Appl Intell (2011) 35:399–410
DOI 10.1007/s10489-010-0230-7

The small-world trust network

Weiwei Yuan · Donghai Guan · Young-Koo Lee · Sungyoung Lee

Published online: 27 April 2010

Abstract The topology of the trust network is important to optimize its usage in the trust-aware applications. However, since the users can join trust network ubiquitously, the structure of the highly dynamic trust network is still unknown. This paper contributes to verify that the trust network is the small-world network, and its small-world topology is independent of its dynamics. This is achieved by verifying the scale-freeness of five trust networks extracted from real online sites. Using the small-world nature of the trust network, we optimize the rating prediction mechanism of the conventional trust-aware recommender system. Experimental results clearly show that our proposed mechanism can achieve the maximum accuracy and coverage with the minimum computation complexity for the rating predictions.

Keywords Trust · Trust networks · Small-world network · Recommender system

1 Introduction

Trust is the measure of willingness to believe in a user based on its competence (e.g. goodness, strength, ability) and behavior within a specific context at a given time. It is a directional relationship from the trustor—the user that evaluates its trust on the target user—to the trustee—the user that is the target of the trust evaluation. Trust is transitive, so if A trusts B and B trusts C, A will trust C to some extent. This enables the trust propagations between users. Trust network is therefore constructed: the users act as the nodes and their trusts act as the edges.

The trust network has been widely used in many applications [1], such as the recommender systems [2, 3] and the security mechanisms [4]. Despite its popularity, little is known about its topology. This is because the trust network is highly dynamic: a user can join at anytime by stating its trust on any existing user. This irregular growth leads to the complex structure of the trust network. In essence, the topology of the trust network is the important information to optimize its usage in the trust-aware applications, so it is essential to make clear its structure. Since some complex networks, such as the World Wide Web [5] and the e-mail network [6], have been verified to have the small-world topology, some works assume that the trust network also has the small-world nature. These works include, for instance, the trust-based security mechanism [7], the trust-based multiagent system [8] and the trust network modeling [9].

Though the existing works assume the small-worldness of the trust network, no one has verified it. This work contributes to experimentally verifying that the dynamic trust network is the small-world network: it is highly clustered while has small average path length, and its small-worldness is independent of its dynamics. This is achieved by employing a novel experimental methodology on five trust networks extracted from real online communities. Specifically, instead of examining the clustering coefficients and the average path lengths on the experimental data respectively, as done by the conventional small-world verification methodology, we ver-

W. Yuan · Y.-K. Lee (✉) · S. Lee
Dept. of Computer Engineering, Kyung Hee Univ., Seoul, Korea
e-mail: yklee@khu.ac.kr

W. Yuan
e-mail: yuanweiwei00@gmail.com

S. Lee
e-mail: sylee@oslab.khu.ac.kr

D. Guan
College of Automation, Harbin Engineering University, Harbin, China
e-mail: donghai@oslab.khu.ac.kr

ify the small-worldness of the trust network via its scale-freeness. Based on the relationship between the small-world network and the scale-free network as well as the basic properties of the scale-free network, our work shows that the trust network continuously has the small-worldness however it changes.

Many trust-aware applications could benefit from the small-world topology of the trust network. This work chooses the trust-aware recommender system (TARS) as an example of such applications. We optimize the conventional TARS model by leveraging the small-worldness of the trust network. Specifically, the values of the maximum trust propagation distance, which is the most important parameter of the conventional TARS model, are suggested for different sized TARS. The effectiveness of the optimized TARS model is verified on three sets of large scale experimental data with respect to the rating prediction accuracy, the coverage and the computational complexity.

The organization of this paper is as follows: in Sect. 2, we introduce the trust network; in Sect. 3, we verify that the dynamic trust network has small-world topology; based on the small-worldness of the trust network, we optimize the conventional TARS model in Sect. 4; the last section concludes this paper.

2 Trust networks

In this section, we introduce some background knowledge of the trust network.

The values of the trust can be measured in different ways for the trust network: (1) Binary measurement: code 1 if the trustor trusts the trustee and code 0 in other cases. (2) Ordinal measurement: code $+1$ if the trustor trusts the trustee, code -1 if the trustor distrusts the trustee, and code 0 if the trustor doesn't care about the trustee. (3) Multiple-category measurement: categorize the trust, such as Definite Trust, Trust, Somewhat Trust, and No Trust, and score these categories, such as "1" type, "2" type etc. (4) Full-rank measurement: score the trust in a rank order from the strongest to weakest. E.g., use a scale from 1 to -1—where 1 means the trustor trusts the trustee, 0 means the trustor feels neutral about the trustee, and -1 means the trustor distrusts the trustee. This measurement can illustrate the strength of trust on a ratio level. The most popular trust measurement is the binary measurement [27], and our work also evaluates trust in binary values.

The data of the trust network, which is named as the trust matrix in this paper, is the collection of all trust statements between the nodes of the trust network. The trust matrix is a square matrix since the users state trust on each other. Each element of the trust matrix describes the trust between two users. An example of the trust matrix is given in Table 1,

Table 1 An example of the trust matrix which records the trusts between 4 users

	Alice	Bob	Carol	David
Alice	0	1	1	0
Bob	0	0	1	0
Carol	0	1	0	1
David	1	1	0	0

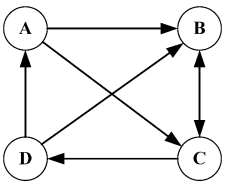


Fig. 1 The graph which represents the trust network with the trust matrix shown in Table 1

which records the trusts between 4 users using the binary trust measurement. Since it is mentioned in [27] that the users' trusts on themselves do not influence the performance of the trust network, the diagonal of the matrix is valued 0 in this work. The sum of the trust values in the row of a user is its outdegree, which is the number of the edges pointing from this user to others in the trust network. For instance, the outdegree of Alice in Table 1 is 2, which is the sum of Alice's row in the trust matrix. The users with higher outdegrees are more likely to trust other users. The sum of the trust values in the column of a user is its indegree, which is the number of the edges pointing from other users to this user in the trust network. For instance, the indegree of Alice in Table 1 is 1, which is the sum of Alice's column in the trust matrix. The users with higher indegrees tend to be more reputable in the trust network.

Graphs can be used to represent the trust networks since they are compact and systematic. Since the trust is asymmetrical, it is the directed graph that is suitable to represent the trust network, where users are represented by nodes and the trust is represented by drawing an arrow from the trustor to the trustee. Due to the binary trust measurement used in this work, the directed graph used to represent the trust network is the binary graph. That is, an arrow pointing to a user represents that this user is trusted, while no arrow represents the absence of trust. For example, Fig. 1 can be used to represent the trust network with the trust matrix shown in Table 1.

The major approach to examine how a user is embedded in the trust network is to measure its distance to others. If A trusts B, A's distance to B is one hop. If A trusts B, and B trusts C (and A does not trust C), A's distance to C is two hops. In this work, the distance from the trustor to the trustee is represented by the number of hops in the shortest path from the trustor to the trustee. The trustor is more likely to trust the trustees with shorter distances. If the distance is too big, the trustee may hardly be trusted by the trustor—even if the trustee is technically reachable.

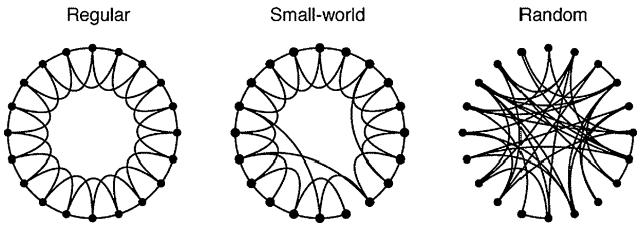


Fig. 2 The comparison between the regular network, the random network and the small-world network [15]

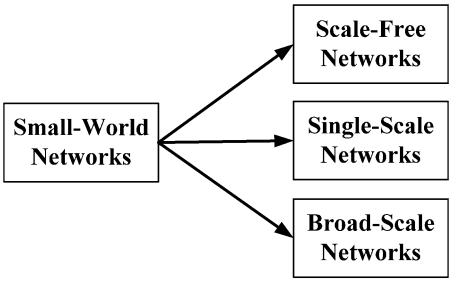


Fig. 3 The relationship between the small-world network and the scale-free network

3 Experimental verifications on the small-worldness of dynamic trust networks

The small-world network is a kind of network between the regular network and the random network. The regular network is highly clustered yet has long distance between two randomly selected nodes. The random network is not clustered yet has short distances between nodes. The small-world network is defined as the network that has large clustering coefficient and small average path length [10]. The relationship between the regular network, the random network and the small-world network is summarized in Fig. 2.

Using the experimental arguments is a very popular way to verify the small-worldness of the networks [5, 11–15]. Moreover, to the best of our knowledge, no work theoretically proves the small-worldness of the practical networks. We therefore experimentally verify the small-worldness of the dynamic trust network using the data extracted from the real online applications.

3.1 Experimental methodology

As shown in the definition of the small-world network, the clustering coefficient and the average path length are the two measures to evaluate the small-worldness. The conventional method [5, 11–15] examines these two properties respectively. On one hand, it checks whether the clustering coefficient of the network is much larger than that of its corresponding random network. A network's corresponding random network refers to the random network that has the same number of nodes and same number of edges per node as this network. On the other hand, it checks whether the average path length of the network is almost as small as that of its corresponding random network. If a network has both properties, the conventional method makes the conclusion that this network is the small-world network.

Despite its popularity, the conventional method suffers from the problem that it only reflects the small-worldness of the network in a static status. This is because the data used for the experimental verification are usually static for the conventional method, i.e., they only reflect the status of the network at one moment. So the conclusion made by the conventional method on the small-worldness only shows the structure of the network at a particular moment, i.e., the moment that the experimental data were extracted. However, some networks, such as the trust network, are dynamically changing. Further verifications are needed to show the small-worldness of the networks in dynamics.

To overcome the limitation of the conventional verification method, we verify the small-worldness of the dynamic trust network via verifying its scale-freeness. The scale-free network is a kind of network whose degree distribution decays as a power law [17]. It is one kind of small-world network [16, 17]. Many large-scale complex networks are scale-free [18]. The relationship between the small-world network and the scale-free network is given in Fig. 3, in which the broad-scale network is characterized by a degree distribution that has a power law regime followed by a sharp cutoff and the single-scale network is characterized by a degree distribution with a fast decaying tail [16].

The scale-freeness of a network ensures that this network still has the scale-free structure in dynamics. This is because the scale-free structure of such a network is independent of its scale [19]. There are some highly connected nodes in the scale-free network, dominating the connectivity. Unlike the random networks, the probability with which a new node connects to the existing nodes is not uniform in the scale-free network. There is a higher probability that it will be linked to a node that already has a large number of connections [19]. This contributes to the network's continuous scale-freeness when the network changes.

Since the scale-free network is a kind of the small-world network, if we can verify that the trust network is the scale-free network by the static network data, we can draw the conclusion that the trust network is a small-world network. Moreover, since the scale-freeness of the network is independent of its dynamics, we can further make the conclusion that the dynamically changing trust network is a small-world network. This verification method only uses the static trust network data. Extra data that describe the status of the trust networks in dynamics are not needed.

In addition to its ability in verifying the small-worldness of the dynamic trust networks, verifying the scale-freeness

is computationally less expensive. The conventional method needs to calculate the clustering coefficient and the average path length of the trust network respectively. The clustering coefficient of a network is the mean of the clustering coefficient of each node, in which the clustering coefficient of a node is the fraction of the allowable edges and the edges that actually exist between the neighbors of this node [10]. To calculate the clustering coefficient, the conventional method needs to make clear the connections between all pairs of nodes in each node's neighborhood. The average path length is the number of edges in the shortest path between two nodes, averaged over all pairs of nodes [10]. To calculate the average path length, the conventional method needs to make clear the trust propagation distance between any two nodes of the trust networks. However, to verify the scale-freeness of the trust network, we only need to calculate the degree distributions of each node. That is, we only need to know the direct trust between the nodes of the trust network, while we do not need to know the trust propagation relationships between these nodes.

3.2 Experimental setup

Five trust networks are used in this work to verify the small-worldness. These trust networks are extracted from five public released datasets respectively. These datasets are the Epinions dataset, the Kaitiaki dataset, the Squeakfoundation dataset, the Robots dataset and the Advogato dataset. They are available at trustlet.org.[1]

The Epinions dataset has two kinds of data files: the rating matrix and the trust matrix. The rating matrix records the users' ratings on items. The trust matrix records the users' trust on other users. The trustors assign the trust value 1 to their trusted trustees and assign the trust value 0 to others. We extract a trust network named Epinions from the Epinions dataset. Epinions consists of 49288 users and 487183 trust statements between these users. Its data are all stated by users from November to December of 2003.

Except the Epinions dataset, all other datasets (Kaitiaki, Squeakfoundation, Robots and Advogato) only consist of the trust matrix. We extract four trust networks named as Kaitiaki, Squeakfoundation, Robots and Advogato from their corresponding datasets respectively. Advogato consists of 5412 users and 54012 trust statements between these users. Its data are all stated by users on June 1, 2009. Its trust statements are in several levels: Observer, Apprentice, Journeyer or Master [20]. Kaitiaki consists of 64 users and 154 trust statements between these users. Its data are all stated by users on September 1, 2008. Its trust statements are in four levels: Kaitiro, Te Hunga Manuhiri, Te Hunga Käinga, Te Komiti Whakahaere. Squeakfoundation consists of 461 users and 2697 trust statements between these users. Its data are all stated by users on November 1, 2008. Its trust statements are in three levels: Apprentice, Journeyer, and Master. Robots consists of 1646 users and 3456 trust statements between these users. Its data are all stated by users on March 1, 2009. Its trust statements are in three levels: Apprentice, Journeyer, and Master.

Table 2 Description of the trust networks used in this work

	Number of nodes	Average degree
Advogato	5412	9.98
Epinions	49288	9.88
Kaitiaki	64	2.41
Robots	1646	2.1
Squeakfoundation	461	5.85

The characteristics of our explored trust networks are summarized in Table 2. All users involved in these trust networks act as the trustors, the trustees or both. By analyzing these trust networks, the following subsection is used to verify the small-worldness of the trust network.

3.3 Experimental results

We examine the degree distributions of the above trust networks to verify their small-worldness via the scale-freeness. The trust is asymmetrical, i.e., if A trusts B, B does not necessarily need to trust A. So the trust network is the directed network. We therefore distinguish the indegree distribution and the outdegree distribution of the trust networks. We present the degree distributions of our explored five trust networks in Figs. 4–8. Note that some parts of axes in the figures are marked as 0(0.1). This is because the indegree or outdegree of some nodes equals to 0, but 0 is not a valid value for the logarithm. To show the degree distributions of these nodes, we use 0.1 to approximately substitute 0 when calculating the logarithm of the degrees.

It is clearly shown in the experimental results that the nodes' indegree distribution and outdegree distribution both follow the power-law in each trust network. That is, the degree distributions follow the rule $P(k) \sim k^{-\gamma}$, in which $P(k)$ is the probability that a randomly selected node has exactly k edges, and γ is the power of the degree distributions. We further list the power of our explored trust networks' degree distributions in Table 3, in which γ_{in} and γ_{out} represent the power of the indegree distribution and the power of the outdegree distribution respectively in Figs. 4–8. We therefore make the conclusion that the trust networks are the scale-free networks according to the definition of the scale-free networks. Based on the analy-

[1] http://www.trustlet.org/wiki/Datasets.

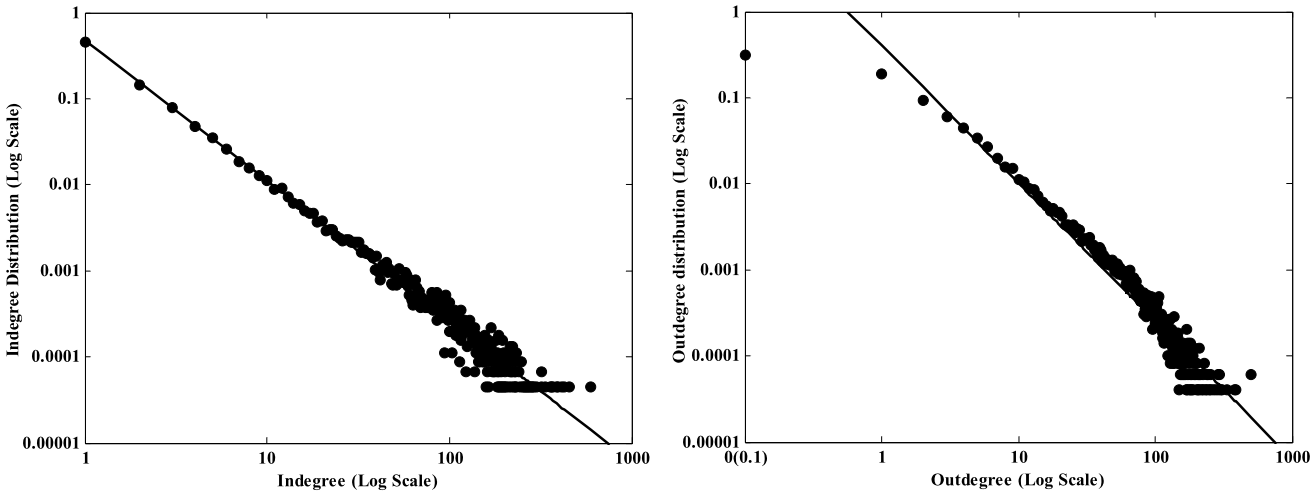


Fig. 4 The indegree distribution and the outdegree distribution of Epinions. The lines have slopes (**a**) $\gamma_{in} = 1.53$, and (**b**) $\gamma_{out} = 1.6$

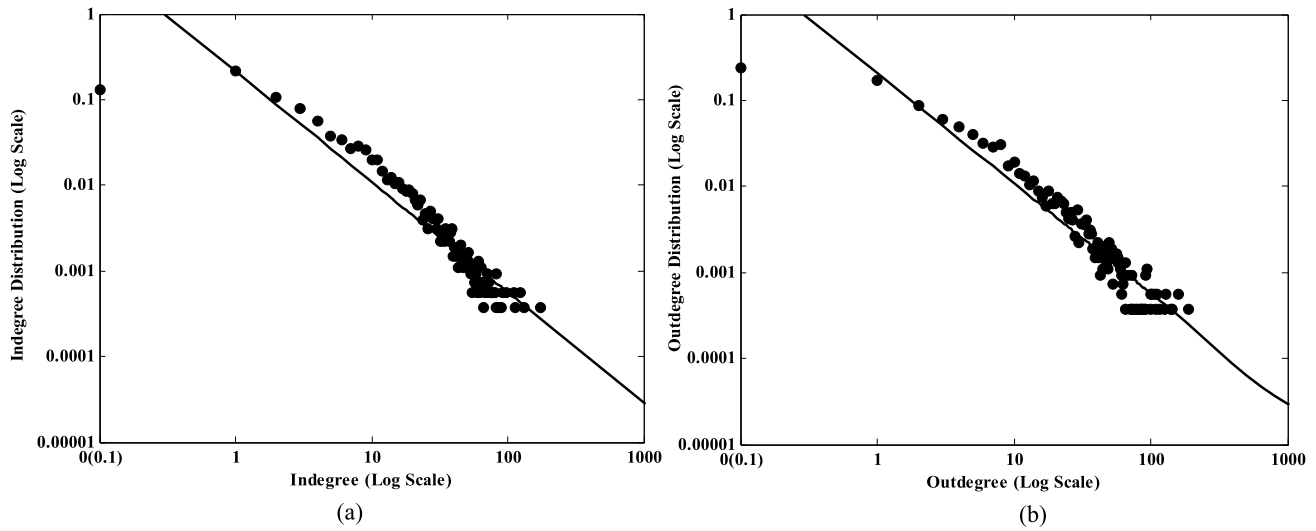


Fig. 5 The indegree distribution and the outdegree distribution of Advogato. The lines have slopes (**a**) $\gamma_{in} = 1.29$, and (**b**) $\gamma_{out} = 1.28$

Table 3 The indegree distribution and the outdegree distribution of the trust networks with n nodes and k average degree

	n	k	γ_{in}	γ_{out}
Advogato	5412	9.98	1.29	1.28
Epinions	49288	9.88	1.53	1.6
Kaitiaki	64	2.41	0.92	0.64
Robots	1646	2.1	1.93	1.23
Squeakfoundation	461	5.85	1.93	0.79

sis shown in Sect. 3.1, we make the further conclusion that the dynamic trust networks are the small-world networks.

Since the trust networks have the small-world structure, they have the common properties of the small-world networks: (1) the local neighborhood is preserved; and (2) the diameter of the network, quantified by the average shortest distance between two nodes, increases logarithmically with the size of the networks [11]. The latter property suggests that the trust networks are of finite dimensionality. In addition, this property also points out that it is possible to connect any two nodes of the trust network through just a few trust propagations. This trust propagation distance is similar to the average path length of the trust network's corresponding random network, which could be easily figured out since

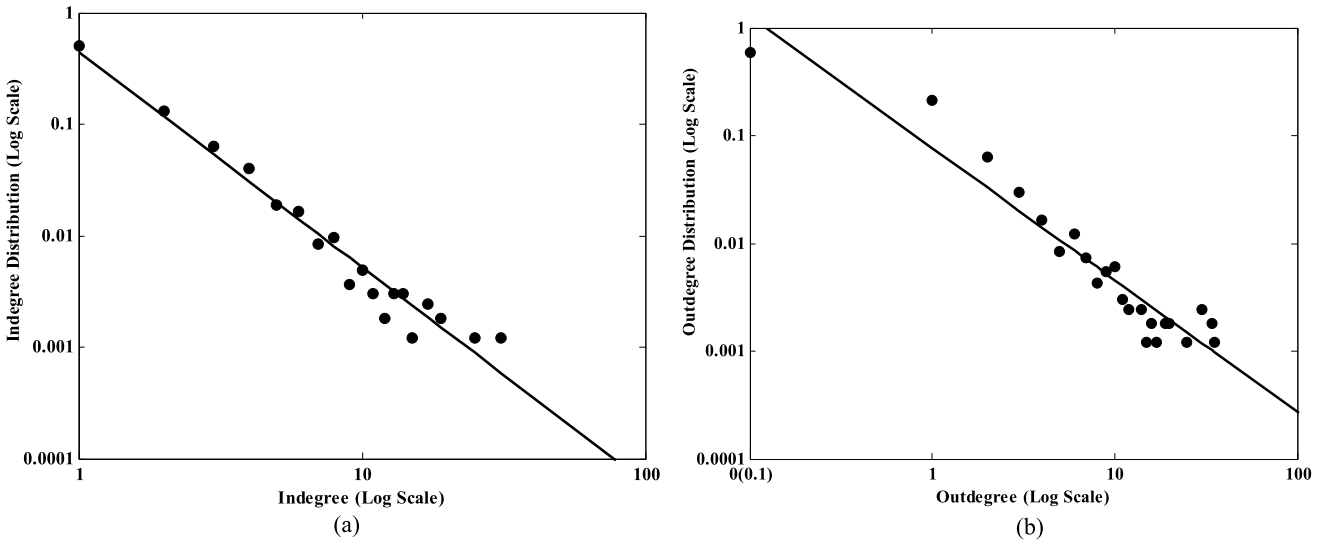


Fig. 6 The indegree distribution and the outdegree distribution of Robots. The lines have slopes (**a**) $\gamma_{in} = 1.93$, and (**b**) $\gamma_{out} = 1.23$

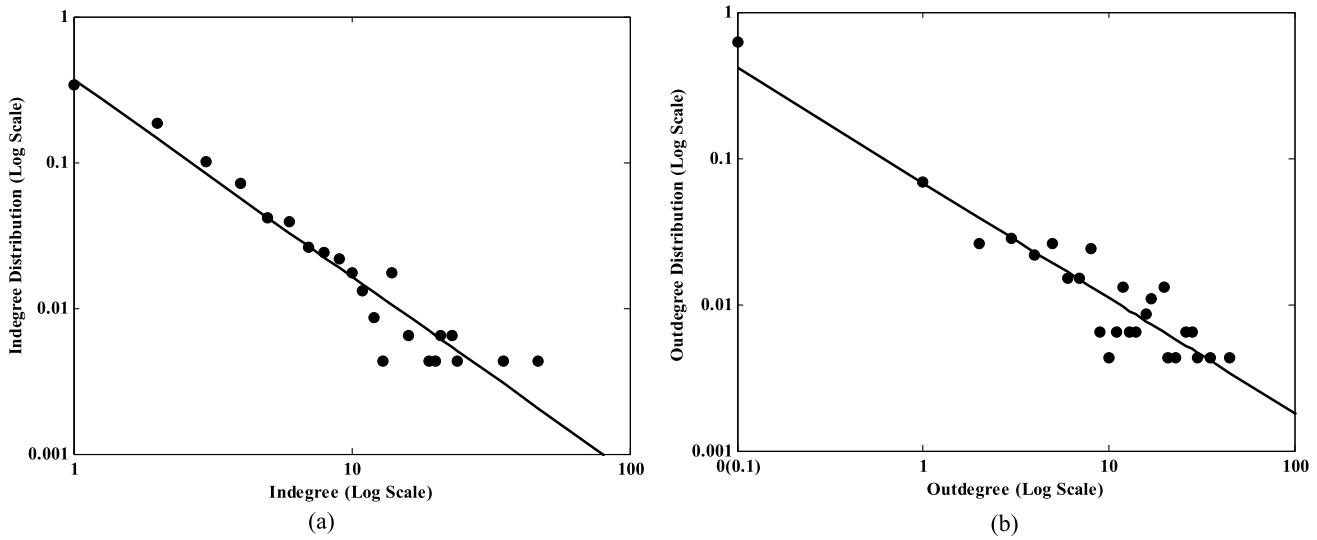


Fig. 7 The indegree distribution and the outdegree distribution of Squeakfoundation. The lines have slopes (**a**) $\gamma_{in} = 1.93$, and (**b**) $\gamma_{out} = 0.79$

it only relates to the size and the average degree of the trust network [10]:

$$L \approx L^R = \frac{\ln(n)}{\ln(k)}, \tag{1}$$

where L represents the trust propagation distance between two randomly selected nodes of the trust network, L^R represents the average path length of the trust network's corresponding random network, n represents the size of the trust network, and k represents the average degree of the trust network.

Using these small-world related properties, it is possible to optimize various trust-aware applications. In this work, we use the trust-aware recommender system as a concrete example of such trust-aware applications, and analyze how the small-worldness of the trust network optimizes TARS in details.

4 Optimizing TARS using small-world properties of trust networks

The trust-aware recommender system (TARS) is the recommender system that suggests the worthwhile information to the users on the basis of trust. TARS has recently been proposed for use since it is able to solve the well-known data sparseness problem of the classical collaborative filtering (CF) [3]. Moreover, the rating prediction accuracy of

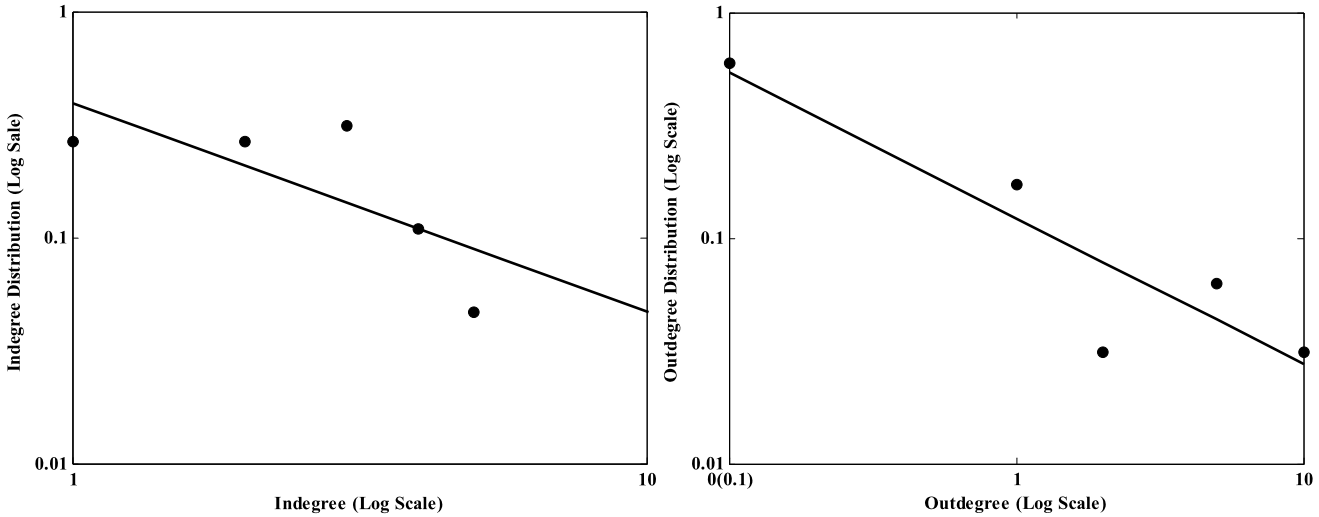


Fig. 8 The indegree distribution and the outdegree distribution of Kaitiaki. The lines have slopes (**a**) $\gamma_{in} = 0.92$, and (**b**) $\gamma_{out} = 0.64$

TARS is no worse than the classical CF [25]. Using our verified small-worldness of the trust network, we show how the small-world properties contribute to optimize the conventional TARS model in this section.

4.1 Conventional TARS model

A number of researchers [2, 3, 21–23] have proposed their TARS models. Among these works, the TARS model proposed by Massa and Avesani [3, 24–26] is the most popular one. Due to its popularity, their TARS model is used as the basis of analysis in this research. The conventional TARS model specifically refers to their model in this work. The architecture of TARS is shown in Fig. 9. The inputs are the trust matrix and the rating matrix. The output of TARS is the predicted ratings on the items for different users. The rating prediction mechanism of the conventional TARS model is described in Table 4. It consists of three phases:

The first phase is the recommender searching. In this phase, the conventional TARS model searches all valid recommenders based on the active user's trust propagation distances to the recommenders. A recommender is valid if (1) there is at least one path from the active user to the recommender in the trust network, and (2) the trust propagation distance from the active user to the recommender is no longer than the maximum trust propagation distance (MTPD).

The second phase is the recommender weighting. In this phase, each valid recommender is weighted based on the relationship between the active user's trust propagation distance to the recommender and MTPD:

$$w_{a,u} = \frac{d_{\max} - d_{a,u} + 1}{d_{\max}}, \tag{2}$$

Table 4 Rating prediction mechanism of the conventional TARS model

Input: T (trust matrix), R (rating matrix)
Parameter: a (active user), i (item), $d_{\max}$ (the maximum trust propagation distance)
Output: $p_{a,i}$ (a's predicted rating on i)
Phase 1: Recommender searching.
Phase 2: Recommender weighting.
Phase 3: Rating calculation.

in which $w_{a,u}$ is the weight of the recommender u with respect to the active user a, $d_{\max}$ is MTPD, and $d_{a,u}$ is the trust propagation distance from a to u.

The third phase is the rating calculation. In this phase, the conventional TARS model predicts the rating by aggregating the recommendations given by the valid recommenders, in which each recommendation is weighted with respect to the weight of the recommender:

$$p_{a,i} = \overline{r_a} + \frac{\sum_{u=1}^{k} w_{a,u}(r_{u,i} - \overline{r_u})}{\sum_{u=1}^{k} w_{a,u}}, \tag{3}$$

in which $p_{a,i}$ is the predicted rating on the item i for the active user a, $\overline{r_a}$ is the active user's average rating on the rated items, $\overline{r_u}$ is the recommender's average rating on the rated items, $r_{u,i}$ is the recommender u's recommendation on the item i, and k is the number of valid recommenders.

4.2 Optimized TARS model

Though the conventional TARS model has high rating prediction accuracy and high rating prediction coverage [25], it

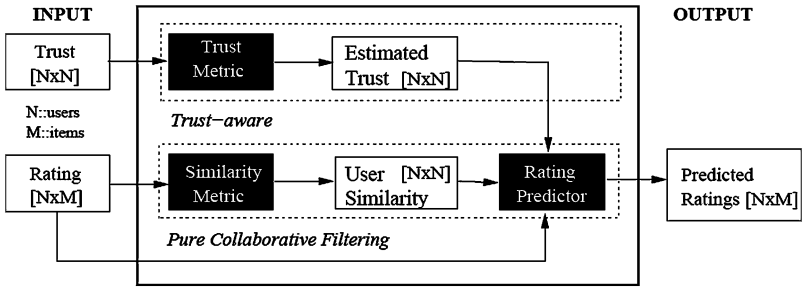


Fig. 9 The architecture of the trust-aware recommender system [3]

suffers from the problem that it is not optimized: its computational complexity can be exponentially more expensive by achieving similar rating predication accuracy and rating prediction coverage, and its rating prediction coverage can be significantly worse by achieving similar rating predication accuracy. This is because the value of MTPD, which is the fundamental parameter of TARS, is not decided for the conventional TARS model. In the rating prediction mechanism of the conventional TARS model, MTPD decides (1) whether the recommendations are valid for the rating prediction, and (2) the weights of the valid recommendations. However, the conventional TARS model just randomly chooses some values for this extremely important parameter [3]. In essence, setting an appropriate value of MTPD for TARS is necessary, because TARS requires more computational efforts by setting a greater value of MTPD, and TARS might lose some valuable recommendations by setting a smaller value of MTPD.

Using our verified small-worldness of the trust network, we optimize the conventional TARS model by setting appropriate value of MTPD for different sized TARS. Though it is hard to predict the value of MTPD from a randomly selected active user to a randomly selected recommender, based on the small-world nature of the trust network, it is easy to get the approximate average trust propagation distance between two randomly selected users of the trust network in TARS. It is similar to the average path length of this trust network's corresponding random network. We only need to know the size and the average degrees of the trust network. Intuitively, the optimized value of MTPD should have some relationship with the average path length of the trust network. And since the value of MTPD is unknown and the average path length of the trust network is the only available information about the distance between two users, we heuristically choose the average path length of the trust network as the value of MTPD to optimize the conventional TARS model. That is, we calculate $\lceil L^R \rceil$ as the value of MTPD for the rating prediction mechanism shown in Table 4, in which $\lceil L^R \rceil$ is the ceiling of the average path length of this trust network's corresponding random network, and L^R is calculated by (1):

$$d_{\max} = \lceil L^R \rceil = \left\lceil \frac{\ln(n)}{\ln(k)} \right\rceil. \tag{4}$$

We examine the performance of the optimized TARS model on the data of the Epinions dataset. Data from other datasets used in Sect. 3 is not used to simulate TARS. This is because these datasets only have the trust matrices while the inputs of TARS need the trust matrix and the rating matrix simultaneously. The Epinions dataset is the only public released dataset for TARS when this work began. Since the conventional TARS model also uses this dataset, we use the Epinions dataset for better comparison with the conventional TARS model.

To provide more evidence on the effectiveness of the optimized TARS model with a single dataset, we extracted three sets of data from the Epinions dataset based on the timestamp of the trust statements and the ratings. These three sets of data are named as Epinions_1, Epinions_2 and Epinions_3 respectively. Each set of data consists of both the trust data and the rating data. Epinions_1 records trust statements and ratings stated by users in January 2001. Its trust data consists of 45275 users and 461064 trust statements. Its rating data consists of 31019 users' 8632163 ratings on 551392 items. Epinions_2 records trust statements and ratings stated by the users in the year 2002, from January to December. Its trust data consists of 4389 users and 37843 trust statements. Its rating data consists of 2275 users' 740422 ratings on 36144 items. Epinions_3 records trust statements and ratings stated by the users in November and December of 2003. Its trust data is the same as Epinions used in section 3. It consists of 49288 users and 487183 trust statements. The rating data of Epinions_3 consists of 20157 users' 664061 ratings on 139633 items. Both Epinions_1 and Epinions_2 are extracted from the "extended epinions dataset".[2] Epinions_3 is extracted from the "epinions dataset".[3] We use Table 5 to summarize these three sets of experimental data. Note that not all users in the trust data are involved in the rating data. This is because some users of the trust network may not give any ratings on the items. E.g. only around 40% users in the trust data of Epinions_3 are involved in the rating data.

Using Epinions_1, Epinions_2 and Epinions_3, we predict ratings on the rated items of each rating data. Since the

[2] http://www.trustlet.org/wiki/Extended_Epinions_dataset.

[3] http://www.trustlet.org/wiki/Downloaded_Epinions_dataset.

Table 5 The description of the TARS experimental data

		Num of users	Num of items	Num of trusts	Num of ratings
Epinions_1	Trust Matrix	45275	–	461064	–
	Rating Matrix	31019	551392	–	8632163
Epinions_2	Trust Matrix	4389	–	37843	–
	Rating Matrix	2275	36144	–	740422
Epinions_3	Trust Matrix	49288	–	487183	–
	Rating Matrix	20157	139633	–	664061

scale of each rating data is huge, it is very effort-consuming to predict ratings on all the rated items. We therefore randomly select 5% of the rating records from each rating data as the object of the prediction. That is, we predict around 400,000 ratings for Epinions_1, around 30,000 ratings for Epinions_2, and around 30,000 ratings for Epinions_3. The MTPD of our proposed rating prediction algorithm is calculated based on the properties of each trust network: for Epinions_1, $d_{\max} = \lceil \frac{\ln(45275)}{\ln(461064/45275)} \rceil = \lceil 4.62 \rceil = 5$; for Epinions_2, $d_{\max} = \lceil \frac{\ln(4389)}{\ln(37843/4389)} \rceil = \lceil 3.9 \rceil = 4$, for Epinions_3, $d_{\max} = \lceil \frac{\ln(49288)}{\ln(487183/49288)} \rceil = \lceil 4.72 \rceil = 5$.

The effectiveness of the optimized TARS model is checked on three aspects: the rating prediction accuracy, the coverage and the computational complexity. The rating prediction accuracy of TARS is measured by the error of the predicted ratings. Specifically, we calculate the Mean Absolute Error (MAE). The coverage of TARS is measured by both the rating coverage and the recommender coverage. The rating coverage is the portion of items that TARS is able to predict, i.e., the portion of items that the active user can get at least one recommendation. The recommender coverage is the portion of recommenders that could be involved in TARS.

By predicting the rating on each rated item of Epinions_1, Epinions_2 and Epinions_3, we report the MAE, the rating coverage and the recommender coverage of TARS with respect to different values of MTPD in Tables 6, 7 and 8 respectively, in which the bold ones are the MAE and coverage calculated by using the optimized TARS model. Since the conventional TARS model does not propose any mechanism to set the value of MTPD, its MAE and coverage could be any value in the tables. In addition, the computational complexity of constructing the trust network for TARS is $O(k^{d_{\max}})$, in which k is the average degree of the trust network, and $d_{\max}$ is the value of MTPD. The simulation results clearly show that: though setting the value of MTPD smaller than our suggested value is computational less expensive, the accuracy and the coverage of TARS are worse, especially the recommender coverage; while setting the value of MTPD greater than our suggested value leads to similar accuracy and similar coverage of TARS, but it is computational exponentially more expensive. We therefore draw the conclusion that $\lceil L^R \rceil$ is a suitable value of MTPD for TARS. This verifies the effectiveness of the optimized TARS model, which is based on the small-world properties of the trust network.

Note that $\lceil L^R \rceil$ is only similar to the average trust propagation distance between two randomly selected users of the trust network, but the experiments show that $\lceil L^R \rceil$ is a ap-

Table 6 The MAE of TARS with respect to different values of MTPD, in which the bold ones are those by using our proposed method

	Epinions_1	Epinions_2	Epinions _3
$d_{\max} = 1$	0.2613	0.2155	0.8136
$d_{\max} = 2$	0.2568	0.2155	0.7542
$d_{\max} = 3$	0.2576	0.2142	0.7319
$d_{\max} = 4$	0.2563	**0.2139**	0.7262
$d_{\max} = 5$	**0.2544**	0.2138	**0.7253**
$d_{\max} = 6$	0.2546	0.2138	0.7251
$d_{\max} = 7$	0.2548	0.2138	0.7252
$d_{\max} = 8$	0.2549	0.2138	0.7253
$d_{\max} = 9$	0.2550	0.2138	0.7254

Table 7 The recommender coverage of TARS with respect to different values of MTPD, in which the bold ones are those by using the optimized TARS model

	Epinions_1	Epinions_2	Epinions _3
$d_{\max} = 1$	12.52%	17.92%	4.10%
$d_{\max} = 2$	74.67%	87.70%	30.80%
$d_{\max} = 3$	97.84%	98.68%	75.31%
$d_{\max} = 4$	99.80%	**99.85%**	95.81%
$d_{\max} = 5$	**99.97%**	99.98%	**99.45%**
$d_{\max} = 6$	100.00%	100.00%	99.91%
$d_{\max} = 7$	100.00%	100.00%	99.98%
$d_{\max} = 8$	100.00%	100.00%	100.00%
$d_{\max} = 9$	100.00%	100.00%	100.00%

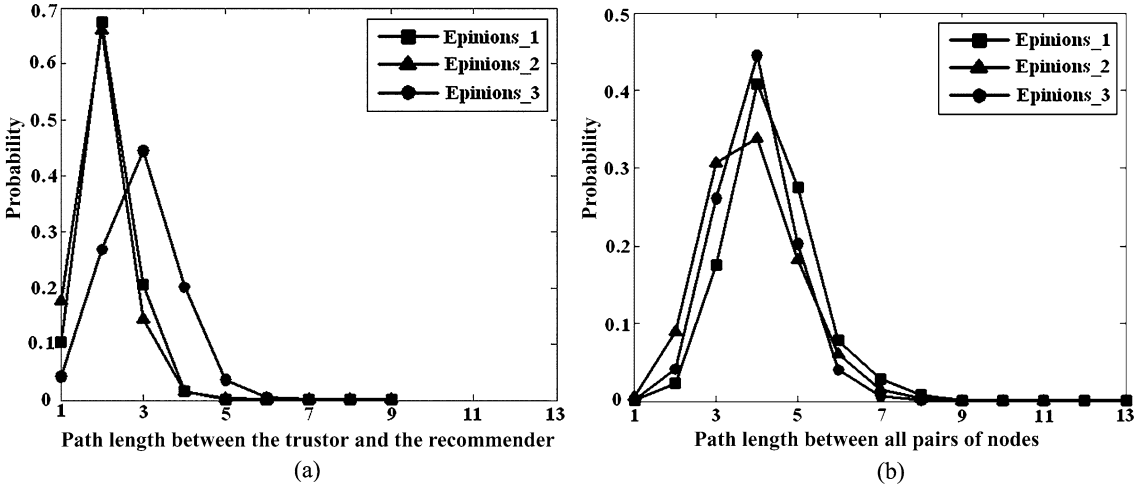


Fig. 10 The distribution of the path length between (**a**) all pairs of nodes of the trust network, and (**b**) the active users and the recommenders

Table 8 The rating coverage of TARS with respect to different values of MTPD, in which the bold ones are those by using the optimized TARS model

	Epinions_1	Epinions_2	Epinions _3
$d_{\max} = 1$	85.41%	91.94%	63.45%
$d_{\max} = 2$	99.29%	99.70%	96.52%
$d_{\max} = 3$	99.94%	100.00%	99.83%
$d_{\max} = 4$	99.98%	**100.00**%	100.00%
$d_{\max} = 5$	**100.00**%	100.00%	**100.00**%
$d_{\max} = 6$	100.00%	100.00%	100.00%
$d_{\max} = 7$	100.00%	100.00%	100.00%
$d_{\max} = 8$	100.00%	100.00%	100.00%
$d_{\max} = 9$	100.00%	100.00%	100.00%

propriate value of MTPD for TARS. This is because it is the average trust propagation distance between all pairs of users that $\lceil L^R \rceil$ is similar to. However, not all users are recommenders. Further analysis on the distribution of the average path length between the active users and the recommenders, which is shown in Fig. 10(b), shows that: compared with the distribution of the average path length between all pairs of users in the trust network, as shown in Fig. 10(a), the average path length between the active users and recommenders are much smaller than that between all pairs of users, and the maximum distance between the active users and the recommenders are always shorter than that between all pairs of users. This indicates that compared with the non-recommenders, the recommenders tend to have shorter distances with the active users. This contributes to the effectiveness of the optimized TARS model by setting $\lceil L^R \rceil$ as the value of MTPD for TARS.

5 Conclusions

Using the experimental data extracted from five public released datasets, this work verified the small-worldness of the trust network. This is achieved by verifying the scale-freeness of the trust network. One basic property of the scale-free network is that its structure and dynamics are independent of its scale. This ensures the continuous scale-freeness of the scale-free network in dynamics. Since the scale-free network is one category of the small-world network, by verifying its scale-freeness, this work shows that the small-worldness of the trust network is independent of its dynamics. Compared with the conventional small-world verification method, our explored verification method greatly decreases the computational efforts: we can verify the small-worldness of the trust network in dynamics with only the static data, while we do not need to reexamine the topology of the trust network when the network changes. In addition, by verifying the scale-freeness of the trust network, we only need to know the direct trust of each node, while we do not need to know how the trust propagates in the trust network. The small-worldness of the trust network indicates that any two nodes of the trust network could be connected within limited number of trust propagations, and the average trust propagation distance is similar to the average path length of this trust network's corresponding random network, which is easy to calculate since it only relates to the size and the average degree of the trust network. We use this property to optimize the conventional trust-aware recommender system: we use the average path length of the trust network to approximately act as the value of the maximum trust propagation distance of TARS. The performances of this optimized TARS model are examined on three large scale real data. The simulations results clearly show that our proposed optimized TARS model can achieve the maximum

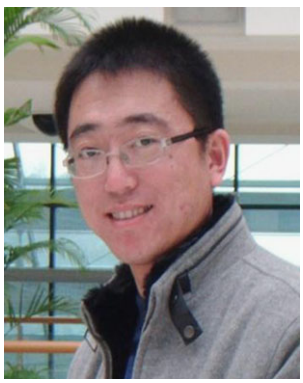
rating prediction accuracy and the maximum rating prediction coverage with the minimum computation complexity.

Acknowledgements The authors would like to thank the anonymous reviewers and the editors of the journal for their valuable comments. This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2010-(C1090-1021-0003)).

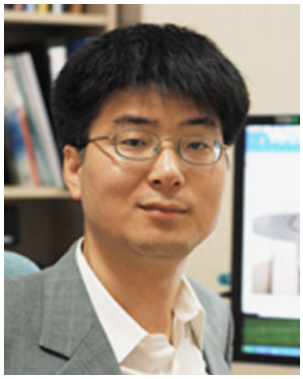
References

1. Artz D, Gil Y (2007) A survey of trust in computer science and the Semantic Web. Web Semant 5:58–71
2. O'Donovan J, Smyth B (2005) Trust in recommender systems. In: Proceedings of the 10th international conference on intelligent user interfaces, San Diego, California, USA, ACM, pp 167–174
3. Massa P, Avesani P (2004) Trust-aware collaborative filtering for recommender systems. In: Proc of federated int conference on the move to meaningful Internet, pp 492–508
4. Coates G, Hopkinson K, Graham S, Kurkowski S (2008) Collaborative, trust-based security mechanisms for a regional utility intranet. IEEE Trans Power Syst 23:831–844
5. Adamic LA (1999) The small world web. In: Proceedings of the third European conference on research and advanced technology for digital libraries. Springer, Berlin, pp 443–452
6. Ebel H, Mielsch L, Bornholdt S (2002) Scale-free topology of e-mail networks. Phys Rev E 66
7. Gray E, Seigneur J, Chen Y, Jensen C (2003) Trust propagation in small worlds. In: Proc of 1st int conf on trust management (iTrust'03), pp 239–254
8. Venkatraman M, Yu B, Singh MP (2000) Trust and reputation management in a small-world network. In: Proceedings of fourth international conference on MultiAgent systems, pp 449—450
9. Guo X, Li X, Qin Y, Chen C (2008) Modeling small-world trust networks. In: International symposium on ubiquitous multimedia computing, 2008, UMC '08, pp 154–159
10. Newman M, Barabasi A, Watts DJ (2006) The structure and dynamics of networks, 1st edn. Princeton University Press, Princeton
11. Watts DJ (1999) Small worlds: the dynamics of networks between order and randomness. Princeton University Press, Princeton
12. Markosova M, Nather P (2006) Language as a small world network. In: Sixth international conference on hybrid intelligent systems, 2006, HIS '06, p 37
13. Achard S, Salvador R, Whitcher B, Suckling J, Bullmore E, Resilient A (2006) Low-frequency, small-world human brain functional network with highly connected association cortical hubs. J Neurosci 26:63–72
14. Bassett DS, Bullmore E (2006) Small-world brain networks. Neuroscientist 12:512–523
15. Watts D, Strogatz S (1998) Collective dynamics of 'small-world' networks. Nature 393:440–442
16. Amaral LAN, Scala A, Barthélémy M, Stanley HE (2000) Classes of small-world networks. Proc Nat Acad Sci USA 97:11149–11152
17. Newman MEJ (2000) Models of the small world: a review. arXiv:cond-mat/0001118
18. Wang XF, Chen G (2003) Complex networks: small-world, scale-free, and beyond. IEEE Circuits Syst Mag 3(1):6–20
19. Barabasi A, Ravasz E, Vicsek T (2001) Deterministic scale-free networks. arXiv:cond-mat/0107419
20. Massa P, Souren K (2008) Trustlet, open research on trust metrics. In: Proceedings of the 2nd workshop on social aspects of the Web (SAW 2008), pp 31–43
21. Bedi P, Kaur H, Marwaha S (2007) Trust based recommender system for semantic web. In: Proceedings of the 2007 international joint conferences on artificial intelligence, Hyderabad, India, pp 2677–2682
22. Andersen R, Borgs C, Chayes J, Feige U, Flaxman A, Kalai A, Mirrokni V, Tennenholtz M (2008) Trust-based recommendation systems: an axiomatic approach. In: Proceedings of WWW-08, pp 199–208
23. Pitsilis G, Marshall L (2006) A trust-enabled P2P recommender system. In: Proceedings of 15th IEEE international workshops on enabling technologies: infrastructure for collaborative enterprises, pp 59–64
24. Massa P, Avesani P (2005) Controversial users demand local trust metrics: an experimental study on Epinions.com community, AAAI, pp 121–126
25. Massa P, Avesani P (2009) Trust metrics in recommender systems. In: Computing with social trust, pp 259–285
26. Massa P, Avesani P (2007) Trust-aware recommender systems. In: Proceedings of the 2007 ACM conference on recommender systems, Minneapolis, MN, USA, ACM, pp 17–24
27. Hanneman RA, Riddle M (2005) Introduction to social network methods, Riverside, CA: University of California, Riverside. http://faculty.ucr.edu/~hanneman/

Weiwei Yuan received B.S. and M.S. in Automation and Computer Engineering in 2002 and 2005 respectively from Harbin Engineering University, China. Currently she is a Ph.D. candidate in the Department of Computer Engineering, Kyung Hee University, South Korea. Her research interests are trust models, reputation systems, information security and machine learning.



Donghai Guan received his B.S. in College of Automation from Harbin Engineering University (HEU), Harbin, China in 2002. He got his M.S. degree in Computer Science from Kumoh National Institute of Technology (KIT), Gumi, South Korea in 2004. He got his Ph.D. degree in Computer Science from Kyung Hee University, South Korea in 2009. From 2009, he was a Post Doctoral Fellow at Computer Science Department, Kyung Hee University. His research interests are Machine Learning, Pattern Recognition, Data Mining, Activity Recognition, and Trust modeling.



Young-Koo Lee received his B.S., M.S., and Ph.D. in Computer Science from Korea Advanced Institute of Science and Technology (KAIST), Korea in 1988, 1994 and 2002, respectively. Since 2004, he has been an assistant professor at the Dept. of Computer Engineering, College of Electronics and Information, Kyung Hee University, Korea. From 2002 to 2004, he was a Post Doctoral Fellow Advanced Information Technology Research Center (AITrc), KAIST, Korea, and a Postdoctoral Research Associate at Dept. of Computer Science, University of Illinois at Urbana-Champaign, USA. His research interests are Ubiquitous Data Management, Data Mining, Activity Recognition, Bioinformatics, On-line Analytical Processing, Data Warehousing, Database Systems, Spatial Databases, and Access Methods.

Sungyoung Lee received his B.S. from Korea University, Seoul, South Korea. He got his M.S. and Ph.D. degrees in Computer Science from Illinois Institute of Technology (IIT), Chicago, Illinois, USA in 1987 and 1991 respectively. He has been a professor in the Department of Computer Engineering, Kyung Hee University, South Korea since 1993. He is a founding director of the Ubiquitous Computing Laboratory, and has been affiliated with a director of Neo Medical ubiquitous-Life Care Information Technology Research Center, Kyung Hee University since 2006. Before joining Kyung Hee University, he was an assistant professor in the Department of Computer Science, Governors State University, Illinois, USA from 1992 to 1993. His current research focuses on Ubiquitous Computing and applications, Context-aware Middleware, Sensor Operating Systems, Real-Time Systems, and Embedded Systems. He is a member of the ACM and IEEE.