INFORMATICA, 2016, Vol. 27, No. 2, 405–432


DOI: http://dx.doi.org/10.15388/Informatica.2016.92

# A Novel Trust Inference Framework for Web-Based Scenarios Harnessed by Social Network and Web of Trust – a Heuristic Approach

Wenjuan FAN[1,2,3], Jun PEI[1,2,3]*, Shuai DING[1,3], Panos M. PARDALOS[2], Min KONG[1,3], Shanlin YANG[1,3]

[1]*School of Management, Hefei University of Technology, Hefei 230009, China*
[2]*Center of Applied Optimization, Department of Industrial and Systems Engineering University of Florida, Florida 32611 USA*
[3]*Key Laboratory of Process Optimization and Intelligent Decision-Making Ministry of Education, Hefei 230009, China*
*e-mail: fanwenjuan@hfut.edu.cn, feiyijun.ufl@gmail.com, dingshuai@hfut.edu.cn pardalos@ufl.edu, kongmin@hfut.edu.cn, yangsl@hfut.edu.cn*

Received: February 2016; accepted: May 2016

**Abstract.** In this paper, we propose a novel trust inference framework in the web-based scenarios which are assumed to have a Web of Trust pre-established, and take the contexts of the trust relationships into account when inferring the recommendation trust. For alleviating the problem of sparse matrix in the Web of Trust, we also incorporate the users' profile and relationship information on the associated social networks into the framework. Based on the Web of Trust established in the discussed web-based scenario (i.e. epinions.com in this paper), and the social relationship information in the associated social networks, the users are classified into four classes. Then different information is used to infer the users' recommendation trust value based on the classifications. The simulation experiments show that our approach has good coverage of inferred trust values, and the accurate rate of the predicted trust relationship is higher than the traditional PCC (Pearson Correlation Co-efficiency). According to the computation results of adjusted parameters, it can be concluded that the threshold which is used to filter the inferred trust values can be removed, i.e. all the inferred trust values should be kept.

**Key words:** trust relationship inference, Web of Trust, recommendation trust, social network.

## 1. Introduction

Trust relationships are vital in many web-based scenarios (e.g. E-commerce, recommender systems, content providers, or knowledge sharing websites) to encourage purchasing behaviours or enhance collaboration and other interactions between participants, while distrust can obstacle those behaviours largely. For example, one buyer may not buy an item or select a service unless he/she trusts the seller or the service provider, and one learner will regard a piece of knowledge as trustworthy when he/she thinks that the provider of

*Corresponding author.

the knowledge is an expert in this area such that can be trusted, in which situations the trust relationship is regarded as the functional trust; or, one user also may not follow a recommendation to something or someone else unless he/she regards the recommender as trustworthy, and under this situation the trust relationship is regarded as the recommendation trust. Under these circumstances, trust relationship is a subjective belief of an individual (trustor) that another individual (trustee) will behave (e.g. provide a service/item or make recommendations, etc.) as the trustor wishes and trust relationships usually involve any two participants, which could be seller, buyer, recommender, etc., according to the different web-based scenarios in particular situation, which could be selling goods, providing services, sharing knowledge or news, etc., determined by the discussed scenarios.

In most recent web-based scenarios, the users' participation ways are diverse and broad, and they can impact each other's judgements widely and largely through publishing feedback, reviews, and comments. In such environments, the functional trust and the recommendation trust are both involved among the participants. There are several ways to generate the recommendation trust relationships. Users can express their trust opinions explicitly or implicitly after the same transaction experiences as the recommender, and they can also find other users who are similar or close to them, since people may regard the recommendations from these users more trustworthy compared to dissimilar or disclosed users. No matter in which way, the recommendation trust relationships are actually built among common users who have received or will receive the items/services/knowledge, therefore we can also regard the recommendation trust as user-user trust. On the other hand, the functional trust can be generated based on the direct interaction experiences from users to providers, or rely on other indirect interaction information such as the reputation or recommendations (i.e. the recommendation trust). Since functional trust relationships are usually built between the users and the providers, it can also be regarded as the user-provider trust. Here, the providers act as the role of special users, who provide items/services/knowledge in the system either for economic benefit or sharing for free. The users would be those who give feedback ratings to the providers or they can also have comments on other users' feedback ratings.

In this way, we can transform the recommendation trust into the user-user trust and the functional trust into the user-provider trust, by separating the participants into two roles, which could be also overlapped. The functional trust is studied more sufficiently than the recommendation trust probably because it directly expresses the trustworthiness of the active participant. However, it is well known in the social psychology theory that the role of a person has a considerable influence on another person's trust assessment if a recommendation is given (Liu *et al*., 2009; Noor *et al*., 2013). Therefore the recommendation trust is also important since a recommender's opinion may significantly impact other users' judgements on the functional trust to the active participant, especially when a user has no direct interaction experiences and has to rely on others' recommendation, the trustworthiness of the recommendation has to be considered in this case and combined into the processes of the functional trust inference. In this paper, we address particularly the recommendation trust inference problem in the web-based scenarios to further expand the study extent of the trust.

Many trust/reputation mechanisms have been studied extensively and applied in different types of web-based scenarios, most of which are online marketplaces, e.g. eBay, Amazon, etc. In those websites, the users can rate the items/providers after they complete any transaction. Some web-based scenarios also involve a Web of Trust which allows users to explicitly express their trust opinion on other users or their generated contents. These mechanisms are mainly devoted to give an overall feedback rating to each provider, also regarded as "global trust" or "reputation", and/or anyone in the system can generate subjective feedback ratings on others if they have direct interaction experiences, which is so called "local trust", and the ranges of rating values and how to calculate or update the trust/reputation values depend on different reputation mechanisms or policies. The feedback ratings given by other users can actually reflect the ability of the user giving recommendations to others, i.e. if the feedback ratings are agreed by or helpful to most other uses, then the raters are of high recommendation trust level, otherwise they may not. Obviously, users cannot always have direct interaction experiences with every provider/user, such that the subjective trust or local trust is empty in these cases. With regard to those unknown participants, trust relationships need to be inferred by leveraging existing trust ratings and other related information which can be obtained inside and/or outside. The inferred trustworthiness score indicates to which extent the trust is or could expect the trustee to perform a given action.

In summary, existing trust mechanisms have to confront the following problems: network density, knowledge sparseness, and the preference heterogeneity among the agents. Suffering from the above problems, most trust frameworks have several drawbacks. A main issue is that the trust relationships are not context-specified, which means they are too overall such that cannot indicate in which context one can trust other users. Another evident drawback is that the user-item ratings matrix is too sparse, i.e. only a few users have rated some of the items, so there are not enough explicit trust ratings, besides, it is always hard for participants to make trust decisions on newcomers, which is so called "*cold start*" problem. Despite these problems, it should be noted that the functional trust and the recommendation trust are different and should be distinguished, i.e. the user-user trust and user-provider trust need to be calculated in different ways. For alleviating the sparse matrix and *cold start* problems, the trust relationship inference should involve more information, i.e., taking advantage of the data from associated social networks to infer trust relationships among never-interacted users. For example, in many apps, users are allowed to log in with their social network accounts. Being authorized to get access to the users' account information, these apps can acquire the social information for more precise and widely-covered trust relationship inference.

In this paper, a novel trust inference framework for web-based scenarios associated with social networks is proposed, which utilizes social relationships, profile analysis, and context-specified Web of Trust, to infer the trust relationship among users. The objective is **to infer the personalized trust value in a specified context on other users that have no interaction before.**

The main contributions of our work can be concluded as follows:

- By considering trust relationship inference problem under specific contexts, the inferred trust relationships are no more general but context-specific.

- By utilizing the social relationships among users in the associated social networks, the cold start problem is alleviated largely.
- By considering the similarity among the users through profile data and interaction data, the trust relationships on the Web of Trust are enhanced reasonably.
- The experiments show that our proposed trust inference framework has better prediction accuracy and coverage than the Pearson Correlation Coefficiency.

The remaining paper is structured as follows: Section 2 is the related work. Section 3 is the illustration of the proposed trust inference framework. Section 4 is the framework formalization, and the experiments are shown in Section 5. The paper is concluded in Section 6.

## 2. Related Work

The current work relates to several streams of work in trust and reputation mechanisms, trust inference in social network, trust propagation, and Web of Trust. We review them selectively in this section to provide a context in this work.

### 2.1. *Trust and Reputation Mechanisms*

Trust and reputation mechanisms have been recognized as key factors for successful electronic commerce adoption and other online service provider systems. The fundamental idea is that all the entities in the system can rate each other, usually after the completion of a transaction. A trust or a reputation score of the service or the provider can be derived based on the aggregation of all the observed ratings. In this way, trust systems can help users and allow them to rate each other even without being direct neighbours (Hamdi *et al*., 2013). There are some works trying to establish a typology for reputation (Mui *et al*., 2002) and trust (McKnight and Chervany, 2001).

Many researchers regard trust and reputation as two distinctive concepts. Reputation can be considered as a collective measurement of trustworthiness (in the sense of reliability) based on the referrals or ratings from members in a community, while an individual's subjective trust can be derived from a combination of received referrals and personal experience (Jøsang *et al*., 2007). Through trust and reputation mechanisms, users of these systems can have a relatively reliable opinion on the services/items or providers, otherwise they will undertake the risk of choosing from the unknown items/services before they actually have some experiences.

Nowadays, commercial implementations of trust and reputation systems are now part of mainstream Web technology (Jøsang, 2012). In real applications, eBay (2002) and Amazon (2002) are representative examples of online markets which use reputation systems. For example, on eBay, users can rate an item after they complete the transaction, by giving three different ratings, which are good (+1), average (0), and bad (−1). The reputation value is computed as the sum of those ratings over the last six months (Sabater and Sierra, 2005). Pranata *et al*. (2013) investigated the usability and effectiveness of the

existing web-based trust rating systems, which focus on three widely used trust rating systems on the internet: the binary trust rating system, the 5-star trust rating system, and the notation based trust rating system. Dellarocas (2003) presented an overview of online reputation mechanisms that have been used in commercial web sites. Besides the areas of electronic commerce and online service provider systems, trust and reputation mechanisms can be found in many other kind of distributed systems, such as the multi-agent systems (Pinyol and Sabater-Mir, 2013), wireless sensor networks (Yu *et al*., 2012), vehicular ad hoc networks (Mármol and Pérez, 2012), etc. Although the applied contexts are varied, the basic idea behind it has some things in common.

It is clear that trust and reputation are both context dependent. We would trust a doctor when she is recommending a medicine but we would not equally trust her when she is recommending a computer. A 'context' is a situation, which influences the building of a trust relationship between the trustor and the trustee. For example, a service provider can provide services to its users. The users build trust relationships with the service provider based on the provided services. In this case, the services can be considered as contexts (Haque and Ahamed, 2007). The context of trust and reputation is not considered in many studies because the method may suffer from more severe matrix sparse problem. However, there are still some works addressing context-aware trust models. Uddin *et al*. (2008) present an interaction-based Context-Aware Trust model for open and dynamic systems by considering services as contexts. Shankaran *et al*. (2009) present a decentralized context-aware framework for building a trust model for MANETs.

### 2.2. *Trust Inference in Social Networks*

Web-based social networks (WBSNs) are those websites trying to simulate real social networks on the web. Analyzing the structure of social networks and the social relationship among the users on WBSNs can provide very valuable information for many research areas. The computational problem of trust inference in social networks is to determine how much one person in the network should trust another person to whom they are not connected (Golbeck, 2005). Trust relationships existing between the users in WBSN have been studied sufficiently in recent years (Golbeck, 2006a). In Chang *et al*. (2015), the authors estimate the trust value by incorporating distance and user-generated ratings. The trust value estimated serves as a metric for filtering and sorting content of any kind based on the trustworthiness of the creator.

Some studies focus on relations between entities. It can be depicted by a directed cyclic graph where a vertex indicates an entity and an edge between two entities indicates that there is a trust relationship between them. With regard to trust propagation in trust networks, Guha *et al*. (2004) addressed the problem of transitivity of distrust. That is, if A distrusts B and B distrusts C, then we can neither say that A trusts C nor A distrusts C. De Cock and Da Silva (2006) modelled a trust network as an intuitive fuzzy relation to address the problem of ignorance and vagueness, and derived trust information through a trusted third party. Hang *et al*. (2009) investigated the operators for trust propagation in social networks, including concatenation and aggregation. Zhang and Yu (2012) proposed

a semantic-based trust reasoning mechanism to mine trust relationships from online social networks automatically. Yuan *et al*. (2010) verified that a trust network is a small-world network, so that it is possible to build a trust relationship between two randomly selected users of the trust network within a limited number of hops. Zolfaghar and Aghaie (2010) have investigated some of the mechanisms that determine the signs of links in trust networks which consist of both trust and distrust relationships. However, the authors only focused on user ratings and did not take into account the category information of user relationships.

One of the major distinguishing characteristics of a trust inference algorithm is whether it considers personalization, and if so it is a local trust algorithm, otherwise if it computes a single trust value for each user, then it is a global trust algorithm. Which algorithm is preferred depends on the application context. For example, if all users agree on the general notions of good and bad contents, then the global algorithm may be appropriate, otherwise the local metric is more appropriate. When trust is personalized, asymmetry of trust and local trust relationships should be considered (Golbeck, 2006b). Some researchers also argue that when computing the trust value, the confidence of the trust should also be considered. Kuter and Golbeck (2007) proposed a trust inference algorithm which computes trust with an explicit probabilistic interpretation for confidence in social networks. The subjective trust inference algorithms also are included in some works (Ziegler and Lausen, 2005; Hang *et al*., 2009; Wang and Wu, 2011).

The existing related studies usually focus on the evaluation only using the trust values between adjacent participants, overlooking the influence of contextual information on trust evaluation (Wang *et al*., 2015). With regard to this problem, Wang *et al*. (2015) presented a contextual social network model considering both participants' personal characteristics which are referred to as the independent social context, including preference and expertise in domains, and mutual relations which are referred to as the dependent social context, including the trust, social intimacy, and interaction context between two participants. Liu *et al*. (2009) proposed a complex social network structure that comprises of the attributes of three impact factors, including trust, social intimacy degree and role impact factor. They argued that these three factors naturally influence the trustworthiness of trust propagation and hence the decision making of a source participant. Zhan and Fang (2011) proposed a trust computing system which simulates the trust between two directly connected individuals on social networks. The system eventually returns a trust score which can reflect the trust from one user to another by integrating the trust values computed through three trust computing components, including the profile similarity, information reliability, and trust ratings. In these hybrid models, trust is expressed as a linear weighted sum of these factors, where each factor owns a weight that indicates its influence on trust (Zhao and Pan, 2014).

### 2.3. *Web of Trust*

Users in online communities are allowed to express who they trust or how much they trust based on their relevant prior experiences, which is called the Web of Trust (Kim *et*

*al*., 2008). In the system, everyone has his/her own Web of Trust regarding verifying or trusting each other. This basic idea of forming a Web of Trust by signing each other's digital certificate arose from the concept of six degrees of separation (Noor *et al*., 2013), With the increase in user-generated content, social trust is needed to capture many types of human behaviour patterns in perspective (Golbeck, 2008). Most of existing work on 'trust prediction' based on Web of Trust considers how to develop a trust inference model which propagates trust relationships through the Web of Trust. However, the Web of Trust may be too sparse to infer the trust relationships since there may be not enough explicit trust values expressed by the users. Kim *et al*. (2008) proposed a framework to predict trust relationships based on users' expertise and users' affinity in certain contexts (topics), using users rating data which is available without explicit trust rating data by building a Web of Trust. This approach provides a much denser Web of Trust. Some other work on propagating trust through the Web of Trust includes (Golbeck *et al*., 2003; Richardson *et al*., 2003; Massa and Avesani, 2004).

In many web-based scenarios, such as online sharing communities and e-commerce sites, Web of Trust which consists of the pre-established (or manually input) social links is not always available and is typically sparse. To address this issue, many researchers have proposed different methods. Yan *et al*. (2013) proposed a method which establishes and exploits a two-faceted Web of Trust on the basis of users' personal activities and relationship networks in web-based scenarios. Combining the user's Web of Trust and user-item rating matrix can alleviate the matrix sparse problem to a certain extent (Jamali and Ester, 2009; Kim and Phalak, 2012; Moradi *et al*., 2015).

In the real application, Epinions.com is a successful product review web site, which provides the functionality to let users build their personal Web of Trust. Unlike traditional social networks built in the daily life, the Web of Trust on Epinions is a virtual community based on indirect interactions through reading reviews or accepting "recommendations" from others (Zhang *et al*., 2008). When other users have added the target user to their Web of Trust, then the target user is trusted by them and appears on the list of users who trust the target user. By effectively using the Web of Trust, Epinions can predict how helpful a review will be to a customer and help him to find the most suitable product (Zhang *et al*., 2008). Liu *et al*. (2008) presented a classification approach for trust prediction problem by studying the Epinions community. It predicts the missing trust relationship values among users and enhances connectivity of a Web of Trust. The authors observed the user behaviour in the community and identified the features that affect trust relationships. Most trust predicting approaches based upon the Web of Trust did not take the context information and the features of recommendation trust into account. That is, the trust relationship actually cannot be propagated through such a Web of Trust since the contexts between connected trust relationships may be totally different. The problem can be shown in Fig. 1.

For example, user A trusts user B in recommending classical literature books (as context 1), while B trusts C in recommending digital products (as context 2), then may trust relationship exist between A and C? In this case, context 1 and context 2 are totally different. If there exists trust relationship between A and B, then in which context it is?

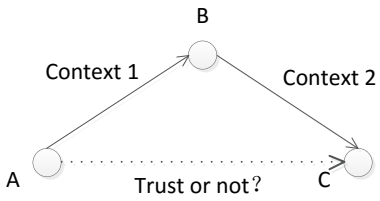


Fig. 1. Combined recommendation trust propagation.

Otherwise, if A trusts B in recommending classical literature books, and B trusts C in recommending modern literature books, may trust relationship exist between A and C? In this case, context 1 and context 2 have something in common. If there exists trust relationship between A and C, then in which context it is? Therefore, when predicting trust relationships based on the existing Web of Trust, especially the expertise and ability of recommenders are the key factors that attract users, the context of trust relationships must be considered, otherwise the recommendation made based on the inferred trust relationships may be inappropriate or indifferent to users. Tavakolifard *et al*. (2008) studied the transferability of trust relationship among similar context. However, since an existing Web of Trust in many web-based scenarios is either hard to achieve or very sparse, if the context information is utilized to infer trust relationships then the sparse problem may be more severe. In this paper, we also consider the users's connection in the associated social networks to alleviate the problem.

## 3. Trust Inference Framework on EC Web Site

### 3.1. *Data to be Collected*

- Profile data

Profile information is descriptive data on each participant. The descriptive data of the providers includes context/category, features, etc., and the descriptive data of ordinary users includes age ranges, gender, location, major/career, roles, interested/preferential context, etc. There are some important attributes that can be extracted from the data. Based on the features of the attributes, they can be divided into:

(1) External attributes, which are used to describe the profile of the users that can be distinguished from the exterior, for example, gender, age, job, location, etc.
(2) Internal attributes, which are used to express the disposition of users, such as hobbies, interests, specialties, bias, etc.

- Context-specified relationship data

In this framework, each user has a Web of Trust, including the trust-in list (i.e. which entities the user trusts), block list (distrust, i.e. which entities the user distrusts), and trusted-by list (i.e. by which entities the user is trusted). All of these relationships should

be context-specific, i.e. under which circumstances they trust others or they are trusted by others.

- Behaviour and interaction data

The behaviour and interaction information involves the dynamic data which is generated from the interactions among entities, including the behaviour records (e.g. the number and time period of different types of interactions), and messages (reviews or feedback rating to the reviews). There are several types of interactions on the EC web site, such as users buying/using/viewing items of the providers, giving feedback ratings to the providers, and giving comments to the feedback ratings given by other users. In many EC web site, users can give positive (e.g. "like" or "helpful") or negative (e.g. "dislike" of "unhelpful") comments to other users' reviews or feedback ratings.

- Social relationship data

Users can be linked through social networks, and a variety of social behaviour on the social networks can reflect a certain extent of trust relationship. In this work, the social relationship data of users on the associated social networks is collected and can be further used to infer the trust relationship.

### 3.2. *Trust Inference Framework Structure*

In the domain of EC web site, the direct trust relationship between participants, which may be unidirectional or bidirectional, is established after several interactions, while the indirect trust relationship is formed based on the reputation of the target user or other users' recommendations. Some newcomers, however, cannot be trusted by other users or have trust on others in a direct or an indirect way, because of lack of interaction information in the system.

Social networks can alleviate the cold start problem. In reality, there are several social networks which can be associated with the discussed E-commerce web site. By linking the users' accounts of the EC web site to these social networks, the social relationship data among these users can also be extracted. In Fig. 2, we can see that there are mainly four types of nodes (or users) denoted by different colors: the green ones are those who have a Web of Trust in the domain of the EC web site and also have associated accounts in the social network; the purple ones are those who have a Web of Trust in the domain of the EC web site but have no associated accounts in the social network; the red ones are those who have no Web of Trust but have associated accounts in the social network; and the black ones are those who have neither Web of Trust nor associated accounts in the social networks.

In Fig. 2, the accounts (indicated by empty circles with different colors) on the EC web site are mapped into the nodes on the social networks, in which way two users who have no trust relationship in the domain of the EC web site could be connected through several hops of social connections. For example, on the EC web site, node (or user) $J$ and node $K$ have no interaction before or trust relationship, but they are connected in the domain of social network (indicated as the node $J'$ and $K'$), which means they can establish trust

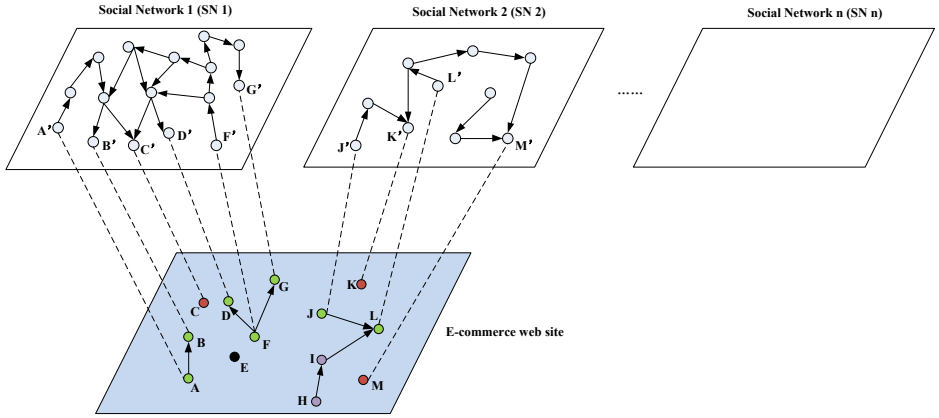


Fig. 2. Framework illustration.

relationship. Since there may be more than one social network associated with the EC web site, users may link their accounts of different social networks with the EC website. For simplicity, we regard these different social networks as a whole one, and only take each of them as an independent domain in different forms of social relationships.

### 3.3. *Trust Relationship Inference*

According to the above analysis, there are several ways to infer trust relationships, by which the strength, last duration, and confidence may be different accordingly. Therefore, when incorporating these factors, we should also consider the reliability.

The main policy of inferring the trust relationship between the users in the domain of EC web site is as follows:

(1) For the green nodes, the information of the Web of Trust, profile similarity, and social relationship is combined, and the trust relationship inferred this way has the highest reliability;
(2) For the purple nodes, the information of the Web of Trust and profile similarity is combined, and the trust relationship inferred this way has the sub-highest reliability;
(3) For the red nodes, the social relationship and profile similarity is combined, and the trust relationship inferred this way has the sub-highest reliability;
(4) For the black nodes, the information of profile similarity is used, and the trust relationship inferred this way has the lowest reliability.

The policy of trust relationship inference is shown in Fig. 3.

### 3.4. *Trust Relationship Inference*

- Reputation based trust inference

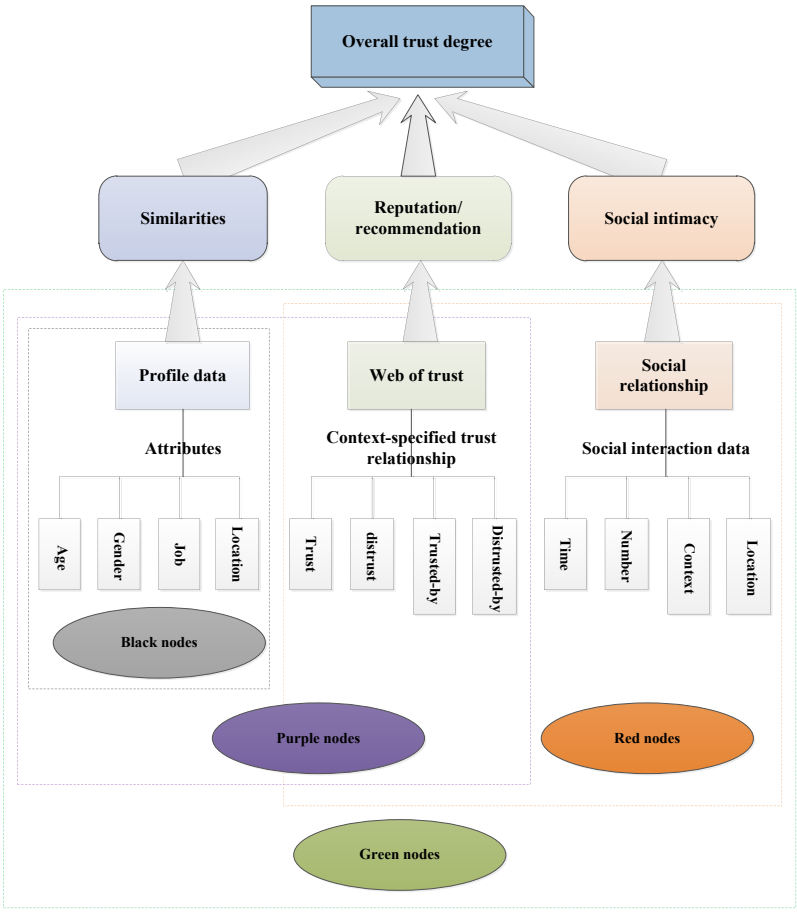


Fig. 3. Trust Relationship inference framework.

Users tend to trust others with better reputation, since higher reputation means they offer more high-quality items in the EC web site and thus receive more positive feedback ratings, or they have given more correct evaluations or feedback ratings to the items and correspondingly they get more positive comments from other users. Thus, the reputation of a user is calculated based on the proportion of positive comments in all comments the user has received.

- Profile similarity based trust inference

Most of online EC web sites rely on the assumptions that users usually trust those who are similar or have similar taste as them, and the higher similarity they have, the more they would trust each other. Thus, the profile similarities should be incorporated into the trust inference process. As mentioned previously, the profile attributes can be classified into two types, and the profile similarity also should be taken differently with the attributes. For example, the users who are in the same age may not trust each other as much as when

they have the same hobbies. In this regard, we think that the profile similarity calculated based on the internal attributes should take more weight than the similarity calculated based on the external attributes.

- Web of Trust based trust inference

On the EC web site, users can explicitly express their trust opinions to others and thus form a Web of Trust, based on which the local and global trust degree of the users can be calculated. In many trust or reputation systems, Web of Trust is one of the most important ways of inferring the trust or reputation values of users. However, it confronts the problems of cold start and sparse trust matrix. Even so, it still has most credibility of inferred trust values. In this paper, trust value inferred based on the Web of Trust will take more weight when calculating the final trust values.

- Social relationship based trust inference

Based on the previous literature, we have the basic assumption that the more intimate social relationship the users are of, the more they trust each other. Thus, how to measure the social intimacy is the first problem in the social relationship based trust inference. In this paper, since we consider the scenario that the EC web site is associated with one or more social networks, the users' social relationship can be extracted from those SNs.

## 4. Framework Formalization

Considering an EC website $E$, on which there are totally $M$ items (all of the items are classified into $k$ categories $C_1, C_2, \ldots, C_k$, which indicates the $k$ context) and $N$ users (here $M$ and $N$ changes with time, so the scalability of the trust inference model has to be considered, but now we leave it to the future to discuss), and $n$ correlated social networks $SN_1, SN_2, \ldots, SN_n$, which have associated with the EC website, on which the users (assuming $U$, $U \leqslant N$) of the Social Networks can give their personal evaluation statements/recommendations regarding the items and the other users.

The information to be collected includes the evaluation by users on items, and comments by users on other users' feedback ratings, some profile information about users, the Webs of Trust which are specified in their own page, and the relationship information from the social networks that the users have linked accounts. Suppose we have two matrices indicating user-user trust ratings, and user-user social relationship. It should be noted that all of the two matrices are sparse, which means that there are a lot of blank entries in these matrices, and the empty entries in the user-user trust matrix are what we need to predict.

### Notations

$E$: the EC website;
$N$: the number of users in $E$;
$i$: the index of the users, $i = 1, 2, \ldots, N$;
$M$: the number of items in $E$;

$j$: the index of the items, $j = 1, 2, \ldots, M$;
$l$: the index of the categories ($l = 1, 2, \ldots, C$);
$A_g$: the $g - th$ attribute describing the profile of users ($g = 1, 2, \ldots, z$);
$s_g$: the max number of the value of the $g$-th attribute;
*Trust-in*($i \to l$): the set of users that user $i$ trusts in category $l$;
*Trusted-by*($i \to l$): the set of users that user $i$ is trusted by in category $l$;
*block*($i \to l$): the set of users that user $i$ distrusts in category $l$;
$m_{ij}^{+}$: the number of positive comments regarding the reviews by user $i$ on item $j$;
$m_{ij}^{-}$: the number of negative comments regarding the reviews by user $i$ on item $j$;
$q_{ip}^{j+}$: the number of positive comments that user $i$ has given to user $p$ regarding the reviews by user $p$ on item $j$;
$q_{ip}^{j-}$: the number of negative comments that user $i$ has given to user $p$ regarding the reviews by user $p$ on item $j$;

Next, we argue that the personalized user-user trust depends on the following factors:

- Reputation based trust inference

Users can give their feedback ratings or comments to other users' reviews, according to the helpfulness of the reviews. Most web-based scenarios provide the function of clicking the button of "like" and "dislike" or "helpful" and "unhelpful" to any review. For simplicity, we can regard them as positive and negative comments respectively. If a user is a professional in one category, then he will receive more positive comments. The reputation of a user in a context actually reflects the user's capability to review the items and his specialty in that context. That is, other users' comments can be used to calculate the discussed user's reputation, and the calculated reputation of users should be context-specified. The reputation of user $i$ in category $l$ ($l = 1, 2, \ldots, C$) is calculated as follows:

$$R_i(l) = \frac{\sum_{j \in \{c_l\}} m_{ij}^{+}}{\sum_{j \in \{c_l\}} m_{ij}^{+} + \sum_{j \in \{c_l\}} m_{ij}^{-}} \tag{1}$$

where $R_i(l)$ is the reputation value of user $i$ in category $l$. It should be noted here that the reliability of the reputation needs to be considered. It is reasonable that we assume if the user receives more comments from other users, then the inferred reputation value will be of greater confidence. For example, the reputation values are the same in the situation when there are 6 positive comments and 4 negative comments, and the situation when there are 60 positive comments and 40 negative comments to the users. But obviously the reliability or the confidence of the two reputation values should not be equal, since there is more evidence in the second case than in the first case. So, the reliability value is dependent on the amount of the evidence, and the trust value is more convincing and reliable when there is more supporting evidence. We have the following formula to calculate the reliability value of user $i$:

$$c_i(l) = 1 - e^{-\alpha x_i(l)}, \qquad R_i^1(l) = c_i(l) \times R_i(l) \tag{2}$$

where $x_i(l)$ indicates the number of comments that user $i$ has received in category $l$, i.e. $x_i(l) = \sum_{j\in\{C_l\}}(m_{ij}^{+} + m_{ij}^{-})$, $\alpha$ ($\alpha \geqslant 1$) is the parameter used to adjust the gradient of the confidence function, and the confidence value increases faster with higher value of $a_i$.

$R_i^1(l)$ is the overall reputation value of user $i$ in context $l$, and the personalized trust value of user $p$ for user $i$ should include user $p$'s own opinion, that is, if user $p$ has given his/her own comments towards user $i$, then these comments should be considered when deriving the personalized trust value:

$$R_{pi}^1(l) = \sigma(l)\frac{\sum_{j\in\{C_l\}} q_{pi}^{j+}}{\sum_{j\in\{C_l\}} q_{pi}^{j+} + \sum_{j\in\{C_l\}} q_{pi}^{j-}} + \big(1-\sigma(l)\big)R_i^1(l), \tag{3}$$

where $\sigma(l)$ is the weight of the personal comments given by user $p$ regarding category $l$. The value of $\sigma(l)$ is calculated as: $\sigma(l) = \frac{n_{i\to j}^{p}}{n_{i\to j}^{p}+\overline{n}_{i\to j}}$, $j \in \{C_l\}$, where $\overline{n}_{i\to j}$ is the average number of comments given by all users regarding the feedback ratings by user $i$ on item $j$, and $n_{i\to j}^{p} = \sum_{j\in\{C_l\}} q_{pi}^{j+} + \sum_{j\in\{C_l\}} q_{pi}^{j-}$ is the number of comments given by user $p$ regarding the feedback ratings by user $i$ on item $j$. Therefore, if there are no comments by user $p$ towards user $i$ in category $l$, then $\sigma(l) = 0$; and if the number of the comments given by user $p$ towards user $i$ is growing, then the former part takes more weight. That is, if the number of comments given by user $p$ is larger than the average number of comments given by all users regarding the feedback ratings by user $i$ on item $j$, then the weight of the personal comments given by user $i$ should be larger than 1/2 and thus takes more weight than the reputation value.

- Web of Trust based trust inference

By utilizing the information of Web of Trust, the trust relationships can be propagated in the trust network. Based on the information of *Trust-in*$(i \to l)$ and *Trusted-by*$(i \to l)$, Web of Trust can be formed as a trust network. However, the trust propagation in trust network under different contexts is still an open problem. In this part, we propose a context-specified trust propagation approach which takes the context information of connected trust relationships into account. In Wang *et al*. (2015), the authors discussed the interaction context in trust propagation problem, i.e. the similarity between the contexts of existing trust relationships is computed. In their work, the similarity between the context $C(l)$ and context $C(m)$ is denoted as $CS_{l,m} \in [0, 1]$. If $CS_{l,m} > u$ ($u$ is a threshold, e.g. 0.6), then the interaction context $C(l)$ is relevant to context $C(m)$, which can be denoted as $C(l) \asymp C(m)$. For example, let $C(1)$ denote the context of recommending classical movies, and let $C(2)$ denote the context of recommending old movies. Since $C(2)$ is relevant to $C(1)$, then the trust relationships can be projected just from context $C(1)$ to $C(2)$. If $C(l)$ is irrelevant to context $C(m)$, which is denoted as $C(l) \not\asymp C(m)$, then the trust relationships cannot be projected from context $C(l)$ to $C(m)$. For example, if $A$ trusts $B$ in recommending digital devices, which is denoted as context $C(3)$, and $B$ trusts $C$ in recommending music, which is denoted as context $C(4)$, and the two contexts are irrelevant, so the trust relationship cannot be projected through this chain. Based on this work, it is

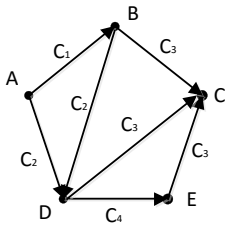


Fig. 4. A small example of Web of Trust.

reasonable to assume that the trust relationship is also propagable since the trust relationship can be projected between similar contexts. Then we can infer the trust relationship which is propagated with different but similar contexts.

Figure 4 is a small example of Web of Trust, in which the arrows indicate the directed trust relationships. For simplicity, each user is trusted by others only in one context. For example, user $B$ is in the trust list of user $A$ in context $C(1)$; user $C$ is in the trust list of user $B$, $D$, and $E$ in context $C(3)$; user $D$ is in the trust list of user $A$ and $B$ in context $C(2)$; and user $E$ is in the trust list of $D$ in context $C(4)$. The trust relationship is binary, i.e. if one user is in the trust list of another user, then the trust value will be 1, otherwise it will be 0. So the trust values between the connected users are all equal to 1. We assume that the similarities between different contexts, i.e. $CS_{1,3}$ , $CS_{2,3}$, $CS_{1,2}$, $CS_{2,4}$, $CS_{4,3}$ are all known.

In Fig. 4, user $A$ and user $C$ have no trust relationship, but there are several paths from $A$ to $C$, including: $A \to B \to C$, $A \to D \to C$, $A \to B \to D \to C$, and $A \to D \to E \to C$. When we calculate the trust value of $C$ from $A$'s perspective, the trust relationship is in the context $C(3)$ by default, since User $C$ is trusted by others only in one context, i.e. $C(3)$. Therefore, we can estimate the trust value $T_{AC}(C_3)$, which can be calculated as follows:

$$T_{AC}(C_3) = \max \left\{ \prod_{k1,\ldots,k_{p_i}} CS_{Ak_1} \cdot CS_{k_1k_2} \cdots CS_{k_{pi}C}, CS_{k_ik_{i+1}} \geqslant u,\ p_i \in \Omega_{A\to C} \right\} \tag{4}$$

where $T_{AC}(C_3)$ is the calculated Web of Trust-based trust value of user $C$ by user $A$, and $\Omega_{(A\to C)}$ is the set of all paths from $A$ to $C$. So, in this paper, the indirect trust value of any two users, say $A$ and $C$, is the maximum product value of the similarity between adjacent trust contexts of all possible paths which can connect $A$ and $C$.

- Similarities of users

As mentioned above, there are two types of similarity between users, i.e. the external similarity based on external profile attributes and internal similarity based on the users' internal attributes such as interests, preferences, and bias. Since the assessments given by users can also reflect the personal preference and bias, we also take advantage of assessments to calculate the internal similarity between users. The external attributes include

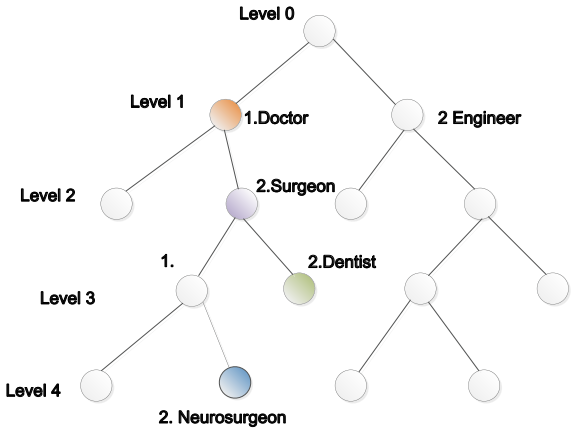


Fig. 5. Categorical attribute classification diagram.

gender, job, location, etc., which are used to calculate the external similarity. In this paper, for simplicity, we choose users' job and location as the representative of the external attributes, and the assessments by users as the representative of the internal attributes. The job attribute belongs to the categorical attributes, i.e. the value range of the attributes is varied by different categories, i.e. the job attribute can be classified into many classes, and further subdivided into more sub-classes.

Assuming that there are $z$ categorical attributes, i.e. $A_g$ $(g = 1, 2, \ldots z)$. With regard to the categorical attributes, we set $n$ levels to indicate the fineness of classifications. For each attribute $A_g$, the value range takes $n_g$ levels (*Level* 0, *Level* 1, ..., *Level* $n_g - 1$), Level 0 is the whole set of the attributes which doesn't make classifications, and Level 1 indicates the meta classification of the attribute, and Level $n_g - 1$ is the finest classification. Take the job attribute for example, in Level 0, the value range includes all jobs, i.e. we cannot distinguish any jobs in this level; in Level 1, there are several "meta jobs", such as doctor, engineers, officers, etc.; and in Level 2, the jobs are further subdivided, such as physician, surgeon, etc. With the number of level rising, the classifications are more and more specified, as shown in Fig. 5. Therefore, we can have: $A_g = \{\{A_g(0)\}, \{A_g(1)\}, \ldots, \{A_g(n_g - 1)\}\}$, and $\{A_g(0)\} \supseteq \{A_g(1)\} \supseteq \cdots \supseteq \{A_g(n_g - 1)\}$ $(g = 1, 2, \ldots, z)$.

To compute the users' external similarity on attribute $A_g$, we make the classification and hierarchy coding of attribute $A_g$ first. We say that $A_g$ can be classified into $n_g$ layers, and the attribute of each layer should be numbered. For example, user $i$ and user $p$ indicate their categorical attribute $A_g$ respectively as $U_i(A_g) = \{A_g(\theta_\gamma^1, \theta_\gamma^2, \ldots, \theta_\gamma^{k_\gamma})\}$, and $U_p(A_g) = \{(\theta_\gamma^1, \theta_\gamma^2, \ldots, \theta_\gamma^{k_\gamma})\}$ as the hierarchy code of attribute $A_g$, where $\theta_\gamma^1, \theta_\gamma^2, \ldots, \theta_\gamma^{k_\gamma}$ denote the index of the attribute in level $\gamma$, and the value of $k_\gamma$ indicates the fineness of the classifications of user's attribute. Then, we should trace the highest level in which $U_i(A_g)$ and $U_p(A_g)$ are not classified. For example, if user $i$'s job is dentist, which belongs to $A_1(0, 1, 2, 2)$, and user $p$'s job is neurosurgeon, which belongs to $A_1(0, 1, 2, 1, 2)$, then the Maximum level in which $U_i(A_1)$ and $U_p(A_1)$ are not classified is in Level 2: Surgeon, and this level is called Maximum Non-Classification Level

(MNCL). Then the similarity between user $i$ and user $p$ on attribute $A_g$ is calculated as: $S_{ip}(A_g) = \frac{MNCL_g\{U_i(A_g), U_p(A_g)\}}{n_g - 1}$. Therefore, if two users' Maximum Non-Classification Level is in Level 0, then they have no similarity, i.e. $S_{ip}(A_g) = 0$; and if two users' Maximum Non-Classification Level is in Level $(n_g - 1)$, then they have the highest similarity, i.e. $S_{ip}(A_g) = 1$. In the case of Fig. 5, the similarity between $U_i(A_1)$ and $U_p(A_1)$ is $S_{ip}(A_1) = \frac{MNCL_g\{U_i(A_g), U_p(A_g)\}}{n_1} = \frac{2}{4} = \frac{1}{2}$.

For all categorical attributes, we calculate the overall external similarity between users, which is as follows:

$$S_{ip}(A) = \sum_{g=1}^{z} \omega_g \cdot S_{ip}(A_g), \quad \omega_g = \frac{n_g - 1}{\sum_{g=1}^{z}(n_g - 1)} \tag{5}$$

where $\omega_j \in [0, 1]$, $\sum_{g=1}^{z} \omega_g = 1$ is the weight of the categorical attribute $A_g$. In this paper, the weight is dependent on the number of all levels which classify the values of attributes, and an attribute with more levels indicates more specifications on this attribute, thus should be of higher weight.

Next, we calculate the internal similarities between users, utilizing the assessment values from any arbitrary two users who both have rated the same items, and the similarity is calculated based on the Pearson Correlation Coefficient (PCC). Suppose user $i$ and $p$ both rate items belonging to category $l$, then the similarity between user $i$ and $p$ in context $l$ can be calculated as:

$$S_{ip}(l) = \frac{\left|\sum_{j \in I_i(l) \cap I_p(l)} (v_{ij} - v_i)(v_{pj} - v_p)\right|}{\sqrt{\sum_{j \in I_i(l) \cap I_p(l)} (v_{ij} - v_i)^2} \sqrt{\sum_{j \in I_i(l) \cap I_p(l)} (v_{pj} - v_p)^2}}. \tag{6}$$

The above function calculates the internal similarity between two users in a specific category. However, if they have no overlapping rated items, we need to consider the similarities of the users in the range of all items. That is, we take the global similarity as the context-specified similarities. The global similarity between user $i$ and $p$ is calculated as follows:

$$S_{ip}(\Delta) = \frac{\left|\sum_{j \in I_i \cap I_p} (v_{ij} - v_i)(v_{pj} - v_p)\right|}{\sqrt{\sum_{j \in I_i \cap I_p} (v_{ij} - v_i)^2} \sqrt{\sum_{j \in I_i \cap I_p} (v_{pj} - v_p)^2}}. \tag{7}$$

Then, we calculate the overall similarity by combining the external similarity and internal similarity. However, for many users, they have no overlapping rated items, so the similarity should be calculated based on different rules. As mentioned earlier, the internal similarity calculated based on assessments should carry more weight than the external similarity calculated based on the external categorical attributes. So we have the following policy:

(1) If two users have overlapping rated items in context $l$, then their similarity is calculated as the internal similarity, i.e. $S_{ip} = S_{ip}(l)$.

(2) If two users have overlapping rated items but not in context $l$, then their similarity is calculated as the combination of the internal and external similarity, i.e. $S_{ip} = \beta S_{ip}(l) + (1-\beta)S_{ip}(A)$.
(3) If two users haven't any overlapping rated items, then their similarity is calculated as the external similarity, i.e. $S_{ip} = S_{ip}(A)$.

- Social relationships among users

If user $i$ and user $p$ of $E$ are also connected in $SN_g$ $(g = 1, 2, \ldots, W)$, we say that they are socially connected in $SN_g$. The social relationships can be measured by their closeness in $SN_g$. Closeness between two entities is reflected in two ways: they are directly connected, i.e. they are friends on the social network, either with common friends or not; or they have common friends but are not direct friends. We argue that two entities is closer when they are friends than when they are not, and two entities are closer when they have common friends than when they have not. Based on the above assumptions, we have the following policies to compute the closeness among users:

(1) When user $i$ and $p$ are directly connected (i.e. they are direct friends), then their closeness would be the highest, i.e. $Closeness_{ip} = 1$.
(2) When user $i$ and $p$ are not direct friends but they can be connected (through $\eta$ intermediate friends) within $(1 \leqslant u \leqslant 3)$ hops, then their closeness can be calculated as: $Closeness_{ip} = [\sum_{j=1}^{g} d(n_i, n_p)]^{-1}$.
(3) When none of the above situations exist, then user $i$ and $p$'s closeness will be zero, i.e. $Closeness_{ip} = 0$.

- The overall trust value

The personalized user-user trust in certain context $l$ can be calculated by the aggregation of the users' reputation based trust value, recommendation-based trust values, similarities of users, and the social closeness between users, which is as follows:

$$t_{ip}(l) = \gamma_1 \cdot R^1_{ip}(l) + \gamma_2 \cdot R^2_{ip}(l) + \gamma_3 \cdot S_{ip}(l) + \gamma_4 \cdot Closeness_{ip} \tag{8}$$

where $\gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 = 1$.

## 5. Experiment

### 5.1. *Experiment Setting*

#### (1) Data Source

The ability of a user to write helpful and reliable reviews can reflect the recommendation trust of the user, and other users who find the reviews are helpful to them can add them into their Web of Trust. Besides, the distrust relationship can also be stored since users are allowed to add others whose review they think is not trustworthy. Therefore, Epinions is a perfect data source for our research. Users in Epinions can add metadata in the following forms (Zhang *et al.*, 2008):

- Users' reviews and ratings of items.
- Users' feedback ratings and comments on reviews.
- Web of Trust of trustworthy friends.

There are 5 different ways that the users can participate in Epinions, which are as follows:

- Trust: the users can add other users (who have written helpful reviews) in their trust list.
- Block: the users can add other users (who have written untrustworthy reviews) in their block list.
- Reviews: the users can write reviews of items that they have used.
- Comments: The users can make comments on a review. In fact, Epinions allows this way for author and other readers to communicate with each other.
- Rate: the users can rate the reviews according to its value to others.

In this experiment, we randomly selected 39 users from the real data source of Epinions, and these users generate 1082 ratings and also include 362 trust relations, and we randomly generated the number of positive and negative comments for each rating as the following Eqs. (9) and (10).

$$m_{ij}^{+} = m_{ij} \cdot Rand(0.5, 1.25) \cdot 0.8 \cdot \frac{f_i}{f_{\max}}, \tag{9}$$

$$m_{ij}^{-} = m_{ij} - m_{ij}^{+}, \tag{10}$$

where $f_i$ denotes the number of other users who trust user $i$, and $f_{\max} = \max_{i=1,2,\ldots,n} f_i$.

**(2) Measure Index**

Here we define the threshold $\lambda$ of the inferred trust value. Suppose there are two users $i$ and $p$, and we set that if $R_{pi}^{1}$ is no smaller than $\lambda$, then the adjusted trust value $t_{pi}$ is 1, otherwise it would be 0. Two measure indexes are proposed to analyse the experiment results, one of which can be used to compare the results of the inferred trust value $t_{pi}$ and the pre-known trust relationships, and another of which indicates how this method can increase the coverage of trust relationship compared to the pre-known trust network. These two measure indexes are defined as error ratio of inferred trust relationship $r_e$ and coverage increasing ratio $r_c$, respectively. If user $i$ is not in the trust list of customer $p$ while the inferred trust value $t_{pi}$ is equal to 1, then the coverage increasing value of user $p$ on user $i$ is equal to 1, and it is defined as $v_{pi}^{c} = 1$. Then, the coverage increasing ratio is defined as equation (11).

$$r_c = \frac{\sum_{i=1}^{n} \sum_{p=1, p\neq i}^{n} v_{pi}^{c}}{T_n}, \tag{11}$$

where $T_n$ is the total number of trust relationships of all users.

With regards to the mean absolute ratio $r_e$, if user $i$ is in the trust list of customer $p$ while the inferred trust value $t_{pi}$ is equal to 0, then the error value of user $p$ on user $i$

is equal to 1, and it is defined as $v^e_{pi} = 1$. Then, the mean error ratio is defined as equation (12).

$$r_e = \frac{\sum_{i=1}^{n} \sum_{p=1, p\neq i}^{n} v^e_{pi}}{T_n}. \tag{12}$$

## 5.2. *Experiment Results Analysis*

### 5.2.1. *The Results of the Reputation Based Trust Inference*

Here we analyse the results of the coverage increasing ratio and error ratio of inferred trust relationships in four situations, i.e. $\alpha = 1, 2, 3, 4$, where $\alpha$ is the parameter used to adjust the gradient of the confidence function. In each situation, different values of the threshold $\lambda$ of reputation based trust value are discussed.

In Fig. 6, when the threshold $\lambda$ increases from 0.1 to 0.9, the coverage increasing ratio is decreased from 0.199 to 0, and the error ratio is increased from 0.36 to 0.45. In Fig. 7, the coverage increasing ratio is decreased from 0.191 to 0.002, and the error ratio is increased from 0.363 to 0.449. In Fig. 8, the coverage increasing ratio is decreased from 0.205 to 0.016, and the error ratio is increased from 0.362 to 0.448. In Fig. 9, the coverage increasing ratio is decreased from 0.209 to 0.022, and the error ratio is increased from 0.361 to 0.447. So, with the value of $\lambda$ increasing, in all situations of $\alpha$, the error ratio is

**(1)** $\alpha = 1$

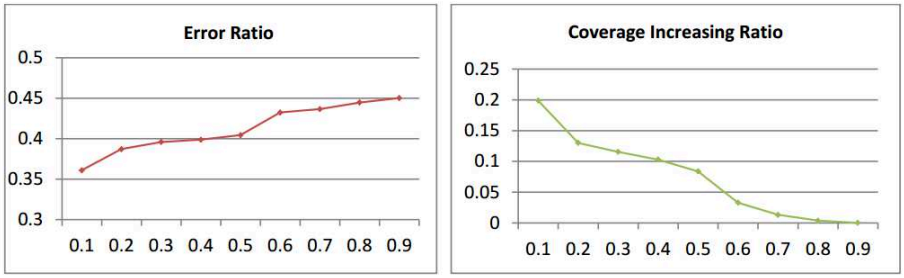


Fig. 6. Error ratio and coverage increasing ratio when $\alpha = 1$.

**(2)** $\alpha = 2$

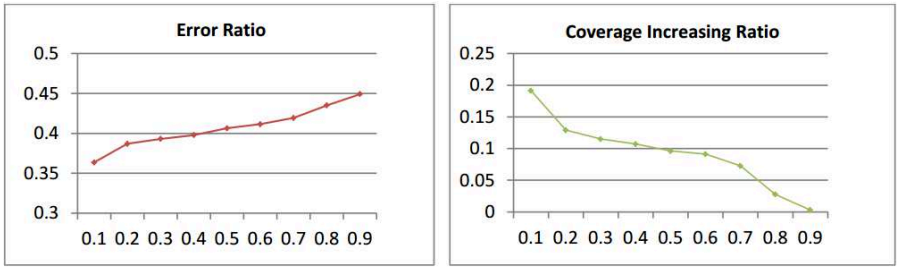


Fig. 7. Error ratio and coverage increasing ratio when $\alpha = 2$.

**(3)** $\alpha = 3$

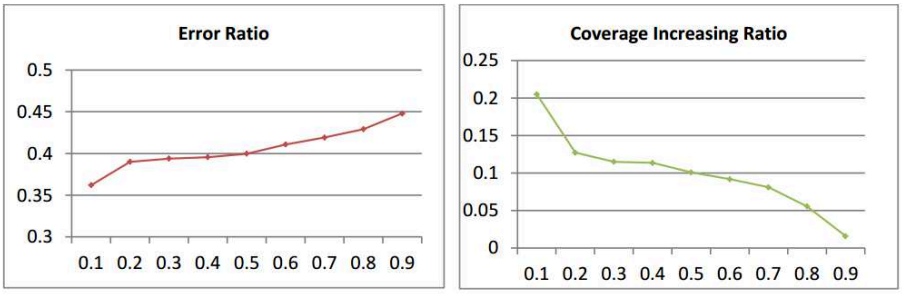


Fig. 8. Error ratio and coverage increasing ratio when $\alpha = 3$.

**(4)** $\alpha = 4$

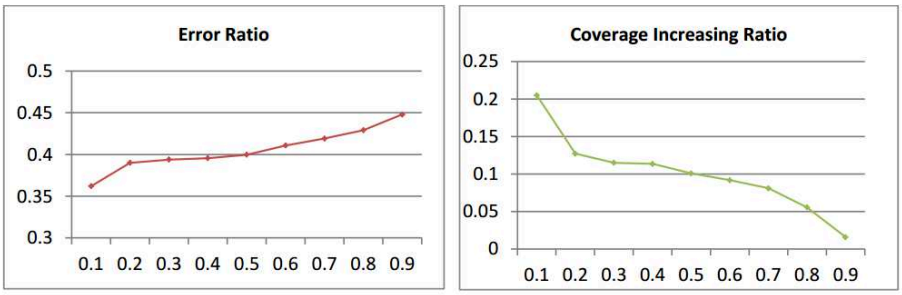


Fig. 9. Error ratio and coverage increasing ratio when $\alpha = 4$.

increasing, and the coverage increasing ratio is decreasing. In this experiment we find that when the value of threshold $\lambda$ is equal to 0.1, then both the error ratio and the coverage increasing ratio reach the best results.

5.2.2. *The Results of Overall Inferred Trust Value*

Here we analyse the results of the coverage increasing ratio and mean error ratio of overall inferred trust value. We give different weights combination of $\gamma_1$, $\gamma_2$, $\gamma_3$, and $\gamma_4$ for the reputation, Web of Trust, similarity, and social closeness based trust values, respectively. In Figs. 10–17, the green lines and the red lines indicate the coverage increasing ratio and the error ratio of the inferred trust relationships, respectively.

In the above figures, the coverage increasing ratios are largely raised up to 1.5 times compared to the pre-known trust network. When $\gamma_1 = 0.1$, $\gamma_2 = 0.2$, $\gamma_3 = 0$, $\gamma_4 = 0.7$, the coverage increasing ratio is up to 1.75 times. Besides, the mean error ratios are also in a relatively low level (below 0.25). We can also find that with the increasing of the weight of the social closeness, the coverage of trust relationship is increased at the meantime.

5.2.3. *Comparison with PCC*

In this part, we can obtain the results by a traditional method of Pearson Correlation Coefficiency (PCC), which is used to calculate the similarity of two users' assessments. Since

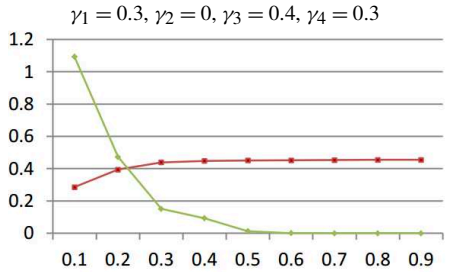


Fig. 10. Combination A.

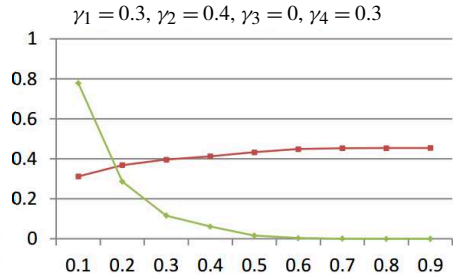


Fig. 11. Combination B.

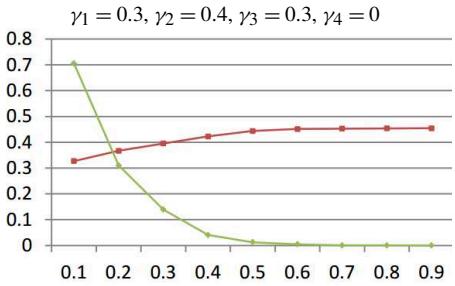


Fig. 12. Combination C.

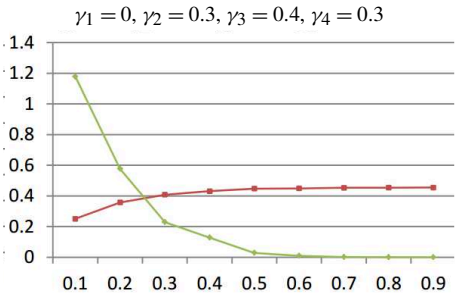


Fig. 13. Combination D.

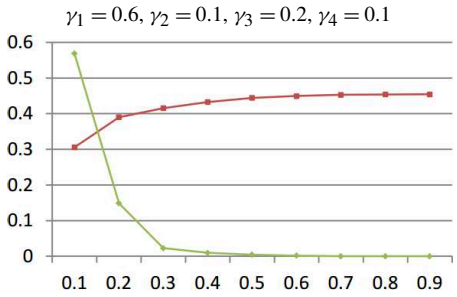


Fig. 14. Combination E.

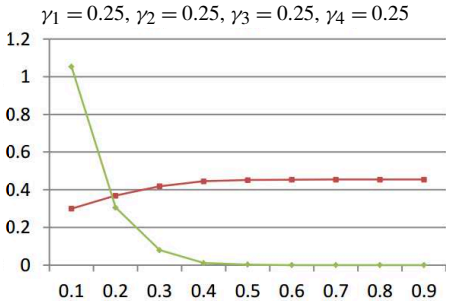


Fig. 15. Combination F.

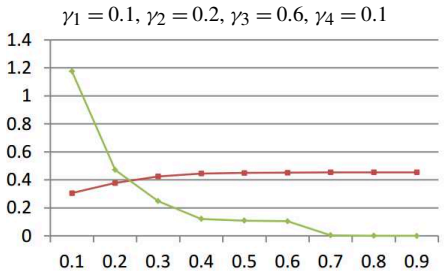


Fig. 16. Combination G.

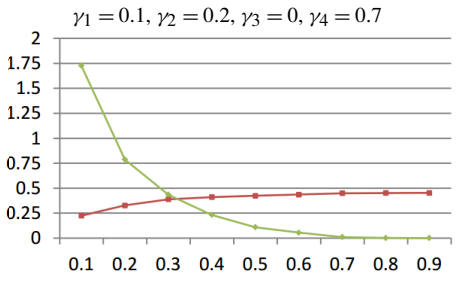


Fig. 17. Combination H.

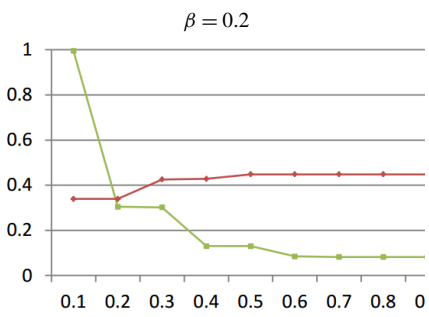


Fig. 18. Results by PCC when $\beta = 0.2$.

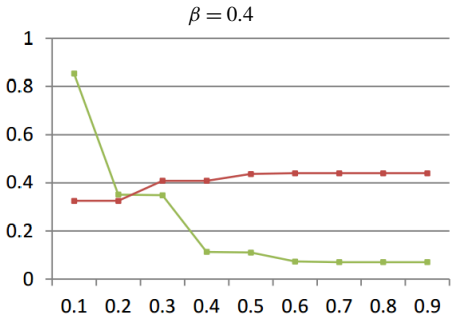


Fig. 19. Results by PCC when $\beta = 0.4$.

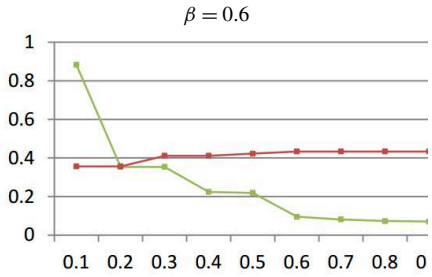


Fig. 20. Results by PCC when $\beta = 0.6$.

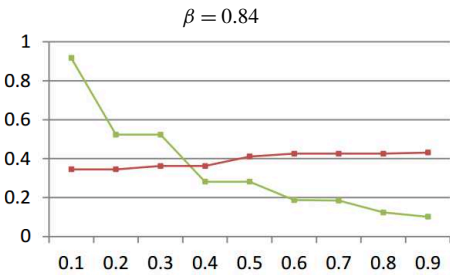


Fig. 21. Results by PCC when $\beta = 0.8$.

this method is also incorporated into our proposed framework, we can compare the two measurement indexes to show how our method has improved the results. In the similarity based trust inference of Section 4, we introduced the weight of the internal similarity, i.e. $\beta$, which is calculated by PCC, and here we can see the different results with varying values of $\beta$. The results are shown in Figs. 18–21.

From the above figures, we can see that the mean error ratios are in the range of $[0.35, 0.45]$, and ours are mainly below 0.3. Besides, the coverage increasing ratios are all below 1, which is worse than the results obtained by our framework.

Based on all the experiments, it can also be concluded that the threshold may be not applied in the referred results, i.e. as long as there is any new trust relationship referred by the model, it should be considered and kept.

## 6. Conclusion

In this paper, we propose a novel trust inference framework for web-based scenarios such as E-commerce websites, knowledge-sharing communities, etc., by incorporating the users' profile information, Web of Trust and associated social networks. The properties of recommendation trust, i.e. the user-user trust are studied and applied to the trust inference processes. We divide the users into four groups according to the available information. That is, the first group is the users who explicitly fill their profile information

and their own Web of Trust and also link their accounts to the social network; the second group is the users who explicitly fill their profile information and their own Web of Trust; the third group is the users who have their Web of Trust and link their accounts to the social network; and the last group is the users who only explicitly express their profile information. For different group of users we have different trust inference policies. The trust relationships are inferred from four aspects. Based on the feedback ratings and comments by other users, the reputation of the discussed user can be calculated. By propagating trust relationships upon the Web of Trust, the coverage of trust relationships can be increased. The simulation experiments show that the threshold value of inferred trust values should be removed and our proposed framework has good performance of both the mean error ratio and coverage increasing ratio.

**Acknowledgements.** This research work is supported by projects of Nature Science Foundation of China (Nos. 71501058, 71131002, 71521001, 71571058, and 71231004), the Humanities and Social Sciences Foundation of the Chinese Ministry of Education (No. 15YJC630097), Anhui Province Natural Science Foundation (No.1608085QG167), the Fundamental Research Funds for the Central Universities (JZ2016HGTA0709, JZ2015HGBZ0117, JZ2016HGTB0727). Panos M. Pardalos is partially supported by the project of "Distinguished International Professor by the Chinese Ministry of Education" (MS2014HFGY026).

## References

Amazon (2002). '*Amazon Auctions*'. http://auctions.amazon.com.

Chang, W.-L., Diaz, A.N., Hung, P.C. (2015). Estimating trust value: a social network perspective. *Information Systems Frontiers*, 17(6), 1381–1400.

De Cock, M., Da Silva, P.P. (2006). A many valued representation and propagation of trust and distrust. In: *Fuzzy Logic and Applications*. Springer, Berlin, pp. 114–120.

Dellarocas, C. (2003). The digitization of word of mouth: promise and challenges of online feedback mechanisms. *Management Science*, 49(10), 1407–1424.

eBay (2002). '*eBay*'. http://www.eBay.com.

Golbeck, J. (2006a). Generating predictive movie recommendations from trust in social networks. In: *iTrust*, pp. 93–104.

Golbeck, J. (2006b). Trust on the world wide web: a survey. *Foundations and Trends in Web Science*, 1(2), 131–197.

Golbeck, J. (2008). Weaving a web of trust. *Science*, 321(5896), 1640–1641.

Golbeck, J.A. (2005). *Computing and applying trust in web-based social networks*. Dissertation, University of Maryland.

Golbeck, J, Parsia, B., Hendler, J.A. (2003). Trust networks on the semantic web. In: *Proceedings of the 7th International Workshop on Cooperative Intelligent Agents*, Helsinki, Finland, August 27–29, 2003, pp. 238–249.

Guha, R., Kumar, R., Raghavan, P., Tomkins, A. (2004). Propagation of trust and distrust. In: *Proceedings of the 13th International Conference on World Wide Web*. ACM, pp 403–412.

Hamdi, S., Bouzeghoub, A., Gancarski, A.L., Ben Yahia, S. (2013). Trust inference computation for online social networks. In: *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 210–217.

Hang, C.W., Wang, Y., Singh, M.P. (2009). Operators for propagating trust and their evaluation in social networks. In: *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems*, Vol. 2, pp. 1025–1032.

Haque, M.M., Ahamed, S. (2007). An omnipresent formal trust model (FTM) for pervasive computing environment. In: *31st Annual International Computer Software and Applications Conference, COMPSAC 2007*. IEEE, pp. 49–56.

Jamali, M., Ester, M. (2009). TrustWalker: a random walk model for combining trust-based and item-based recommendation. In: *15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ACM, New York, pp. 397–406.

Jøsang, A., Ismail, R., Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2), 618–644.

Jøsang, A. (2012). Robustness of trust and reputation systems: does it matter? In: *Trust Management VI*. Springer, Berlin, pp. 253–262.

Kim, Y., Le, M.T., Lauw, H.W., Lim, E.P., Liu, H., Srivastava, J. (2008). Building a web of trust without explicit trust ratings. In: *IEEE 24th International Conference on Data Engineering Workshop*, pp. 531–536.

Kim, Y.A., Phalak, R. (2012). A trust prediction framework in rating-based experience sharing social networks without a web of trust. *Information Sciences*, 191, 128–145.

Kuter, U., Golbeck, J. (2007). Sunny: a new algorithm for trust inference in social networks using probabilistic confidence models. *AAAI*, 7, 1377–1382.

Liu, G., Wang, Y., Orgun, M. (2009). Trust inference in complex trust-oriented social networks. *IEEE International Conference on Computational Science and Engineering*, 4, 996–1001.

Liu, H., Lim, E.P., Lauw, H.W., Le, M.T., Sun, A., Srivastava, J., Kim, Y. (2008). Predicting trusts among users of online communities: an epinions case study. In: *Proceedings of the 9th ACM Conference on Electronic Commerce*, pp. 310–319.

Mármol, F.G., Pérez G.M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, 35(3), 934–941.

Massa, P., Avesani, P. (2004). Trust-aware collaborative filtering for recommender systems. In: *Proceedings of the International Conference on Cooperative Information Systems*, Larnaca, Cyprus, October 25–29, pp. 492–508.

McKnight, D.H., Chervany, N.L. (2001). Conceptualizing trust: a typology and e-commerce customer relationships model In: *Proceedings of the 34th Hawaii International Conference on System Sciences*.

Moradi, P., Ahmadian, S., Akhlaghian, F. (2015). An effective trust-based recommendation method using a novel graph clustering algorithm. *Physica A: Statistical Mechanics and Its Applications*, pp. 462–481.

Mui, L., Halberstadt, A., Mohtashemi, M. (2002). Notions of reputation in multi-agent systems: a review. In: *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS-02)*, Bologna, Italy, July 15–19, pp. 280–287.

Noor, T.H., Sheng, Q.Z., Zeadally, S., Yu, J. (2013). Trust management of services in cloud environments: obstacles and solutions. *ACM Computing Surveys (CSUR)*, 46(1), 12.

Pinyol, I., Sabater-Mir, J. (2013). Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review*, 40(1), 1–25.

Pranata, I., Skinner, G., Athauda, R. (2013). A survey on the usability and effectiveness of web-based trust rating systems. In: *2013 IEEE/ACIS 12th International Conference on Computer and Information Science (ICIS)*, pp. 455-460.

Richardson, M., Agrawal, R., Domingos, P. (2003). Trust management for the semantic web. In: *Proceedings of the 2nd International Semantic Web Conference*, Sanibel Island, Florida, USA, October 20–23, pp. 351–368.

Sabater, J., Sierra, C. (2005). Review on computational trust and reputation models. *Artificial Intelligence Review*, 24(1), 33–60.

Shankaran, R., Varadharajan, V., Orgun, M.A., Hitchens, M. (2009). Context-aware trust management for peer-to-peer mobile ad-hoc networks. In: *2009 33rd Annual IEEE International Computer Software and Applications Conference, COMPSAC'09*, Vol. 2. IEEE, pp. 188–193.

Tavakolifard, M., Knapskog, S.J., Herrmann, P. (2008). Trust transferability among similar contexts. In: *Proceedings of the 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks*. ACM, pp. 91–97.

Uddin, M.G., Zulkernine, M., Ahamed, S.I. (2008). CAT: a context-aware trust model for open and dynamic systems. In: *Proceedings of the 2008 ACM Symposium on Applied Computing*. ACM, pp. 2024–2029.

Wang, G., Wu, J. (2011). Multi-dimensional evidence-based trust management with multi-trusted paths. *Future Generation Computer Systems*, 27, 529–538.

Wang, Y., Li, L., Liu, G. (2015). Social context-aware trust inference for trust enhancement in social network based recommendations on service providers. *World Wide Web*, 18(1), 159–184.

Yan, S., Zheng, X., Chen, D., Wang, Y. (2013). Exploiting two-faceted web of trust for enhanced-quality recommendations. *Expert Systems with Applications*, 40(17), 7080–7095.

Yu, Y., Li, K., Zhou, W., Li, P. (2012). Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. *Journal of Network and Computer Applications*, 35(3), 867–880.

Yuan, W., Guan, D., Lee, Y., Lee, S., Sung, J. (2010). Improved trust-aware recommender system using small-worldness of trust networks. *Knowledge-Based Systems*, 23(3), 232–238.

Zhan, J., Fang, X. (2011). A novel trust computing system for social networks. In: *2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing*, pp. 1284–1289.

Zhang, Y., Yu, T. (2012). Mining trust relationships from online social networks. *Journal of Computer Science and Technology*, 27(3), 492–505.

Ziegler, C.N., Lausen, G. (2005). Propagation models for trust and distrust in social networks. *Information Systems Frontiers*, 7, 337–358.

Zhao, K., Pan, L. (2014). A machine learning based trust evaluation framework for online social networks. In: *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 69–74.

Zolfaghar, K., Aghaie, A. (2010). Mining trust and distrust relationships in social web applications. In: *Proceedings of the 2010 IEEE International Conference on Intelligent Computer Communication and Processing*, Cluj-Napoca, Romania, August 26–28, pp. 73–80.

Zhang, Y., Wu, Z., Chen, H., Sheng, H., Ma, J. (2008). Mining target marketing groups from users' web of trust on epinions. In: *AAAI Spring Symposium: Social Information Processing*, pp. 116–121.

**W. Fan** is currently a lecturer and Master supervisor at the School of Management, Hefei University of Technology, Hefei, China. She obtained her BS degree from Nanjing University of Aeronautics and Astronautics in 2009 and PhD degree from Hefei University of Technology in 2014. Her research interests include trust inference models, social network, and cloud computing.

**J. Pei** is currently a lecturer and Master supervisor at the School of Management, Hefei University of Technology, Hefei, China. He obtained his BS and PhD degrees from Hefei University of Technology in 2009 and 2014. His research interests include supply chain scheduling, artificial intelligence, and information systems.

**S. Ding** is currently an associate professor and Master supervisor at the School of Management, Hefei University of Technology, Hefei, China. His research interests include trust modeling, cloud service recommendation, social network.

**P.M. Pardalos** serves as a distinguished professor of industrial and systems engineering at the University of Florida, Gainesville, FL, USA. He is also the director of the Center for Applied Optimization. Dr. Pardalos is a world leading expert in global and combinatorial optimization. His recent research interests include network design problems, optimization in telecommunications, e-commerce, data mining, biomedical applications, and massive computing.

**M. Kong** is currently working on his PhD degree at the School of Management, Hefei University of Technology. He obtained his BS degrees from Hefei University of Technology in 2015. His research interests include supply chain scheduling and application of Internet of Things.

**S. Yang** is at present a professor and PhD adviser at the School of Management, Hefei University of Technology, Hefei, China. He is also a member of the Chinese Academy of Engineering. His recent research fields include decision theory, artificial intelligence, information management, and information systems.

# Naujas pasitikėjimo nustatymo karkasas su socialiniu tinklu ir pasitikėjimo tinklu internetiniams scenarijams: euristinis būdas

Wenjuan FAN, Jun PEI, Shuai DING, Panos M. PARDALOS, Min KONG, Shanlin YANG

Šiame straipsnyje siūlome naują pasitikėjimo nustatymo karkasą internetiniams scenarijams, kuriuose numatomas pasitikėjimo tinklas ir pasitikėjimo sąryšiai įvertinami pagal pasitikėjimo rekomendaciją. Retos matricos pasitikėjimo tinkle problemai sumažinti įtraukiame vartotojų profilių ir sąryšių informaciją susijusiame socialiniame tinkle. Vartotojai yra suklasifikuojami į keturias klases pagal pasitikėjimo tinklą aptartame internetiniame scenarijuje, epinions.com šiame straipsnyje, ir socialinių sąryšių informaciją susijusiame socialiniame tinkle. Paskui įvairi informacija yra naudojama nustatyti vartotojų pasitikėjimo rekomendacijų reikšmėm remiantis klasifikacija. Modeliavimo eksperimentai rodo, kad pasiūlytas būdas gerai atitinka nustatytas pasitikėjimo reikšmes, o numatyto pasitikėjimo sąryšio tikslumo rodiklis yra aukštesnis negu tradicinio būdo.