International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 5 1214– 1219

Reputation Management using Trust Based Decision Making System through Temporal and Correlation Analysis

Dr. S. Jabeen Begum,
Associate Professor & Head/ IT,
Velalar College of Engineering and Technology, Erode – 638012,
Tamilnadu, India.
e-mail : sjabeenbegum@gmail.com

Mr. G. Rajesh Kumar
Assistant Professor (Sr.Gr.)
Velalar College of Engineering and Technology, Erode – 638012,
Tamilnadu, India.
e-mail:grajesh.grk@gmail.com

R. Varanambigai
IT Final Year IT Student,
Velalar College of Engineering and Technology, Erode – 638012,
Tamilnadu, India.

***Abstract*—** With the rapid development of online reputation systems in various online social networks, manipulations against such online reputation systems are evolving quickly. 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. TATA, the abbreviation of joint Temporal And Trust Analysis, which protects online reputation systems from a new angle: the combination of time domain anomaly detection and Dempster–Shafer theory-based trust computation. The problem is how the online participants protect themselves by judging the quality of strangers or unfamiliar items beforehand. To address this problem, Online Reputation System (ORS) 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.

Keywords-*component; formatting; style; styling; insert (key words)*

*****

I. INTRODUCTION

The Internet has been very beneficial to daily life by providing vast information and convenient services. For instance, electronic mail reduces the message sending time and makes communication much easier. Online shopping makes it possible to purchase at home. Search engines can get the relevant information immediately. Moreover, the Internet has enabled the proliferation of online business and interpersonal interactions between individuals who have never interacted before. Usually, these interactions are not completed without a certain concern given that private information as well as the exchange of money and goods are involved.

An online reputation system is an approach to systematically evaluate opinions of online community members on various issues (e.g., products, services, events, etc.) and their opinions on the trustworthiness of other community members. Online reputation systems first collect and combine all relevant opinions, draw conclusions about the trustworthiness of all opinions from the subjective perspective of a given user and calculate the trustworthiness of all opinions referring to certain issues. Then, all opinions referring to a particular issue are combined according to their trustworthiness, and the result is returned to the requesting user or application, where it can be used to make a decision, e.g., to recommend the highest ranked restaurant.

The use of online reputation systems has been proposed for various applications, for example to validate the trustworthiness of sellers and buyers in online auctions, to detect free-riders in peer-to-peer networks and to ensure the authenticity of signature keys in a web of trust. 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 online reputation systems.

A reputation defense scheme, named TATA, for feedback-based online reputation systems. Here, TATA is the abbreviation of joint Temporal And Trust Analysis. It contains two modules: a time domain anomaly detector and a trust model based on the Dempster–Shafer theory. Specifically, considering 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. A trust analysis is then conducted based on the anomaly detection results. The concept of user behavior uncertainty from the Dempster–Shafer theory to model users' behavior patterns, and evaluate whether a user's rating value to each item is reliable or not.

The performance of TATA, two other representative reputation schemes, and previous scheme TATA is evaluated against real user attack data collected through a cyber-competition. TATA demonstrates significant advantages in

terms of identifying items under attack, detecting malicious users who insert dishonest ratings, and recovering reputation scores. In TATA, it is used to detect anomaly from a new angle: analyzing time domain information. Specifically, an organizing the ratings to a given item as a sequence in the descending order according to the time when they are provided. If there are rapid changes in the rating values, such changes can serve as indicators of anomaly. Therefore, 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 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 change detector.

The following are the main objective of the system

- To detect the malicious users who provide dishonest ratings.
- To recover reputation score of the target item, that receives dishonest ratings.
- To avoid interference to normal items' reputation scores.
- To prevent manipulation against the reputation system.

II STATE OF ART

Filtering Out Unfair Ratings in Bayesian Online reputation systems, in this paper Andrew Whitby, Audun Jøsang and Jadwiga Indulska proposed a altering technique that applies to both unfairly positive and unfairly negative ratings in Bayesian online reputation systems The assumption behind altering method is that ratings provided by different raters on a given agent will follow more or less the same probability distribution. When an agent changes its behaviour, it is assumed that all honest raters who interact with that agent will change their ratings accordingly. By comparing the overall reputation score of a given agent with the probability distribution of the ratings on that agent from each rater, the scheme dynamically determines an upper and lower threshold for which raters should be judged unfair and thereby excluded. Instead of using a sliding time window, the scheme uses a longevity factor that gradually reduces the weight of received ratings as a function of their age.

Detection and Filtering of Collaborative Malicious Users in Online online reputation system using Quality Repository approach, in this paper Jnanamurthy HK and Sanjay Singh proposed a new method to detect malicious users in online reputation systems using Quality Repository Approach (QRA). It is mainly concentrated on anomaly in both rating-values domain and the malicious user domain. In complex collusion attack, malicious users work together to reduce the reputation score by providing dishonest ratings. QRA is very efficient to detect malicious users rating and provides aggregate trustful rating. Threshold is a region in which mark a boundary for a new state. Threshold selection plays important role in ending malicious users and decision making whether user is a true user. The selection of threshold for newly launched product is not an easy task, because it is impossible predict the newly launched product whether it is a good product or a bad product.

Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior, in this paper Chrysanthos Dellarocas proposed a contribute in the construction of more robust online reputation systems by identifying, and proposing mechanisms for addressing, two important classes of reputation system fraud: scenarios where buyers intentionally provide unfairly high or unfairly low ratings for sellers, as well as scenarios where sellers attempt to "hide" behind their cumulative reputation in order to discriminate on the quality of service they provide to different buyers. The results presented indicate that the combination of controlled anonymity and cluster filtering is a powerful technique for "immunizing" online reputation reporting systems in the presence of unfair ratings and discriminating seller behavior. Given the increasing importance of online reputation mechanisms in building trust and managing risks in online trading communities, further research is needed in order to discover additional ways in which such systems may be compromised, as well as to propose mechanisms for coping with them.

Information filtering via Iterative Refinement, in this paper Laurite, Mortal, Y.C. Zhang and Y.K. Yu proposed that the explosive growth of accessible information, especially on the Internet, evaluation-based filtering has become a crucial task. Various systems have been devised aiming to sort through large volumes of information and select what is likely to be more relevant. A new ranking method, where the reputation of information providers is determined self-consistently. The study of complex networks dynamical processes taking place on these structures has recently attracted.

An Evidential Model of Distributed Reputation Management, in this paper Bin Yu and Munindar P. Singh proposed a alternative technique for agents to function effectively in large and open networks, they must ensure that their correspondents. So no central authorities may exist, the only way agents can find trustworthy correspondents is by collaborating with others to identify those whose past behavior has been untrustworthy. Finding trustworthy correspondents reduces to the problem of distributed reputation management. When evaluating the trustworthiness of a correspondent; an agent combines its local evidence with the testimonies of other agents regarding the same correspondent.

Trust-based decision making for electronic transactions, in this paper Auden Johan proposed a new technique to make financial transactions that are made in an environment of imperfect knowledge will always contain a degree of risk. When dealing with humans or human organizations the relative knowledge about the co-operative behavior of others can be perceived as trust, and trust therefore is a crucial factor in the decision making process. Assessing trust becomes a problem in electronic transactions due to the impersonal aspects of computer networks. A scheme for propagating trust through computer networks based on public key certificates and trust relationships, and demonstrates how the resulting measures of trust can be used for making decisions about electronic transactions.

The anatomy of a large-scale hyper textual web search engine, in this paper Sergey Brim, Lawrence Page proposed that web search engine is designed to crawl and index the Web efficiently and produce much more satisfying search results than existing systems. To engineer a search engine is a challenging task. Search engines index tens to hundreds of millions of Web pages involving a comparable number of distinct terms. They answer tens of millions of queries every day. Despite the importance of large-scale search engines on the Web, very little academic research has been done on them. Due to rapid advance in technology and Web proliferation, creating a Web search engine today is very different from three years ago. This provides an in-depth description of our large-scale Web search engine - the first such detailed public description know of to date.

A Novel Attack on Feedback-based Online reputation systems in this paper Yafei Yang, Qinyuan Fang, Yan Lindsay Sun and Yafei Dai proposed that the online reputation systems are playing critical roles in securing to-day's distributed computing and communication systems. Similar to all other security mechanisms, online reputation systems can be under attack. It reports the discovery of a new attack, named Rep Trap, against feedback-based online reputation systems, such as those used in P2P sharing systems and E-commerce websites.

Detecting Cheating Behaviors in Cyber Competitions by Constructing Competition Network, in this paper Yuhong Liu and Yan Sun proposed an alternative technique that the Cyber Competition has been recognized as an efficient way to facilitate research and education in cyber security. Cyber Competition has been recognized as an efficient way to facilitate research and education in cyber security field .They have discovered that the participants (i.e. players) in cyber competitions can cheat in order to gain a higher rank or collect more prizes. The clients use data collected from the competition to analyze such cheating behavior and propose to build a competition social network to detect cheating behaviors in cyber competitions.

Detecting Cheating Behaviors in Cyber Competitions by Constructing Competition Network in this paper, Yuhong Liu and Yan Sun proposed the value of online reputation systems is widely recognized and the incentive to manipulate such systems is rapidly growing. TAUCA, a scheme that identifies malicious users and recovers reputation scores from a novel angle: combination of temporal analysis and user correlation analysis. It also effectively reduces the bias in the recovered reputation scores.

Advanced Features in Bayesian Online reputation systems, in this paper Auden Josang and Walter Quattrociocchi proposed that Bayesian online reputation systems are quite flexible and can relatively easily be adapted to different types of applications and environments. It is to provide a concise overview of the rich set of features that characterizes Bayesian online reputation systems and also it demonstrate the importance of base rates during bootstrapping, for handling rating scarcity and for expressing long term trends.

A Personalized Approach to Address Unfair Ratings in Multiagent Online reputation systems, first survey different approaches for handling unfair ratings, and their advantages and disadvantages. List the capabilities that an effective approach should have and compare these approaches based on their capabilities. The categorize of these approaches in terms of two dimensions, a “public-private” dimension and a “global-local” dimension. The impact of online reputation system architectures on the selection of approaches for handling unfair ratings. A personalized approach for effectively handling unfair ratings in enhanced centralized online reputation systems. Where consumer agents elicit reputation ratings of provider agents from other consumer agents, known as advisor agents. The personalized approach first calculates what refer to as the “private reputation” of an advisor agent, based on the consumer and advisor agents’ ratings for commonly rated provider agents. When the consumer agent is not confident in its private reputation ratings it can also use what refer to as the “public reputation” of the advisor agent. This public reputation is estimated based on the advisor agent’s ratings for all provider agents in the system. The personalized approach ultimately computes a weighted average of private and public reputations to represent the trustworthiness of the advisor agent.

As diverse manipulations against online reputation systems appear and develop rapidly, defense schemes protecting online reputation systems are also evolving accordingly. The defense approaches limit the maximum number of ratings. 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. Real user attack data collected from a cyber-competition is used to construct the testing data set. They consider ratings as random variables and assume dishonest ratings have statistical distributions different from normal ratings. Users with bad rating history tend to provide dishonest ratings. An approach determines the weight of a rating based on the reputation of the user who provides this rating. The reputation is also referred to as trust or reliability.

The draw backs are listed below.

- The lack of realistic attack data can hurt the performance evaluation.
- The defense approaches limit the maximum number of ratings each user could provide within certain time duration.

III PROPOSED SYSTEM

The ORS 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. The TATA is used to detect anomaly from a new angle: analyzing 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. If there are rapid changes in the rating values, such changes can serve as indicators of anomaly. Therefore, a change detector in TATA as the

 ISSN: 2321-8169
1214– 1219

anomaly detector, which takes the rating sequences as inputs and detects changes occurring in the rating sequences. The 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 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, organizing the ratings to a given item as a sequence in the descending order according to the time which they are provided. In many practical online reputation systems, items have intrinsic and stable quality, which should be reflected in the distribution of normal ratings. Therefore, rapid changes can serve as indicators of anomaly. The CUSUM detector (cumulative sum) as the anomaly detector, which reliably detects changes occurring in the rating sequences of an online item.

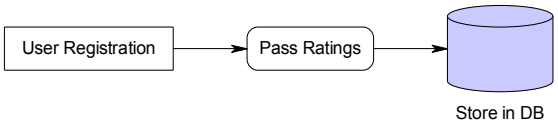

Figure 1. Shows Temporal Analysis

B. *Trust Model Based On The Time Domain Anomaly Detection*

Based on the anomaly detection results, to evaluate users' trust values in this section. In most trust models, users' trust values are determined only by their good and bad behaviors. However, it is not sufficient. Consider two trust 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.

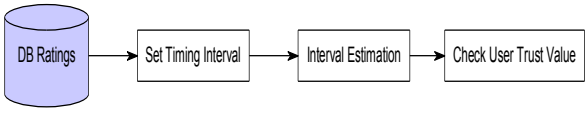

Figure 2. A trust model based on the Dempster-Shafer theory

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.

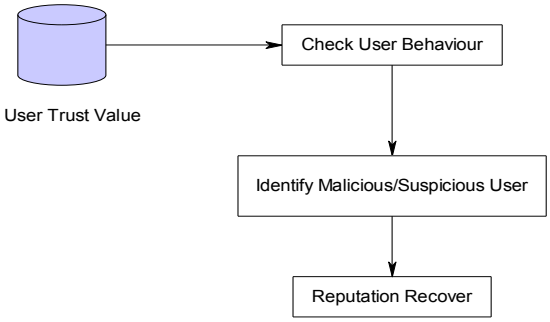

Figure 3. Recovering Reputation Scores

IV IMPLEMENTATION

As diverse manipulations against online reputation systems appear and develop rapidly, defense schemes protecting online reputation systems are also evolving accordingly. They are classified into four categories:

In the first category, 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.

In the second category, the defense schemes aim to increase the cost of launching an attack. Some online 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. However, it has little impact on attacks in which attackers buy their own products for reputation boosting. Some other schemes increase the costs of acquiring multiple user IDs by binding identities with IP addresses or using network coordinates to detect sybil attacks. Such schemes will greatly increase the attack costs, but cannot defeat the attackers with plenty of resources.

TABLE I. PERFORMANCE OF ORS

SCHEMES / No. Of Users	5	10	15	20
BETA-DR	0.366	0.6128	0.5452	0.668
TAUCA-DR	0.8552	0.9456	0.904	0.9229
TATA-DR	0.9914	0.9969	0.9925	0.9442
ORS-DR	0.9953	0.9987	0.9967	0.9623
BETA-FR	0.5698	0.57	0.57	0.57
TAUCA-FR	0.0221	0.0304	0.0347	0.0377
TATA-FR	0.0169	0.0183	0.0241	0.0376
ORS-DR	0.0083	0.0097	0.0132	0.0278

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

 ISSN: 2321-8169
1214– 1219

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. An entropy based approach identifies the ratings that bring a significant change in the uncertainty of the rating distribution as dishonest ratings. In dishonest rating analysis is conducted based on Bayesian model. Controlled anonymity and cluster filtering are used to eliminate dishonest ratings.

The defense approaches in the fourth category investigate users' rating behavior. 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. In a personalized trust structure is introduced so that different users may assign different trust values to the same user.

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.

Second, most defense schemes in the third category follow the "majority rule", which detects dishonest ratings by examining whether some rating values are far away from the majority's opinions. This rule works fine when the attackers insert a small number of dishonest ratings that are very different from normal users' rating values. However, it may generate misleading results when the number of dishonest ratings is large and yield high false alarm rate when normal ratings have a large variance and dishonest ratings are not too far away from the majority's opinions.

Third, schemes in the fourth category, trust based approaches, are relatively vulnerable to attacks where malicious users conduct good and bad behavior alternatively. Malicious users could first accumulate high trust values by providing normal ratings to the items that they do not care and then provide dishonest ratings to the items that they want to manipulate.

Fourth, to evaluate an online reputation system, the 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.

V RESULTS AND DISCUSSIONS

To compare the performance of different schemes, first demonstrate the malicious user detection results. In the detection rates and false alarm rates for scheme Beta, scheme TAUCA and scheme TATA are demonstrated. First, scheme Beta performs the worst with low detection rates and high false alarm rates. For example, when there are 20 malicious users, the detection rate of scheme Beta is only 0.67, while the false alarm rate is 0.57, meaning that to detect 13 out of 20 malicious users, 57% of 300 normal users will be misidentified as malicious users. Second, TATA outperforms TAUCA when malicious user number is not large. And when increases, TATA will have a slightly worse performance than TAUCA. The reason is that TAUCA focuses more on the correlation among users whereas TATA focuses more on individual users past behavior patterns. When the number of malicious users is small, the collusion among them is not very strong. Comparing all these schemes, the first three schemes perform worse than the ORS scheme. The RS scheme performs best with high detection rate and low false alarm rates. For example, where there are 20 malicious users, the detection rate for ORS scheme is 0.97 and the false alarm rate for ORS scheme is 0.27.

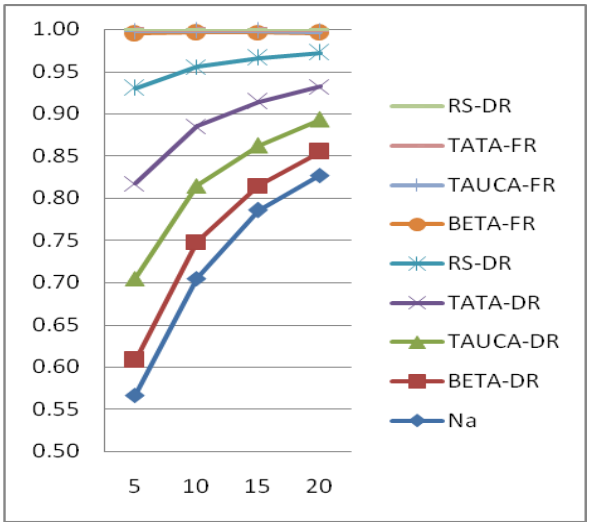

Figure 4. Comparison Graph

CONCLUSION AND FUTURE ENHANCEMENT

A comprehensive anomaly detection scheme, ORS 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 used. 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. For different attacks, the detection rate of TATA is 0.87 0.99, whereas IR fails to detect malicious users and Beta model achieves 0.37, 0.72 detection rate. The RS scheme performs best with high detection rate and low false alarm rates. For example, where there are 20 malicious users, the detection rate for ORS scheme is 0.97 and the false alarm rate for ORS scheme is 0.27. When the number of malicious users is not very large, examining individual user's behavior is a very effective defense approach. When the number of malicious users is very large, investigating user behavior similarity (such as in the ORS scheme) becomes a promising method. In the future, one possibility is to jointly consider trust evaluation and user correlation analysis.

REFERENCES

[1] Dellarocas.C, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in Proc. 2nd ACM Conf. Electronic Commerce, 2000, pp. 150–157.

ISSN: 2321-8169
1214– 1219

[2] Jøsang.A and Quattrociocchi.W, "Advanced features in bayesian online reputation systems," TrustBus,2009, pp. 105–114.
[3] Laureti.P, Moret.L, Zhang.Y-C, and Yu.Y-K, "Information filtering via iterative refinement," Europhys. Lett., vol. 75, no. 6, 2006, pp.1006–1012.
[4] Lee.R and Paul.H, Use of Online Rating Systems Oct. 20, 2004 [Online]
[5] Liu.Y and Sun.Y, "Anomaly detection in feedback-based online reputation systems through temporal and correlation analysis," in Proc. 2nd IEEE Int. Conf. Social Computing, Aug. 2010, pp. 65–72.
[6] Weng.J, Miao.C, and Goh.A, "An entropy-based approach to protecting rating systems from unfair testimonies," IEICE Trans. Inf. Syst., vol. E89-D, no. 9,Sep.2006, pp. 2502–2511.

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

[8] Yang.Y, Feng.Q, Sun.Y, and Dai.Y, "Reputation trap: A powerful attack on online reputation system of file sharing p2p environment," in Proc. 4th Int. Conf. Security and Privacy in Communication Networks, Istanbul, Turkey, Sep. 2008.
[9] Yu.H, Kaminsky.M, Gibbons.P.B, and Flaxman.A, "Sybilguard: Defending against sybil attacks via social networks," in Proc. 2006 Conf. Applications, Technologies, Architectures, and Protocols for Computer Communications, 2006, pp. 267–278.
[10] Zhang.J and Cohen.R, "A personalized approach to address unfair ratings inmultiagent online online reputation systems," in Proc. Fifth Int. Joint Conf. Autonomous Agents and Multiagent Systems (AAMAS) Workshop on Trust in Agent Societies, 2006, pp. 89–98.