Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Generating trusted graphs for trust evaluation in online social networks

Wenjun Jiang [a,b], Guojun Wang [a,*], Jie Wu [b]

[a] School of Information Science and Engineering, Central South University, Changsha, Hunan Province 410083, PR China

[b] Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA

ARTICLE INFO

Article history:
Received 1 February 2012
Received in revised form
4 June 2012
Accepted 18 June 2012
Available online 26 June 2012

Keywords:
Trusted graph
Trust evaluation
Online social network
Small-world network
Weak tie

ABSTRACT

We propose a novel trust framework to address the issue of "Can Alice trust Bob on a service?" in large online social networks (OSNs). Many models have been proposed for constructing and calculating trust. However, two common shortcomings make them less practical, especially in large OSNs: the information used to construct trust is (1) usually too complicated to get or maintain, that is, it is resource consuming; and (2) usually subjective and changeable, which makes it vulnerable to vicious nodes. With those problems in mind, we focus on generating small trusted graphs for large OSNs, which can be used to make previous trust evaluation algorithms more efficient and practical. We show how to preprocess a social network (PSN) by developing a simple and practical *user-domain-based trusted acquaintance chain discovery* algorithm through using the small-world network characteristics of online social networks and taking advantage of "weak ties". Then, we present how to build a trust network (BTN) and generate a trusted graph (GTG) with the adjustable width breadth-first search algorithms. To validate the effectiveness of our work and to evaluate the quality of the generated trusted graph, we conduct many experiments with the real data set from Epinions.com. Our work is the first that focuses on generating small trusted graphs for large online social networks, and we explore the stable and objective information (such as *domain*) for inferring trust.

1. Introduction

Millions of people are joining online social networks every day, interacting with others who they did not know before. Establishing trust among those indirectly connected users plays a vital role in improving the quality of social network services and enforcing the security for them. The way in which a system discovers, records, and utilizes reputation information to form trust, and uses trust to influence a user's behavior, is referred to as a "reputation and trust-based system" [1]. Reputation and trust systems are seen as "soft security" mechanisms, which use collaborative methods for assessing the behavior of members in the community against the ethical norms, making it possible to identify and sanction those participants who breach the norms, and to recognize and reward members who adhere to the norms [2]. Two common shortcomings make previous trust systems less practical, especially in large OSNs, that is, the information used to construct trust is (1) usually too complicated to get or maintain—it is resource consuming; and (2) usually subjective and changeable, which makes it vulnerable to vicious nodes. With those problems in mind, we focus on generating small trusted graphs for large OSNs, which can be used to make previous trust evaluation algorithms more efficient and practical, as well as resistant to vicious attacks.

1.1. Application scenario and our motivation

Most interactions between two users in online social networks can be broken down into the scenario seen in Fig. 1: Alice is a *service requester*, and Bob is a *service provider*. Bob is the *target* whose trust is to be evaluated along with the *topic* of one of his services, and Alice's question, "Can I trust Bob on this service?"

An effective trust evaluation algorithm is expected to provide a proper answer for Alice. However, most of the existing trust evaluation algorithms are only effective on small-scale networks, which are often represented by several short trusted paths or small trusted graphs. Furthermore, how we can get such small trusted graphs has not been solved in any related literature. Therefore, there is a large gap between large social networks and small trusted graphs [3,4]. Our motivation is to bridge this gap.

In this paper, we mainly focus on Web-based social networks where users can provide user-generated content and construct a list of trusted neighbors, and most importantly, the content can be classified into categories by design. The categories are important, for they will be used to define the users' domain,

[*] Corresponding author. Tel.: +86 731 88877711; fax: +86 731 88877711.
E-mail addresses: wenjj8a@gmail.com (W. Jiang), csgjwang@gmail.com, csgjwang@mail.csu.edu.cn (G. Wang), jiewu@temple.edu (J. Wu).

0167-739X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2012.06.010

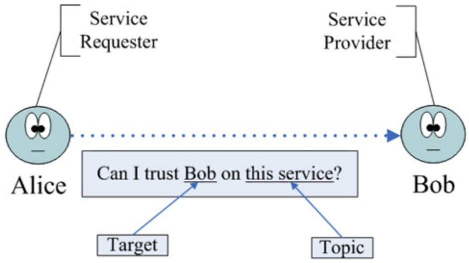

Fig. 1. A scenario of trust evaluation.

which will be further used to compute the social distance between a user and his neighbor. Based on this, we propose the PSN (preprocessing the social network) algorithm. The fundamental theory is Granovetter's [5] famous theory (a highly-influential sociology paper with over 20,000 citations, according to Google Scholar). This theory, known as "The Strength of Weak Ties", discussed the spread of information in social networks. In his theory, it is discovered that weak ties are dramatically valuable, because they are usually the source of new information.

Let us take a look at the scenario in Fig. 1. To make a decision about whether or not to trust Bob, it is natural for Alice to ask her neighbors for suggestions. Next, her neighbors will ask their own neighbors. They will continue to repeat this asking process until they connect with someone who knows Bob. This process is a typical breadth-first search.

It has been widely documented that social networks bear significant traits of small-world networks [6]. Small-world network theory tells us that there exist short path(s) for any two persons (at least most, if not all) in the world. However, in online social networks, a user usually has hundreds of neighbors, which results in the high complexity of the breadth-first search. So, it is very challenging to efficiently locate the short paths hidden within the enormous network.

Some existing research provided a solution that sets a limit to the search length, based on small-world network theory, such as the work in [7,8]; others made use of small-world network models for analysis or simulation. For instance, Watts's small-world network model [6] was used in [9,10]. In this paper, we propose a flexible approach in which the width of the breadth-first search is adjustable. Our key idea is: (1) to select long contacts to reach the target quickly, according to the theory of "weak ties"; and (2) to discover capable neighbors who can give effective suggestions in each step of the breadth-first search based on their topic-related degrees and target-related degrees.

1.2. The concept of trust

We take the natural definition of "trust", that is, Golbeck's [9] definition in the context of a social web where "trust in a person is a commitment to an action based on a belief that the future actions of that person will lead to a good outcome".

We also distinguish "referral trust" from "functional trust", which were first proposed by Jøsang [11]. In our work, "referral trust" represents the ability to recommend a good target, while "functional trust" represents the true ability of a target from his direct neighbor's point of view. For example, Alice needs to have her car serviced, so she asks Bob for his advice about where to find a good car mechanic in town. Bob is thus trusted by Alice to know about a good car mechanic (which is called "referral trust"). Also, Bob trusts Eric to be a good car mechanic because of his direct experience; this kind of trust is called "functional trust".

Another challenge with trust evaluation is taking proper information for inferring trust through trusted paths. Frequently used information, such as reputation, similarity, and explicit ratings, is often subjective, and can be easily changed by users. In this paper, we explore stable and objective information for inferring trust.

1.3. Our contribution

Based on the above analysis, we propose a trust framework called *SWTrust*. In this paper, we do not extend our work into developing integrated trust evaluation models, but rather, we focus on generating trusted graphs from large online social networks that could then be incorporated in the existing models to make them more efficient and practical. Our key ideas and contributions are as follows:

- In order to solve the key challenge of "discovering short trusted paths efficiently", we propose a novel *user-domain-based trusted acquaintance chain discovery* algorithm for preprocessing a large social network (*PSN*), based on the theory of "weak ties".
- We provide both centralized and distributed breadth-first search algorithms for building a trust network, based on the trusted acquaintance chains discovered by the *PSN* process. Moreover, we differentiate between *referral trust* and *functional trust*, and explore the stable and objective information (such as *domain*) for inferring trust, which can weaken the effect of vicious nodes.
- We conduct a lot of experiments with the data set from Epinions.com, and the results show the effectiveness of our work. In addition, we obtain many interesting and useful findings from the experiments.

The remainder of this paper is organized as follows: Section 2 surveys related work in the literature and presents our approach. Section 3 describes the overview of the *SWTrust* framework. Sections 4–6 respectively describe one of the three key steps of the *SWTrust* framework. Section 7 describes the experimental design, shows the numerical results that are obtained through the evaluation of *SWTrust*, and provides their physical interpretations. Finally, Section 8 concludes this paper and suggests future work.

2. Related work

Relationship-oriented networking tries to provide better security, usability, and trust in the system, and allows different users and institutions to build trust relationships within networks similar to those in the real world [12]. Online social networks are one of such networks. Therefore, building trust relationships is a key issue for online social networks.

Wang and Wu proposed FlowTrust to infer trust with network flows [3] and MeTrust for trust management with multi-trusted paths, based on multi-dimensional evidence [4]. In both papers, they presented the strong necessity of generating small trusted graphs.

Mármol and Pérez [13] summarized features of trust and reputation models, in which "gathering behavioral information, scoring and ranking entities, entity selection, transaction, and rewarding and punishing entities" are five components of a complete model. In this paper, we do not extend our work into developing an integrated trust evaluation model, but rather, we focus on generating trusted graphs that could then be incorporated in the existing models, which can be taken as the first three components of a complete model.

2.1. Local and global trust

The advantages and disadvantages of local and global trust metrics are discussed in detail in [7]. The authors pointed out that the local trust metric is more accurate when considering a personal view. In this paper, we mainly go the way of the local