IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

GROUP SHILLING ATTACKS DETECTION USING BISECTING K-MEANS

[1]B.RAJESHWARI, [2]L.NAVEEN, [3]N.NIKHITHA,[4] MA.NITIN, [5]I.SAIKRISHNA

[1]Assistant Professor in Department of CSE Teegala Krishna Reddy Engineering College

[2,3,4,5] UG Scholars in Department of CSE Teegala Krishna Reddy Engineering College

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

I 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

II LITERATURE SURVEY

Title: Understanding Shilling Attacks and Their Detection Traits:

Author: Corresponding author: Feng Li

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.

Title: Analyzing Online Review Helpfulness Using a Regressional ReliefF-Enhanced Text Mining Method

Author: Thoma s Ngo-Ye

Within the emerging context of Web 2.0 social media, online customer reviews are playing an increasingly important role in disseminating information, facilitating trust, and promoting commerce in the e-marketplace. The sheer volume of customer reviews on the web produces information overload for readers. Developing a system that can automatically identify the most helpful reviews would be valuable to businesses that are interested in gathering informative and meaningful customer feedback. Because the target variable---review helpfulness---is continuous, common feature selection techniques from text classification cannot be applied. In this article, we propose and investigate a text mining model, enhanced using the Regression ReliefF (RReliefF)feature selection method, for predicting the helpfulness of online reviews from Amazon.com. We find that RReliefF significantly outperforms two popular dimension reduction methods. This study is the first to investigate and compare different dimension reduction techniques in the context of applying text regression for predicting online review helpfulness. Another contribution is that our analysis of the keywords selected by RReliefF reveals meaningful feature groupings

Title: A user preference based automatic potential group generation method for social media sharing and recommendation

Author: Da-Wen Jia, Cheng Zeng, Zhi-Yong Peng, Peng Cheng

Social media applications have become the mainstream of Web application. User-oriented and content generated by users are pivotal characteristics of social media sites. Data sharing and recommendation approaches play an important role in dealing with the problem of information overload in social media environment. In this paper, we analyze the flaws of current group-based information sharing mechanism and the common problem of traditional recommender approaches,and then we propose a novel approach of group automatic generating for social media sharing and recommendation. Intuitively, the essential idea of our approach is that we switch user's preference from the media objects to the interest elements which media objects imply. Then we gather the users who have common preference, namely users have the same interestingness in a set of interest elements, together as Common Preference Group (CPG). We also propose a new social media data sharing and recommendation system architecture based on CPG and designs a CPG automatic mining algorithm. By compare our CPG mining algorithm with other algorithm which has similar functionality, it is shown that our algorithm could be applicable to real social media application with massive users.

III 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.

IV PROBLEM STATEMENT

Online recommender systems are widely used to help users discover relevant items such as products, movies, or articles. However, these systems are vulnerable to manipulation by malicious users who engage in shilling attacks. In a shilling attack, a group of users collude to artificially promote or demote items, leading to biased recommendations and reduced system reliability.

Objective

The objective of this project is to develop a method for detecting group shilling attacks in online recommender systems using k-means clustering. The goal is to identify groups of users who exhibit similar suspicious behavior, which may indicate a coordinated shilling attack.

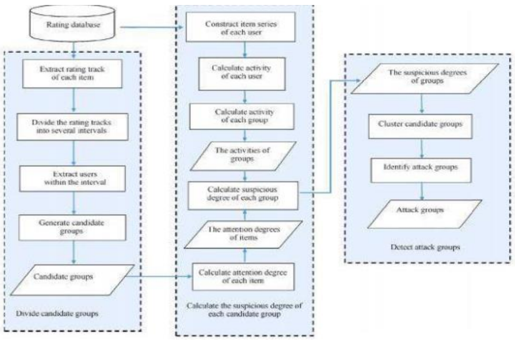
V PROPOSED SYSTEM

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.

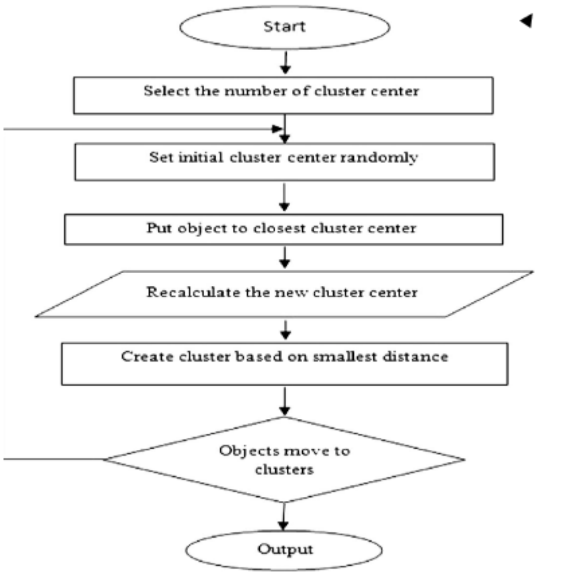
We propose metrics of item attention degree and user activity (UA) to analyze the candidate groups, making the judgment of attack groups more accurate. Based on the divided candidate groups, the item attention degree and the UA for each candidate group are calculated, and the suspicious degrees of these 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.

VI ARCHITECTURE


Rating database
Construct item series of each user
Extract rating track of each item
Calculate activity of each user
The suspicious degrees of groups
Divide the rating tracks into several intervals
Calculate activity of each group
Cluster candidate groups
The activities of groups
Extract users within the interval
Identify attack groups
Calculate suspicious degree of each group
Generate candidate groups
The attention degrees of items
Attack groups
Detect attack groups
Candidate groups
Calculate attention degree of each item
Divide candidate groups
Calculate the suspicious degree of each candidate group

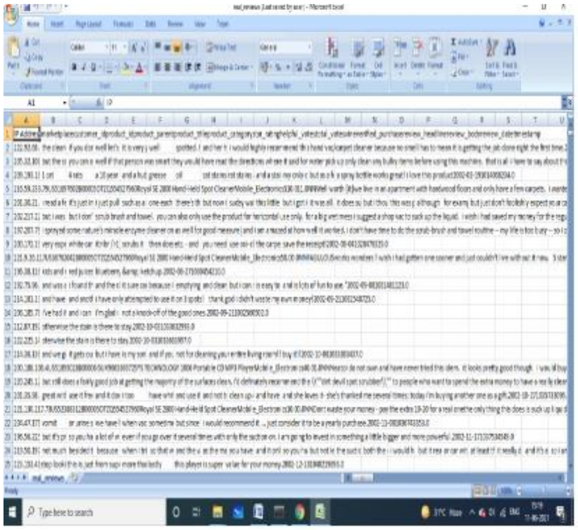
VII IMPLEMENTATION


Start
Select the number of cluster center
Set initial cluster center randomly
Put object to closest cluster center
Recalculate the new cluster center
Create cluster based on smallest distance
Objects move to clusters
Output

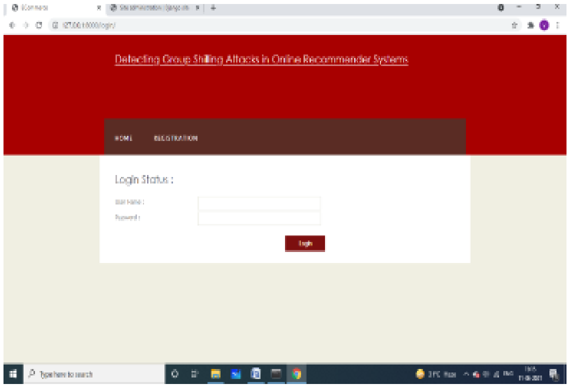
Algorithms When using the bisecting K-means Clustering technique, the starting point is to group all training datasets into a single cluster. In the next step, we split the data into two groups based on which clustering minimizes the segmentation lower bound (the aggregate of absolute residuals). This procedure is repeated until K clusters have been generated. The bisecting K-means algorithm's key operations are outlined below. All previous records will be split in half using the basic K-means method and then added to the existing clustered. After identifying the groupings in the groups or clusters that best reduces the measurement errors, we may split it in half using the fundamental K-means tend to cluster method and then add the halves to the separate cluster. Detecting shilling assaults has been a topic of intense research during the last decade. There are two types of techniques for identifying shilling malicious activities: supervised learning and unsupervised. To categorise attack profiles, supervised approaches (such kNN, C4.5-,and SVM-based classification techniques) first utilise a large number of labelled examples to traina classification model. Zhou et al. introduced anSVM-based two-stage detection approach. To remedy the imbalanced classification scenario, they first used Borderline-SMOTE and produced a preliminary result using support vector machines(SVM). Following that, they used a technique based on the study of targets in order to pin down the perpetrators. To identify shilling assaults, Li et al.modified the ID3 decision tree and used information collected from the item's acceptance degree. When the filler and assault sizes are both low, this strategy is not particularly useful. In order to identify certain forms of shilling assaults, the Aforementioned methods need labeling summary statistics and training a classification model. There have been proposals for unsupervised approaches to help get over the constraints of supervised ones.

Data augmentation (PCA) was utilised to study the similarity structures in attack profiles by Mehta and Nejd. The H-score was used to rank users, and then the desired items were gathered from the top-ranked users. When the target object deviated from the norm after the first two stages, attack profiles

VIII RESULTS



Data Set



Detecting Group Shilling Attacks in Online Recommender Systems

HOME REGISTRATION

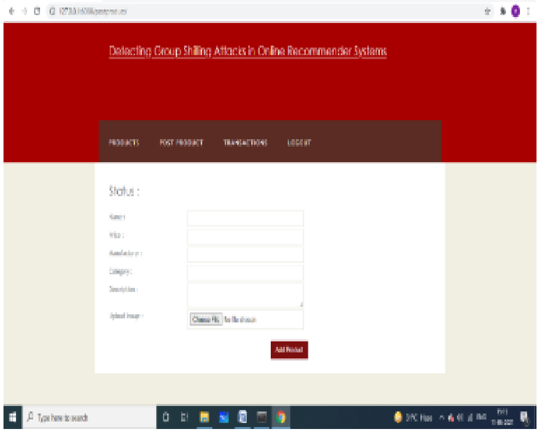
Login Status :

User Name :

Password :

Login

USER Login



Detecting Group Shilling Attacks in Online Recommender Systems

PRODUCTS POST PRODUCT TRANSACTIONS LOGOUT

Status :

Name :

Price :

Manufacturer :

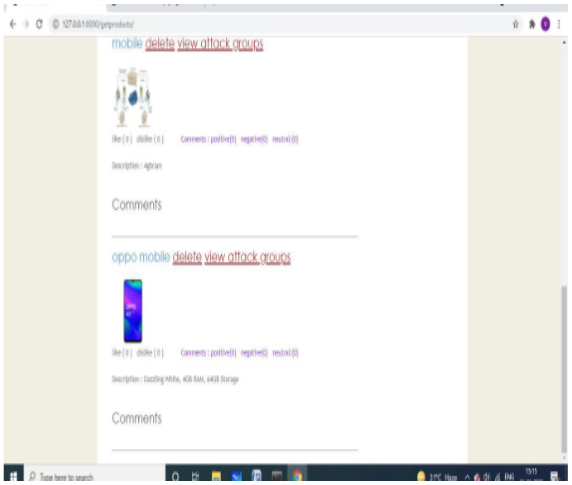
Category :

Description :

Upload Image : Choose File No file chosen

Add Product

Admin



127.0.0.1:8000/getproducts/

mobile delete view attack groups

like (0) dislike (0) Comments : positive(0) negative(0) neutral (0)

Description : 4gbram

Comments

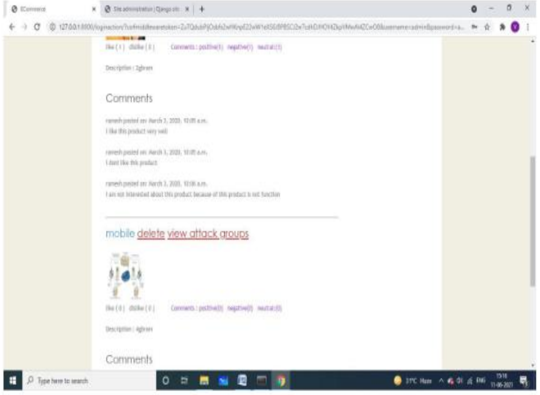
oppo mobile delete view attack groups

like (0) dislike (0) Comments : positive(0) negative(0) neutral (0)

Description : Dazzling White, 4GB RAM, 64GB Storage

Comments

Admin View Products



like (1) dislike (0) Comments : positive(1) negative(1) neutral (1)

Description : 2gbram

Comments

ramesh posted on: March 1, 2020, 10:05 a.m.
I like this product very well

ramesh posted on: March 1, 2020, 10:05 a.m.
I dont like this product

ramesh posted on: March 1, 2020, 10:06 a.m.
I am not interested about this product because of this product is not function

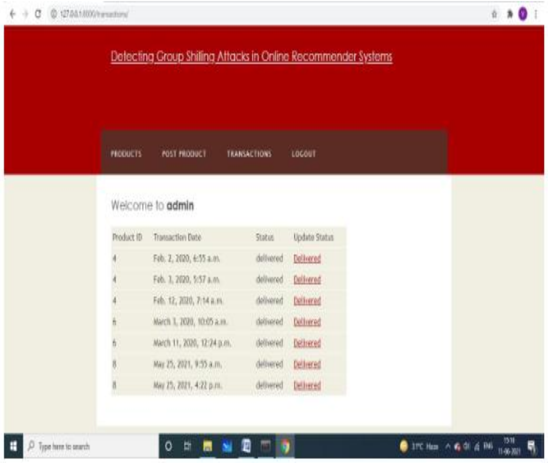
mobile delete view attack groups

like (0) dislike (0) Comments : positive(0) negative(0) neutral (0)

Description : 4gbram

Comments

Admin Manage Products

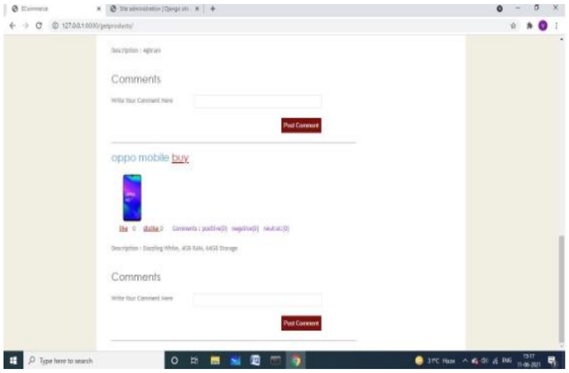


Detecting Group Shilling Attacks in Online Recommender Systems

Welcome to **admin**

Product ID	Transaction Date	Status	Update Status
4	Feb. 2, 2020, 6:55 a.m.	delivered	Delivered
4	Feb. 3, 2020, 5:57 a.m.	delivered	Delivered
4	Feb. 12, 2020, 7:14 a.m.	delivered	Delivered
6	March 3, 2020, 10:05 a.m.	delivered	Delivered
6	March 11, 2020, 12:24 p.m.	delivered	Delivered
8	May 25, 2021, 9:55 a.m.	delivered	Delivered
8	May 25, 2021, 4:22 p.m.	delivered	Delivered

Admin View Transactions



Description : [illegible]

Comments

Write Your Comment Here

oppo mobile buy

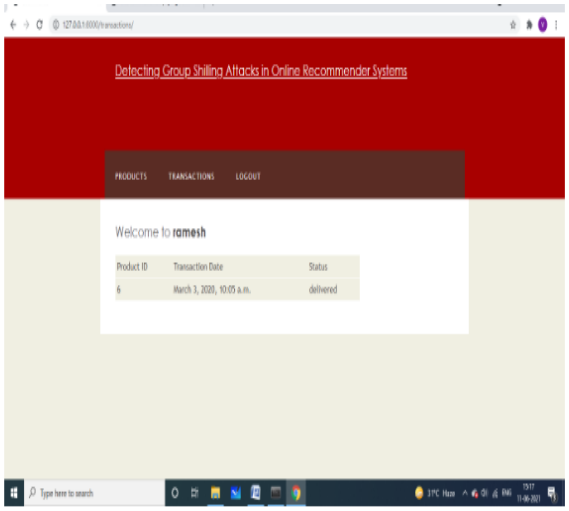
like 0 dislike 0 Comments : positive(0) negative(0) neutral(0)

Description : Dazzling White, 4GB RAM, 64GB Storage

Comments

Write Your Comment Here

User Buy Products

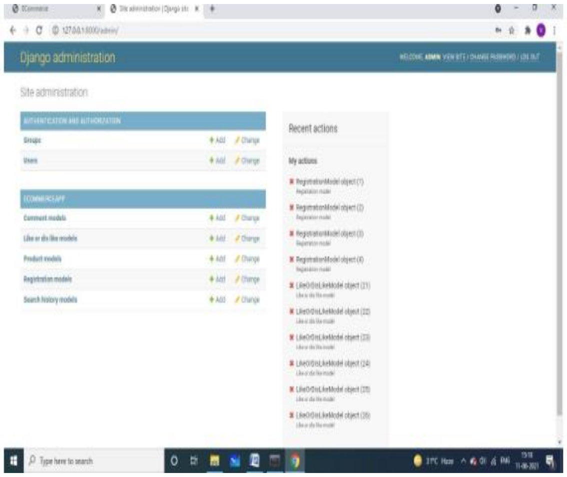


Detecting Group Shilling Attacks in Online Recommender Systems

Welcome to **ramesh**

Product ID	Transaction Date	Status
6	March 3, 2020, 10:05 a.m.	delivered

User Buy Product



Recent actions

My actions

- RegistrationModel object (1) Registration model
- RegistrationModel object (2) Registration model
- RegistrationModel object (3) Registration model
- RegistrationModel object (4) Registration model
- LikeOrDisLikeModel object (21) Like or dis like model
- LikeOrDisLikeModel object (22) Like or dis like model
- LikeOrDisLikeModel object (23) Like or dis like model
- LikeOrDisLikeModel object (24) Like or dis like model
- LikeOrDisLikeModel object (25) Like or dis like model
- LikeOrDisLikeModel object (26) Like or dis like model

Data Base Table

IX 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 coated 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.

REFERENCE

[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] 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.

[3] 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.

[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. 960–961.55

[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 detection method based on SVM and target item analysis in recommender systems,” Neurocomputing, vol. 210, pp. 197–205, Oct. 2016.

[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, Feb.2009