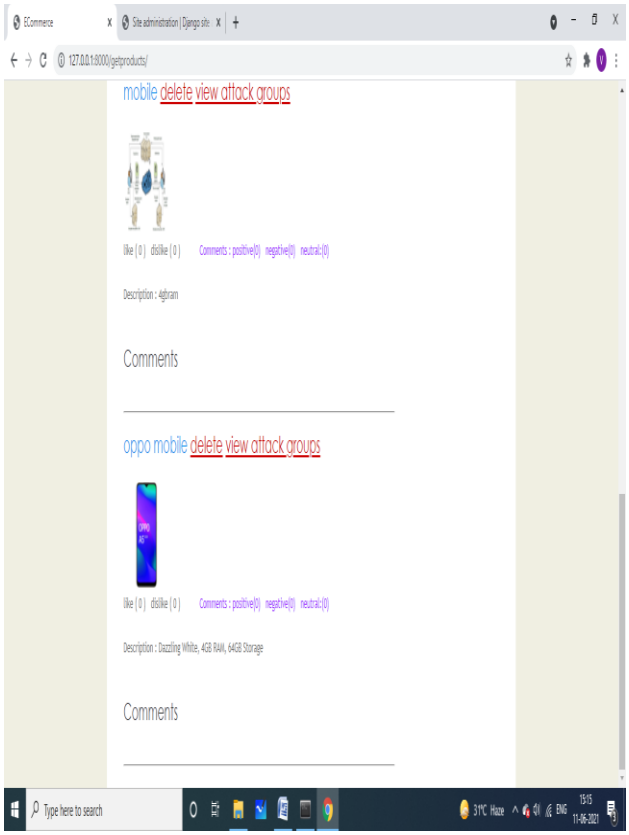


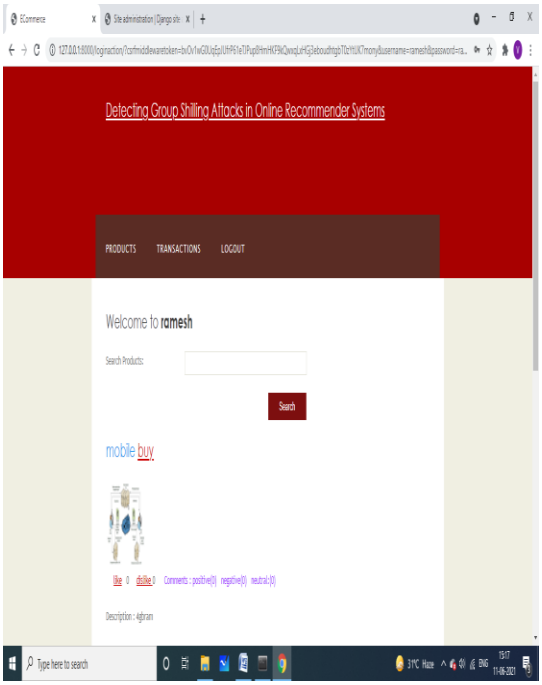
ISSN2321-2152

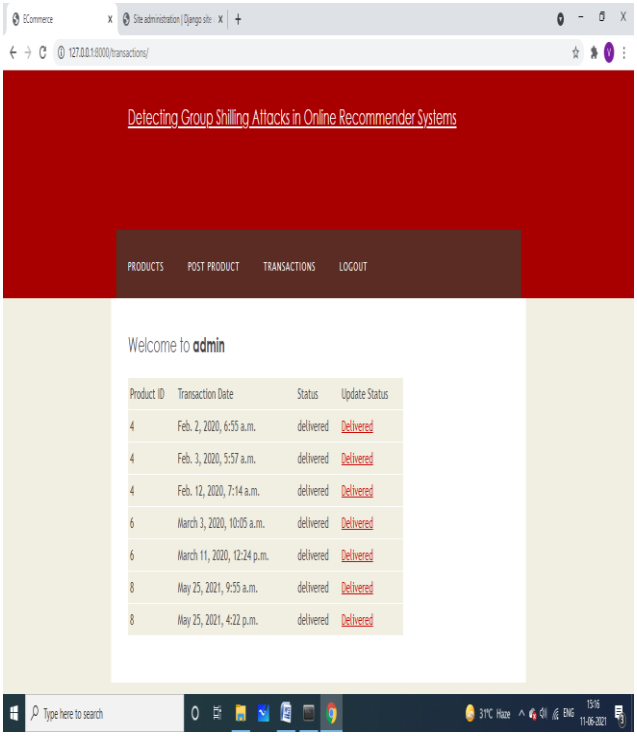
www.ijmece .com

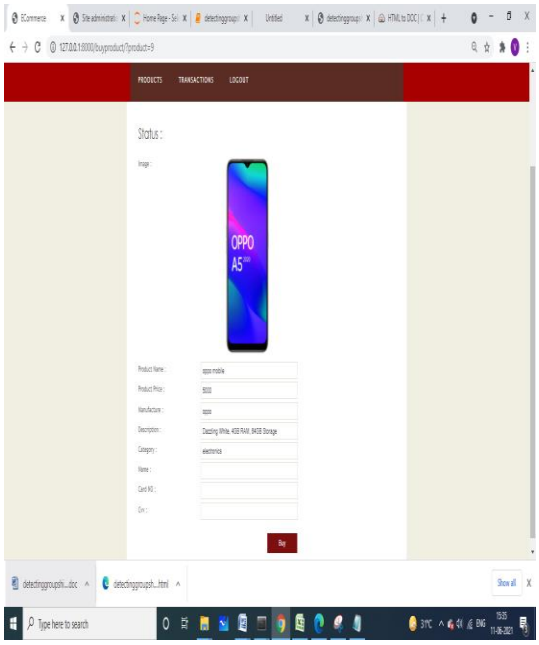
Vol 12, Issue.2 May 2024

Output





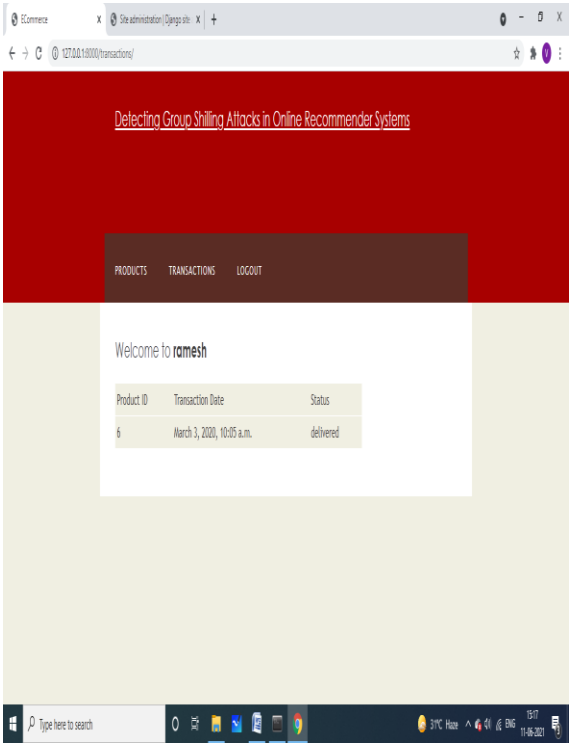


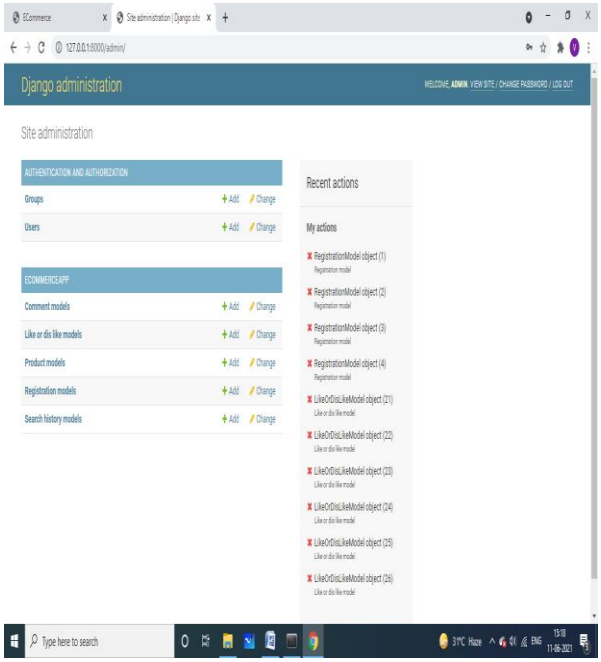


ISSN2321-2152

www.ijmece .com

Vol 12, Issue.2 May 2024





CONCLUSION

Group shilling attacks are a great threat to recommender systems. To detect such attacks, we propose a group attack detection model based on the bisecting K-means algorithm. The proposed detection model can overcome the problem that the performance is poor when attackers have a few corated items. In order to divide candidate groups, we use the fixed time length and dynamically select the starting time point to divide each item's rating track. We combine the features of items and users to calculate the GSDs. Based on the GSDs, the bisecting K-means algorithm is utilized to identify attack groups from the candidate groups. The experimental results on two data sets illustrate the effectiveness of our method.

REFERENCES

[1] T. L. Ngo-Ye and A. P. Sinha, "Analyzing online review helpfulness using a regressional relief F- Enhanced text mining method," ACM Trans. Manage. Inf. Syst., vol. 3, no. 2, pp. 10:1–10:20, Jul. 2012.

[2] I. Gunes, C. Kaleli, A. Bilge, and H. Polat, "Shilling attacks against recommender systems: A comprehensive survey," Artif. Intell. Rev., vol. 42, no. 4, pp. 767–799, Dec. 2014.

[3] D. Jia, C. Zeng, Z. Y. Peng, P. Cheng, Z. M. Yang, and Z. Lu, "A user preference based automatic potential group generation method for social media sharing and recommendation," (in Chinese) Jisuanji Xuebao, vol. 35, no. 11, pp. 2382–2391, Nov. 2012.

4] S. K. Lam and J. Riedl, "Shilling recommender systems for fun and profit," in Proc. 13th Conf. World Wide Web WWW, 2004, pp. 393–402.

[5] B. Mobasher, R. Burke, R. Bhaumik, and J. J. Sandvig, "Attacks and remedies in collaborative recommendation," IEEE Intell. Syst., vol. 22, no. 3,
pp. 56–63, May 2007.

[6] B. Mobasher, R. Burke, R. Bhaumik, and C. Williams, "Toward trustworthy recommender systems: An analysis of attack models and algorithm robustness," ACM Trans. Internet Technol., vol. 7, no. 4, p. 23, Oct. 2007.

[7] C. Williams, B. Mobasher, R. Burke, J. Sandvig, and R. Bhaumik, "Detection of obfuscated attacks in collaborative recommender systems," in Proc. 17th Eur. Conf. Artif. Intell., 2006, pp. 19–23.

[8] X.-F. Su, H.-J. Zeng, and Z. Chen, "Finding group shilling in recommendation system," in Proc. Special Interest Tracks Posters 14th Int. Conf. World Wide Web WWW, 2005, pp. 960–961.

[9] R. Burke, B. Mobasher, C. Williams, and R. Bhaumik, "Classification features for attack detection in collaborative recommender systems," in Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining KDD, 2006, pp. 542–547.

[10] Y. Wang, Z. Wu, J. Cao, and C. Fang, "Towards a tricksy group shilling attack model against recommender systems," in Proc. 8th Int. Conf. Adv. Data Min. Appl., Nanjing, China, 2012, pp. 675–688.

[11] K. Murugesan and J. Zhang, "Hybrid bisect K-Means clustering algorithm," in Proc. Int. Conf. Bus. Comput. Global Informatization, Jul. 2011, pp. 216–219.

[12] C. A. Williams, B. Mobasher, and R. Burke, "Defending recommender systems: Detection of profile injection attacks," Service Oriented Comput. Appl., vol. 1, no. 3, pp. 157–170, Oct. 2007.

[13] W. Zhou, J. Wen, Q. Xiong, M. Gao, and J. Zeng, "SVM-TIA a shilling attack

[14] W. Li, M. Gao, H. Li, Q. Xiong, J. Wen, and B. Ling, “An shilling attack detection algorithm based on popularity degree features,” (in Chinese) Acta Automatica Sinica, vol. 41, no. 9, pp. 1563–1575, Sep. 2015.

[15] B. Mehta and W. Nejdl, “Unsupervised strategies for shilling detection and robust collaborative filtering,” User Model. User-Adapted Interact., vol. 19, nos. 1–2, pp. 65–97.