International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 3 Issue: 1 26-Jun-2014,ISSN_NO: 2321-3337

Reputation Management using Trust based Decision making System through Temporal and correlation analysis

V.Raja Gopal[1]*,S.Sumathi*[2] *,*

Asst.Professor, Dept of Information Technology, Sri Krishna Engineering College, India[1].
Asst.Professor, Dept of Information Technology, Sri Krishna Engineering College, India[2].

.

ABSTRACT— *With the rapid development of reputation systems in various online social networks, manipulations against such systems are evolving quickly. In this paper, we propose scheme TATA, the abbreviation of joint Temporal and Trust Analysis, which protects reputation systems from a new angle: the combination of time domain anomaly detection and Dempster–Shafer theory-based trust computation. Real user attack data collected from a cyber-competition is used to construct the testing data set. Compared with two representative reputation schemes and our previous scheme, TATA achieves a significantly better performance in terms of identifying items under attack, detecting malicious users who insert dishonest ratings, and recovering reputation scores.*

Keywords: TATA (TemporalAndTrustAnalysis), Change detector, Dempster-Shafer theory

1. INTRODUCTION

As more people use the Internet for entertainment, building personal relationships, and conducting businesses the Internet has created vast opportunities for online interactions. However, due to the anonymity of the Internet, it is very difficult for normal users to evaluate a stranger's Trustworthiness and quality, which makes online interactions risky. To address this problem, online reputation systems have been built up. The goal is to create large-scale virtual word-of-mouth networks where individuals share opinions and experiences, in terms of reviews and ratings, on various items, including products, services, digital contents and even other people. These opinions and experiences, which are called users' feedback, are collected as evidence, and are analysed, aggregated, and disseminated to general users.

The disseminated results are called reputation score. Such systems are also referred to as feedback based reputation systems. Online reputation systems are increasingly influencing people's online purchasing decisions. For example, according to comScore Inc., products or services with a 5-star rating could earn 20% more than products or services with a 4-Star rating could. More and more people refer to yelp rating system before selecting hotels to Amazon product ratings before purchasing products online; to video ratings before viewing a video clip etc. Furthermore, a recent survey indicates that around 26% of adult Internet users in the U.S. have rated at least one item through online reputation systems.

2. PROBLEM STATEMENT

The problem is how the online participants protect themselves by judging the quality of strangers or unfamiliar items before hand. To address this problem, online reputation systems have been built up. To evaluate a reputation system, the researchers need data representing malicious attacks. However, it is extremely difficult to obtain attack data from real systems mainly because there is no ground truth indicating whether particular ratings are from attackers or not. The real human users can create multifaceted, coordinated, and sophisticated attacks that are not well understood yet. Thus, the lack of realistic attack data can hurt the performance evaluation.

3. RELATED WORK

As diverse manipulations against reputation systems appear and develop rapidly, defense schemes protecting reputation systems are also evolving accordingly. In this section, we roughly divide them into four categories.

3.1 Limit the maximum number of rating

The defense approaches limit the maximum number of ratings each user could provide within certain time duration. Such type of approaches actually restricts the rating power of each user ID this can prevent the attackers from inserting a large amount of dishonest ratings through a few user IDs within a short time.

3.2 Increase the cost of launching an attack

In the second category, the defense schemes aim to increase the cost of launching an attack. Some reputation systems in practice, such as Amazon, assign higher weights to users who commit real transactions. This method can effectively increase the cost to manipulate competitors' item reputation.

3.3 The defense approaches investigate rating statistics

In the third category, the defense approaches investigate rating statistics. They consider ratings as random variables and assume dishonest ratings have statistical distributions different from normal ratings. Representative schemes are as follows. A Beta-function based approach assumes that the underlying ratings follow Beta distribution and considers the ratings outside (lower) and (upper) quantile of the majority's opinions as dishonest ratings.

3.4 Investigate users rating behaviours

The defense approaches in the fourth category investigate users' rating behaviors. Assuming that users with bad rating history tend to provide dishonest ratings, such approaches determine the weight of a rating based on the reputation of the user who provides this rating. Such reputation is also referred to as trust or reliability. Several representative schemes are as follows.

3.5 Some of limitation in protecting reputation system

Although many schemes have demonstrated very good performance in protecting reputation systems, there are still limitations that are not fully addressed. First, time domain, which contains rich information, is not fully exploited. The current approaches address the time factors in two ways. In the first way, all the ratings are treated equally and the time when these ratings are provided is ignored. In the second way, recent ratings are given larger weights when computing the reputation scores. These simple approaches neglect the great potential of investigating time-domain information.

3.6 Temporal and trust analysis

In this work, we propose a reputation defense scheme, 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.Specifically, TATA is a combination of an anomaly detector, which belongs to the third category, and a Dempster–Shafer theory based trust model, which belongs to the fourth category.

4. PROJECT DESCRIPTION

4.1 Change Detector

Propose a change detector in 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.

4.2 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.

4.3 Trust Analysis

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. Furthermore, based on the Dempster–Shafer theory, the proposed trust model introduces user behavior uncertainty.

4.4 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. 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.

4.5 Recovered reputation offset of the target item

The detection rate of malicious users cannot fully describe the performance of TATA. Obviously, the amount of damage caused by different malicious users can be very different.

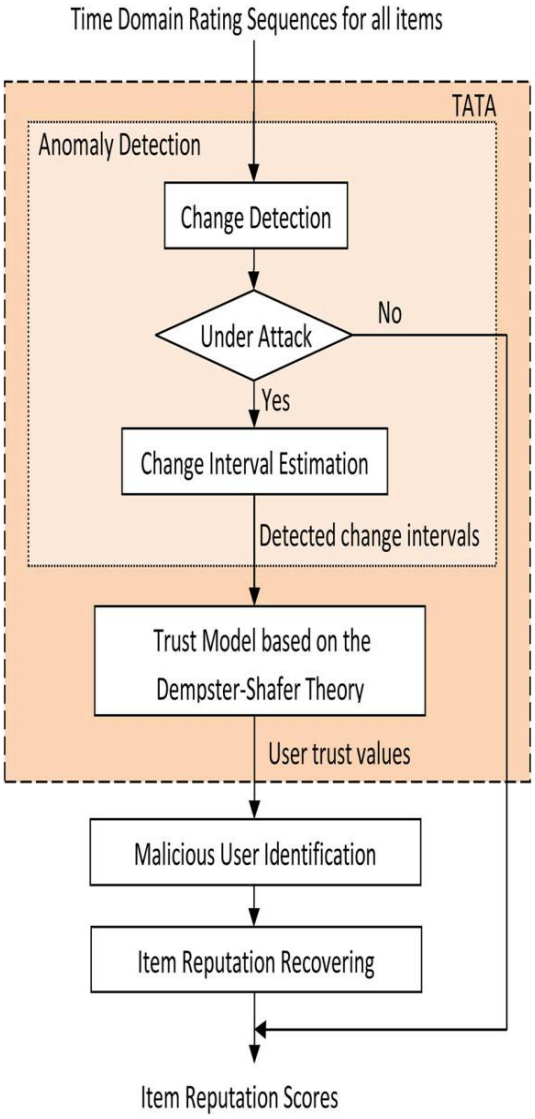

Figure 1.System architecture.

5. CONCULSION AND FUTUREWORK

In this paper, a comprehensive anomaly detection scheme, 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, TATA achieves similar RRO values, which represent items' reputation distortion, but much higher detection rate in malicious user detection.

REFERENCES

[1]. Press Release: "Online Consumer-Generated Reviews Have Significant Impact on Offline Purchase Behaviour", Nov. 2007 [Online]. Available: http://www.comscore.com/press/release.asp?press=1928

[2]. R. Lee and H. Paul, "Use of Online Rating Systems" Oct. 20, 2004 [Online]. Available:http://www.pewinternet.org/Reports/2004/Use-of-Online-Rating-sytems.aspx

[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].Available:http://ir.comscore.com/releasedetail.cfm?ReleaseID=539354

[4]. "Buy iTunes Ratings and Comments—Increase iTunes Sales and Downloads [Online]". Available: http://www.youtube.com/watch?v=TWV4XaxCo

BIOGRAPHY

Mr.V.Raja gopal M.E., works as an Assistant Professor in Department of Information Technology at Sri Krishna Engineering College. He has 3 years of teaching experiences in various Engineering Colleges. He has presented in 2 National Conferences.

Mrs.S.Sumathi M.E., works as an Assistant Professor in Department of Information Technology at Sri Krishna Engineering College. She has 4 Years of experience in teaching and 2 years of experience in various companies. She has presented papers in 1 International conference and 5 National Conferences.