MobiFuzzyTrust: An Efficient Fuzzy Trust Inference Mechanism in Mobile Social Networks

Fei Hao[1,2], Geyong Min[1], *Member, IEEE,* Man Lin[3] *Member, IEEE,* Changqing Luo[2], Laurence T. Yang[2,3] *Member, IEEE*

***Abstract*—Mobile Social Networks (MSNs) facilitate connections between mobile users and allow them to find other potential users who have similar interests through mobile devices, communicate with them and benefit from their information. As MSNs are distributed public virtual social spaces, the available information may not be trustworthy to all. Therefore, mobile users are often at risk since they may not have any prior knowledge about others who are socially connected. To address this problem, trust inference plays a critical role for establishing social links between mobile users in MSNs. Taking into account the non-semantical representation of trust between users of the existing trust models in social networks, this paper proposes a new fuzzy inference mechanism, namely *MobiFuzzyTrust*, for inferring trust semantically from one mobile user to another that may not be directly connected in the trust graph of MSNs. Firstly, a mobile context including an intersection of prestige of users, location, time and social context is constructed. Secondly, a mobile context aware trust model is devised to evaluate the trust value between two mobile users efficiently. Finally, the fuzzy linguistic technique is utilized to express the trust between two mobile users and enhance the human's understanding of trust. Real-world mobile dataset is adopted to evaluate the performance of the *MobiFuzzyTrust* inference mechanism. The experimental results demonstrate that *MobiFuzzyTrust* can efficiently infer trust with a high precision.**

***Index Terms*—Mobile Social Networks, Trust, Fuzzy Inference, Mobile Context, Linguistic Terms.**

I. Introduction

The increasing usage and popularity of mobile devices, such as smartphones, laptops and PDAs, have led to the rise of Mobile Social Networks (MSNs). MSNs are a type of newly-emerging large-scale distributed systems that integrate online social computing services and mobile devices and allow mobile social users to discover and interact with friends and further enjoy some distributed network service, such as friends recommendation and dynamic content dissemination, even in the absence of network infrastructure or end-to-end connectivity [1], [2]. However, there exists a certain risk when mobile users try to interact with others anytime and anywhere. For example, using mobile phone when you are waiting for flight at airport you may find that your friend's friend is in the next aisle and then you can talk with him/her face to face. Or when you are searching a restaurant in your visiting country, by virtue of mobile phones you may find some nearby restaurants recommended by someone who has the similar tastes. To take a proper action in these two cases, you need a trust value for establishing a social link with your new friend or a restaurant found through MSNs. Development of trust-based collaborations is the solution to reduce vulnerability to risk and to fully exploit the potential of spontaneous social networking [3], [4].

There have been a number of related studies on trust computation and inference in social networks to reduce the risk of social interactions. For example, Golbeck and Hendler [8] proposed an algorithm, namely TidalTrust, for inferring the trust relationships between people in social networks. A recursive search method was adopted in TidalTrust to compute the trust based on the social paths connecting people in the social network, and then obtain the trust rating on those paths. In [9], Golbeck further studied the features of profile similarity and investigated how the profile similarity is related to the way in which users determine trust. They have shown that there is a correlation between the profile similarity of users and their trust. Lesani and Bagheri [17] proposed a fuzzy trust inference mechanism using fuzzy linguistic terms to specify the trust to other users and presented an algorithm for inferring the trust from one user to another that may not be directly connected in the trust graph of a social network. It is a desirable way for users to obtain and understand the trust values with the fuzzy linguistic expressions. However, this method just works for traditional social networks only, but not for the emerging MSNs. Bhuiyan, Xu and Josang [13] proposed a trust and reputation aware decision mechanism in location-based social networks, but it did not provide the calculation approach of reputation. Seyedi, Sasdi and Issarny [10] proposed a proximity-based trust inference approach using the behavioral data of users from their mobile devices or other types of social interactions. Unfortunately, their approach cannot cope with fuzzy trust inference using linguistic terms.

This paper aims at developing a fuzzy trust inference mechanism based on fuzzy linguistic terms for MSNs. Due to the ambiguity and imprecision of the trust concept, it is better to represent the trust by linguistic expression for enhancing the understanding of users' interaction in MSNs. The main challenges faced in MSNs include:

- How to calculate the trust values from one mobile user to other direct or indirect users in MSNs?
- How to represent the trust using linguistic terms?
- How to predict the trust relationships between an existing MSN user and an unknown mobile user?

[1]Department of Computing, University of Bradford, Bradford, UK
[2]School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China
[3] Department of Computer Science, St. Francis Xavier University, Antigonish, Canada

The trust inference mechanism proposed in this paper is distinguishing from the existing models because it integrates the mobile context of users and returns the trust values as the parameters of the fuzzy membership functions of trust linguistic terms. The linguistic expressions (*for example: high trust, medium trust, low trust*) are then produced to reveal the trust relationship between mobile users. The main contributions of this paper are summarized as follows:

- **Mobile Context**: By analyzing the critical properties of MSNs, a mobile context, including an intersection of prestige of users, location, time and social context is constructed. The proposed mobile context is robust with the considerations of MSNs' features. Therefore, it paves the way for establishing the mobile context aware trust model.
- **Mobile Context Aware Trust Model**: A mobile context aware trust model is devised to evaluate the trust value between two mobile users efficiently. The proposed trust model aggregates the prestige-based trust value, the social context aware trust value, the spatio-temporal factors related trust values and the risk of trust between mobile users in MSNs to generate an overall trust value between them. It interprets the evaluation of trust between users reasonably in MSNs.
- **MobiFuzzyTrust**: A new trust inference mechanism, namely *MobiFuzzyTrust*, is proposed to enhance the human's understanding of the trust. Because the fuzzy linguistic technique is much more desirable for the user to obtain and understand the trust values, we also propose the algorithm for trust transitivity inference and evaluate the precision of the proposed algorithm.
- **Evaluation based on real-world mobile dataset**: We conduct the extensive experiments on real-world mobile dataset. The experimental results demonstrate that *MobiFuzzyTrust* infers trust well both theoretically and practically with a high precision.

The remainder of this paper is structured as follows. Section II presents the preliminaries and problem statement. The proposed fuzzy trust inference mechanism is described in Section III. The experimental evaluation and performance results are presented in Section IV. Finally, Section V concludes this paper.

II. Preliminaries and Problem Statement

This section presents the concepts of fuzzy relationship and fuzzy graph, then introduces the fuzzy graphs representing the trust networks. Finally, we present a methodology, Computing with Words, which can bridge a gap between the linguistic descriptions and formalization of social networks [5], [6].

A. Fuzzy Graphs

The concept of a fuzzy relationship plays a fundamental role in modeling a type of weighted graphs called fuzzy graphs [7], [14].

Definition 1: (**Fuzzy Relationship**) Let X be a set of elements. A fuzzy relationship on X is a mapping

$$R : X \times X \rightarrow [0, 1] \tag{1}$$

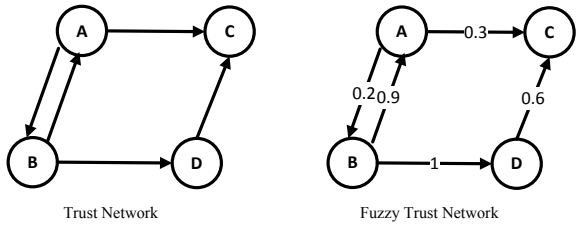


Fig. 1. Structures of Trust Network and Fuzzy Trust Network

where $R(x, y)$ indicates the degree of trust relationship between x and y.

Fuzzy relationships satisfy the following properties [5]:

1) **Reflexivity**: $\forall x, R(x, x) = 1$.
2) **Symmetry**: $R(x, y) = R(y, x)$.
3) **Transitivity**: $R(x, z) \supseteq Max_y[R(x, y) \wedge R(y, z)]$.

Definition 2: (**Fuzzy Graph**) A fuzzy graph $\widetilde{G}$ is represented by a set of vertices and a fuzzy set of edges between vertices.

$$\widetilde{G} = (V, \widetilde{E}, R) \tag{2}$$

where V is the set of vertices, $\widetilde{E}$ is the fuzzy set of edges between vertices, and R is a reflexive fuzzy relationship on V.

In particular, if R is symmetric, $\widetilde{G}$ is called as an undirected fuzzy graph. Otherwise, $\widetilde{G}$ is a directed fuzzy graph. In a fuzzy graph, $R(x, y)$ is the weight associated with the edge $x \rightarrow y$. In other words, there exists $R(x, y) = R(y, x)$ in the undirected fuzzy graph, but $R(x, y)$ may not be equal to $R(y, x)$ in the directed fuzzy graph. The fuzzy graph is an expression of fuzzy relation and thus is frequently expressed as fuzzy matrix.

B. Trust Network and Fuzzy Trust Network

A trust network is modeled as a directed graph $G = (V, E)$, with V indicating the users in the network and E indicating the trust relationships between users. A fuzzy trust network is defined as a fuzzy graph $\widetilde{G} = (V, \widetilde{E}, R)$, where V is a non-empty set of the users and R is an asymmetric fuzzy relation on trust between users.

Figure 1 illustrates the basic structure of the trust network and fuzzy trust network. Obviously, the general trust network considers the links between its users as binary (1 if present, or 0 if not). However, the various degrees of relationships are considered in the fuzzy trust network.

The trust and trust network have four obvious properties: 1) Asymmetry; 2) Transitivity; 3) Composability: people naturally compose the trust value when they receive them from different sources by giving higher importance to more trusted sources [17]; 4) Decay: the trust decays as the number of transitivity hops increases along a social trust path [18], [19].

C. Computing with Words

Computing with Words (CWW) is a methodology for reasoning, computing and decision-making with information described in natural language [15], [16]. Central to CWW is a translation process that involves taking the linguistically

expressed information and translating it into a machine manipulative format (*i.e.*, fuzzy sets on domain).

In fuzzy trust networks, CWW provides a way to bridge the gap in man-machine communication with respect to the analysis of social networks. By allowing the human to build a vocabulary of linguistic terms associated with an attribute, CWW provides a representation for these terms by fuzzy sets, $e.g.$, the degree of trust between two people. The linguistic term is an attribute whose domain is defined in an interval $I = [0, 1]$. For example, the linguistic terms *strong*, *weak*, and *none* would be part of a vocabulary associated with the attribute. In particular, the term *strong* as a fuzzy subset $\widetilde{f}_{str}$ of $[0, 1]$ such that, for any $x \in [0, 1]$, the value $\widetilde{f}_{str}(y)$ would indicate the degree to which x satisfies the working definition of the concept *strong*.

D. Problem Statement

Definition 3: (**Trust Semantics**) Consider a trust network $G = (V, E)$, trust semantics is a triple $(e_{ij}, l_{ij}, \mu_{l_{ij}})$, where $e_{ij} \in E$ indicates the directed trust relationship from user u_i to u_j, $l_{ij} \in L$ is a label represented with linguistic-based trust terms associated with e_{ij} and L is the set of linguistic terms of trust, $\mu_{l_{ij}}$ is the degree of membership of l_{ij} which is used for trust degree evaluation between user u_i and user u_j.

To infer the trust semantics in an MSN, different factors should be considered to evaluate the degree of trust between two users, such as prestige of users, social context, location and time that are referred to as mobile context. The mobile context will be discussed in Section III.A.

Fuzzy Trust Inference in MSNs: In an MSN, there exists trust relationship between two interactive mobile users. It can be formalized as a trust network $G = (V, E)$. The target of the addressed problem is to return the expected linguistic term of trust $\widehat{l_{ij}}$ according to the principle of maximum degree of membership.

$$\widehat{l_{ij}} := \arg \max_{l_{ij} \in L} \mu_{l_{ij}} \tag{3}$$

where L is the set of linguistic terms of trust.

The above formulation of trust inference focuses on mining trust semantics using fuzzy logic.

III. MobiFuzzyTrust: Fuzzy Trust Inference in MSNs

This section presents the construction of mobile context, establishment of the mobile context aware trust model and the proposed fuzzy trust inference model, namely, *MobiFuzzyTrust*. First of all, the related impact factors of trust computation are analyzed and the mobile context of each pair of users is constructed. Furthermore, we figure out a key element of a general trust computation model including the basic trust computation, similarity-based trust computation, familiarity-based trust computation, and loss caused by the risk of trust. To this end, the impact factors corresponding to various computational modules in a general trust model are then investigated.

As shown in Figure 2, the framework of *MobiFuzzyTrust* contains three main parts: 1) mobile context; 2) trust computation; 3) fuzzy trust inference. Firstly, the mobile context based on the collected MSN data is extracted. Then, the trust computation model using mobile context, namely mobile context aware trust model is established. Finally, these numerical trust values with the linguistic terms by corresponding fuzzy membership functions are represented.

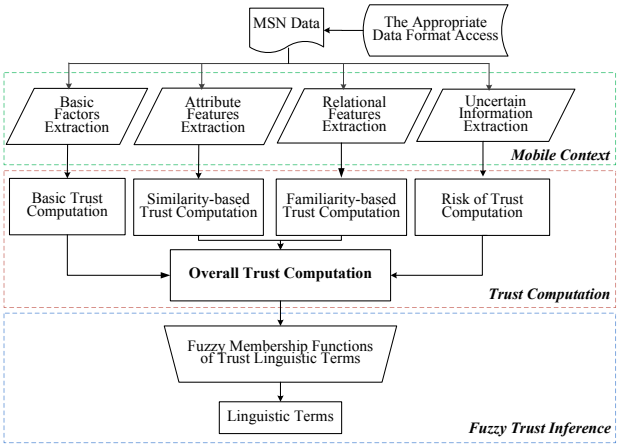


Fig. 2. The Framework of MobiFuzzyTrust

A. Mobile Context

The mobile context is the intersection among spatio-temporal features such as location, time, prestige and the social context that reflects the familiarity between two mobile users, as shown in Figure 3. Obviously, as the social context updates, the prestige of the users is changing dynamically. Hence, there exists an influence flow from the social context module to prestige module.

To derive a mobile context aware trust model, the trust computation generated from the following four impact factors of the mobile context is studied in detail and presented below.

1) The prestige-based basic trust value can be calculated according to user's reputation in MSNs.
2) The familiarity-based trust value can be calculated according to their social context, *i.e.*, social interactions among users.
3) The similarity-based trust value is calculated from two aspects: location similarity and time similarity between mobile users.
4) The risk of trust is incorporated into the proposed mobile context by considering that a certain risk exists when one trusts another in MSNs.

1) Prestige-based Basic Trust Value: We evaluate the prestige of mobile users as a basic trust value. There exist some measurement approaches for calculating the prestige of mobile users, such as degree-based prestige computational approach [20], proximity-based prestige computational approach [22], and rank prestige computational approach [21]. In particular, the degree-based prestige computational approach, an efficient and quick basic trust evaluation way has been widely used. Therefore, we adopted the degree-based prestige evaluation method to obtain the basic trust value of each mobile user in MSNs.

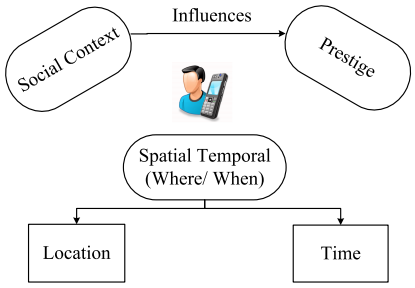


Fig. 3. Mobile Context

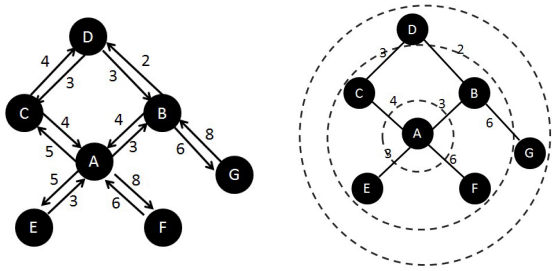
Definition 4: The basic trust value of user u, $BT(u)$ is given by

$$BT(u) = \frac{N(u)}{m-1} \tag{4}$$

where $N(u)$ is the number of neighboring users of u, m is the total number of users in an MSN. Eq. (4) reveals the fact that the more neighboring users of u, the higher $BT(u)$.

2) Familiarity-based Trust Value: The familiarity between two mobile users are usually generated through their social interactions. For example, if mobile users A and B communicate frequently, then they are considered to have a higher familiarity [23]. To address this problem, we develop an efficient approach for evaluation of the familiarity-based trust value between mobile users.

Consider a communication interaction graph of an MSN as a directed graph $G^{(m)} = (V, E, W)$, where V denotes the set of nodes (users), E denotes the edges (interactions between users), W refers to the weights of edges, *i.e.*, the number of interactions. Figure 4(a) shows the structure of the communication interaction graph of an MSN.



(a) CIG of an MSN (b) TUIG of A

Fig. 4. Communication Interaction Graph (CIG) of an MSN and Target User Interaction Graph (TUIG) of A

Let us consider users A and C. User A called C or sent message to C for 5 times. However, user C called A or sent message to A for 4 times. An intuition is "*the more interactions between them, the more familiar they are*". We consider the minimal value of interaction between the target user A with other users as the familiarity. Hence, we transform the communication interaction graph $G^{(m)}$ into the target user interaction graph $G^{(m)}(A) = (V, \widetilde{E}, \widetilde{W})$ as shown in Figure 4(b). Obviously, Figure 4(b) is a simplified undirected graph in which all edges preserve the edges with smaller weights on the basis of directed graph as depicted in Figure 4(a). For example, the weight between users A and C, *i.e.*, $\widetilde{W}(A,C)$=$min(W(A,C), W(C,A)) = W(C,A) = 4$.

$FT(A,v)$	trust value
B	0.5
C	0.667
D	0.5
E	0.5
F	1
G	0.5

TABLE I
A CALCULATION EXAMPLE FOR FAMILIARITY-BASED TRUST COMPUTATION

Definition 5: **Familiarity-based Trust Computation** Suppose two users u and v in an MSN and a communication interaction graph $G^{(m)}(u) = (V, \widetilde{E}, \widetilde{W})$ of u, the familiarity-based trust value from v to u , $FT(u,v)$, can be defined as follows:

$$FT(u,v) = \begin{cases} \frac{w(u,v)}{max(FT(u,\widetilde{v}))} & (u,v) \in \widetilde{E} \\ \frac{max(min(w(u^{'},v^{'})))}{max(FT(u,\widetilde{v}))} & (u,v) \notin \widetilde{E}. \end{cases} \tag{5}$$

where $\widetilde{v} \in N(u)$, $w(u,v) \in \widetilde{W}$, $(u^{'}, v^{'}) \in path(u,v)$.

Example 1: Let us take Figure 4(b) as an example. The $FT(A,v), v \in \{B,C,D,E,F,G\}$ is calculated as shown in Table I. This table shows that $FT(A,F)$ has the highest trust value and $FT(A,B), FT(A,D), FT(A,E), FT(A,G)$ have the same trust value.

3) Similarity-based Trust Value: The similarity between mobile users in MSNs contains two aspects, *i.e.*, *External Similarity* and *Internal Similarity*. The calculation of external similarity depends on the location and time of users. The calculation of internal similarity depends on the interests of users, such as the profile and taste of users. Hence, a trust computational model based on similarity is defined as follows with the considerations of *External Similarity* and *Internal Similarity* under a tunable parameter λ. Intuitively, the parameter λ is associated with the MSNs application. If the most social interactions occur in a relative multi-scale space, we can set a bigger λ, otherwise, a small λ should be assigned.

$$ST(u,v) = \lambda ST_e(u,v) + (1-\lambda) ST_i(u,v) \tag{6}$$

where $ST(u,v)$ denotes the similarity-based trust value from v to u, λ is a tunable parameter, $ST_e(u,v)$ and $ST_i(u,v)$ refer to the external similarity-based trust value and internal similarity-based trust value, respectively. In what follows, we will present how to calculate $ST_e(u,v)$ and $ST_i(u,v)$.

- ***External Similarity aware Trust Computation*** $ST_e(u,v)$

First, $ST_e(u,v)$ depends on the location and time factors. Because there is no further consideration of the weights for location and time factors, we assign the same weight to each of them. So, the computational model of the external similarity-based trust value is expressed as follows,

$$ST_e(u,v) = ST_e^l(u,v) + ST_e^t(u,v) \tag{7}$$

where $ST_e^l(u,v)$ indicates the trust value from v to u caused by location similarity, and $ST_e^t(u,v)$ indicates the trust value

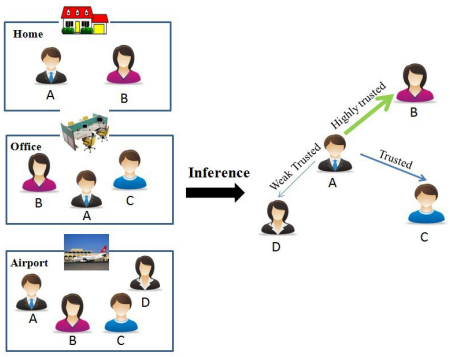


Fig. 5. Observations for location similarity aware trust inference

from v to u caused by time similarity. To obtain $ST_e^l(u,v)$, location similarity aware trust computation is defined as follows,

Definition 6: **Location Similarity aware Trust Computation** $ST_e^l(u,v)$

Suppose two users u and v in an MSN have several expected locations (e.g., home, office, apartment, restaurant, and school). The location similarity aware trust value from v to u can be defined as follows:

$$\mathrm{ST}_e^l(u,v) = \begin{cases} 1 & l(u) = l(v) = \text{“}Home\text{”} \\ 0.9 & l(u) = l(v) = \text{“}Apartment\text{”} \\ 0.8 & l(u) = l(v) = \text{“}Office\text{”} \\ 0.7 & l(u) = l(v) = \text{“}Movie\ theater\text{”} \\ 0.6 & l(u) = l(v) = others \\ 0 & l(u) \neq l(v). \end{cases} \quad (8)$$

Figure 5 shows the important observations for location similarity aware trust inference. The $ST_e^l(u,v)$ is experimentally set according to mobile context. For example, mobile users A and B have the social activities at home, office, and airport. In particular, “*home*” is a very close and trusted place unlike other public places, such as “*office*”, and “*airport*”. Therefore, the weight of “*home*” is set to be “1” and a bigger trust value between A and B is assigned. Figure 5 also shows that users A and C have the social activities in both office and airport that are with the lower weights compared to that of “*home*”. A and C probably have the relationship of colleagues. Compared to the trust value from A to B, the trust value from A to C is smaller. Besides, mobile user D appears in airport and D is waiting for her flight for a business trip. A may or may not know D in this special case. So, there exists a weak trust value from A to D. For the sake of semantically understanding of trust value between mobile users, we assign the fuzzy linguistic terms “*highly trusted*”, “*trusted*”, and “*weak trusted*” to represent the degree of trust between mobile users.

Actually, except the location factor, the time factor also plays an important role for calculation of external similarity between mobile users. The time similarity aware trust computational approach will be presented as follows.

Definition 7: **Time Similarity aware Trust Computation** Suppose two users u and v in an MSN communicate at any time slots by their mobile phones. For simplicity, we divide a clock cycle into three time slots, *i.e.*, day time ($8:00AM \sim 6:00PM$) (C_1), night time ($6:00PM \sim 00:00AM$) (C_2), and sleeping time ($00:00AM \sim 8:00AM$) (C_3). The time similarity aware trust computation model can be represented as follows,

$$ST_e^t(u,v) = C_i \frac{t_e - t_s}{argMax(t_e^u - t_s^u)} \quad (9)$$

where t_e and t_s denote the end time and start time of mobile communication, and C_i indicates the i^{th} time slot. Intuitively, we assign the different weights to different time slots. Actually, the weights $w(C_i)$ are the system parameters decided by users. In other words, different users have different cognitive preference for social interactions during different time slots. In this paper, the weight parameters for night time, day time, and sleeping time are set to be 0.8,0.6,0.4, respectively, because the slot of night time is more trustworthy and has the highest weight while sleeping time takes a certain risk of trust and has the smallest weight.

Therefore, there are some interesting conclusions based on sociological observations and behavioral science of users: the more during of communication in the time slot with a higher weight, the greater trust value between them.

- ***Internal Similarity aware Trust Computation*** $ST_i(u,v)$

Definition 8: **Internal Similarity aware Trust Computation** Internal similarity usually refers to the users' interest similarity such as the behavior similarity and profile similarity of users. In this paper, we evaluate the taste similarity of users according to the model of their mobile phones. For example, if *Peter* and *Jessie* use the same mobile phone “*Nokia 6600*”, it reflects they have similar taste in some extents.

For two users u and v who communicate through their mobile phones in an MSN, the internal similarity aware trust computation model can be represented as follows,

$$ST_i(u,v) = sim(mp_u, mp_v) \quad (10)$$

where mp_u and mp_v denote the strings of name of the mobile phones. $sim(x,y)$ indicates the similarity between strings x and y. Intuitively, if two mobile users have the same phone model phones, they may have the higher similarity and the trust between them in terms of taste should be higher than others.

To guarantee the completeness of the overall trust model based on the aforementioned methods for trust calculation according to the prestige of user, familiarity between users, location, time as well as similarity of user's taste, the risk of trust is introduced and studied in following subsection.

4) Risk of Trust: The risk of trust indicates the fact that there exists a risk value when user B tries to trust another user A. Risk means the loss of certainty due to the negative deviation between the results caused by uncertainty and the intended target. As mentioned before, the trust has the decay property, which causes the risk. In other words, as the transitive hops increase, the risk increases but trust value decreases. Therefore, the risk of trust is a dual problem. It follows the

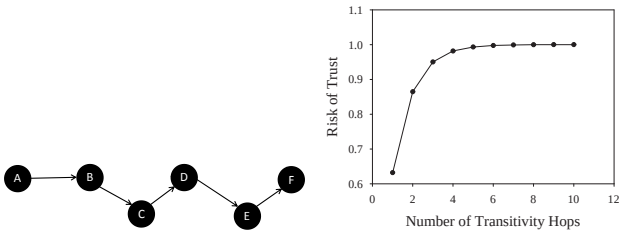
increment "*S*" shape curve. As a generalized logistic curve can efficiently model the "S-shaped" behavior (abbreviated S-curve) of its growth, the risk of trust considered in this paper follows the logistic curve [1].

Definition 9: **(Risk of trust)** The risk of trust from user v to user u, $RT(u,v)$, in an MSN is defined as follows:

$$RT(u,v) = r_{max} - \frac{1}{\varepsilon * e^{d(u,v)}} \tag{11}$$

where r_{max} is the upper bound of risk and is called as the risk parameter. ε is a constant environment parameter dependent on the studied case; ε is set to be 5 in this study. $d(u,v)$ is the number of transitivity hops between u and v.

Example 2: Suppose there are six mobile users A, B, C, D, E, F in an MSN. There exists a trust transitivity path from A to F, as shown in Figure 6(a).



(a) A calculation example of risk of trust

(b) The correlation between the number of transitivity hops and risk of trust

Fig. 6. Risk of Trust Calculation and Its Correlation with Transitivity Hops

We set $r_{max} = 0.1$ in order to have a relative lower risk of trust, *i.e.*, less than 0.1. According to Equation (11), we can obtain the risk of trust from *A* to *F*

$$RT(A,F) = 0.1 - \frac{1}{5 * e^5} = 0.099$$

To study the correlation between the number of transitivity hops and risk of trust, we plot the correlation curve on the range from 0 to 10 as shown in Figure 6(b).

This figure reveals an important conclusion that as the number of transitivity hops increases, the risk of trust increases also, but it will eventually approach to "0.1" because the upper bound of $RT(u,v)$ is r_{max}. Clearly, the shape in the figure coincides with the logistic curve of risk of trust.

B. Mobile Context Aware Trust Model

By aggregating mobile context, the proposed mobile context aware trust computational model can be defined as follows:

$$T(A,B) = \alpha BT(A) + \beta FT(A,B) + \gamma ST(A,B) \\ -(1-\alpha-\beta-\gamma)RT(A,B) \tag{12}$$

where $T(A,B)$ denotes the trust value from B to A. $BT(A)$ refers to the basic trust value of A caused by A's prestige. $FT(A,B)$, $ST(A,B)$, and $RT(A,B)$ indicate the familiarity-based trust value, similarity-based trust value, and the risk of trust from B to A, respectively. The parameters α, β, γ are empirically set. However, these parameters can be learnt from the history of social interaction.

[1] http://en.wikipedia.org/wiki/Logisticfunction

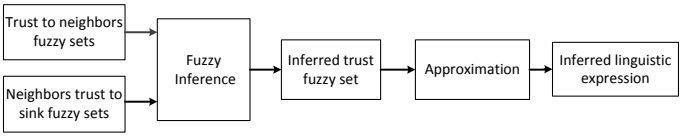


Fig. 7. The Fuzzy Trust Inference

C. Fuzzy Trust Inference

To improve human's understanding of trust represented by numbers, we explore the fuzzy trust inference using fuzzy linguistic terms. In this section, we present the conversion from the numerical trust to linguistic values-expressed trust which is more understandable by users in real world. The entire fuzzy trust inference procedure is illustrated in Figure 7.

Let us use a set of pre-defined linguistic terms given by our *iFriend* system to describe the degree of trust, *i.e.*, $L = \{high(H), mediumhigh(MH), medium(M), mediumlow(ML), low(L)\}$. The inference target is to return the expected linguistic terms for describing the degree of trust instead of the current numerical trust values.

The proposed *MobiFuzzyTrust* supports the linguistic terms as trust rating of a user for another in MSNs. The fuzzy membership functions for the linguistic terms such as *high, medium high, medium, medium low, low* can be defined with the triangular membership function as depicted in Figure 8. Due to the difficulties in design of fuzzy membership functions in fuzzy logic, in particular, as for the fuzzy linguistic area, the triangular membership function is most commonly used to represent the shapes of various linguistic terms so as to reduce the design overhead of fuzzy membership functions [15]. The membership function of linguistic terms of trust (*high, medium high, medium, medium low, low*) can be formalized with the following conditional equations:

$$\mu_L(x) = \begin{cases} 1-4x & x \in (0, 0.25] \\ 0 & x \geq 0.25. \end{cases} \tag{13}$$

$$\mu_{ML}(x) = \begin{cases} 4x & x \in (0, 0.25] \\ 2-4x & x \in (0.25, 0.5] \\ 0 & x \geq 0.5. \end{cases} \tag{14}$$

$$\mu_M(x) = \begin{cases} 0 & x \in (0, 0.25] \\ 4x-1 & x \in (0.25, 0.5] \\ 3-4x & x \in (0.5, 0.75] \\ 0 & x \geq 0.75. \end{cases} \tag{15}$$

$$\mu_{MH}(x) = \begin{cases} 0 & x \in (0, 0.5] \\ 4x-2 & x \in (0.5, 0.75] \\ 4-4x & x \in (0.75, 1]. \end{cases} \tag{16}$$

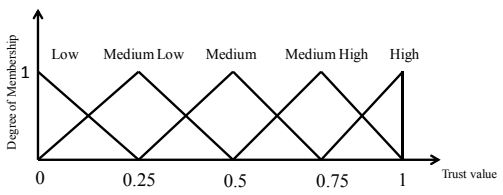


Fig. 8. Fuzzy Membership Functions of Linguistic Terms of Trust

$$\mu_H(x) = \begin{cases} 0 & x \in (0, 0.75] \\ 4x - 3 & x \in (0.75, 1]. \end{cases} \quad (17)$$

The algorithm of fuzzy trust inference for linguistic expressed trust from user v to user u is described as follows:

Algorithm 1 : The Algorithm of MobiFuzzyTrust

Input:

User (u);
Friends list of user u ($v \in F$);
Number of friends of user u (M);
System parameters: $\alpha, \beta, \gamma, \lambda$;

Output:

Expected linguistic terms of trust $\widehat{l_{uv}}$;

1: **for** $i = 1$ **to** M **do**
2: ***begin***
3: $T_i = T(u, v_i)$;
4: Calculate the degree of membership for five linguistic terms
5: $d_1 = \mu_H(T_i)$;
6: $d_2 = \mu_{MH}(T_i)$;
7: $d_3 = \mu_M(T_i)$;
8: $d_4 = \mu_{ML}(T_i)$;
9: $d_5 = \mu_L(T_i)$;
10: $\widehat{l_{uv}} := \arg \max_{l_{uv} \in L} (d_1, d_2, d_3, d_4, d_5)$;
11: ***end***
12: Return the expected linguistic terms of trust in terms of principle of maximum degree of membership;

In this algorithm, the inputs are a given user u, its friend list, and system parameters $\alpha, \beta, \gamma, \lambda$. Line 3 is to calculate the trust value between u and others v_i. Lines 5-9 are to calculate the degrees of membership for five linguistic terms $high, mediumhigh, medium, mediumlow, low$, respectively. Line 10 returns the expected linguistic terms of trust in terms of the principle of maximum degree of membership.

D. Fuzzy Trust Transitivity Inference

Trust transitivity and asymmetry are two major attributes for trust computation [26]. For numerical trust transitivity, multiplication mechanism of trust transitivity computation is widely used. If user A highly trusts user B with value T_{AB} and user B highly trusts user C with value T_{BC}, then A is able to trust user C, to some extent, with T_{AC}. According to multiplication mechanism, $T_{AC} = T_{AB} * T_{BC}$. However, as shown in Figure 9, there exist many reachable paths for trust transitivity from A to C, and thus many trust values accordingly. The trust maximization approach [28] can be used to obtain the final trust value from A to C.

Generally, suppose there exist $|P|$ reachable paths $p \in P$ from u to v, then the trust transitivity computation from u to v is defined as follows

$$T(u, v) = max_{p \in P} T(u, .) \otimes T(., v) \quad (18)$$

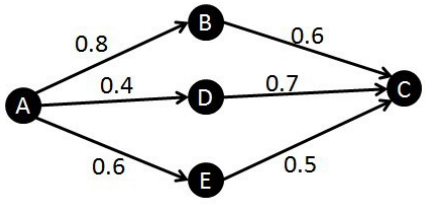


Fig. 9. Many reachable paths for trust transitivity from A to C

In Figure 9, if the operator $\otimes$ is "*multiplication*", then we can easily obtain the trust value from A to C: $T_{AC} = max\{0.8 * 0.6, 0.4 * 0.7, 0.6 * 0.5\} = 0.48$ according to Equation (18).

Here is a natural question: how to infer the linguistic terms expressed trust when it transmits in an MSN. A motivating example for this issue is presented as follows: if A medium highly trusts B, and B lowly trusts C, what is the linguistic term for describing the degree of trust from A to C?

$$condition1 : IfA \xrightarrow{\textbf{\textit{medium high}}} B$$

$$condition2 : IfB \xrightarrow{\textbf{\textit{low}}} C$$

$$Inference : A \xrightarrow{\textbf{\textit{??}}} C$$

In this section, we propose a general inference mechanism for fuzzy trust transitivity in MSNs. We define a transitivity operator "$\otimes$" which is used to calculate the trust value from a user to 2-hops away users. The pseudo code of our inference mechanism of fuzzy trust transitivity is listed in Algorithm. 2.

In this algorithm, the inputs are a given user u, the list of n-hop neighbors v_n, the size of List v_n (*i.e*, M), and system parameters $\alpha, \beta, \gamma, \lambda$. Lines 3-6 are to calculate the transitivity trust value between u and others v_i through $|P|$ reachable paths according to trust maximization principle. Lines 8-12 are to calculate the degrees of membership for five linguistic terms $high, mediumhigh, medium, mediumlow, low$, respectively. Line 13 returns the expected linguistic terms of trust in terms of the principle of maximum degree of membership.

IV. Experimental Evaluation and Performance Results

In this section, extensive experiments based on real mobile social networking dataset are conducted to evaluate the performance of the proposed approach with the goal of validating the effectiveness of the proposed approach for inferring the trust in MSNs.

A. Experiment Setup

In the experiment, we used the *Reality Mining* dataset [2] collected in the *Reality Mining Project* by the MIT Media Lab by using 100 Nokia 6600s with context logging software. They have gathered 330000 hours of continuous behavioral data logged by the mobile phones of one hundred users

[2] http://reality.media.mit.edu/

Algorithm 2 A General Inference Mechanism for fuzzy trust transitivity in MSNs.

Input:
User (u);
List of n-hop neighbors v_n ($v_i \in v_n$);
Size of List v_n (M);
System parameters: $\alpha, \beta, \gamma, \lambda$;
Output:
Expected linguistic terms of trust $\widetilde{l_{uv}}$;

for $i = 1$ **to** M **do**
begin
for *j*=1 **to** $|P|$ **do**
begin
$T_i = max_{p_j \in P} T(u, .) \otimes T(., v_i)$;
end
Calculate the degree of membership for five linguistic terms
$d_1 = \mu_H(T_i)$;
$d_2 = \mu_{MH}(T_i)$;
$d_3 = \mu_M(T_i)$;
$d_4 = \mu_{ML}(T_i)$;
$d_5 = \mu_L(T_i)$;
$\widehat{l_{uv}} := \arg \max_{l_{uv} \in L} (d_1, d_2, d_3, d_4, d_5)$;
end
Return the expected linguistic terms of trust in terms of principle of maximum degree of membership;

(either students or faculty in the MIT Media Laboratory). The collected dataset includes call logs, Mobile/Bluetooth devices in proximity, cell tower IDs, application usage, phone status (such as charging and idle), which comes primarily from the Context application, users' location, and communication and device usage behavior.

We run the experiments with the following steps. First, we calculate the mobile context aware trust values between users. In particular, we set an initial mobile user u who is a student in Boston. In this experiment, we aim to study trust computation in his trust network. Then, we convert the numerical trust values to the linguistic expressed trust by the proposed fuzzy trust inference technique. Finally, we study the linguistic expressed trust transitivity in MSNs.

B. Performance Results and Analysis

We run the experiments on a 2.83 GHz quad core machine with 2G memory. First, the results of prestige-based trust value, familiarity-based trust value, similarity-based trust value, and risk of trust are presented in this section. Further, we discuss the effectiveness and rationality of the proposed trust inference model.

1) Basic Trust Value of Initial User u: According to Equation (4), we can obtain

$$BT(u) = \frac{N(u)}{m-1} = \frac{62}{100-1} = 0.626 \tag{19}$$

2) Familiarity-based Trust Computational Results: To measure the familiarity between two users in an MSN, we utilize

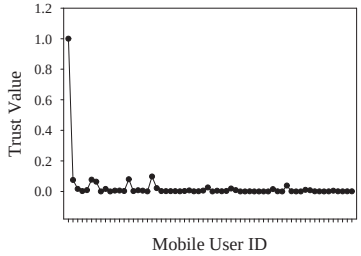
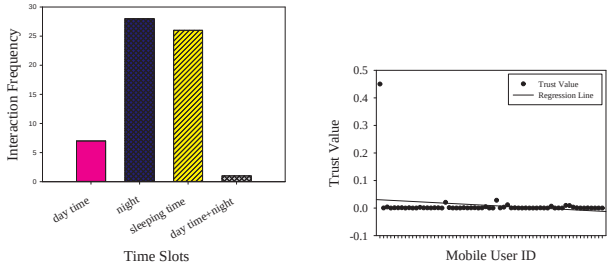


Fig. 10. Familiarity-based Trust Computational Results for $FT(u, v)$

the number of interactions (*i.e.*, the number of calls in this study) between two users to measure the familiarity. The more calls they have, the more familiar they are. Base on this idea, Figure 10 depicts the familiarity-based trust computational results for $FT(u, v)$.

Figure 10 reveals that most of mobile users have almost the same familiarity with the given initial user u. However, several mobile users (the leftmost mobile users) are quite familiar with u with the higher trust values.

3) Time Similarity Aware Trust Computational Results: Figure 11 shows the distribution of interaction by time slots and time similarity aware trust computational results for $ST_e^t(u, v)$. As shown in Figure 11(a), user u often has the most frequent communication with other mobile users on the night. But, they rarely communicate on the day time as well as day time and night together. According to Equation (9), we can calculate the trust values between u and other users v, these results are presented in Figure 11(b). These figures illustrate that most of mobile users have almost the same trust values with the given initial user u in terms of time similarity. This phenomena is caused by either weights of time slots or communication duration.



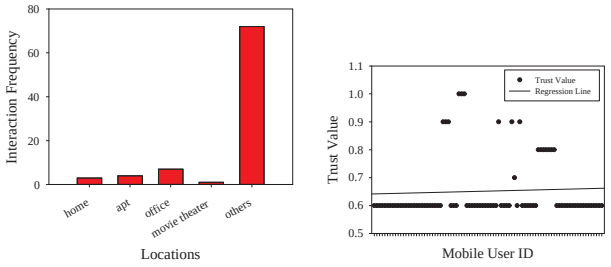
(a) Distribution of Interaction by Time Slots

(b) Time Similarity Aware Trust Computational Results for $ST_e^t(u, v)$

Fig. 11. Distribution of Interaction by Time Slots and Time Similarity Aware Trust Computational Results for $ST_e^t(u, v)$.

4) Location Similarity Aware Trust Computational Results: Figure 12 depicts the distribution of interaction by locations and time similarity aware trust computational results for $ST_l^l(u, v)$. As shown in Figure 12(a), user u often has the most frequent communication with other mobile users in the other places. According to Equation (8), we can easily calculate the trust values between u and other users v, these results are presented in Figure 12(b). Obviously, several scattered points

are distributed at the upper/lower of the regression line as shown in Figure 12(b). The upper scattered points show that these mobile users have the higher trust values with initial user u, and u often has some social interactions with them in the same locations with the higher weights, such as at Home and Apartment. Therefore, the location similarity has much impact on trust computation between u and others in the experiment.



(a) Distribution of Interaction by Locations (b) Location Similarity Aware Trust Computational Results for $ST_e^l(u,v)$

Fig. 12. Distribution of Interaction by Locations and Location Similarity Aware Trust Computational Results for $ST_e^l(u,v)$.

5) Results of Risk of Trust: In MSNs, it is difficult to obtain the information of hops count from a mobile user to another user. For example, a stranger called you at the later night, how to know the hop count information based on interaction in an MSN. In this paper, we simulate the hop information between a given user and another with a random approach. According to small world theory [27], *i.e.*, you can have the connections and recognize with any other strangers within six hop counts. Hence, we should calculate the risk of trust between two users within six hop counts. Actually, as the number of hop counts increases, the risk of trust first increases then reaches a stable value as shown in Figure 6(b). We set the maximum hop count as 6, then we randomly choose a number from 1 to 6 as the hop count between initial mobile user to another. Figure 13 presents the risk of trust between initial mobile user and other users. It shows that as the hop count increases, the risk of trust increases.

6) Mobile Context Aware Trust Computational Results: In this subsection, we aggregate all of the impact factors and calculate the trust value between the initial mobile user and others by using our proposed computational model as presented in Eq.(12).

We calculate the trust values by several combinations of parameters $p = \{\alpha, \beta, \gamma, \lambda\}$. Without loss of generality, we set $p_1 = \{0.7, 0.1, 0.1, 0.8\}$, $p_2 = \{0.1, 0.7, 0.1, 0.2\}$, $p_3 = \{0.1, 0.1, 0.7, 0.5\}$, $p_4 = \{0.3, 0.3, 0.3, 0.6\}$ for performance evaluation.

Figure 14 shows the trust values and distribution of linguistic terms for trust under various combinations of parameters. In particularly, in Figure 14(b) with the parameter set p_1, most of users *medium trust* initial mobile user. Hence, the linguistic term *medium* dominates the other terms. Furthermore, Figure 14(a) shows clearly more relative higher trust values subject to the parameter set p_1 .

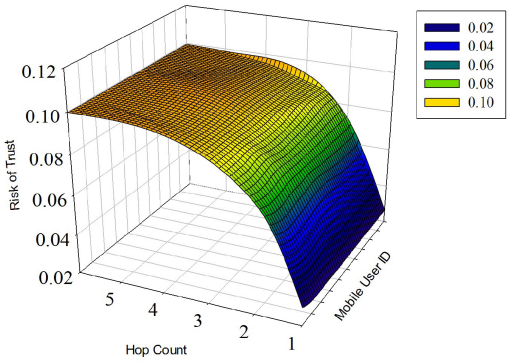
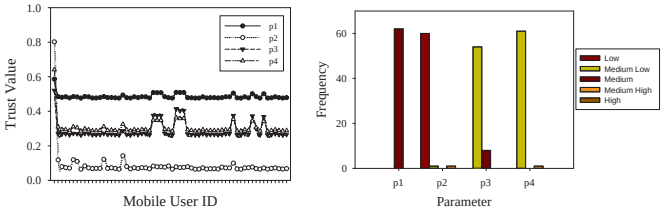


Fig. 13. Risk of Trust $RT(u,v)$



(a) Mobile Context Aware Trust Values for p_1, p_2, p_3, p_4 (b) Distribution of Linguistic Terms for Trust

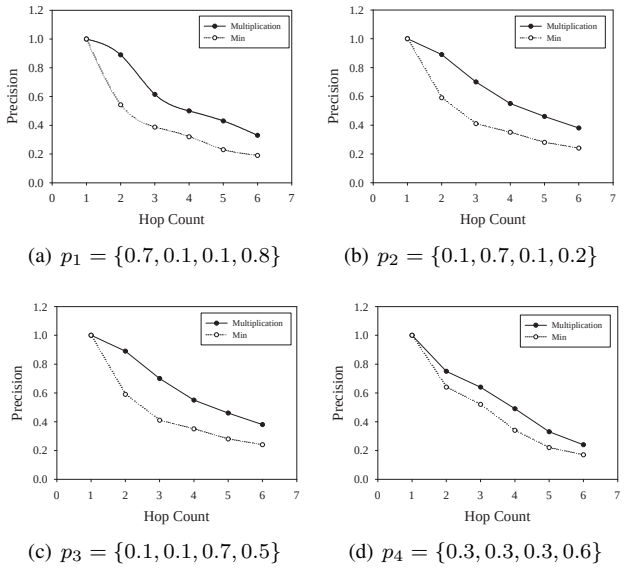
Fig. 14. Experimental Results.

7) Trust Transitivity Inference Results: To evaluate the effectiveness of trust transitivity inference using Algorithm 2, we set the results obtained from the proposed mobile context aware trust model as the ground of truth, and adopt the operation " $\otimes$ " as the *Multiplication* between two trust values. The inference precision $\eta(l)$ is utilized to evaluate the effectiveness of our inference mechanism when the hop count is l.

$$\eta(l) = \frac{|\{v|\widetilde{l_{uv}} = \widehat{l_{uv}}\}|}{|\{v|L(u,v) = l\}|} \tag{20}$$

where $\widetilde{l_{uv}}$ is the trust transitivity inference result and $\widehat{l_{uv}}$ is the ground of truth based on mobile context. $\{v|L(u,v) = l\}$ represents the set of users who are the l-hop neighbors. $\eta(l)$ implies that how many l-hop neighbors of u have the ground truth trust with u by using the proposed inference mechanism. We evaluate the proposed inference mechanism of trust transitivity subject to various parameter sets p_1, p_2, p_3, p_4, respectively. Figures 15(a)-15(d) show the precision of trust transitivity inference with different hop count l under the two cases of operation $\otimes$ (*i.e.*, *Multiplication* and *Min*). The *Min* operation [28], [29] is used to return the minimal trust value along the transitivity path as the inferencing trust value.

These figures reveal that the precision of trust transitivity inference decreases as the hop count increases under both cases. However, the precision of trust transitivity inference with *Multiplication* operation is higher than that with *Min* operation under various hop counts. Besides, when a high weight of risk of trust between two mobile users is given, *Multiplication* operation outperforms *Min* operation significantly, as shown in



(a) $p_1 = \{0.7, 0.1, 0.1, 0.8\}$ (b) $p_2 = \{0.1, 0.7, 0.1, 0.2\}$

(c) $p_3 = \{0.1, 0.1, 0.7, 0.5\}$ (d) $p_4 = \{0.3, 0.3, 0.3, 0.6\}$

Fig. 15. Precision of Trust Transitivity Inference with Various Parameters Set

Figure 15(c). Furthermore, Figures 15(a) and 15(d) show that the proposed inference mechanism achieves a higher precision of trust transitivity if a high weight of basic trust between two mobile users is assigned.

V. Conclusions

This paper aims at inferring the trust using linguistic terms in MSNs in order to enhance the understanding of trust between mobile users. By analyzing the critical properties of MSNs, a mobile context, that is an intersection of prestige of users, location, time, and social context, was constructed. Then, a mobile context aware trust model was proposed. To enhance the human's understanding of trust values, the fuzzy linguistic technique that is much more desirable for the user to describe the trust values was adopted to express the trust. In addition, we studied the fuzzy trust inference and proposed the *MobiFuzzyTrust* inference mechanism in MSNs that was evaluated by virtue of a real mobile dataset. The experimental results demonstrate that *MobiFuzzyTrust* infers trust well practically. In particular, the precision of trust transitivity inference with *Multiplication* operation is higher than that with *Min* operation under various hop counts. In the future, we plan to investigate the dynamical fuzzy trust inference mechanism in MSNs because of the changeable trust relationships between mobile users. To better characterize the trust semantics between them, an adaptive design approach of membership functions should be studied in details.

References

[1] W. Dong, V. Dave, L. Qiu and Y. Zhang, Secure Friend Discovery in Mobile Social Networks, In *Proc. of INFOCOM 2011*, pages 1647–1655, 2011.

[2] J. Fan, J. Chen, Y. Du, W. Gao, J. Wu, and Y. Sun, Geo-Community-Based Broadcasting for Data Dissemination in Mobile Social Networks, In *IEEE Transactions on Parallel and Distributed Systems*, 24(4), pages 734–743, 2013.

[3] L. Capra, Engineering Human Trust in Mobile System Collaborations, In *SIGSOFT Softw. Eng. Notes*, 29(6), pages 107–116, 2004.

[4] W. Sherchan, S. Nepal, C. Paris, A Survey of Trust in Social Networks, In *ACM Computing Surveys*, 45(4), 2013.

[5] R. R. Yager, Concept Representaion and Database Structures in Fuzzy Social Relational Networks, *IEEE Transcation on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 40(2), pages 413–419, 2010.

[6] R. R. Yager, M. Z. Reformat, Determining Affinity of Users in Social Networks Using Fuzzy Sets, In *Proc. of IPMU 2012*, pages 149–160, 2012.

[7] D. Crandall, D. Cosley, D. Huttenlocher, J. Kleinberg, and S. Suri, Feedback Effects between Similarity and Social Influence in Online Communities, In *Proc. of KDD 2008*, pages 160–168, 2008.

[8] J. Golbeck, J. A. Hendler, Inferring Binary Trust Relationships in Web-based Social Networks, *ACM Transaction on Internet Technology*, 6(4), pages 497–529, 2006.

[9] J. Golbeck, Trust and Nuanced Profile Similarity in Online Social Networks, *ACM Transaction on Web*, 3(4), pages 1–33, 2009.

[10] A. Seyedi, R. Saadi, V. Issarny, Proximity-based Trust Inference for Mobile Social Networking, In *Proc. of International Conference on Trust Management*, pages 253–264, 2011.

[11] S. D. Kamvar, M. T. Schlosser, EigenRep: Reputation Management in P2P Networks, In *Proc. of WWW 2003*, pages 123–134, 2003.

[12] L. Xiong, L. Liu, PeerTrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communities, *IEEE Transcation on Knowledge and Data Engineering*, 16(7), pages 843–857, 2004.

[13] T. Bhuiyan, Y. Xu, A. Josang, Integrating Trust with Public Reputation in Location-based Social Networks for Recommendation Marketing, In *Proc. of IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, pages 107–110, 2008.

[14] R. J. Xiang, J. Neville, and M. Rogati, Modeling Relationship Strength in Online Social Networks, In *Proc. of WWW 2010*, pages 981–990, 2010.

[15] L. A. Zadeh, Fuzzy Logic: Computing With Words, *IEEE Transactions on Fuzzy Systems*, 4(2), pages 103–111, 1996.

[16] J. M. Mendel, L. A. Zadeh, E. Trillas, R. Yager, J. Lawry, H. Hagras, S. Guadarrama, What Computing with Words Means to Me, *IEEE Computational Intelligence Magazine*, 5(1), pages 20–26, 2010.

[17] M. Lesani, S. Bagheri, Applying and Inferring Fuzzy Trust in Semantic Web Social Networks, In *Proc. of CSWWS 2006*, pages 23–43, 2006.

[18] G. Liu, Y. Wang, M. A. Orgun, Trust Transitivity in Complex Social Networks, In *Proc. of the AAAI Conference on Artificial Intelligence*, pages 1222–1229, 2011.

[19] N. Verbiest, C. Cornelis, P. Victor, and E. Herrera-Viedma, Trust and distrust aggregation enhanced with path length incorporation, *Fuzzy Sets and Systems*, pages 61–74, 2012.

[20] P. Carrington, J. Scott, S. Wasserman, Models and Methods in Social Network Analysis, *Cambrige University Press*, Cambrige, 2005.

[21] K. Musial, P. Kazienko, P. Brodka, User Position Measures in Social Network, In *Proc. of SNA-KDD 2009*, pages 6–6, 2009.

[22] S. Wasserman, K. Faust, Social Network Analysis: Methods and Applications, *Newyork: Cambridge University Press*, 1994.

[23] X. Qiao, X. Li, Z. Su, D. Cao, A Context-Awareness Dynamic Friend Recommendation Approach for Mobile Social Network Users, *International Journal of Advanced Intelligence*, 3(2), pages 155–172, 2011.

[24] A. Jonsang, E. Gray, M. Kinaterder, Simplification and Analysis of Transitive Trust Networks, *Web Intelligence and Agent Systems*, 4(2), pages 139–161, 2006.

[25] J. Golbeck, Combining Provenance with Trust in Social Networks for Semantic Web Content Filtering, In *Proc. of the International Provenance and Annotation Workshop*, pages 101–108, 2006.

[26] J. Golbeck, J. Hendler, Inferring Trust Relationships in Web-based Social Networks, *ACM Transactions on Internet Technology*, 6(4), pages 497–529, 2006.

[27] J. Kleinberg. The Small-World Phenomenon: An Algorithmic Perspective. In *Proc. of the 32nd ACM Symposium on Theory of Computing (STOC00)*, pages 163–170, 2000.

[28] J. Zhan, X. Fang. Trust Maximization in Social Networks. In *Proc. of the 4th international conference on Social computing, behavioral-cultural modeling and prediction*, Pages 205–211, 2011.

[29] Y. Chen, T. Bu, M. Zhang, H. Zhu, Measurement of Trust Transitivity in Trustworthy Networks, *Journal of Emering Technologies in Web Intelligence*, 2(4), Pages 319–325, 2010.