World Wide Web (2015) 18:159–184
DOI 10.1007/s11280-013-0241-5

Social context-aware trust inference for trust enhancement in social network based recommendations on service providers

Yan Wang · Lei Li · Guanfeng Liu

Received: 15 January 2013 / Revised: 31 May 2013 /
Accepted: 5 July 2013 / Published online: 23 August 2013
© Springer Science+Business Media New York 2013

Abstract In Service-Oriented Computing environments, there is a large number of service providers providing a variety of services to service customers. Conventional recommender systems, which adopt the information filtering techniques, can be used to automatically generate recommendations of service providers to service customers who are also the system users. However, data sparsity and trust enhancement are the traditional problems in recommender systems. Targeting the data sparsity problem, recent studies on recommender systems have started to leverage information from online social networks to collect recommendations from more participants and derive the final recommendation. However, this requires the methods to infer the trust between participants without any direct interactions in online social networks, which should take into account both the social context of participants and the context of the target services to be recommended, for trust enhanced recommendations. In this paper, we first present a contextual social network model that takes into account both participants' personal characteristics (referred to as the *independent social context*, including preference and expertise in domains) and mutual relations (referred to as the *dependent social context*, including the trust, social intimacy, and interaction context between two participants). In addition, we propose a new probabilistic approach, *SocialTrust*, as the first solution in the literature, to social context-aware trust inference in social networks. The result delivered by this approach is particularly

Y. Wang (✉)
Department of Computing, Macquarie University, Sydney, Australia
e-mail: yan.wang@mq.edu.au

L. Li
School of Computer and Information, Hefei University of Technology,
Hefei, Anhui, China
e-mail: lilei@hfut.edu.cn

G. Liu
School of Computer Science and Technology, Soochow University, Suzhou,
Jiangsu, China
e-mail: gfliu@suda.edu.cn

important in evaluating the trust from a source participant to an end recommender who recommends a target service or service provider, via the sub-network consisting of intermediate participants/recommenders between them and relevant contextual information. Moreover, we propose algorithms that consider cycles and information updates in social networks. Experiments demonstrate that our approach is effective and superior to existing trust inference methods, and can deliver more reasonable and trustworthy results. The proposed algorithms considering cycles and information updates in social networks are efficient and applicable to real social networks.

Keywords Contextual trust · Context-aware trust inference · Social networks · Recommender systems

1 Introduction

Conventional recommender systems mainly employ information filtering techniques for making recommendations. In such systems, collaborative filtering approaches [12] or content-based filtering approaches [8, 37] are adopted for making recommendations. These approaches collect ratings from the users with similar profiles or the items that are similar to the one a user liked in the past. However, these conventional approaches consider users individually and rarely address the trustworthiness of recommendations directly. In addition, as pointed out in [40], the sparsity of data in recommender systems has been a long-standing problem, which makes the filtering techniques less effective.

The ultimate goal of recommender systems is to provide high quality and trustworthy recommendations that can very likely be accepted by users. To this end, using the reviews/recommendations from social networks has been the focus in recent studies [28, 29]. In reality, people would like to turn to trusted friends or friends' friends to solicit recommendations [4]. Moreover, the new generation of social network based web application systems has drawn the attention from both academia and industry. The study in [18] has pointed out that it is a trend to build up social network based web applications (e.g., a new generation of social network based e-commerce systems or a new generation of social network based online recruitment systems). In real applications, according to a survey on 2,600 hiring managers in 2008 by CareerBuilder (careerbuilder.com, a popular job hunting website), 22 % of those managers used social networking sites to manually investigate potential employees. The ratio increased to 45 % in June 2009 and 72 % in January 2010. In Oct. 2011, eBay announced their strategic plan to deepen the relationship with Facebook[1] for creating a new crop of e-commerce applications with social networking features, which will integrate both their e-commerce platform and social networking platform seamlessly.[2]

In the meantime, this new trend clearly demands the investigations of new techniques for trust inference in social networks, which evaluates the trust between two non-adjacent participants mainly based on the trust values of the intermediate

[1] http://www.facebook.com

[2] Reuters news "eBay and Facebook unveil e-commerce partnership" at http://www.reuters.com/article/2011/10/12/ebay-facebook-idUSN1E79B22Y20111012

participants between them [10, 16, 46]. More importantly, as pointed in [31], trust inference is context sensitive. This is particularly the case when the inferred trust result is used for deriving recommendations. Also, as pointed out in the study in [44], in online social networks, it is rare for a person to have full trust in another in all facets (i.e., the case of full trust in all aspects is less than 1 % at Epinions.com and Ciao.co.uk, both of which are popular product review sites). In the society, a person's trust in another person varies in contexts, as a recommender may have different levels of expertise in different domains [1, 48]. For example, A fully trusts B in teaching C++. It doesn't mean A can also fully trust B's service in repairing a car as the two services have significantly different natures and contexts.

In the literature, there are a few studies on social network based service provider selections. In [21], an approximation algorithm has been proposed, which searches the near-optimal social trust path for satisfactory service providers. Though some contextual factors are considered in the constraints of searching, the trust evaluation uses a multiplication model, without taking into account any contextual information. In [24], the approximation algorithm was further improved for better efficiency. But there is no change in trust evaluation.

In the literature, there are also a number of studies on trust inference in social networks [10, 14, 46]. But they usually focus on the evaluation using the trust values between adjacent participants only, overlooking the influence of contextual information on trust evaluation. The study in [15] also considers the confidence (a probabilistic value) from a person to another, used in FilmTrust[3] – a prototype of social network based movie review/recommendation system. But it is unclear whether the confidence is context-based and how to evaluate it. In [22], some contextual information has been taken into account for trust transitivity. But the model considers some typical cases only without designing a generic model. As a matter of fact, the trust transitivity along a path, e.g., $A \rightarrow B \rightarrow C$, is actually quite specific to the social properties of participants, their relations, and the context of recommended targets (e.g., buying a textbook on computer security or looking for a car repairer). Thus, particularly when a recommender and a recommendation receiver are unknown to each other, a social context-aware trust inference model is needed. Such a model is expected to differentiate the social contexts relevant to the participants and recommendations, properly taking them into account in trust inference and yielding objective trust results that can be used for deriving more reasonable and trustworthy recommendations.

In this paper, we first present a contextual social network model that takes into account both participants' personal characteristics (e.g., preference and expertise in domains) and mutual relations (e.g., the trust, social intimacy, and interaction context between two adjacent participants). In addition, we propose a new probabilistic approach, *SocialTrust*, as the first solution in the literature, to social context-aware trust inference in social networks (referred to as the *contextual trust inference*). The result delivered by this approach is particularly important to evaluating the trust from a source participant to an end recommender, who recommends a target service or service provider, via the sub-network consisting of the intermediate participants between them and relevant contextual information. Based on it, we also propose

[3] http://trust.mindswap.org/FilmTrust/

an iterative algorithm for trust inference in social networks with information cycles, and an algorithm for information updates in social networks. In addition, an algorithm for trustworthy end recommender selection has been proposed. Experiments demonstrate that our approach is superior to existing trust inference methods and can deliver more reasonable and trustworthy results. The proposed iterative algorithm is efficient.

This paper is organized as follows. Section 2 reviews related work. Section 3 presents a novel contextual social network structure. In Section 4, the contextual trust inference approaches are presented. Section 5 presents our analytical and empirical studies on the effectiveness and efficiency of our proposed algorithms. Finally Section 6 concludes our work.

2 Related work

The studies of social network properties can be traced back to 1960's when the *small-world characteristic* in social networks was validated by Milgram [34] (i.e., the average path length between two Americans was found to be about 6.6 hops). In recent years, sociologists and computer scientists investigated the characteristics of popular online social networks (OSNs) [36] (e.g., Facebook (footnote 1), MySpace[4] and Flickr[5]), and validated the *small-world* and *power-law* characteristics. I.e., the probability that a node has a degree k is proportional to k^{-r} (the $-r$ power of k and $r > 1$). Next, we briefly review the work in different areas in the literature that is related to our work.

2.1 Information filtering in recommender systems

The information filtering techniques have been widely adopted in conventional recommender systems. In such systems, collaborative filtering approaches [12] or content-based filtering approaches [8, 37] are used for making recommendations, which collect ratings from the users with similar profiles or the items that are similar to the one a user liked in the past. The aim of collaborative filtering techniques is to provide recommendations that are expected to be accepted by users. But the proposed approaches usually do not address the trustworthiness of recommendations directly.

2.2 Trust-aware recommender systems

Social influence occurs when one's emotions, opinions or behaviours are affected by others.[6] As indicated in Social Psychology [4, 9, 50], in the real society, a person prefers the recommendations from trusted friends. In addition, based on statistics, Sinha et al. [41] and Bedi et al. [3] have demonstrated that given a choice between

[4] http://myspace.com

[5] http://flickr.com

[6] http://qualities-of-a-leader.com/personal-mbti-type-analysis/

the recommendations from trusted friends and those from recommender systems, in terms of quality and usefulness, trusted friends' recommendations are preferred.

Some later studies consider the propagated trust of other users [3, 32], in addition to the similarity measures of users or items. Such an approach aims to enhance the trustworthiness of recommendations generated by a system. But this raises the new need of trust evaluation/inference in social networks with more impact factors to be taken into account.

2.3 Social network based service provider searching and selection

In the literature, there are a few studies on social network based service provider searching and selection. In [25], a randomised algorithm is proposed for searching a subnetwork between a source participant and a sink participant. The proposed model considers some contextual factors, such as recommender's role and social intimacy. The subnetwork is expected to contain important participants with important contextual information for the trust evaluation from the source to the sink. In [26], an approximation algorithm is proposed for the same purpose. In [21], an approximation algorithm has been proposed, which searches the near-optimal social trust path to satisfactory service providers, with some contextual factors considered as the constraints of searching. The searching problem is modeled as a Multi-Constrained Optimal Patch (MCOP) problem, which is NP-Complete. Some contextual factors, including trust, social intimacy and role impact factor, are considered in the constraints for searching, rather than trust inference. However, the trust evaluation uses a multiplication model. In [24], the approximation algorithm has been further improved for better efficiency. But there is no change in trust evaluation. In [23], another approximation algorithm is proposed for searching top K near-optimal social trust paths, based on which the best service provider can be determined. However, we argue here that the trust of a participant in a social network depends on his/her trusters (i.e. predecessors in terms of the network structure), Thus trust inference should take into account network structures, rather than paths only, as well as contextual factors.

2.4 Trust propagation/inference in social networks

Social networks are important to recommender systems due to the data sparsity problem [28, 40] and the scenarios in real life that people turn to trusted friends and friends' friends for soliciting opinions [4, 50], raising the need of trust propagation/inference in social networks (i.e., evaluating the trust between two non-adjacent participants). Earlier studies have adopted averaging strategies (AVG for short) [10], multiplication strategies (MUL for short) [16, 46], or probabilistic approaches (PRO for short) [14, 15] based on the trust values between adjacent participants. However, they ignore contextual factors that influence trust relations and trust inference (e.g., a person's recommendation role [48] or the social intimacy between people [19]), and/or simply take the confidence to other people as a probabilistic value without discussing from where the confidence comes. Most of the existing studies usually model their approaches intuitively, without following the principles from Social Science or Social Psychology. In some recent work [19–21], following the principles in Social Psychology [1, 35], both the recommendation role resulting from

social positions (e.g., a professor) and expertise, the trust and social intimacy degree between adjacent participants in social networks have been taken into account.

2.5 Social context awareness in recommender systems

Social context awareness is very important for recommender systems because it is a means of knowing a person's social positions, preferences, and social relations with other people. All of these factors are crucial to not only adopting conventional collaborative filtering techniques but also evaluating the the trustworthiness of recommendations. A recent study in recommender systems [20, 29] takes into account social tags (or social bookmarks - a user's keyword annotations shared with friends in social networks) for measuring the preference similarity with friends. But social tags are limited in their capacity to reflect an individual's personal preferences as they do not consider the expertise of individuals in given domains and the individual's relations and intimacy with other people [6]. The scope of social context should also be naturally extended to an individual's social positions/titles/expertise, and any indication to reflect the social relations with other people, which can be obtained from a user's profile or mined from online comments and blogs [5, 7, 33, 47].

3 Contextual social networks

In this section, we propose a contextual social network structure that contains social contextual impact factors with significant influence on social interactions and trust evaluation. This structure describes the social networks in the real world better.

Conceptually, context is any information that can be used to characterize the situation of an entity [45]. An entity can be a person, a place, or an object that is relevant to the interaction between a user and an application, including themselves.

In social network based recommender systems, a typical case is that a participant p_1 trusts a participant p_2 after an interaction. The context related to adjacent participants p_1 and p_2 is referred to as the *social context*, and the context related to the interaction is referred to as the *interaction context*. If p_2 recommends a target (e.g., to teaching C++), the context of the target is referred to as the *target context*.

3.1 Social context

Social Context is the social environment of a participant in a social network [2], which can be classified into *independent social context*, such as the *role impact factor* and *preference*, and *dependent social context*, such as the *trust* and *social intimacy degree* between *adjacent participants*, which are the participants with prior interactions in social networks.

3.1.1 Independent social context

The independent social context of a participant in a social network refers to the personal characteristics that influence interactions, trust and recommendations. Typical independent social context includes a role impact factor and preference [19, 21, 25].

- **Role Impact Factor:** Rich activities of participants in social networks can be categorized into different domains (e.g., hiring employees or selling products) based on their characteristics [48]. As illustrated in the following principle, the recommendation role of a participant has significant influence on trust.
  Principle 1. The recommendation from a person who has expertise in the domain is more credible than the recommendation from a person who has no or less knowledge in that domain [1].
  Let $RIF_{R_1}^{c_i} \in [0, 1]$ denote the participant R_1's *Role Impact Factor* in the interaction context c_i, illustrating the impact of R_1's social position and expertise on the trustworthiness of R_1's recommendations. Here $RIF_{R_1}^{c_i} = 1$ indicates that R_1 is a domain expert in the interaction context c_i, while $RIF_{R_1}^{c_i} = 0$ indicates that R_1 has no knowledge in c_i. The higher the $RIF_p^{c_i}$, the more the influence of p in the interaction context c_i.
  Though it is difficult to construct the comprehensive role hierarchies in all domains for the whole society and obtain their global values, it is feasible to build them up in a specific social community. For example, through mining the subjects and contents of emails in *Enron* Corporation[7], the social position between each email sender and receiver can be discovered (e.g., a project manager or an accountant) and their roles can be known. Then the corresponding role impact factor values can be estimated based on probabilistic models. In addition, in academic social networks formed by large databases of Computer Science literature (e.g, DBLP[8] or ACM Digital Library[9]), the role of scholars (e.g., a professor in the field of data mining) can be mined from publications or their homepages. The role impact factor values can be calculated as an example by applying the PageRank model [43]. The role impact factor of a person in online networks can also result from the recognition of his/her recommendation from other participants. This can be mined from online information. Furthermore, in addition to mining these values, the social position of a participant can be specified directly [49], e.g. in LinkedIn. If the participant becomes a recommender, this social position information could illustrate his/her role impact factor in the recommendation of a specific domain.
- **Preference:** Preference could be conceived of as an individual's attitude towards a set of objects, typically reflected in an explicit decision-making process [17]. A person can have different preferences in different interaction contexts.
  The following principle in Social Psychology illustrates the influence of preference similarity on trust.
  Principle 2. The more preferences one shares with another, the more likely for them to trust each other [27].
  Let $PS_{R_1,R_2}^{c_i} \in [0, 1]$ denote the *Preference Similarity* between R_1 and R_2 in the interaction context c_i. $PS_{R_1,R_2}^{c_i} = 1$ indicates R_1 and R_2 have the same preference in the interaction context c_i, while $PS_{R_1,R_2}^{c_i} = 0$ indicates that they have no similar preference in the interaction context c_i. The higher the $PS_{p_1,p_2}^{c_i}$, the higher similarity of the preferences between p_1 and p_2 in the interaction context c_i.

[7] http://www.cs.cmu.edu/~enron/

[8] http://www.informatik.uni-trier.de/~ley/db/

[9] http://portal.acm.org/

In some existing online social networks, like at Facebook, the preference similarity between participants can be mined from their profiles [36].

3.1.2 Dependent social context

The dependent social context is the context between adjacent participants. Typically dependent social context includes trust and social intimacy degree [19, 21].

- **Trust:** Trust is the belief of one participant in another, based on their interactions, with the extent to which a future action to be performed by the latter will lead to an expected outcome [13]. As pointed in [30, 48], the trust value between two participants can be different in different interaction contexts. For example, a participant R_1 trusts a recommender R_2 in teaching C++, but R_1 may not trust R_2 in repairing a car. In our model, let $T^{c_i}_{R_1,R_2} \in [0, 1]$ denote the trust value that R_1 assigns to R_2 in an interaction context c_i. If $T^{c_i}_{R_1,R_2}=1$ indicates R_1 completely believes that R_2's future action can lead to the expected outcome in the interaction context c_i while $T^{c_i}_{R_1,R_2}=0$ indicates that R_1 completely has no trust on R_2 in the interaction context c_i. $T^{c_i}_{R_1,R_2}$ can be specified by R_1, based on the performance of the trustee R_2 in prior interactions in c_i. The higher the $T^{c_i}_{p_1,p_2}$, the more p_1 trusts p_2 in c_i.
- **Social Intimacy Degree:** The following principle in Social Psychology illustrates the influence of the social intimacy between participants on trust.
  Principle 3. A participant can trust the participants with whom he/she has more intimate social relationships than those with whom he/she has less intimate social relationships [35].
  Let $SID^{c_i}_{R_1,R_2} \in [0, 1]$ denote the *Social Intimacy Degree* between R_1 and R_2 in the interaction context c_i. $SID^{c_i}_{R_1,R_2} = 1$ indicates R_1 and R_2 have the most intimate social relationship in the interaction context c_i, while $SR^{c_i}_{R_1,R_2} = 0$ indicates that they have the least intimate social relationship in the interaction context c_i. The higher the $SID^{c_i}_{p_1,p_2}$, the greater intimacy between p_1 and p_2 in c_i.
  In the literature, in order to compute the social intimacy degree, through mining the subjects and contents of the emails the social relationship between each pair of email sender and receiver (e.g., a CEO and his/her assistant) can be discovered in the email based social network, *Enron* email (footnote 7). Then the corresponding social intimacy degree can also be estimated based on probabilistic models. In addition, in academic social networks, e.g., DBLP[8] and ACM Digital Library,[9] the social relationships between two scholars (e.g., co-authors, a supervisor and his/her students) be mined from publications or their homepages. The social intimacy degree can also be calculated as an example by applying the PageRank model [43].
  Detailed mining methods are out of the scope of this paper.

In our previous work [19, 21, 25], these factors have been taken into account respectively in the modeling of complex social networks. However, it is the first time to categorize them in the classes in terms of context, i.e. independent social context and dependant social context. In the following subsections, we will further anaylyse

the relations between interaction context and target context, and connections based on them, which are useful for designing the context-aware trust inference approach to be introduced in Section 4.

3.2 Interaction Context

The interaction context is the context in which participant p_k interacts with p_l. In social networks, after an interaction between participant p_x and participant p_y, p_x trusts p_y with the value $T^{c_i}_{p_x,p_y} \in [0, 1]$ in the interaction context c_i. For example, a participant p_1 trusts a participant p_2 who recommends the selection of teaching C++ (denoted as the interaction context c_1) with $T^{c_1}_{p_1,p_2} = 0.8$.

In the literature, there are existing methods [39, 42, 45] to compute the similarity $CS_{c_i,c_j} \in [0, 1]$ between the interaction context c_i and the interaction context c_j. The interaction context c_i is *relevant* to the interaction context c_j, if $CS_{c_i,c_j} > \mu$ (μ is a threshold, e.g., 0.7), which is denoted as $c_i \asymp c_j$. Then $T^{c_j}_{p_x,p_y}$ can be projected from $T^{c_i}_{p_x,p_y}$. For example, let c_1 denote the context of selecting the service of teaching C++. Let c_2 denote the context of selecting the service of teaching computer architecture. As c_2 is relevant to c_1, $T^{c_2}_{p_1,p_2}$ can be projected from $T^{c_1}_{p_1,p_2}$ if $T^{c_1}_{p_1,p_2}$ is known. Otherwise, if c_i is *irrelevant* to c_j, which is denoted as $c_i \not\asymp c_j$, $T^{c_j}_{p_x,p_y}$ cannot be projected from $T^{c_i}_{p_x,p_y}$. For example, let c_3 denote the context of selecting car repair services. As c_3 is irrelevant to c_1, $T^{c_3}_{p_1,p_2}$ cannot be inferred from $T^{c_1}_{p_1,p_2}$.

3.3 Transference degree of trust in contexts

In this section, we first introduce *transference degree of trust in contexts*.

With the social contexts introduced in Section 3.1, the evaluation of trust transference degree in contexts follows the following rules.

1. Based on Principle 1 from Social Science [1], the higher the role impact factor RIF of a participant p_y, the higher the transference degree of p_y's trust values given to other participants;
2. Similarly, based on Principle 2 from Social Psychology [27], the higher the preference similarity PS between two adjacent participants p_x and p_y, the higher the transference degree of p_x's trust value given to p_y;
3. In addition, based on Principle 3 from Social Psychology [35], the higher the social intimacy degree SID between two adjacent participants p_x and p_y, the higher the transference degree of p_x's trust value given to p_y.

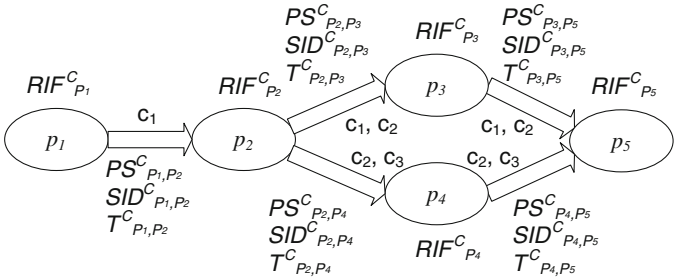
According to these rules, the trust transference degree in contexts can be evaluated by using the following formula.

Definition 1 Assume participant p_x trusts participant p_y with the trust value $T^{c_i}_{p_x,p_y}$ after an interaction in context c_i. Given a target context c_j in which p_y recommends a service provider, the *trust transference degree in contexts* $\alpha^{c_i,c_j}_{p_x,p_y}$ between two participants p_x and p_y can be evaluated with the social context of participants p_x and p_y as follows

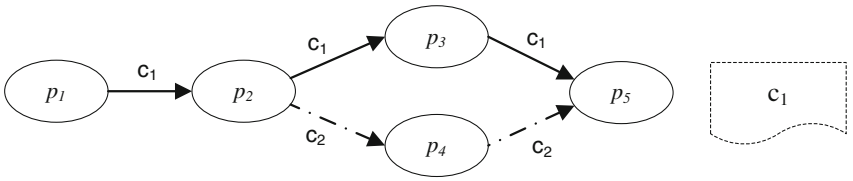
$$\alpha^{c_i,c_j}_{p_x,p_y} = \omega_1 \cdot \mathrm{RIF}^{c_j}_{p_x} + \omega_2 \cdot \mathrm{RIF}^{c_j}_{p_y} + \omega_3 \cdot \mathrm{PS}^{c_i}_{p_x,p_y} + \omega_4 \cdot \mathrm{SID}^{c_i}_{p_x,p_y} + \omega_5 \cdot CS_{c_i,c_j}, \quad (1)$$

where ω_1, ω_2, ω_3, ω_4 and ω_5 are the weights ($\sum \omega_i = 1$) specified in a source participant's trust-oriented enquiry. The sum of the weights equals 1.

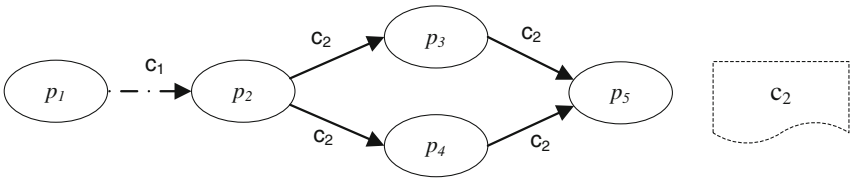
With the trust $T^{c_i}_{p_x,p_y}$ under the interaction context c_i and trust transference degree in contexts c_i and c_j $\alpha^{c_i,c_j}_{p_x,p_y}$, we can estimate the trust value $T^{c_j}_{p_x,p_y}$ in the interaction context c_j.



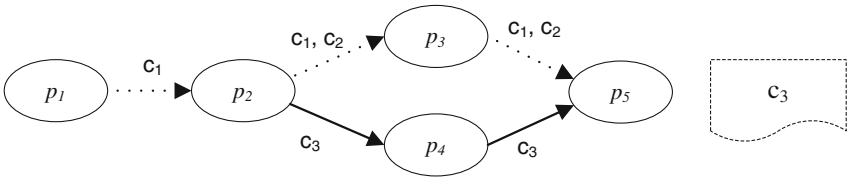
(a) a complete contextual social network (C={c_1,c_2,c_3}) where $c_1 \asymp c_2$, $c_1 \nasymp c_3$, and $c_2 \nasymp c_3$



(b) a contextual social network with a strong connection from p_1 to p_5 w.r.t. the target context c_1



(c) a contextual social network with a weak connection from p_1 to p_5 w.r.t. the target context c_2



(d) a contextual social network with no connection from p_1 to p_5 w.r.t. the target context c_3

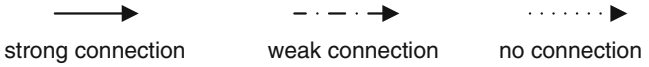


Figure 1 Contextual social networks

Definition 2 With $T^{c_i}_{p_x,p_y}$ and $\alpha^{c_i,c_j}_{p_x,p_y}$, the trust value $T^{c_j}_{p_x,p_y}$ can be evaluated as

$$T^{c_j}_{p_x,p_y} = \alpha^{c_i,c_j}_{p_x,p_y} \cdot T^{c_i}_{p_x,p_y} \tag{2}$$

3.4 A contextual social network structure

Based on the above-mentioned social context and interaction context, we propose a new structure of *contextual social networks*. In this contextual social network, each node includes the role impact factor RIF of a participant, and each link includes the preference similarity PS, trust T, and social intimacy degree SID between the adjacent participants in their interaction contexts $\{c_i\}$, where a trust value is an aggregation based on all prior interactions in the same interaction context (refer to Figure 1(a)).

In social networks, there is a basic type of trust-oriented enquiry: What is the trust value $T^{c_j}_{p_1,p_n}$ from a source participant p_1 to an end recommender p_n (the sink) who recommends a service or a service provider in the target context c_j?

With different target contexts, we can have different contextual social networks. For example, Figure 1(b), (c), (d) represent parts of the complete social network in Figure 1(a) after being filtered by the target contexts c_1, c_2 and c_3, respectively, where $c_1 \asymp c_2$, $c_1 \asymp c_3$ and $c_2 \asymp c_3$.

Regarding the inference of $T^{c_j}_{p_1,p_n}$, there are three types of connections from p_1 to p_n in contextual social networks as follows, with regard to the similarity between the interaction context of adjacent participants and the target context.

- **Strong connection:** Given a target context c_j, if each link in the subnetwork from p_1 to p_n has the same interaction context as c_j, then there is a *strong connection from p_1 to p_n w.r.t. the target context c_j* (represented by a solid line, refer to Figure 1(b)).
- **Weak connection:** Given a target context c_j, in the subnetwork from p_1 to p_n, if the interaction context of each link is the same as c_j or relevant to c_j, and the interaction context of at least one link is relevant to c_j, then there is a *weak connection from p_1 to p_n w.r.t. c_j* (represented by a dashed line, see Figure 1(c)).
- **No connection:** Given a target context c_j, if there is no path from p_1 to p_n, or any path from p_1 to p_n contains at least one link with its interaction context irrelevant to c_j, then there is *no connection from p_1 to p_n w.r.t. the target context c_j* (represented by a dotted line, refer to Figure 1(d)).

4 Contextual trust inference

Trust inference in social networks is context sensitive, influenced by the factors in both social context and interaction context identified in Section 3.1.

4.1 Probabilistic contextual trust inference in a social network with a strong connection

In order to process the contextual trust inference from the source p_1 to sink p_n in a social network with a strong connection with regard to the target context c_j, firstly we need to analyse the network structure between p_1 and p_n. Trust inference happens

in a structure with at least 2 hops. There are three types of atomic trust inference structures in social networks, which are depicted in Figure 2(a), (b), (c). Each atomic structure has up to 2 hops from the source to the sink, based on which the number of nodes and the number of links are the least. Any structure in social networks can be represented as the composition of these atomic structures.

Conceptually, trust is the subjective probability, with which a person p_1 expects that another person p_2 performs a given action, if the trust value is in the range [0,1] [13]. The network structure between p_1 and p_n in a trust inference problem can be modeled as a probabilistic network [38]. Regarding the trust from p_1 to p_2 with a link $p_1 \rightarrow p_2$, let the probability $P^{c_j}(p_2)$ denote the trustworthiness $T^{c_j}_{p_2}$ of p_2 in the interaction context c_j, $P^{c_j}(\neg p_2)$ denote the possibility of p_2 for not being trusted in the interaction context c_j; let $P^{c_j}(p_2|p_1)$ denote the trustworthiness of p_2 from the viewpoint of p_1 in the interaction context c_j, and $P^{c_j}(p_2|\neg p_1)$ denote the trustworthiness of p_2 from the viewpoint of p_2's trusters excluding p_1 in the interaction context c_j.

Atomic structure (a) (Figure 2(a)): Regarding the trust inference from the source participant p_1 to the end recommender p_3, according to the law of total probability, we have

$$\begin{aligned} T^{c_j}_{p_2} &= P^{c_j}(p_2) \\ &= P^{c_j}(p_2|p_1)P^{c_j}(p_1) + P^{c_j}(p_2|\neg p_1)P^{c_j}(\neg p_1) \\ &= P^{c_j}(p_2|p_1)P^{c_j}(p_1) + P^{c_j}(p_2|\neg p_1)(1 - P^{c_j}(p_1)) \\ &= P^{c_j}(p_2|p_1)P^{c_j}(p_1), \end{aligned} \tag{3}$$

$$\begin{aligned} T^{c_j}_{p_3} &= P^{c_j}(p_3) \\ &= P^{c_j}(p_3|p_2)P^{c_j}(p_2) + P^{c_j}(p_3|\neg p_2)P^{c_j}(\neg p_2) \\ &= P^{c_j}(p_3|p_2)P^{c_j}(p_2) + P^{c_j}(p_3|\neg p_2)(1 - P^{c_j}(p_2)) \\ &= P^{c_j}(p_3|p_2)P^{c_j}(p_2). \end{aligned} \tag{4}$$

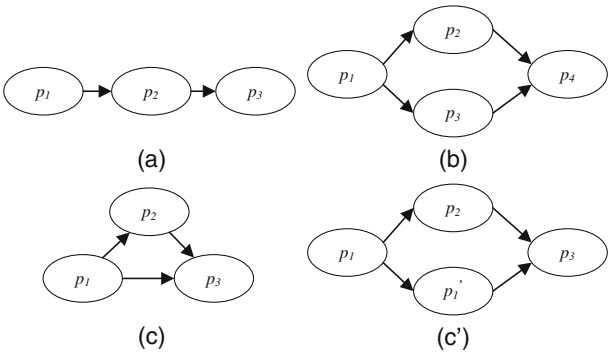


Figure 2 Atomic trust inference structures

In (3), $P^{c_j}(p_2|p_1)$ is the trustworthiness of p_2 from the viewpoint of p_1 in the interaction context c_j and it is known. As $P^{c_j}(p_1)$ represents the trustworthiness of p_1 from all p_1's trusters (predecessors) in the interaction context c_j, after the computation of the trust for each of its trusters, $P^{c_j}(p_1)$ can be obtained.

For $P^{c_j}(p_2|\neg p_1)$, it represents the trustworthiness of p_2 from the viewpoint of p_2's trusters excluding p_1 in the interaction context c_j. In the atomic structure (a), because p_1 is the only truster of p_2, we have $P^{c_j}(p_2|\neg p_1) = 0$.

Hence, with (3), $P^{c_j}(p_2) = T^{c_j}_{p_2}$ can be inferred from p_1.

Similarly, in (4), as $P^{c_j}(p_3|p_2)$ is known and $P^{c_j}(p_3|\neg p_2) = 0$, the trustworthiness of p_3 in the atomic structure (a) can be finally inferred from p_2.

Atomic structure (b) (Figure 2(b)): Regarding the trust inference from the source participant p_1 to the end recommender p_4, according to the law of total probability, we have

$$\begin{aligned} T^{c_j}_{p_2} &= P^{c_j}(p_2) \\ &= P^{c_j}(p_2|p_1)P^{c_j}(p_1) + P^{c_j}(p_2|\neg p_1)P^{c_j}(\neg p_1) \\ &= P^{c_j}(p_2|p_1)P^{c_j}(p_1), \end{aligned} \tag{5}$$

$$\begin{aligned} T^{c_j}_{p_3} &= P^{c_j}(p_3) \\ &= P^{c_j}(p_3|p_1)P^{c_j}(p_1) + P^{c_j}(p_3|\neg p_1)P^{c_j}(\neg p_1) \\ &= P^{c_j}(p_3|p_1)P^{c_j}(p_1), \end{aligned} \tag{6}$$

$$\begin{aligned} T^{c_j}_{p_4} &= P^{c_j}(p_4) \\ &= P^{c_j}(p_4|p_3 \cap p_2)P^{c_j}(p_3 \cap p_2) + P^{c_j}(p_4|\neg(p_3 \cap p_2))P^{c_j}(\neg(p_3 \cap p_2)). \end{aligned} \tag{7}$$

In the above process, similar to the calculation process in (3), $P^{c_j}(p_2)$ and $P^{c_j}(p_3)$ in (5) and (6) can be inferred respectively from p_1.

As in (7) p_3 and p_2 are independent to each other, we have

$$\begin{aligned} T^{c_j}_{p_4} &= P^{c_j}(p_4) \\ &= P^{c_j}(p_4|p_3)P^{c_j}(p_4|p_2)P^{c_j}(p_3)P^{c_j}(p_2) \\ &\quad + P^{c_j}(p_4|\neg(p_3 \cap p_2))P^{c_j}(\neg(p_3 \cap p_2)), \end{aligned} \tag{8}$$

where

$$\begin{aligned} P^{c_j}(p_4|\neg(p_3 \cap p_2)) = P^{c_j}(p_4|\neg p_3) + P^{c_j}(p_4|\neg p_2) \\ - P^{c_j}(p_4|\neg p_3)P^{c_j}(p_4|\neg p_2), \end{aligned} \tag{9}$$

and

$$P^{c_j}(\neg(p_3 \cap p_2)) = P^{c_j}(\neg p_3) + P^{c_j}(\neg p_2) - P^{c_j}(\neg p_3)P^{c_j}(\neg p_2). \tag{10}$$

With the results of (5) and (6), $P^{c_j}(\neg(p_3 \cap p_2))$ in (10) can be obtained.

As $P^{c_j}(p_4|\neg p_3)$ and $P^{c_j}(p_4|\neg p_2)$ can be calculated, $P^{c_j}(p_4|\neg(p_3 \cap p_2))$ can be obtained in (9).

In addition, as $P^{c_j}(p_4|p_3)$ and $P^{c_j}(p_4|p_2)$ can be calculated, with (8) the trustworthiness of p_4 in the atomic structure (b) can be finally inferred from p_1.

Atomic structure (c) (Figure 2(c)): Regarding the trust inference from the source participant p_1 to the recommender p_3, here we take p_1' as a mirror participant of p_1, which is depicted in Figure 2 (c'). In addition, $P^{c_j}(p_1'|p_1) = 1$, $P^{c_j}(p_1'|\neg p_1) = 0$ and $P^{c_j}(p_3|p_1') = P^{c_j}(p_3|p_1)$. Then we can apply the approach for structure (b) to structure (c) in Figure 2. Hence, in structure (c), the trustworthiness of p_3 can be finally inferred from p_1.

Composition For a complex social network from p_1 to p_n composed of atomic structures, let us illustrate the details of the trust inference process, which starts from p_1 (the source) and ends at p_n (the sink). For any intermediate participant p_y, we only consider its direct predecessors $\{p_{x_s}\}$ whose

$$RIF^{c_i}_{R_{k_s}} > \gamma_1, \quad PS^{c_i}_{R_{k_s},R_l} > \gamma_2, \quad \text{and} \quad SID^{c_i}_{R_{k_s},R_l} > \gamma_3, \tag{11}$$

where γ_1, γ_2 and γ_3 are the thresholds specified for trust inference. This is due to the fact that if the value of one of the social context factors is too small, the corresponding link is untrustworthy and it should be filtered out. When $\{p_{x_s}\}$ has been calculated, we can obtain $P^{c_j}(\bigwedge p_{x_s})$ and $P^{c_j}(\neg \bigwedge p_{x_s})$. In addition, $P^{c_j}(p_y|\bigwedge p_{x_s})$ and $P^{c_j}(p_y|\neg \bigwedge p_{x_s})$ are the trust between adjacent participants caused by prior interactions. Then according to the law of total probability, we can calculate

$$\begin{aligned} T^{c_j}_{p_y} &= P^{c_j}(p_y) \\ &= P^{c_j}(p_y|\bigwedge p_{x_s})P^{c_j}(\bigwedge p_{x_s}) + P^{c_j}(p_y|\neg\bigwedge p_{x_s})P^{c_j}(\neg\bigwedge p_{x_s}). \end{aligned} \tag{12}$$

Hence, with the trust $T^{c_j}_{p_x,p_y}$ in the target context c_j between any adjacent participants, the contextual trust $T^{c_j}_{p_n}$ of p_n in c_j can be inferred from p_1. Note before trust inference, the subnetwork between p_1 and p_n should be identified. In the literature, there are some models for this purpose [25, 26].

The details of our contextual trust inference approach for a social network with a strong connection are presented in Algorithm 1. It extends the *topological sort algorithm* [11], which guarantees that any node in a directed graph is always visited after all its predecessors. This algorithm incurs a complexity of $O(N_n + N_l)$, where N_n is the number of participants (nodes) in social networks between p_1 and p_n, and N_l is the number of interactions (links). Note before any trust inference, the subnetwork between the source p_1 and the sink p_n should be identified. This can be done by following the approaches proposed in [25, 26].

4.2 Contextual trust inference in a social network with a weak connection

Given a target context c_j in a trust-oriented enquiry, for any intermediate link (such as the one from p_x to p_y) between p_1 and p_n, if there are several prior interactions with contexts $\{c_h\}$ on this link, we select the interaction in context c_i with $CS_{c_i,c_j} = \max\{CS_{c_h,c_j}\}$, and take its trust value $T^{c_i}_{p_x,p_y}$ to infer trust $T^{c_j}_{p_1,p_n}$. This is due to the fact that the largest CS_{c_i,c_j} means the most influence on trust inference, leading to the most convincing results in trust inference.

Algorithm 1 Contextual trust inference for a social network with a strong connection

Data: the contextual social network between the source p_1 and the sink p_n with a strong connection w.r.t. the target context c_j
Result: the contextual trust $T_{p_n}^{c_j}$ of p_n in c_j inferred from p_1

```
1  begin
2      Create a stack S; mark all nodes as unvisited;
3      Push the source p_1 into S, and mark it as visited;
4      while S is not empty do
5          Pop up the node p_y on the top of S, and mark it as visited;
6          Denote all the predecessors of p_y that satisfy Eq. (11) as {p_{x_s}};
7          P^{c_j}(p_y) = P^{c_j}(p_y | ⋀ p_{x_s}) P^{c_j}(⋀ p_{x_s}) + P^{c_j}(p_y | ¬⋀ p_{x_s}) P^{c_j}(¬⋀ p_{x_s});
8          for each successor p_z of p_y that satisfies Eq. (11) do
9              if p_z has no unvisited predecessors then
10                 Push p_z into S;
11             end
12         end
13     end
14     return P^{c_j}(p_n)=T_{p_n}^{c_j} inferred from p_1 (p_n is the last node popped up from S);
15 end
```

Now let us explain how to evaluate $T_{p_x,p_y}^{c_j}$ from $T_{p_x,p_y}^{c_i}$. With the trust value $T_{p_x,p_y}^{c_i}$ and the transference degree of trust in contexts $\alpha_{p_x,p_y}^{c_i,c_j}$, the trust value $T_{p_x,p_y}^{c_j}$ for any intermediate link $p_x \to p_y$ between p_1 (the source) and p_n (the sink) can be calculated according to (2). Then, the contextual trust inference in a social network between p_1 and p_n with a weak connection w.r.t. c_j (see Figure 1 (c)) can follow the contextual trust inference in a social network with a strong connection, which can be completed by Algorithm 1.

4.3 Contextual trust inference in a social network with cycles

In Sections 4.1 and 4.2, we have proposed the contextual trust inference approaches for a social network with a strong connection and a weak connection respectively w.r.t. the target context c_j. However, these approaches assume there are no cycles. But in fact cycles widely exist in social networks. Hence, in this section, we propose an iterative approach for contextual trust inference in social networks to take cycles into account.

As the trust of a participant is subject to his/her direct predecessors, the occurrence of a cycle can pass the influence of a successor back to a predecessor, which hereafter influences the successor again. Thus, trust inference in a cycle requires iterations to pass the influence of a predecessor to a successor via the cycle repeatedly until the trust values of all participants in the cycle become stable.

The iterative algorithm (Algorithm 2) works as follows.

Step 1: Mark all nodes (participants) as unvisited. Set p_1 as the current node p_y, and mark it as visited ($O(n)$) (lines 4–5 in Algorithm 2).

Step 2: For the current node p_y, consider all its predecessors $\{p_{x_s}\}$ that satisfy (11). If p_{x_s} has not been processed in this round φ, take its value $P^{c_j}(p_{x_s})^{(\varphi-1)}$ in the last round $\varphi - 1$ as $P^{c_j}(p_{x_s})^{(\varphi)}$. Then evaluate $P^{c_j}(p_y)^{(\varphi)}$ following (12). If all nodes have been visited, go to Step 3. Otherwise, set the unvisited node p_z that is the successor of p_y and satisfies (11) as the current node

p_y, mark it as visited and go back to the beginning of Step 2 ($O(n)$) (lines 6–16).

Step 3: Repeat Step 1 and Step 2 until for each p_y between p_1 and p_n we have $|P^{c_j}(p_y)^{(\varphi)} - P^{c_j}(p_y)^{(\varphi-1)}| < \epsilon$ or p_n has been visited for λ times (lines 3–18).

Step 4: The contextual trust of p_n is inferred from p_1 (line 19).

This algorithm incurs a complexity of $O(\lambda(N_n + N_l))$, where N_n is the number of participants (nodes) in social networks between p_1 and p_n, N_l is the number of interactions (links) and λ is the iteration times.

Algorithm 2 Iterative contextual trust inference approach for a social network with cycles

Data: a contextual social network with cycles from the source p_1 to the sink p_n, the interactive times threshold λ (such as 1000), and the trust difference threshold ϵ (such as 0.01).
Result: the contextual trust $T_{p_n}^{c_j}$ of p_n in the target context c_j inferred from p_1.

1 **begin**
2 Set $\varphi = 0$; mark all nodes as unvisited;
3 **while** $\exists p_y$ between p_1 and p_n *satisfying* $|P^{c_j}(p_y)^{(\varphi)} - P^{c_j}(p_y)^{(\varphi-1)}| > \epsilon$ **and** $\varphi \in [1, \lambda]$ **do**
4 Create a stack S;
5 Push the source participant p_1 into S, and mark it as visited;
6 **while** S is not empty **do**
7 Pop up the top node p_y in S, and mark it as visited;
8 Let $\{p_{x_s}\}$ denote all the predecessors of p_y that satisfy Eq.(11);
9 **if** $p_{x'_s} \in \{p_{x_s}\}$ has not been computed **then**
10 $P^{c_j}(p_{x'_s})^{(\varphi)} = P^{c_j}(p_{x'_s})^{(\varphi-1)}$
11 **end**
12 $P^{c_j}(p_y)^{(\varphi)} = P^{c_j}(p_y|\bigwedge p_{x_s})^{(\varphi)} P^{c_j}(\bigwedge p_{x_s})^{(\varphi)} + P^{c_j}(p_y|\neg\bigwedge p_{x_s})^{(\varphi)} P^{c_j}(\neg\bigwedge p_{x_s})^{(\varphi)}$;
13 **for** each successor p_z of p_y that satisfies Eq. (11) **do**
14 Push p_z into S;
15 **end**
16 **end**
17 Mark all nodes as unvisited and set $\varphi = \varphi + 1$;
18 **end**
19 **return** the contextual trust $T_{p_n}^{c_j} = P^{c_j}(p_n)$ inferred from p_1;
20 **end**

4.4 Contextual trust inference in a social network with updates

Within a social network, there would updates from time to time. Whenever there is a new link added from participant p_x to participant p_y or any value update between p_x to p_y, it incurs the need of trust re-evaluation of p_y and its successors. The corresponding process can be completed in the following two cases.

Case (1): p_y is not in any cycle. In such a case, p_y and its successors can be visited in sequence and the trust re-evaluation is completed at each visit to a node.

Case (2): p_y is in a cycle. In such a case, the trust re-evaluation of p_y's successors will finally affect p_y's trust value. Thus, iterations along the cycle that p_y

Algorithm 3 Iterative contextual trust inference approach for a social network with updates

Data: the contextual trust network between p_1 and p_n, the interactive times λ (such as 1000), a threshold ϵ (such as 0.01), the changed recommendation from p_x to p_y.
Result: the contextual trust of p_n inferred from p_1.

begin
  while $\exists p_t$ between p_1 and p_n *s.t.* $|P^{c_j}(p_t)^{(\varphi)} - P^{c_j}(p_t)^{(\varphi-1)}| > \epsilon$ **and** $\varphi \in [1, \lambda]$ **do**
    Create a stack S; mark all nodes as unvisited;
    Push the source participant p_y into S, and mark it as visited;
    while S is not empty **do**
      Pop up the top node p_y in S, and mark it as visited;
      Denote all the predecessors of p_y that satisfy Eq.(11) as $\{p_{x_s}\}$;
      if $p_{x'_s} \in \{p_{x_s}\}$ has not been computed **then**
        $P^{c_j}(p_{x'_s})^{(\varphi)} = P^{c_j}(p_{x'_s})^{(\varphi-1)}$
      end
      $P^{c_j}(p_y)^{(\varphi)} = P^{c_j}(p_y|\bigwedge p_{x_s})^{(\varphi)} P^{c_j}(\bigwedge p_{x_s})^{(\varphi)} + P^{c_j}(p_y|\neg\bigwedge p_{x_s})^{(\varphi)} P^{c_j}(\neg\bigwedge p_{x_s})^{(\varphi)}$;
      for each successor p_z of p_y that satisfies Eq. (11) **do**
        Push p_z into S;
      end
    end
    Mark all nodes as unvisited; set $\varphi = \varphi + 1$;
  end
  return the contextual trust $P^{c_j}(p_n) = T^{c_j}_{p_n}$ inferred from p_1;
end

belongs to should be performed until the trust values of the nodes in the cycle become stable.

The details of this approach are presented in Algorithm 3

4.5 Trustworthy recommender selection in a social network

Now let us illustrate the trustworthy recommender selection in contextual social networks. Given a target context c_j, with the contextual trust inference approaches in a social network with either a strong connection or a weak connection proposed in Sections 4.1 and 4.2, the trust value $T^{c_j}_{p_1,p_n}$ of an end recommender p_n can be inferred from the requesting participant p_1. This trust value indicates the trustworthiness of p_n in the target context c_j. Meanwhile, given a target and its context c_j, if there are a set of end recommenders (sinks) $\{p_n^{(h)}\}$ recommending this target, with the above trust inference algorithms for a social network with either a strong connection or a weak connection, the trustworthiness of each $p_n^{(h)}$ in c_j can be calculated. Based on them, the most trustworthy recommender can be selected. The detailed trustworthy recommender selection algorithm (Algorithm 4) works as follows.

Intuitively, for the network between p_1 and each $p_n^{(h)}$, we can process separately and thus obtain $T^{c_j}_{p_n^{(h)}}$. But this incurs higher complexity. Rather, the network between

Algorithm 4 Trustworthy recommender selection in a social network

Data: the trust network between p_1 and end recommenders $\{p_n^{(h)}\}$, a threshold κ of the number of hops NoH, a trust difference threshold ϵ (such as 0.01).
Result: the maximum contextual trust $p_n^{(optimal)}$ inferred from p_1.

```
1  begin
2      Create a stack S; mark all nodes as unvisited;
3      Push the source participant p_1 into S, and mark it as visited;
4      while S is not empty do
5          Pop up the top node p_y from S, and mark it as visited;
6          Evaluate P(p_y);
7          if the number of hops NoH_{p_1,p_y} < κ then
8              for each successor p_z of p_y that satisfies Eq. (11) do
9                  Push p_z into S;
10                 NoH_{p_1,p_z} = NoH_{p_1,p_y} + 1;
11             end
12         end
13     end
14     return the maximum trust P^{c_j}(p_n^{(optimal)}) = max(P^{c_j}(p_n^{(h)})) inferred from p_1
       selected from visited end recommenders;
15 end
```

p_1 and all $\{p_n^{(h)}\}$ can be processed as a whole. The one-off process is described below, which extends Algorithm 1.

Step 1: Mark all nodes (participants) as unvisited. Set p_1 as the current node, and mark it as visited ($O(n)$) (lines 2–3 in Algorithm 4).

Step 2: For the current node p_y, if its number of hops from p_1 is no more than the threshold κ, its trust value $P^{c_j}(p_y)$ is evaluated, and mark it as visited. If each node with the number of hops from p_1 no more than κ has been visited, go to Step 3. Otherwise, push the successor p_z of p_y into the stack if p_z has no unvisited predecessors, and go back to Step 2 ($O(n)$) (lines 4–13).

Step 3: The contextual trust of each recommenders in $\{p_n^{(h)}\}$ is inferred from p_1, from which optimal contextual trust $p_n^{(optimal)}$ can be selected (line 14).

This algorithm incurs a complexity of $O(N_n + N_l)$, where N_n is the number of participants (nodes) in social network from p_1 to $\{p_n^{(h)}\}$, and N_l is the number of links between p_1 and $\{p_n^{(h)}\}$. By contrast, if we take the network between p_1 and each $p_n^{(h)}$ separately, the complexity will be $O(m(N_n + N_l))$ where $m = |\{p_n^{(h)}\}|$. Certainly, Algorithm 4 does not take cycles into account. But this can be easily extended as in Algorithm 2.

5 Experiments

In our experiments, firstly, we consider some typical cases to study the effectiveness of our model with no connection, weak connection and strong connection respectively between a source participant and a sink participant. These cases can cover the basic structures of social networks (serial and parallel structures) in real world

Table 1 The target contexts used in studies

Context ID	Context	Context relation
c_1	Teaching C++	$c_1 \asymp c_2$ and $c_1 \not\asymp c_3$
c_2	Teaching computer architecture	$c_2 \asymp c_1$ and $c_2 \not\asymp c_3$
c_3	Car repair service	$c_3 \not\asymp c_1$ and $c_3 \not\asymp c_2$

scenarios. Secondly, we compare our model with the trust inference models adopting the multiplication strategy (MUL for short) [16, 46] and the averaging strategy (AVG for short) [10]. Since the determination of confidence (a probabilistic value) is not introduced in the probabilistic models (PRO for short) [14, 15], we cannot compare our model with PRO. Finally, without loss of generality, the trust value between two participants is generated by using function rand in Matlab, and set $\omega_1 = \omega_2 = \omega_3 = \omega_4 = \omega_5 = 0.2$ and $CS = 0.8$. The target contexts and their relationships used in the cases are listed in Table 1.

The *Enron* email dataset (footnote 7) has been proved to possess the small-world and power-law characteristics of social networks, and it has been widely used in the studies of social networks [21, 22, 33]. Thus, we extract 4 social networks from the *Enron* email dataset (footnote 7) with 87,474 nodes (participants) and 300,511 links (formed by sending and receiving emails) by randomly selecting 4 pairs of source and sink nodes with cycles in their subnetworks, and they are used to investigate the performance of our iterative algorithm in the real world scenarios. The maximal path length in each of these social networks is 7 hops, fitting the small-world phenomenon.

In addition, in the following studies 1–3, we analyse the effectiveness of our proposed trust inference approach. As trust decays in multiple hops [30], we consider a network with up to 3 hops between a source and a sink, covering the most popular case with a user's friends and friends' friends.

At last, the experiment is implemented using Matlab R2008a running on a Desktop with an Intel Core i5 2.80 GHz CPU, 4 GB RAM, Windows 7 Professional SP1 operating system and MySql 5.1.35 relational database.

5.1 Study 1: No connection between source and sink

In order to investigate the performance of our trust inference model in a social network with *no connection* from the source to the sink, we consider a case as shown in Figure 3, with a social network containing three participants p_1, p_2 and p_3, and their RIF, SID, PS and T values. In this case, given a target context c_3, based on the context relationship in Table 1, the interaction context (i.e. c_1, teaching C++)

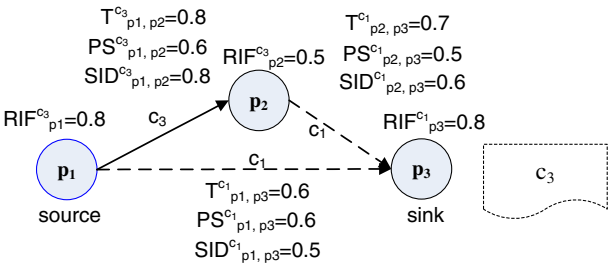


Figure 3 Study 1: No connection from R_1 to R_3 w.r.t. c_3

Table 2 Experimental results in study 1

Trust inference models	Trust inference results
MUL	0.58
AVG	0.68
Our model	No inference performed

between p_1 and p_3, and between p_2 and p_3 are irrelevant, leading to a social network with "no connection" from p_1 to p_3 w.r.t. c_3.

Results and analysis From the results listed in Table 2, we could see that our model does not infer any trust value because of no connection w.r.t. the target context and the principle that trust inference is context sensitive [31]. By contrast, the MUL model[10] and AVG model[11] deliver high trust values in the recommendation of a *teaching C++*, based on the recommendations of an irrelevant *car repair service*, leading to unreasonable results that do not make any sense.

5.2 Study 2: Strong connection with different social contexts

With a *strong connection* between a source and a sink in different social contexts, we consider the following four cases with the social networks containing different RIF, SID and PS values as listed from Figures 4, 5, 6 and 7. In these cases, given a target context c_3, each of the interaction contexts between two adjacent participants in the four cases is the same as the target context. The values of RIF, SID and PS are listed in these figures, where $RIF_{p_7}^{c_3}$ in *Case 2*, $PS_{p_7,p_8}^{c_3}$ in *Case 3* and $SID_{p_7,p_8}^{c_3}$ in *Case 4* are modified to be less than the corresponding values in *Case 1*, in order to see changes in different models.

Results and analysis From Table 3, we could see that our trust inference results in *Cases 2–4* (i.e., 0.71, 0.71, 0.69) are less than the one in *Case 1* (i.e., 0.77). This is because our model considers the influence of transference degree on trust and trust inference. Namely, the higher the RIF of a participant, and the SID and PS between adjacent participants, the higher the transference degree of the trust between them in trust inference, following the *Principles 1–3* validated in Social Science (see Section 3.1). By contrast, each of MUL and AVG models delivers the same trust inference result in all four cases, without considering any impact of social context on trust and trust inference. Therefore, our model can deliver more reasonable trust inference results than each of MUL and AVG.

5.3 Study 3: Weak connection from source to sink

In this study, we consider two cases as shown in Figures 8 and 9, where there are the same social context values, but different interaction contexts between p_{10} and p_{12}, and between p_{11} and p_{12} (i.e., c_2 in *Case 1* and c_1 in *Case 2*). Then given a target context c_2, we get a strong connection (see Figure 8) and a weak connection (see Figure 9) respectively from the source to the sink.

[10] $T_{MUL} = T_{p_1,p_2}^{c_3} \cdot T_{p_2,p_3}^{c_1}$

[11] $T_{AVG} = (T_{p_1,p_2}^{c_3} + T_{p_2,p_3}^{c_1})/2$

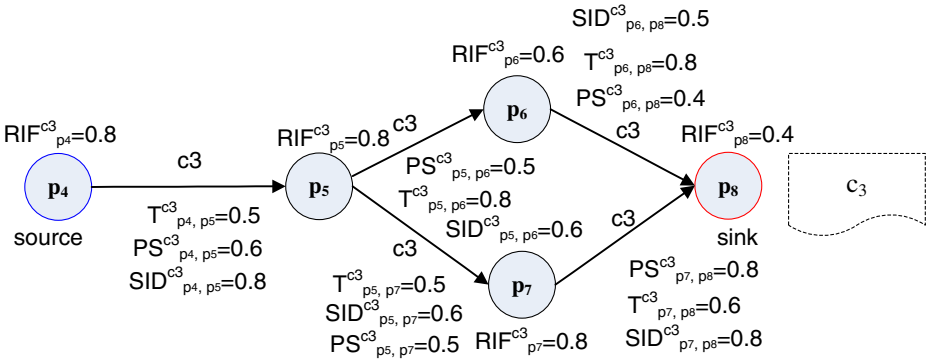


Figure 4 Study 2-Case 1: Strong connection from p_4 to p_8 w.r.t. the target context c_3

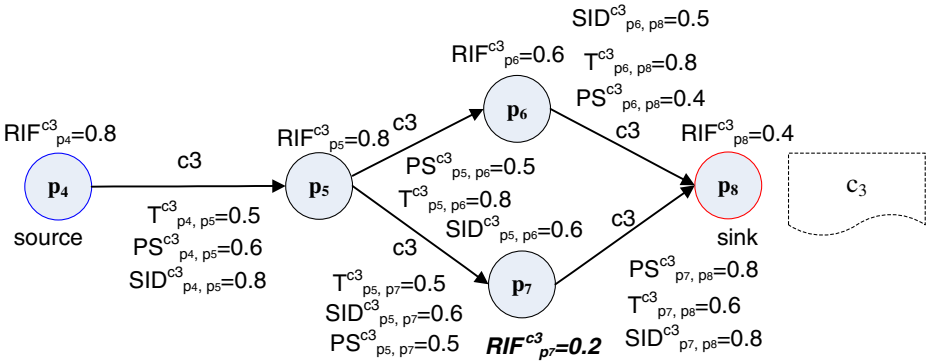


Figure 5 Study 2-Case 2: Strong connection with $RIF_{p_7}^{c_1} = 0.2$ w.r.t. the target context c_3

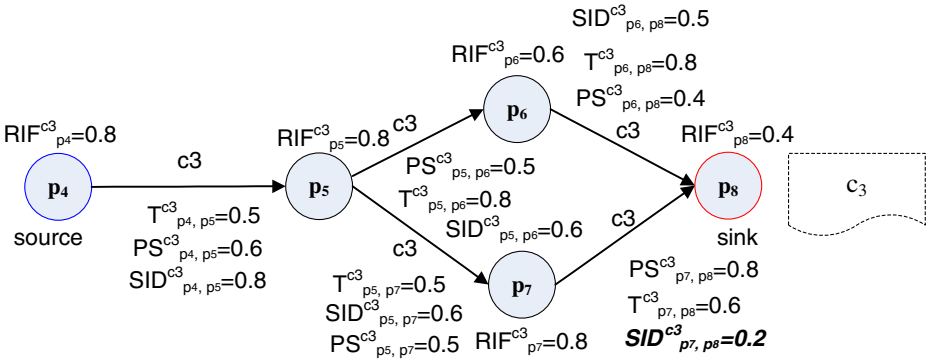


Figure 6 Study 2-Case 3: Strong connection with $SID_{p_7,p_8}^{c_1} = 0.2$ w.r.t. the target context c_3

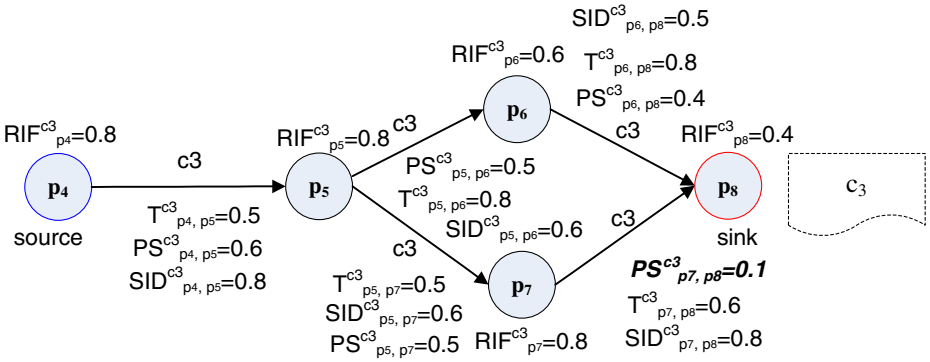


Figure 7 Study 2-Case 4: Strong connection with $PS^{c_1}_{p_7,p_8} = 0.1$ w.r.t. the target context c_3

Table 3 Results in study 2

Trust inference models	Trust inference results			
	Case 1	Case 2	Case 3	Case 4
MUL	0.24	0.24	0.24	0.24
AVG	0.61	0.61	0.61	0.61
Our model	0.77	0.71	0.71	0.69

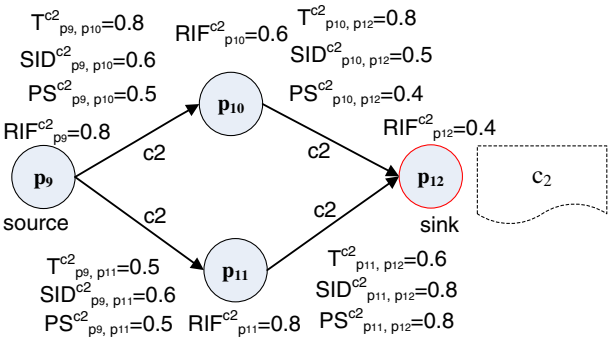


Figure 8 Study 3-Case 1: Strong connection from p_9 to p_{12} w.r.t. the target context c_2

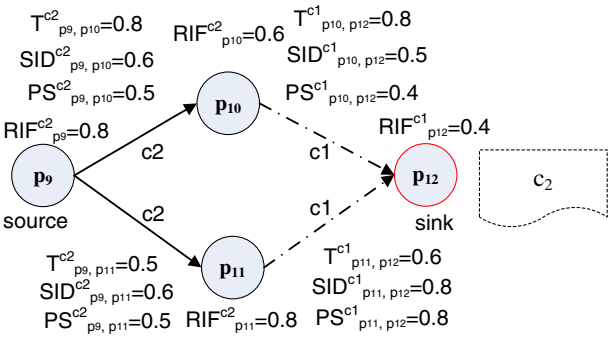


Figure 9 Study 3-Case 2: Week connection from p_9 to p_{12} w.r.t. the target context c_2

Table 4 Results in study 3

Trust inference models	Trust inference results	
	Case 1	Case 2
MUL	0.47	0.47
AVG	0.67	0.67
Our model	0.72	0.62

Results and analysis From Table 4, we could see that our trust inference result in *Case 2* (i.e., 0.62) is less than the one in *Case 1* (i.e., 0.72). This is because our model discounts trust values during trust inference with relevant interaction contexts, following the principles in Social Science [4]. Namely, the target context c_2 of *teaching computer architecture* is an enquiry is relevant to the context c_1 of the interactions between p_{10} and p_{12}, and between p_{11} and p_{12} on the recommendation of *teaching C++*, but not the same. By contrast, each of MUL and AVG models delivers the same trust inference results in the two cases without considering any difference in contexts.

5.4 Study 4: Iterations of the trust inference in social networks with cycles

In this experiment, we aim to investigate our iterative method introduced in Section 4.5. We conduct the experiments in four social networks listed in Table 5. The largest network has 321 nodes and 860 links. Its longest path has 7 hops. The iterative process is conducted in all nodes of these social networks.

Results and analysis Table 6 lists the experimental results in *Study 4*, where each execution time is averaged based on 5 independent runs. From it, we could see that after no more than 6 iterations, the variation Δ of the trust inference results at all nodes in all four social networks is less than $1.0 * 10^{-4}$ between two adjacent iterations. Namely, our iterative method is an efficient method to deliver stable trust inference results in the social networks with cycles. This feature is important for applying our approach to large-scale social networks where information and link updates happen frequently. By contrast, the existing trust inference models do not provide any specific strategies for the trust inference in a social network with cycles.

5.5 Summary

From the above case studies, we could see that our context-aware trust inference model considers social context, interaction context and target context, which have significant influence on trust inference. Thus, it follows the principles indicated in Social Science well. However, both MUL [16, 46] and AVE [10] models neglect these contexts, and thus cannot deliver reasonable trust inference results. In addition,

Table 5 The extracted social networks

ID	Nodes	Links	Maximal hops
#1	61	124	7
#2	110	293	7
#3	179	488	7
#4	321	860	7

Table 6 Results of iterations

ID	Δ	Iteration times	Execution time (sec.)
#1	$1 * 10^{-2}$	4	5.57
	$1 * 10^{-3}$	5	7.2
	$1 * 10^{-4}$	5	7.8
#2	$1 * 10^{-2}$	5	0.95
	$1 * 10^{-3}$	6	1.23
	$1 * 10^{-4}$	6	1.25
#3	$1 * 10^{-2}$	5	65
	$1 * 10^{-3}$	6	82
	$1 * 10^{-4}$	6	82.1
#4	$1 * 10^{-2}$	4	72.8
	$1 * 10^{-3}$	5	100.1
	$1 * 10^{-4}$	5	100.3

PRO model [14, 15] has the similar weakness as it does not consider context either. Therefore, our context-aware trust inference model is superior to existing models and can deliver more reasonable trust inference results. Furthermore, our iterative method is efficient for the trust inference in social networks with cycles in the paths between a source and a sink.

6 Conclusions

Conventional recommender systems leverage the collaborative filtering technique which relies the recommendations from the users who have similar preferences or profiles to the requesting user. It is effective when there are sufficient similar users with recommendations. But the long-standing data sparsity problem causes ineffectiveness to this technique. The emerge of online social networks provide more participants and information for recommender systems to make recommendations, providing a new avenue to the traditional problem [28, 29]. Meanwhile, in reality, people would like to turn to friends or friends' friends for recommendations [4]. Thus, a trust inference approach is in demand for trustworthy recommender selection and trust enhanced recommendation generation.

As trust transitivity is dynamic and context sensitive, the evaluation of trust is a challenging and a very complex task. In this paper, we first identify some social contextual factors with significant influence on trust relations and trust inference, and propose a new contextual social network structure. Based on it, a novel probabilistic approach has been proposed for contextual trust inference in social networks. To the best of our knowledge, this is the first solution in the literature to social context-aware trust inference in social networks. Because both independent social context (e.g. preference and recommendation expertise) and dependent social context (e.g. trust and social relation) have been taken into account in trust inference, the proposed approach can deliver more reasonable results and is superior to existing trust inference models in social networks. The proposed approach is particularly helpful to overcome the traditional data sparsity problem in recommender systems, and is particularly important when seeking recommendations from participants in social networks who are unknown to the end user (i.e. the source participant). In addition, our proposed algorithms also consider social networks with cycles and

information updates, which widely exist or frequently happen in social networks. The conducted experiments have demonstrated that our model and approaches could yield more reasonable and trustworthy results and recommendations by considering contextual factors. The proposed iterative algorithm is efficient and can be applied to real social networks.

Though recommending services and service providers is taken as the application in this paper, our contextual trust inference approach can be applied to the recommendation of products and potential employees if a contextual social network is available as the backbone. It can also be applied to social network based e-commerce systems, where our model will help analyse the trust relation between buyers with ratings and the trustworthiness of them. Regarding future work, though there have been some existing studies on social media mining and social influence mining [5, 7, 33, 44], further work is needed for the mining of all four contextual factors that are taken into account in our model.

References

1. Adler, P.S.: Market, hierarchy, and trust: The knowledge economy and the future of capitalism. Organ. Sci. **12**(2), 215–234 (2001)
2. Barnett, E., Casper, M.: A definition of social environment. Am. J. Public Health **91**(3), 465 (2001)
3. Bedi, P., Kaur, H., Marwaha, S.: Trust based recommender system for semantic web. In: IJCAI 2007, pp. 2677–2682 (2007)
4. Berscheid, E., Reis, H.T.: Attraction and close relationships. In: The Handbook of Social Psychology (1998)
5. Cho, Y.-S., Steeg, G.V., Galstyan, A.: Co-evolution of selection and influence in social networks. In: AAAI 2011 (2011)
6. Cui, P., Wang, F., Yang, S., Sun, L.: Item-level social influence prediction with probabilistic hybrid factor matrix factorization. In: AAAI 2011 (2011)
7. Deng, H., King, I., Lyu, M.R.: Formal models for expert finding on dblp bibliography data. In: ICDM 2008, pp. 163–172 (2008)
8. Deshpande M., Karypis G.: Item-based top-*n* recommendation algorithms. ACM Trans. Inf. Syst. **22**(1), 143–177 (2004)
9. Fiske, S.: Social Beings: Core Motives in Social Psychology. John Wiley and Sons Press (2009)
10. Golbeck, J.: Generating predictive movie recommendations from trust in social networks. In: iTrust 2006, pp. 93–104 (2006)
11. Gross, J., Yellen, J.: Handbook of Graph Theory. CRC Press (2003)
12. Herlocker, J.L., Konstan, J.A., Borchers, A., Riedl, J.: An algorithmic framework for performing collaborative filtering. In: SIGIR 1999, pp. 230–237 (1999)
13. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decis. Support Syst. **43**(2), 618–644 (2007)
14. Kuter, U., Golbeck, J.: Sunny: a new algorithm for trust inference in social networks using probabilistic confidence models. In: AAAI 2007, pp. 1377–1382 (2007)
15. Kuter, U., Golbeck, J.: Using probabilistic confidence models for trust inference in web-based social networks. ACM Trans. Internet Technol. **10**(2) (2010)
16. Li, L., Wang, Y., Lim, E.-P.: Trust-oriented composite service selection and discovery. In: ICSOC/ServiceWave 2009, pp. 50–67 (2009)
17. Lichtenstein, S., Slovic, P.: The Construction of Preference. Cambridge University Press (2006)
18. Liu, G., Wang, Y., Li, L.: Trust management in three generations of web-based social networks. In: CPSC 2009, pp. 446–451 (2009)
19. Liu, G., Wang, Y., Orgun, M.A.: Optimal social trust path selection in complex social networks. In: AAAI 2010, pp. 1391–1398 (2010)
20. Liu, G., Wang, Y., Orgun, M.A.: Quality of trust for social trust path selection in complex social networks. In: AAMAS 2010, pp. 1575–1576 (2010)

21. Liu, G., Wang, Y., Orgun, M.A., Lim, E.-P.: A heuristic algorithm for trust-oriented service provider selection in complex social networks. In: IEEE SCC 2010, pp. 130–137 (2010)
22. Liu, G., Wang, Y., Orgun, M.A.: Trust transitivity in complex social networks. In: AAAI 2011, pp. 1222–1229 (2011)
23. Liu, G., Wang, Y., Orgun, M.A.: Finding K optimal social trust paths for the selection of trustworthy service providers in complex social networks. In: ICWS'11, pp. 41–48 (2011)
24. Liu, G., Wang, Y., Orgun, M.A., Lim, E.P.: Finding the optimal social trust path for the selection of trustworthy service providers in complex social networks. IEEE Trans. Serv. Comput. (TSC) **6**(2), 152–167 (2013)
25. Liu, G., Wang, Y., Orgun, M.A.: Social context-aware trust network discovery in complex contextual social networks. In: AAAI'12, pp. 101–107 (2012)
26. Liu, G., Wang, Y., Orgun, M.A., Liu, H.: Discovering trust networks for the selection of trustworthy service providers in complex contextual social networks. In: ICWS'12, pp. 384–4391 (2012)
27. Luhmann, N.: Trust and Power. Wiley (1979)
28. Ma, H., Yang, H., Lyu, M.R., King, I.: Sorec: social recommendation using probabilistic matrix factorization. In: CIKM 2008, pp. 931–940 (2008)
29. Ma, H., Zhou, T.C., Lyu, M.R., King, I.: Improving recommender systems by incorporating social contextual information. ACM Trans. Inf. Syst. **29**(2), 9 (2011)
30. Mansell, R., Collins, B.: Trust and Crime in Information Societies. Edward Elgar Publishing (2005)
31. Marsh, S.: Formalising Trust as a Computational Concept. University of Stirling, UK (1994)
32. Massa, P., Avesani, P.: Trust-aware collaborative filtering for recommender systems. In: CoopIS/DOA/ODBASE 2004, pp. 492–508 (2004)
33. McCallum, A., Wang, X., Corrada-Emmanuel, A.: Topic and role discovery in social networks with experiments on enron and academic email. J. Artif. Intell. Res. (JAIR) **30**, 249–272 (2007)
34. Milgram, S.: The small world problem. Psychol. Today **2**(30), 61–67 (1967)
35. Miller, R., Perlman, D., Brehm, S.: Intimate Relationships. McGraw-Hill College Press (2007)
36. Mislove, A., Marcon, M., Gummadi, P.K., Druschel, P., Bhattacharjee, B.: Measurement and analysis of online social networks. In: Internet Measurement Comference, pp. 29–42 (2007)
37. Mooney, R.J., Roy, L.: Content-based book recommending using learning for text categorization. In: ACM DL 2000, pp. 195–204 (2000)
38. Pearl, J.: Reasoning with belief functions: an analysis of compatibility. Int. J. Approx. Reason. **4**(5–6), 363–389 (1990)
39. Ray, I., Ray, I., Chakraborty, S.: An interoperable context sensitive model of trust. J. Intell. Inf. Syst. **32**(1), 75–104 (2009)
40. Sarwar, B.M., Karypis, G., Konstan, J.A., Riedl, J.: Item-based collaborative filtering recommendation algorithms. In: WWW 2001, pp. 285–295 (2001)
41. Sinha, R.R., Swearingen, K.: Comparing recommendations made by online systems and friends. In: DELOS Workshop: Personalisation and Recommender Systems in Digital Libraries (2001)
42. Strang, T., Linnhoff-Popien, C., Frank, K.: Cool: a context ontology language to enable contextual interoperability. In: IFIP WG6.1 International Conference on Distributed Applications and Interoperable Systems, pp. 236–247 (2003)
43. Tang, J., Zhang, J., Yan, L., Li, J., Zhang, L., Su, Z.: Arnetminer: extraction and mining of academic social networks. In: KDD'08, pp. 990–998 (2008)
44. Tang, J., Gao, H., Liu, H.: mtrust: discerning multi-faceted trust in a connected world. In: WSDM 2012, pp. 93–102 (2012)
45. Toivonen, S., Lenzini, G., Uusitalo, I.: Context-aware trust evaluation functions for dynamic reconfigurable systems. In: Proceedings of the WWW'06 Workshop on Models of Trust for the Web (MTW'06) (2006)
46. Walter, F.E., Battiston, S., Schweitzer, F.: A model of a trust-based recommendation system on a social network. Auton. Agent. Multi-Agent Syst. **16**(1), 57–74 (2008)
47. Wang, C., Han, J., Jia, Y., Tang, J., Zhang, D., Yu, Y., Guo, J.: Mining advisor-advisee relationships from research publication networks. In: KDD 2010, pp. 203–212 (2010)
48. Wang, Y., Varadharajan, V.: Role-based recommendation and trust evaluation. In: CEC/EEE 2007, pp. 278–288 (2007)
49. Yang, S., Zhang, J., Chen, I.: Web 2.0 services for identifying communities of practice. In: SCC'07, pp. 130–137 (2007)
50. Yaniv, I.: Receiving other peoples' advice: Influence and benefit. Organ. Behav. Hum. Decis. Process. **93**, 1–13 (2004)