Future Generation Computer Systems 55 (2016) 391–400

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Cluster-group based trusted computing for mobile social networks using implicit social behavioral graph

Shuhong Chen [a], Guojun Wang [a,*], Weijia Jia [b]

[a] School of Information Science and Engineering, Central South University, Changsha 410083, China
[b] Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai, 200240, China

HIGHLIGHTS

- A hierarchical trust model for MSNs based on cluster-group structure is presented.
- We construct an *implicit social behavioral graph* to describe trust relationships.
- To extract the actual communities, a novel clustering algorithm is proposed.
- We evaluate intragroup trust values using the hierarchical trust model for MSNs.
- Trust values are aggregated and propagated based on intragroup trust values.

ARTICLE INFO

Article history:
Received 1 January 2014
Received in revised form
9 April 2014
Accepted 1 June 2014
Available online 12 June 2014

Keywords:
Cluster-group trust
Contact
Mobile social networks
Implicit social behavioral graph

ABSTRACT

Mobile Social Networks (MSNs) facilitate connections between mobile devices, and are capable of providing an effective mobile computing environment for users to access, share, and distribute information. However, MSNs are virtual social spaces, the available information may not be trustworthy to all. Therefore, trust inference plays a critical role for establishing social links between mobile users. In MSNs, users' transactions will more and more be complemented with group contact. Hence, future usage patterns of mobile devices will involve more group contacts. In this paper, we describe the *implicit social behavioral graph*, i.e., *ego-i graph* which is formed by users' contacts, and present an algorithm for initiating *ego-i graph*. We rate these relationships to form a dynamic contact rank, which enables users to evaluate the trust values between users within the context of MSNs. We, then, calculate group-based trust values according to the level of contacts, interaction evolution, and users' attributes. Based on group-based trust, we obtain a cluster trust by the aggregation of inter group-based trust values. Due to the unique nature of MSNs, we discuss the propagation of cluster trust values for global MSNs. Finally, we evaluate the performance of our trust model through simulations, and the results demonstrate the effectiveness of group-based behavioural relationships in MSNs' information sharing system.

1. Introduction

With the emergence of new generation mobile devices, such as smartphones, laptops and PDAs, mobile social networks (MSNs) have experienced a tremendous success. MSNs are a type of newly-emerging large-scale distributed systems that integrate online social computing services and mobile devices and allow mobile social users to discover and interact with friends and further enjoy some distributed network service, such as friends recommendation and dynamic content dissemination [1]. However, there exists a certain risk when mobile users try to interact with others anytime and anywhere [2,3]. Because users of such mobile social network do not have any previous interactions, it is more important to establish an acceptable level of trust relationships among participating users [4].

A mobile social network is essentially a dynamic virtual network with trust relationships between users. Many social mobile applications such as Weixin,[1] LinkedIn,[2] and Facebook[3] have

* Corresponding author.
E-mail addresses: shchenannabell@csu.edu.cn (S. Chen), csgjwang@gmail.com, csgjwang@mail.csu.edu.cn, csgjwang@csu.edu.cn (G. Wang), wei.jia@cityu.edu.hk (W. Jia).

1 weixin.qq.com.
2 m.linkedin.com.
3 m.facebook.com.

http://dx.doi.org/10.1016/j.future.2014.06.005
0167-739X/

steadily been growing and became ubiquitous on the Internet. Therefore, various kinds of information and data produced through diverse mobile applications in mobile social environment. In such novel mobile social paradigms, each mobile device such as a smart phone performs its own role and the outputs are collected into mobile social networks. This environment allows for resource sharing and distribution of computing load [5]. Compared to traditional social networks in which only a select few produce and share data, this environment explosively increases not only the amount but also the complexity of data. Data collected with user experience is also possible, thus a method to measure trust worthiness of user data is necessary [6]. In smart phone's network environment, many people communicate mainly with their friends (such as family, and coworkers) through social network services. Mobile users share their roles within their MSNs via interactive behaviors, thereby increasing the overall trustworthiness of the relationship between the users being carried out. However, online social relationships always depend on physical world relationships. Hence, we can infer a level of users' trust relationships that underpins the online community where they exist according to some attributes of the real world [7–11].

There have been a number of related studies on trusted computation and inference in social networks to reduce the risk of social interactions [12–27]. These researches establish the foundation for our work. Unfortunately, one major aspect falls short in these research activities is the effect of contact and group homogeneity on inferring trust. Actually, in MSNs, we can communicate with everyone instantly everywhere all the time, and the differences between personal and remote communication patterns are diminishing. Thus, the one to one conversation scheme known from traditional remote communication will more and more be complemented with group contact, much as when socializing in the real world. Hence, future-oriented trust relationships in mobile social services have to adequately address the related issues. In particular, they should facilitate trust communication and offer support to calculate trust value.

In this paper, we propose an approach to rate the contact according to group affiliations. In our approach, a cluster is a subset of vertices of a social graph that is highly connected. In particular, we assume that the density of edges within a cluster (intra-cluster edges) is larger than the density of edges connecting vertices from inside the cluster to vertices outside of the cluster. In this work, we will refer to a cluster c as a set of contacts which belong to different communication groups. By contrast, a group g refers to a set of contacts as identified by a user and these contacts belong to the same communication group, such as family, coworkers, and classmates. Thus, a cluster includes many hierarchies, and each hierarchy is denoted as a group. Based on the findings, we provide a global social trust model building system by seamlessly integrating the one-dimensional trust relationship. We suggest a method to quantify a trusting relation based on contact rank and group homogeneity. The quantified social trust model supports inter-user trust relationship and integration. In other words, the proposed approach not only helps decide the communicating path of trustworthy users in mobile environment but also helps address security issues with increased trustworthiness of user behaviors by ranking trustworthy relationships between users.

By doing so, a communicating path for trustworthy users under mobile environment is suggested. With the enhanced trustworthiness, the issue of security also can be addressed. Furthermore, the implicit trust along with the application of socially corrective mechanisms inherent in social networks can also be applied to other domains. In fact, social networking platforms already provide a multitude of integrated applications that deliver particular functionality to users, and more significantly, social network credentials provide authentication in many diverse domains, for example, many sites support Facebook Connect as a trusted authentication mechanism [28]. Our key ideas and contributions are as follows:

- We propose a clustering algorithm to produce a finer grained hierarchy of clusters by subsequent partitioning which can extract the actual communities and be able to deal with overlapping clusters. And then, we construct *implicit social behavioral graph* which contains sufficient information to evaluate trust relationships.
- Using the above implicit social behavioral graph, we present a hierarchical trusted computing model for mobile social networks based on cluster-group structures. We calculate the intragroup trust values (group-based trust values) according to the level of contacts, interaction evolution, and users' attributes. Based on intragroup trust, we discuss the aggregation and propagation of trust values, which enable us to calculate the cluster trust and indirectly trust values for global mobile social networks (MSNs).
- We evaluate the performance of our trust model through simulations, and the results demonstrate the effectiveness of cluster-group based behavioural relationships in MSNs' information sharing system.

The rest of the paper is organized as follows. Some related works are addressed in Section 2. Section 3 provides some important definitions and concepts. Section 4 presents an algorithm to initialize a communication group. Sections 5 and 6 discuss how to calculate the group-based trust values and the propagation and aggregation of group-based trust, respectively. We analyze some performances of our trust model by simulation in Sections 7 and 8 is the conclusion.

2. Related work

If without trust relationships between users in a mobile social environment, the reliability of the total network would drop. Hence, many works have attempted to discover relationships between communication entities with social trust models. Grandison and Sloman [11] have surveyed several existing trust models and they have defined the trust as "the firm belief in the capability of an entity to act consistently, securely and reliably within a specified context". Kuada et al. [12] propose the provisioning and management approach based on collaborative strategy with social relationships in mobile computing services. Jennifer Golbeck et al. [13] and Kim et al. [14] propose a method to quantitatively infer trust between users for a recommendation system in a Web-based social network.

To support mobile phones in mobile network to plan, schedule, and reflect on group activities, Kikin-Gil [15] and Counts [16] propose to create privately shared group spaces on mobile devices where each group is able to communicate and collaborate. Chen et al. [17] study cooperative device-to-device (D2D) communications based on social trust and social reciprocity and propose a coalitional game theoretic approach to find the efficient D2D cooperation strategy and developed a network assisted relay selection mechanism for implementing the coalitional game solution. In order to enhance trustworthiness on the social network, Pezzi [18] defines a social network as a means of cultivating collective intelligence and facilitating the development of self-organizing communities. According to Pezzi et al., the social network and its services are provided by network nodes owned by members of the network rather than by centralized servers owned by the social network. Traditionally, social network platforms provide only marginal functionality for enhanced communication on mobile devices [19]. However, a truly mobile social network will offer functionality to improve service by considering users' mobile behavior patterns.