IJETIE

International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

Securing Collaborative Filtering Recommender System Against Profile Injection Attack

Kalaivani.R B.Tech., (M.E).,
Computer science and engineering,
V.P.Muthiahpillai Meenakshi ammal engineering college for women,
Krishnankoil, Viruthunagar (Dist),
Tamilnadu.
kalaigolden@gmail.com

ABSTRACT

Collaborative recommender systems are weak to profile injection attack. Malicious users can inject fake profile into the genuine users rating to collapse the recommender systems output. To reduce this risk many algorithms are used to detect such kinds of attacks. That's while, propose the HHT-SVM (Hilbert Huang Transform and Support Vector Machine). Under HHT-SVM method construct feature extraction to each user in the dataset. In which rating series and Hilbert spectrum to characterize the profile injection attacks.

Keywords

Collaborative filtering recommender system, Hilbert Huang Transform algorithm and SVM.

1. INTRODUCTION

Recommender systems based on collaborative filtering play an increasing role in filtering information in an overloaded information system. They are not only helping users find relevant items, but are also beneficial to companies producing items by increasing both selling rate and cross-sales. The most collaborative filtering algorithms are based on following types,

1. ***User-based*** algorithms build for each user a neighborhood of users with similar opinions (i.e., ratings) in the system. Ratings from these users are then employed to generate recommendations for the target user.
2. ***Item-based*** algorithms compute a set of similar items for each item and use these similarities to compute recommendations.

Good ratings promise a good selling rate, these systems are prone to manipulation from producers or malicious users. Fake user can highly rate their own items and give low rating to their opponent items. This attack called the shilling attack. Shilling attack consists of push or nuke attack. Attacks on recommender system can affect the quality of the recommendation and reducing the satisfaction to the user.

1.2 Attack models

An attack model is an approach for attackers to construct a set of attack profiles based on the knowledge about the recommender system's rating database, products, users, and so on.

^{I}S			^{I}F			$^{I}\varnothing$			I_t
$^{i}S,1$	…	$^{i}S,l$	$^{i}F,1$	…	$^{i}F,p$	$^{i}\varnothing,1$	…	$^{i}\varnothing,q$	i_t
$\alpha(i_{S,1})$	…	$\alpha(i_{S,l})$	$\chi(i_{F,1})$	…	$\chi(i_{F,p})$	$\perp$	…	$\perp$	$\beta(i_t)$

Fig.1 The general form of an attack profile.

- I_S is the set of selected items.
- I_F is the set of filler items usually chosen randomly.

COPYRIGHT TO IJETIE

- I_t is the set of target items.
- $I_Ø$ is the set of unrated items.

1.3. Attack types

Random attack

All item ratings of the injected profile (except the target item rating, of course) are filled with random values drawn from a normal distribution that is determined by the mean rating value and the standard deviation of all ratings in the database.

Average attack

The average rating per item is used to determine the rating values for the profile to be injected.

Bandwagon attack

Inject profiles that - besides the high or low rating for the target items - contain only high rating values for very popular selected items and random values to some filler items.

Segment attack

Inject profiles with positive ratings for similar items (belong to the same category or segment), e.g., fancy books, and low ratings for filler items.

Reverse bandwagon

Reverse Bandwagon attack defines the target item is associated with other items that are disliked by many people. The selected item set is filled with minimum ratings.

Love/hate attack

Love/hate attack defines the minimum value is given to the target item and the highest possible rating value is given to the filler items. The serious effect on systems' recommendation is to nuke an item.

2. EXISTING SYSTEM

The existing system investigated the use of statistical metrics for detecting patterns of shilling attackers in a recommender system. Collaborative filtering techniques have been successfully employed in recommender systems in order to help users deal with information overload by making high quality personalized recommendations. The algorithm can be employed for monitoring user ratings and removing shilling attacker profiles from the process of computing recommendations. The existing system based on User-based collaborative filtering. The most popular collaborative filtering algorithm is the kNN-based algorithm. An algorithm computes, the probability of a user to be a shilling attacker by studying the rating patterns within the system, namely exploiting the RDMA and Average Similarity metrics. The various evaluation and detection metrics are used to predict the recommendations.

K Nearest Neighbor (KNN) Algorithm

The item-based K-nearest neighbor (KNN) algorithm used to find similarity between items i and j:

$$sim(i,j) = corr_{i,j} = \frac{\sum_{u\in U}(R_{u,i} - \bar{R}_i)(R_{u,j} - \bar{R}_j)}{\sqrt{\sum_{u\in U}(R_{u,i} - \bar{R}_i)^2}\sqrt{\sum_{u\in U}(R_{u,j} - \bar{R}_j)^2}}.$$

Where R(u,i) = rating of user u on item i.
R(i) = average ratings of item.

Adjusted Cosine Similarity (user-based) – each pair in the co-rated set corresponds to a different user.

$$sim(i,j) = \frac{\sum_{u\in U}(R_{u,i} - \bar{R}_u)(R_{u,j} - \bar{R}_u)}{\sqrt{\sum_{u\in U}(R_{u,i} - \bar{R}_u)^2}\sqrt{\sum_{u\in U}(R_{u,j} - \bar{R}_u)^2}}$$

Where R(u,i) = rating of user u on item i.
R(u) = average of the user.

3. PROPOSED SYSTEM

One of the main strengths of collaborative recommender systems is the ability for users with unusual tastes to get meaningful suggestions by the system identifying users with similar peculiarities. It is one of the challenges in securing recommender systems.

Fig.2. illustrates HHT-SVM method works in feature extraction and detection of profile injection attack presents in the recommender system. In feature

COPYRIGHT TO IJETIE

extraction HHT method extract the features of each user profile in the dataset.

In detection phase consists of test set and training set. When inserting the new user, find similarity between new user and existing user in the test set. SVM classifier used to detect the fake user in user profile.

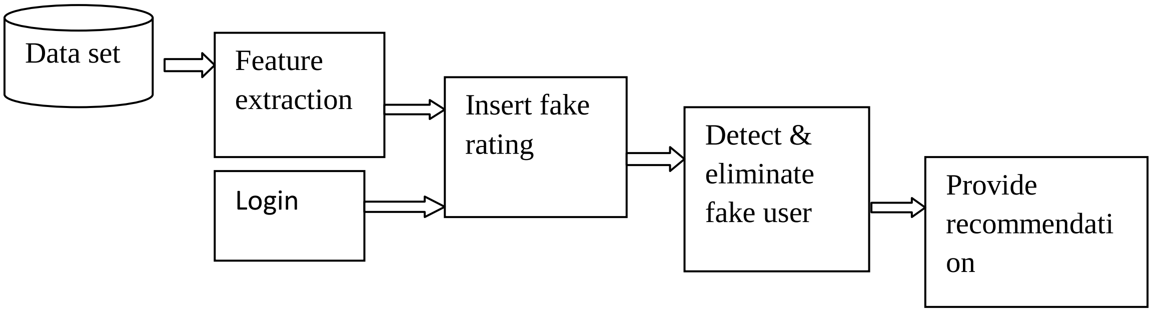

Fig.2. HHT-SVM framework

3.1. Algorithm

HHT (Hilbert Huang Transform)

This algorithm used to produce rating series for feature extraction of user profile. These rating series are based on the features of individual user in the user profile. This method can decompose any time varying signal into its fundamental intrinsic oscillatory modes with the so-called empirical mode decomposition (EMD). Using the Hilbert transformation to any of these disintegrated intrinsic mode functions (IMF) subsequently provides the Hilbert spectrum with significant instantaneous frequencies.

HHT method used to analyze the rating of an individual user profile. IMF to extract the ratings of the genuine user as well as attackers in the data set.

$$y(t) = \frac{1}{\pi} p \int_{-\infty}^{\infty} \frac{x(\tau)}{t-\tau} d\tau$$

Where p is indicates Cauchy principal value.

SVM (Support Vector Machine)

The “traditional” approach to developing the mathematics of SVM is to start with the concepts of *separating hyperplanes* and *margin*.

The hypothesis is usually developed in a linear space, beginning with the idea of a perception, a linear hyperplane that separates the positive and the negative examples.

$$f(x) = \text{sign}(w \cdot x).$$

w represents the normal vector to the hyperplane separating the classes.

We define the boundaries of the margin by (w, x) = ±1.

4. PROCEDURE

4.1. Feature extraction

Feature extraction held in offline. The novelty and popularity of items are to construct rating series for user profiles, and HHT to transform the rating series in order to extract HHT-based features. The novelty of an item refers to the degree to which it is unusual with respect to the user’s normal tastes. Generate the amplitude, phase and instantaneous frequency by using the HHT on the first IMF. And generate the feature vector.

4.2. Give fake rating

MovieLens dataset consists of 1,000,209 ratings on 3952 movies by 6050 users. Ratings are between1-5(1-lowest &5- highest). Genuine profile in dataset based on its filler size. If filler size increases the genuine user profile will be reduced. By Inserting attackers, they may use same are similar filler sizes as genuine users do. In Collaborative recommender system, genuine users only rate a small no. of items. Attacker use features of the genuine users and give ratings to the target item.

4.3. Detect and eliminate fake user

The user profile consists of genuine user as well as attacker. To find whether the present user is genuine or attacker by using SVM detection method.SVM method separating the user profiles based on their ratings given to an item. By the classification, the uncorrelated user might be neglected.

SVM also be a machine learning algorithm to detect profile injection attack. Based on the filler will increase the number of genuine user will be decrease in level. To gradually varying the filler sizes (1%, 3%, 5%, and 10%) calculate the genuine user level at each filler size.

4.4. Provide recommendation

To provide recommendation, the similarity and prediction will be calculated for each user in the user data set. Recommender system provides recommendations based on prediction metrics.

By the result of fake user elimination, the user data set contains only the genuine user profiles. So recommender system will provide good recommendation also satisfaction.

5. CONCLUSION

Collaborative RSs are vulnerable to profile injection attacks, in which cruel kind of users insert fake profiles to the rating db in order to biasing the systems output. The purpose of this injection is promote or demotes products. This issue generates poor recommendation to the users or customers. To overcome the problem first fake profile is identified and eliminates them out to produce good recommendation for the user. In this phase, we used movieLens datasets for feature extraction. Feature extraction is based on the user behavior, genre, etc…

Propose HHT-SVM method to detect profile injection attacks by combining Hilbert Huang Transform and Support Vector Machine. The attackers will be eliminated from system. After that we are getting the genuine user profiles. Then calculate similarities and predictions with other users. Finally, generate the good recommendation to users or customers.

6. REFERENCES

[1] Fuzhi Zhang, Quanqiang Zhou, HHT-SVM: An online method for detecting profile injection attacks in collaborative recommender systems, journal Knowledge-Based System, vol no 65, pp 96-105, 2014.

[2] R. Burke, B. Mobasher, R. Bhaumik, Limited knowledge shilling attacks in collaborative filtering systems, in: Proceedings of Workshop on Intelligent Techniques for Web Personalization, 2005.

[3] P.A. Chirita, W. Nejdl, C. Zamfir, Preventing shilling attacks in online recommender systems, in: Proceedings of the 7th Annual ACM International Workshop on Web Information and Data Management, pp. 67–74, 2005.

COPYRIGHT TO IJETIE

[4] R. Burke, B. Mobasher, C. Williams, R. Bhaumik, Detecting profile injection attacks in collaborative recommender systems, in: Proceedings of the 8th IEEE International Conference on E-Commerce Technology and the 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and EServices, 2006.

[5] K. Bryan, M. O’Mahony, P. Cunningham, Unsupervised retrieval of attack profiles in collaborative recommender systems, in: Proceedings of the 2nd ACM International Conference on Recommender Systems, pp. 155–162, 2008.

[6] Zhang xL, Lee TMP, Pitsilis G.”Securing recommender systems against shilling attacks using social-based clustering” Journal of computer science & technology, vol no 28, pp 616-624, 2013.