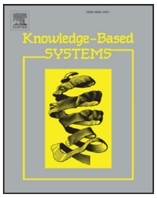
Knowledge-Based Systems 103 (2016) 1–18

Contents lists available at ScienceDirect

Knowledge-Based Systems

journal homepage: www.elsevier.com/locate/knosys



A pre-evolutionary advisor list generation strategy for robust defensing reputation attacks

Shu-juan Ji[a,*], Hai-yan Ma[a], Shu-lian Zhang[b], Ho-fung Leung[c], Dickson Chiu[d], Chun-jin Zhang[e], Xian-wen Fang[f]

[a] Shandong Provincial Key Laboratory of Wisdom Mine Information Technology, Shandon University of Science and Technology, Qingdao, China
[b] College of Information Engineering, Qingdao University of Technology, Qingdao, China
[c] Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong, China
[d] Faculty of Education, The University of Hong Kong, Hong Kong, China
[e] Center of network, Shandon University of Science and Technology, Qingdao, China
[f] Department of Information and Computing Science, Anhui University of Science and Technology, Huainan, 232001, China

ARTICLE INFO

Article history:
Received 3 November 2015
Revised 17 February 2016
Accepted 19 March 2016
Available online 9 April 2016

Keywords:
Trust and reputation systems
Unfair rating attacks
Robust trust network
Evolutionary algorithm

ABSTRACT

Trust and reputation systems are vital in large open distributed electronic commerce environments. Although existing various mechanisms have been adopted to guarantee trust between customers and sellers (or platforms), self-interested agents often impose various attacks to trust and reputation systems. As these attacks are usually deceptive, collusive, or strategic, it is difficult to keep trust and reputation systems robust to multifarious attacks. Many defense strategies employ a robust trust network (such as a trustable advisor list) for protecting buyers. However, in the evolution of a trust network, existing strategies consider only historical ratings of given buyers and advisors, while neglecting the timeliness of these ratings. Besides, only a single trust network is utilized to evaluate all sellers, leading to problems such as lack of pertinence and quite large deviation of evaluation. This paper proposes a novel pre-evolutionary advisor generation strategy, which first pre-evolves an optimal advisor list for each candidate seller before each trade and then evaluate each seller according to its corresponding list. After evaluating and selecting the seller, the buyer's own advisor list is evolved based on the pre-evolved optimal advisor list of chosen seller. Two sets of experiments have been designed to verify the general performance of this strategy, including accuracy, robustness, and stability. Results show that our strategy outperforms existing ones, especially when attackers use popular attack strategies such as Sybil, Sybil and Camouflage, and Sybil and Whitewashing. Besides, our strategy is more stable than compared ones, and its robustness will not change with the ratio of dishonest buyers.

1. Introduction

Trust has attracted widely attention in the fields such as sociology, psychology, economics, and computer science. Although these disciplines have different definitions and research emphasizes, it is widely agreed that trust means the confidence that one or many entities behave as they expected [1]. According to the source of trust, it can be divided into direct trust and referral trust. The former kind of trust comes from one's own experience, while the latter is calculated according to recommenders' reviews. If a given pair of trustor and trustee have interacted for many times, the trustor's trust about the trustee may rely much on its direct trust accumulated according to their interaction experience. Otherwise, the trustor may refer to the referral trust recommended by its advisors.

Trust plays a vital role in open, large, distributed, and dynamic multi-agent systems where self-interested agents may be deceptive and strategic. For example, in multi-agent based e-marketplaces, dishonest selling agents often employ "ballot stuffing" reviewers providing unfairly high ratings to promote the seller's reputation [2], which may result in the quality of the delivered products not as good as the buyers' expectations. In such cases, the buyers will be disappointed or even annoyed, and they will feel risky of subsequent transactions with that seller. Thus, the buyers will distrust these sellers or even distrust the electronic commerce platform after several times of unsatisfactory transactions. Therefore,

[*] Corresponding author: Tel.: +8613884979026; fax: +8653286057622.
E-mail addresses: jane_ji2003@aliyun.com (S.-j. Ji), 295340370@qq.com (H.-y. Ma), 958007736@qq.com (S.-l. Zhang), lhf@cuhk.edu.hk (H.-f. Leung), dicksonchiu@ieee.org (D. Chiu), zhangchjin@163.com (C.-j. Zhang), fangxianwen@hotmail.com (X.-w. Fang).

http://dx.doi.org/10.1016/j.knosys.2016.03.015
0950-7051/© 2016 Elsevier B.V. All rights reserved.

reputation systems are designed for buyers to model the trustworthiness of sellers based on ratings shared by other buyers (called *advisors* in this paper) and make decisions on which sellers to transact with.

However, unfair rating attacks (such as the collusive unfair ratings, Sybil, Camouflage, Whitewashing, and discrimination attacks) from dishonest advisors render reputation systems' vulnerable to mislead buyers to transact with dishonest sellers [3, 4]. Dishonest advisors may also employ sophisticated attack strategies to avoid being detected or defended. For example, Luca and Zervas [5] show that appropriately 16% of Yelp restaurant reviews are fraudulent thought Yelp adopts an authentication algorithm to filter out suspicious reviews. Besides, scalping is prevalent on the Taobao platform, which has even led American Apparel and Footwear Association (AAFA) to submit its worry to the United States Trade Representative (USTR) and the Securities and Exchange Commission (SEC) [6].

As further explained in the next section of literature review, existing defending strategies either has limitations in defending some strategic attacks or neglect timeliness of advisor's ratings. To address such problems, we design a new robust algorithm for improving intelligent agents' capabilities in defending various types of attacks, accurately estimating the trustworthiness of sellers and reducing the risk of purchase. An overview of our approach is highlighted as follows. Before making a decision in selecting which recommended seller as trading partner, the buyer agent should first pre-evolve an optimal advisor list for each recommended seller as well as the trustworthiness of all member of each list (see Algorithm 1). In this process, not only the ratings given by the buyer agent and its advisors are considered, those rated by the recommended seller's recent reviewers are also taken into consideration. Based on the optimal advisor list for each recommended seller, the buyer agent can then evaluate the trustworthiness of the corresponding sellers (see Algorithm 2). According to the evaluation results, the buyer agent will select one recommended seller as trading partner. Finally, the advisor list of the buyer is evolved based on the pre-evolved optimal advisor list of chosen seller (see Algorithm 3).

In contrast to existing advisor list generation algorithm, the novel features of this algorithm are as follows. First, the evolution algorithm aims at pre-computing an optimal advisor list for each seller, in which includes the buyers that our buyer agent should consult in evaluating the trustworthiness of the seller. If h sellers are recommended by the search agent, we will get h optimal customized advisor lists. Therefore, the efficiency of this algorithm is O(hG), where h is the number of sellers that are considered in recommendation list, G is the generation that evolution process should be proceeded. This algorithm is inevitably h times that of the strategy of Jiang et al. [7], as their strategy only include one G-generation of evolution process. Secondly, in the computation of optimal advisor list, the involved advisors come from two sources: (i) the buyer's own witness list; (ii) the seller's recent reviewers. As different sellers have different recent reviewers, the resultant optimal advisor list for the recommended sellers are updated in a timely manner, as improved over the strategy of Jiang et al. [7]. Thirdly, the computation of optimal advisor list is only a pre-calculation process before selecting trading partner. In that process, the buyer agent's advisor list is not evolved, as opposed to the strategy of Jiang et al. [7], but is postponed after the seller is chosen, and therefore evolving the buyer's advisor list according to its recent trading experience.

The rest of our paper is developed as follows. Section 2 reviews related literature. Section 3 gives a framework for electronic commerce platform with advisor mechanism. Section 4 illustrates the pre-evolutionary advisor lists generation strategy given in this paper, which is composed of three algorithms, i.e., the optimal advisor lists pre-evolution algorithm, the seller evaluation and chosen algorithm, and the buyer's advisor list evolution algorithm. Section 5 demonstrates the merits of our approach with the experimental settings and results. Section 6 concludes this paper with our future work directions.

2. Literature review

Trust problem has attracted wide attention from electronic commerce and social network related academic community and industry field for many years. The aim of this section is to review the modeling of trust, including techniques for detecting and defending against malicious agents. Since our work is based on a buyer's view, not the electronic platform's view, we only review approaches designed from buyers' viewpoint. In general, the defense models can be generally divided into three categories, i.e., filtering approaches, discounting approaches, and evolutionary approach. Following paragraphs illustrate these models in detail.

2.1. Filtering approach

As early as 2000, Dellarocas [2] presented a cluster filtering model to reduce the effect of unfairly high ratings and positive discrimination. He first used collaborative filtering techniques to identify the nearest neighbor set N of given buyer B based on their similarity with B on commonly rated sellers. As colluders might have taken collaborative filtering into account and cleverly picked buyers with tastes similar to those of B in everything else except their ratings, hence, the resulting set N will include some fair raters and some unfair raters. To filter the unfair rater cluster N_u and the fair rater cluster N_l from the buyer's neighbor set N, Dellarocas used the cluster filtering method proposed by Macnaughton-Smith et al. [8]. Furthermore, to deal with the scenarios that sellers may vary their service quality over time (e.g., improving it, deteriorating it, or even oscillating between phases of improvement and phases of deterioration) and to counter attempts to inflate a seller's reputation using unfair ratings flooding, Dellarocas enhanced the cluster filtering algorithm by considering the values of buyers' ratings and the frequency of ratings as well. Although these algorithms can filter out the unfairly high ratings very well, they cannot handle unfairly low ratings.

Liu et al. [9, 10] propose an *iClub* clustering algorithm, which applies clustering to divide buyers into different 'clubs' according to the similarity between the buyer and the witness (a witness represents the buyer agent who has common trading partners with buyer B, who may be an honest or a dishonest reviewer) of the buyer. If the transaction volume between the buyer and the given seller is smaller than a threshold, the 'global' cluster process will be triggered. Otherwise, only local information is considered in the generation of clusters. In the local-based cluster process, to find the honest reviewer about a given seller, the *iClub* approach first collects local information about this seller and normalizes the ratings, and then applies a density-based clustering routine DBSCAN [11] to get various clusters. The buyers whose ratings are included in the same cluster with the buyer agent's rating are regarded as honest ones. The global-based cluster process makes use of the buyer's experience with sellers in the reputation system to find a set of advisors who are honest regarding those sellers, and then uses this information to find honest advisors regarding the seller who is currently under evaluation. However, when having little evidence about sellers, a buyer relies on the club with the maximum number of advisors. In this scenario, *Sybil* attackers forming a club with many members will mislead buyers to follow their opinions. Thus, *iClub* is also vulnerable to *Sybil*-based attacks, though it is effective in filtering various types of unfair testimonies.