Computer Communications 123 (2018) 11–23

Contents lists available at ScienceDirect

Computer Communications

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

A dynamic algorithm for stochastic trust propagation in online social networks: Learning automata approach

Mina Ghavipour, Mohammad Reza Meybodi*

Department of Computer Engineering and IT, Amirkabir University of Technology, Tehran, Iran

ARTICLE INFO

Keywords:
Trust
Trust propagation
Trust network
Social network
Stochastic network
Learning automata

ABSTRACT

The dynamic nature of trust has been universally accepted in the literature. As two users interact with each other, trust between them evolves based on their interaction's experience, in such a way that the level of trust increases if the experience is positive and otherwise, it decreases. Since social interactions in online networks, especially in activity and interaction networks, occur continuously in time, trust networks can be considered as stochastic graphs with continuous time-varying edge weights. This is while previous work on the trust propagation has assumed trust network as a static graph and developed deterministic algorithms for inferring trust in the graph. The problem becomes more challenging since trust propagation based algorithms are too time-consuming and therefore it is highly probable that trust weights change during their running time. In order to tackle this problem, this paper proposes a dynamic algorithm called DyTrust to infer trust between two indirectly connected users. The proposed algorithm utilizes distributed learning automata (DLA) to capture the dynamicity of trust during the trust propagation process and dynamically update the found reliable trust paths upon the trust variations. To the best of our knowledge, DyTrust is the first dynamic trust propagation algorithm presented so far. We conduct several experiments on the real trust network dataset, Kaitiaki, and evaluate the performance of the proposed algorithm DyTrust in comparison with the well-known trust propagation algorithms. The results demonstrate that by considering the dynamicity of trust, DyTrust can infer trust with a higher accuracy.

1. Introduction

Online social networks provide an appropriate infrastructure for people interacting with each other without face-to-face interactions. Millions of people are joined these networks every day and interact with others who they did not know before. Due to some features of behaviors in social networks, such as anonymity, interactions are threatened seriously by vicious users. Trust is considered as one of the most effective methods to provide guidance for users identifying these vicious users or behaviors. Inferring trust among indirectly connected users plays a vital role in enforcing the security for social network sites and improving the quality of them.

Considerable number of studies has been done on trust in online social networks, and various methods have been proposed for inferring the trustworthiness of an unknown user. A popular family of these methods focuses on the trust inference via propagating trust through friendship networks whenever there exist at least one path between two users in these networks [1–10]. The problem with existing trust propagation-based methods is that they do not take into consideration the dynamic nature of trust. Trust is updated over time as a result of repeated interactions between users. Based on this, trust networks are stochastic graphs in which edge weights change rapidly and continuously in time. This is while, existing methods take an instant snapshot of trust network and then run a deterministic trust propagation algorithm on that snapshot. Since these methods are too time-consuming, it is highly probable that trust weights change during their running time and therefore the trust values estimated by them may become less relevant because of these trust variations.

In this paper, we address the dynamicity property of trust and propose a dynamic trust propagation algorithm based on distributed learning automata, called DyTrust, to infer the trustworthiness of an unknown target user while considering the changes of trust during its running time. Using learning automata, DyTrust first finds the most reliable trust path from the source user to each user directly trusting the given target. After that, the trust value of the source on the target user is estimated by propagating trust along the found reliable paths and then aggregating the opinions of the target's direct neighbors weighted by their reliability values. To the best of our knowledge, the proposed dynamic algorithm DyTrust is the first to consider the dynamicity of trust during the trust inference process and dynamically update the

* Corresponding author.
E-mail address: mmeybodi@aut.ac.ir (M.R. Meybodi).

https://doi.org/10.1016/j.comcom.2018.04.004
Received 1 November 2017; Received in revised form 22 January 2018; Accepted 8 April 2018
Available online 11 April 2018

found reliable trust paths upon the trust variations. We conduct several extensive experiments on the real trust network dataset, Kaitiaki, and compare the performance of DyTrust with that of the well-known trust propagation algorithms, such as TidalTrust and MoleTrust. The results validate the effectiveness of our algorithm DyTrust: considering the changes of trust over time significantly improves the trust prediction accuracy.

The remainder of this paper is organized as follows. The Section 2 surveys some related work in the literature of trust. In Section 3, learning automata and distributed learning automata are briefly reviewed. Sections 4 and 5 respectively present the details of our proposed dynamic trust propagation algorithm DyTrust and its convergence proof to the optimal solution. The experimental evaluation is described in Section 6. Eventually, Section 7 discusses and concludes our work.

2. Related work

2.1. Trust in online social networks

Online social networks provide a convenient opportunity for people to interact with each other and share their information. Trust is considered as a vital factor in forming social interactions. Researchers have proposed various definitions for trust in different contexts. In the context of a social web, Golbeck [11] has defined trust in a person as “a commitment to an action based on a belief that the future actions of that person will lead to a good outcome”. Therefore, reliability in previous interactions with a person give rise to positive expectations about that person's intentions [12]. As two users interact with each other, trust between them evolves based on their interaction's experience, in such a way that the level of trust increases if the experience is positive and otherwise, it decreases. Trust may also decay with time. Experiences of more recent interactions are given higher importance than those of old ones, since experiences of old interactions may become irrelevant with time [13]. This property refers to the dynamicity of trust.

Various techniques have been proposed for modeling this dynamicity, such as aging of old experiences [14–16], giving more weight to recent experiences [17–19], considering only the most recent experience [20,21], using temporal window [22–25] and periodically computing the value of trust [26,27].

2.2. Related studies for inferring trust

Existing models for inferring trust are classified into two categories from the standpoint of trust propagation: non-propagating and propagating trust models. One of the famous models in the first category is PeerTrust [24], which was the first to introduce the concept of feedback credibility and its role for defending against dishonest feedbacks. PeerTrust included a coherent adaptive trust model to quantify and compare the trustworthiness of peers by using a transaction-based feedback system. Another model without trust propagation process was proposed by work in [28]. In this paper, Authors provided a trust model for virtual communities based on a reputation mechanism and direct experiences. Liu et al. [29] presented a supervised learning approach that automatically predicts trust among users of online communities using two factors: user factor and interaction factor, where the former refers to evidence derived from actions of individual users and the latter is interactions between pairs of users. Caverlee et al. [30] proposed the SocialTrust framework for supporting tamper-resilient trust establishment in online social networks. SocialTrust initially gives all users the same level of trust. Then, it dynamically revises trust ratings according to three components: the current quality of trust, the interaction history, and the adaptation to change. Authors in [31] proposed a decision support method for estimating trust in virtual teams. Their proposed trust estimation framework has two dimensions: Reputation and Collaboration, where the former represents the trustworthiness of members and the later represents the cooperation situations between members in a team. Works in [32–35] are also subcategorized in non-propagating classification, since they discussed trust inference models relying on past observed behaviors. As another example of trust model without propagation, game theory [36–38] has been utilized in recent years for inferring trust. Most of the work in this area has focused on designing some mechanism to make individuals cooperate with each other rather than defecting. Although there have been some attempts at using game theory for trust among agents [39,40], this approach is still not among the primary focuses of research in the scope of trust management.

Trust models based on propagation are more popular than non-propagating trust models. In the trust propagation approach, users propagate their trust value to others through trust network following their direct trust relationships. One of the most famous trust models with propagation has been proposed by Golbeck [11]. The author studied the concept of trust in web-based social networks and observed that the accuracy of trust inference decreases as the trust path length increases. Therefore, she suggested that the shortest and strongest paths are the best for the estimation of trust and presented a trust propagation model called TidalTrust for inferring the trust value of a source user related to a target one based on averaging trust values along the strongest shortest trust paths. Another famous model based on trust propagation is MoleTrust [41], which finds all shortest trust paths from a source to a target user and combines all direct trust values issued by users whose trustworthiness is more than 0.6. Authors in [42] investigated the impact of the path length and strength on the accuracy of trust inference and observed that the strength of a trust path can be more important than its length, such that stronger trust paths are favored to weaker but shorter ones. Although their fuzzy trust inference algorithm considering all strongest paths performs more precisely the inference process, it has the time complexity of exponential and therefore cannot be applicable to large scale social networks. Work in [43] described a trust inference algorithm called SUNNY, which estimates the confidence by using a probabilistic sampling technique and computes trust only based on the information sources with highest confidence estimates. Actually, this algorithm executes the trust inference procedure from the TidalTrust algorithm on a more confident sub network.

With a variation on the PageRank algorithm, Kamvar et al. [14] proposed a distributed trust propagation model called EigenTrust for estimating trust values in P2P networks. EigenTrust measures trust values through iterative multiplication and aggregation of trust values along transitive chains until the trust values for all agents converge to stable values. While the EigenTrust algorithm shows a satisfied performance on simple threat models, it could not offer good attack resilience when encountering more sophisticated threat ones. Authors in [44] analyzed the vulnerabilities of EigenTrust and proposed the trust model ServiceTrust which has a better performance on some sophisticated attack models by utilizing pairwise feedback similarity weighted trust propagation into the trust model. Kim and Song [7] studied the impact of two factors: the length of trust paths and aggregation functions, on the trust inference accuracy and proposed four strategies for estimating trust based on reinforcement learning. They found that the best combination is the strategy of weighted mean aggregation among all trust paths. Based on this strategy, Kim also proposed an enhanced trust propagation approach by combining a homophily-based trust network with an expertise-based one [1]. Using this approach, author tackled the sparsity problem of trust networks. Work in [45] presented a content-driven trust propagation framework that discovers credible claims and estimates trustworthiness of sources based on the quality of evidence. In fact, their proposed techniques for identifying and scoring relevant posts could be used to instantiate a model for computing the trustworthiness of medical claims and sources. Authors in [46] proposed a method called PIN-TRUST to measure the trustworthiness of