International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Online rating malicious user identification and calculating original score using detective TATA

N.D.Sowmiya[1], S.Santhi[2]
[1]PG student, Department of computer science and engineering, Valliammai engineering college, Chennai.

[2]Assistant Professor, Department of computer science and engineering, Valliammai engineering college, Chennai.

Abstract- *With the evaluating development of reputation systems (rating system) in various online social networks, administrations against such systems are evolving rapidly. In this paper, we propose scheme detective TATA, the acronym of joint Temporal and Trust Analysis, which guards reputation systems from a new angle: the blend of time domain anomaly detection and Dempster Shafer theory based trust computation. Original all user attack data collected from a cyber-competition is used to build the testing data set. Compared with two illustrative reputation schemes and our earlier scheme, detective TATA achieves a significantly better performance in terms of detecting items under attack, detecting malicious users who insert dishonest ratings, and recuperating reputation scores.*

Keywords*: Detective TATA (Temporal and Trust Analysis), Change detector, Dempster-Shafer theory.*

1. INTRODUCTION

As millions of people use the Internet for entertainment, education, building personal relationships, and conducting businesses the Internet has created more opportunities for online processing and accessing. Network security defines about the policies should to be prevent and monitor unauthorized access, misuse of data, modification, or condition of a computer network and network-accessibility of resources. Network security involves the authorization of accessing of data in a network, which is maintained by the network admin(administrator).

Users choose are assigned with an user ID and password or other authenticating information that allows accessing to information and programs within their authority condition. Network security defines both varieties of public and private computer networks that are used in everyday jobs and in every work; processing of conducting transactions and communications among different departments they are businesses, government agencies and individuals. Networks can be private, when such as within a system and others which may be open to public access of data. Network security is involved in the organizations, enterprises, and o institutions. Securing the network, protecting and overseeing operations being done correctly are measuring. The most common way of protective a network resource is by handover it a unique name value and a with password.The goal line is to create more virtual word-of-mouth networks where every person's share opinions and experiences, in terms of reviews and ratings, on different items, including yields, facilities, digital contents and even hacker or malicious people. The molecular results are called reputation score or rating score. Such systems are also referred to as feedback or online based reputation systems.

Online reputation systems more people interest online purchasing decisions. We propose a reputation defence scheme, named detective TATA, for feedback-based reputation systems. Here, detective TATA is the abbreviation of joint Temporal and Trust Analysis. It covers 2 modules: a time domain anomaly detector and a trust model based on the Dempster–Shafer theory. Specifically, we consider the ratings to a given item as a time sequence and a time domain irregularity detector is introduced to detect disbelieving time intervals where anomaly occurs. A trust analysis is then conducted based on the irregularity detection results. We borrow the concept of user behaviour uncertainty from the Dempster–Shafer theory to model users' behaviour patterns.

2. PROBLEM STATEMENT

The problem is how the online participants protect themselves by declaring the quality of strangers or unknown items beforehand. To address this problem, online reputation systems have been built up. To evaluate a reputation system, the researchers need data representing malicious attacks. Thus, the more of realistic attack data can injure the performance evaluation.

To address this problem, online reputation systems have been built up. The aim is to make large-scale virtual word-of-mouth networks where persons share feelings and practices, in terms of reviews and ratings, on various items, including products, services, digital contents and even other people. The problem is how the online participants protect themselves by judging the quality of strangers or unknown items beforehand. To address these problems, online reputation systems have been built

up. To evaluate a reputation system, the researchers need data on behalf of malicious attacks.

3. RELATED WORK

As diverse actions against reputation systems appear and develop quickly, defense schemes caring reputation systems are also evolving consequently. In this section, we unevenly divide them into 4 categories.

3.1 LIMIT THE MAXIMUM NUMBER OF RATING

The defense approaches limit or reduce the maximum number of ratings each user could provide within certain time duration.

3.2 INCREASE THE COST OF LAUNCHING AN ATTACK

The defense schemes aim to increase the cost of launching an attack. This method can effectively increase the cost to manipulate competitors' item reputation.

3.3 THE DEFENSE APPROACHES INVESTIGATE RATING STATISTICS

The defense approaches examine rating statistics. They consider ratings as haphazard variables and assume untruthful ratings have statistical distributions different from other normal ratings. Representative schemes are as follows. A Beta-function based approach assumes that the fundamental ratings follow Beta distribution and considers the ratings outside (lower) and (upper) quantile of the mass's opinions as dishonest ratings.

3.4 INVESTIGATE USERS RATING BEHAVIORS

Iteration refinement approach proposed in assigns weights to a user's ratings according to the inverse of this user's rating variance. In a personalized trust structure is introduced so that different users may assign different trust values to the same user. In a user's trust is obtained by accumulating neighbours' beliefs through belief theory. Iteration refinement approach proposed in assigns weights to a user's ratings according to the inverse of this user's rating variance.

3.5 TEMPORAL AND TRUST ANALYSIS

In this work, we propose a reputation defense scheme, detective TATA. The objective of the proposed scheme is to detect the malicious users who provide dishonest ratings; recover reputation score of the target item that receives dishonest ratings; avoid interference to normal items' reputation scores. Detective TATA detects dishonest ratings from a new angle: investigating time domain information.

4. PROPOSED SYSTEM

The ORS approaches define the time factors in two ways. In the first way, taking the all rating equally and ignore the time when rating is provided. In the second way, recent ratings are taken as larger rating score. The TATA (*Temporal and Trust Analysis)* a is used to detect anomaly and malicious actives from a new way: analysing and finding time domain information. Specifically, organizing the ratings to a given item as a sequence in the descending order according to the time when they are provided.

When any changes is made in the actives indication is made and passed, such changes is defined as anomaly detection, which takes the rating sequences as inputs and detects changes occurring in the rating sequences. The change detector only measure the sudden rapid changes also measure and all the changes will be calculated and measurement identification of original data is identified.

In this way, even if when the malicious user insert the dishonest rating with small shift of value is defined as mislead items' all the changes detected identified and find the original reputation score the items or product, finally be detected by the change detector. The advantages are

- Detects the malicious users who provide dishonest ratings.
- Recover reputation score of the target item that receives dishonest ratings.
- Avoid interference to normal items' reputation scores.

A. Temporal Analysis - Change Detector

In the temporal analysis, defines the rating given to the item and arranging the given rating score in the descending order affording to time when the rating is provided. In many of the rating system or reputation system, normal rating calculation is made so original score cannot be detected so by using CUSUM detector anomaly person is defined by using the cumulative sum, which is used to find the abnormal users and changes occurs in the rating sequences.

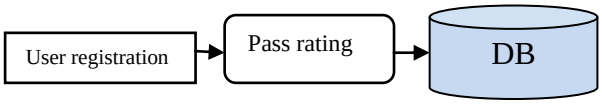

Figure 1.shows temporal analysis

B. Trust Model Based On the Time Domain Anomaly Detection

Anomaly detection result stored in the database is evaluated to get the original score items. Trust models finder based upon the bad and good behaviors of the users whom they are providing the rating for the items but also it is not a sufficient thing to malicious user. Calculation scenarios First, user *A* has conducted 5 good behaviors and 5 bad behaviors. Second, user *B* is a new coming user and has no behavior history. In several trust models both of their trust values will be calculated as 0.5, although there are more confident in user *A*'s trust value. To differentiate these two cases, the concept of behavior uncertainty is introduced by the Dempster-Shafer theory, to represent the degree of the ignorance of behavior history. In this work, the behavior uncertainty is adopted to introduce a trust model based on the Dempster-Shafer theory.

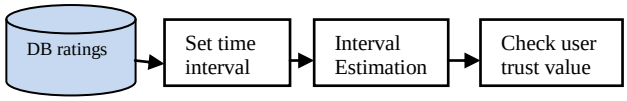

Figure 2. A trust model based on the Dempster-Shafer theory

C. Trust Model Using the Dempster-Shafer Theory

On the anomaly detector, for each given item, it determines which ratings are suspicious. The user's behavior value is defined on a single item as a binary value to indicate whether his/her rating behavior is good or bad it is said to be behavior value. The user's behavior value is defined on a multiple item it is said to be combined behavior value. It is to detect the malicious user and recover the reputation scores.

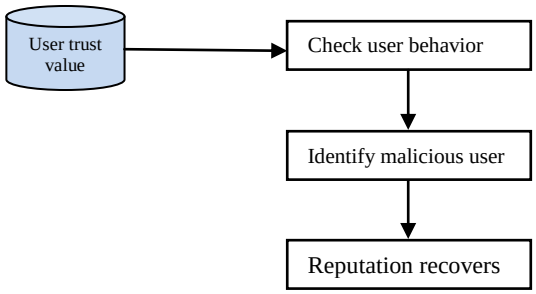

Figure 3. Recovering Reputation Scores.

5. PROJECT DESCRIPTION

5.1 CHANGE DETECTOR

Propose a change detector in DETECTIVE TATA as the anomaly detector, which takes the rating sequences as inputs and detects changes occurring in the rating sequences. The proposed change detector will detect not only sudden rapid changes but also small changes accumulated over time. In this way, even if malicious users insert dishonest ratings with small shifts to gradually mislead items' reputation scores, such type of changes will still be accumulated and finally be detected by the proposed change detector.

5.2 INTERVAL ESTIMATION

The ratings to a given item as a time sequence, and a time domain anomaly detector is introduced to detect suspicious time intervals where anomaly occurs. The change detector is triggered by an item; the time intervals in which the changes occur are called change intervals. We consider the ratings to a given item as a time sequence, and a time domain anomaly detector is introduced to detect suspicious time intervals where anomaly occurs.

5.3 TRUST ANALYSIS MODULE

Instead of assigning a user with an overall trust value, the proposed trust model evaluates each user's reliability on different items separately. It can reduce the damage from the malicious users who aim to accumulate high trust values by providing "spare ratings" to uninterested items.

5.4 MALICIOUS USERS IDENTIFICATION

We define users who provide ratings during the detected change intervals as suspicious users. Not all suspicious users are malicious users because normal users may occasionally provide "biased ratings" due to personal reasons or even human errors. Therefore, we propose to further differentiate normal users from malicious users by trust analysis. The users with low trust values will be identified as malicious users and their ratings to the detected target items will be removed. The remaining ratings are used to calculate the item reputation.detective TATA achieves a significantly better performance in terms of identifying items under attack, detecting malicious users who insert dishonest ratings, and recovering reputation scores.

For example, some malicious users may directly provide dishonest ratings to the target item, while some others may accumulate high trust values to assist the former malicious users and at the same time, keep themselves hidden. Assume that detective TATA is tested against attack profiles. Let denote the number of profiles, for which detective TATA

accurately detects as the target item. Then, the detection rate is defined as. Let denote the total number of items that are not under attack but detected as target items. Then, the false alarm rate is calculated as.

5.5 RECOVERED REPUTATION OFFSET OF THE TARGET ITEM

The detection rate of malicious users cannot fully describe the performance of Detective TATA. Obviously, the amount of damage caused by different malicious users can be very different. We care more about whether the undetected malicious users can cause large damage to the final reputation scores. We consider the ratings to a given item as a time sequence, and a time domain anomaly detector is introduced to detect suspicious time intervals where anomaly occurs.

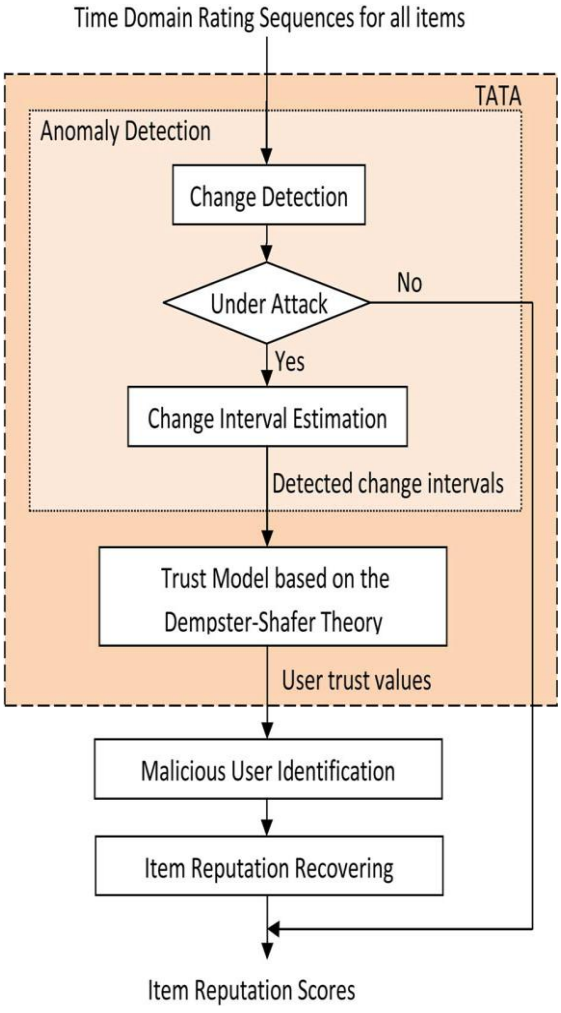

Figure 4.System architecture

6. OUTPUT SCREENSHOT

Figure5.home page

Description

The home page of online reputation system.

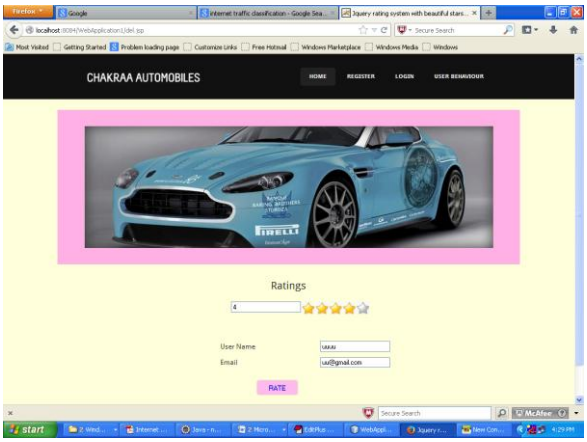

Figure 6.user rating page

Description

This shows the user rating page for the company.

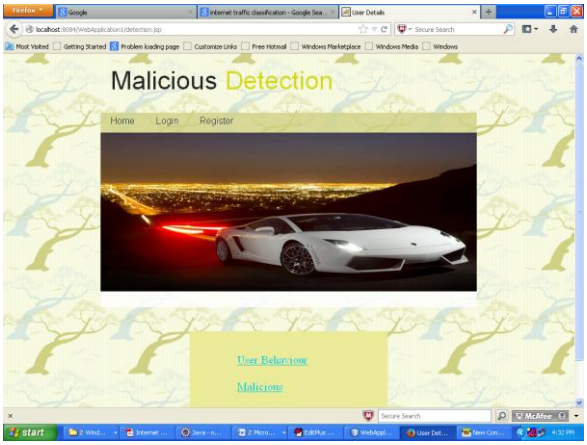

Figure 7.malicious detection page

Description

This shows the malicious detection page and it consist of user behavior and malicious user.

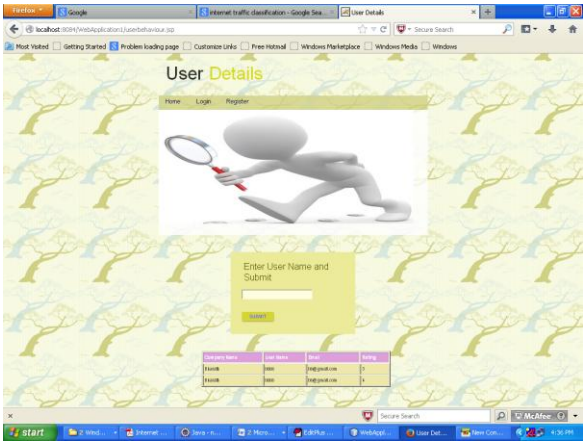

Figure 8.user rating details

Description

This shows the user rating and information.

7. FUTURE WORK

When the number of malicious users is not very large, examining individual user's behaviour (such as through a well-designed trust model in this paper) is a very effective defense approach. When the number of malicious users is very large, investigating user behaviour similarity (such as in the TAUCA scheme) becomes a promising method. In the future, one possibility is to jointly consider trust evaluation and user correlation.

8. CONCLUSION

In this paper, a comprehensive anomaly detection scheme, detective TATA, is designed and evaluated for protecting feedback-based online reputation systems. To analyse the time-domain information, a revised-CUSUM detector is developed to detect change intervals. To reduce false alarms, a trust model based on the Dempster–Shafer theory is proposed. Compared with the IR and the Beta model methods, detective TATA achieves similar RRO values, which represent items' reputation distortion, but much higher detection rate in malicious user detection. For different attacks, the detection rate of detective TATA is 0.87 0.99, whereas IR fails to detect malicious users and Beta model achieves 0.37 0.72 detection rate. Compared with our previous scheme TAUCA, which investigates user correlation, detective TATA achieves a much smaller and more stable RRO values of all items, indicating a small interference on normal items.

REFERENCES

[1] Press Release: *"Online Consumer-Generated Reviews Have SignificantImpact on Offline Purchase Behaviour"*, Nov. 2007 [Online].

[2] R. Lee and H. Paul, "*Use of Online Rating Systems*" Oct. 20, 2004 [Online].

[3] "*ComScore, Final Pre-Christmas Push Propels U.S. Online Holiday Season Spending"* Through December 26 to Record $30.8 Billion Dec. 29, 2010[Online].

[4] "*Buy iTunes Ratings and Comments—Increase iTunes Sales and Downloads [Online]"*.

[5] A. Whitby, A. Jøsang, and J. Indulska, "*Filtering out unfair ratings in Bayesian reputation systems*," Icfain J. Manage. Res., vol. 4, no. 2, pp.48–64, Feb. 2005.

[6] P. Laureti, L. Moret, Y.-C. Zhang and Y.-K. Yu, "*Information filtering via iterative refinement*," *Europhys. Lett.* vol. 75, no. 6, pp. 1006–1012, 2006.

[7] Y. Liu and Y. Sun, "*Anomaly detection in feedback-based reputation systems through temporal and correlation analysis*," in *Proc. 2nd IEEE Int. Conf. Social Computing*, Aug. 2010, pp. 65–72.

[8] Y. Yang, Q. Feng, Y. Sun, and Y. Dai, "*Reputation trap: A powerful attack on reputation system of file sharing p2p environment*," in *Proc.4th Int. Conf. Security and Privacy in Communication Networks*, Istanbul, Turkey, Sep. 2008.

[9] M. Abadi, M. Burrows, B. Lampson, and G. Plotkin, "*A calculus for access control in distributed systems*," *ACM Trans. Program. Lang.Syst.*, vol. 15, no. 4, pp. 706–734, 1993.

[10] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: Defending against Sybil attacks via social networks," in *Proc. 2006 Conf. Applications, Technologies, Architectures, and Protocols for Computer Communications*, 200
6, pp. 267–278.