A Trust Model Using Implicit Call Behavioral Graph for Mobile Cloud Computing

Shuhong Chen[1], Guojun Wang[1], and Weijia Jia[2]

[1] School of Information Science and Engineering, Central South University, Changsha 410083, China
{shchenannabell,csgjwang}@csu.edu.cn
[2] Department of Computer Science, City University of Hong Kong 83 Tat Chee Avenue, Kowloon, Hong Kong
wei.jia@cityu.edu.hk

Abstract. Behavior patterns of users in mobile social cloud are always based on real world relationships and can be used to infer a level of trust between users. In this paper, we describe the *implicit call behavioral graph* which is formed by users' interactions with call. We rate these relationships to form a dynamic local cloud trust, which enables users to evaluate the trust values between users within the context of a mobile social cloud network. We, then, calculate local trust values according to users' behavioral attributes, such as call frequency, relevance, call moment, and satisfaction. Due to the unique nature of the social cloud, we discuss the propagation and aggregation of local trust values for global social cloud network. Finally, we evaluate the performance of our trust model through simulations, and show simulation results that demonstrate the importance of interaction-based behavioural relationships in recommendation system.

Keywords: Trust relationships, Mobile social cloud, Call behavioral graph, Trust entropy.

1 Introduction

The mobile social cloud is essentially a dynamic virtual network with trust relationships between users. With the emergence of a new generation of powerful mobile devices, novel mobile cloud computing paradigms are possible: various kinds of information and data produced through diverse mobile applications. A smart phone's cloud environment with trustworthiness is a representative scenario of trust in mobile cloud computing [1]. Compared to traditional social networks, a smart phone's cloud environment allows for data collecting with user experience, thus a method to measure trustworthiness of user is necessary [2]. In smart phone's network environment, many people communicate mainly with their friends (such as family, and coworkers) through social network services. In fact, users are more likely to trust their friends, that is based on the physical world relationship, rather than a purely online digital relationship. Mobile users

G. Wang et al. (Eds.): CSS 2013, LNCS 8300, pp. 387–402, 2013.

share their roles within their cloud via interactive behaviors, thereby increasing the overall trustworthiness of the relationship between the users being carried out. However, online social relationships always depend on physical world relationships. Hence, we can infer a level of users' trust relationships that underpins the online community where they exist according to some attributes of real world [3].

In mobile social networks, a call detail log (CDL) contains various details pertaining to each call, such as who called whom, when was it made, etc. Based on these information, one can construct a *call behavioral graph* with customer mobile numbers as nodes and the calls as edges. The weight of an edge captures the strength of the relationship between two nodes. An edge with a high weight signifies a strong tie, while an edge with a low weight represents a weak one. Consequently, one can view the call behavioral graph as a social network consisting of n users (nodes) and a relationship $R_{i,j}$ measured on each ordered pair of users $i, j = 1, \cdots, n$. We consider the call behavioral graph obtained from CDL data.

In this paper, hence, we propose a global social trust model building system by seamlessly integrating the one-dimensional trust relationship values based on interactions between users in mobile social computing environment. We suggest a method to quantify a trusting relation based on the analysis of telephone CDL from mobile devices. The quantified social trust model supports inter-user trust relationship and integration. In other words, the proposed approach not only helps decide communicating path of trustworthy users in mobile cloud environment but also helps address security issues with increased trustworthiness of user behaviors by ranking trustworthy relationships between users. By doing so, a communicating path for trustworthy users under cloud environment is suggested. With the enhanced trustworthiness, the issue of security also can be addressed. Furthermore, the implicit trust along with the application of socially corrective mechanisms inherent in social networks can also be applied to other domains. In fact, social networking platforms already provide a multitude of integrated applications that deliver particular functionality to users, and more significantly, social network credentials provide authentication in many diverse domains, for example, many sites support Facebook Connect as a trusted authentication mechanism [4].

The rest of the paper is organized as follows. Some related work are addressed in Section 2. Section 3 provides the system model and some important definitions. Section 4 and Section 5 discuss how to calculate the local trust values and global trust values, respectively. We analyze some performances of our trust model by simulation in Section 6. Finally, we conclude in Section 7.

2 Related Work

If without trust relationships between users in a mobile social cloud environment, the reliability of the total network would drop. Hence, many works have attempted to discover relationships between communication entities with social trust models. Kuada et al. [6] propose the provisioning and management

approach based on collaborative strategy with social relationships in cloud computing services. Jennifer Golbeck et al. [7] and Kim et al. [8] propose a method to quantitatively infer trust between users for a recommendation system in a Web-based social network. To support mobile phones in mobile cloud to plan, schedule, and reflect on group activities, Kikin-Gil [9] and Counts [10] propose to create privately shared group spaces on mobile devices where each group is able to communicate and collaborate. In order to enhance trustworthiness on the social network, Pezzi [11] defines a social cloud as a means of cultivating collective intelligence and facilitating the development of self-organizing communities. According to Pezzi et al., the social network and its services are provided by network nodes owned by members of the network rather than by centralized servers owned by the social network. Traditionally, social cloud platforms provide only marginal functionality for enhanced communication on mobile devices [12]. However, a truly mobile social cloud will offer functionality to improve communication service by considering users' mobile behavior patterns. To support mobile awareness and collaboration, Oulasvirta et al. [13] design a named *ContextContact* approach. S. Farnham and P. Keyani. [14] provide smart convergence through mobile group text messaging, i.e., *Swarm*. However, *ContextContact* and *Swarm* are designed to enhance communication within a large group including all of a user's contacts. Kim et al. [15,16] propose a trust model that is appropriate for online communities using the user profiles. Interest in analysis and utilization of data obtained from smartphones have increased as smartphones have spread widely. In [17], the authors propose a method to filter out voice spam calls on the IP telephony system that recognizes relationships between users by analyzing sustained phone-calling behavioral pattern (i.e. duration, frequency, recent history etc.) extracted from smartphone CDL. Ankolekar et al. [18] extract the behavioral pattern of each user according to the contact lists and the phone call histories of smartphone users. It is helpful to make a decision by a recommended user list for a user. In [19], Roth et al. describe the implicit social graph which is formed by users' interactions with contacts and groups of contacts, and which is distinct from explicit social graphs in which users explicitly add other individuals as their "friends". Then, the authors describe a novel friend suggestion algorithm that uses a user's implicit social graph to generate a friend group, given a small seed set of contacts which the user has already labeled as friends. However, Roth et al do not consider the relative importance of different interaction types in determining the social relationships between users. In this paper, hence, we propose a trust model for mobile cloud computing using implicit call behavioral graph by considering these issues.

3 System Model and Definitions

3.1 System Model

In a mobile social cloud, users are more likely to trust information from a "friend" if the digital relationship between the two is based on a real world relationship (such as family, colleague, etc.) rather than a purely online relationship [4]. In a

social context formal, individuals are socially motivated and subject to personal repercussions outside the functional scope of the social cloud, and Service Level Agreements (SLAs) are not as critical. Therefore, we use social incentives and the underlying real world relationships as a substitute foundation for trust. We consider a mobil social cloud computing system shown in Fig. 1.

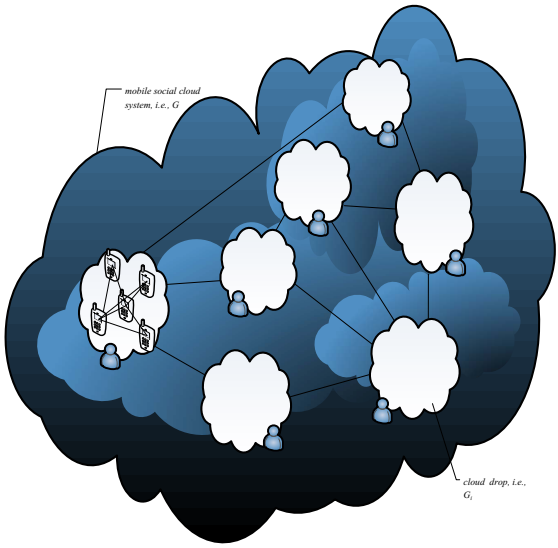

Fig. 1. System model

Let a graph $G = G(V, E)$ denote a mobil social cloud system, where the set V of vertices represents users (nodes), and the set E of edges denotes friendships between these users. If user i trusts user j, there exists a directional edge from user i to user j, and vice versa. In this paper, we ignore the direction of edge, and each edge means a bidirectional edge. We assume the graph G can be divided into multiple sub-graph, and each sub-graph G_k consists of a user k of interest and his/her direct neighbors, as shown in Fig. 2. We assume that there are N_k nodes in G_k. Each edge in G_k is formed by the sending and receiving of call. We call each G_k as *implicit call behavioral graph*, even though it may consist of a single node. A *implicit call behavioral graph* is a subset of vertices of a mobile social network that is highly connected. Edges in the *implicit call behavioral graph* have both direction and weight. The direction of an edge is determined by whether it was formed by an outgoing call sent by the user, or an incoming call received by the user. The weight of an edge is determined by the call behavioural patterns between users. An individual is added into G_k as a "friend", and it implies that at least, the user k has some degree of knowledge about the individual being added. Such connectivity between individuals can be used to infer that a trust relationship exists between them. However, it does not describe the level

of trust or the context of the relationship. Therefore, it is important to provide a quantitative method to describe the trust relationship.

In our approach, the social trust relationship between users in mobile social cloud environments is inferred by users' call behaviors without external enforcement. This kind of trust with one-dimensional perspective is called *local trust*. However, it is not easy to facilitate the expansion of information using the social network in explicit or implicit relationship. Therefore, it is very important to establish a global trust social network using each user's *local trust* in the process of inferring information using social network integrations. We, next, introduce some basic definitions.

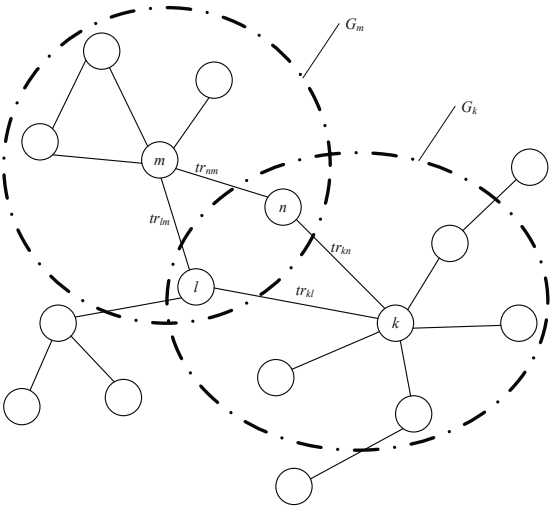

Fig. 2. Cloud drops and their trust relationships

3.2 Basic Definitions

Let $\mathbf{U}$ be the universe set of discourse, f and g are random functions with a stable tendency $f : \mathbf{U} \to [0, 1]$ and $g : \mathbf{U} \to [0, 1]$, respectively. To capture the intimacy degree of trust relationships, we denote ρ as an weighted value of intimacy. For the convenience of discussion, we define the relationship model between user i and user j, R, as a tuple of $\langle f, g, \rho \rangle$.

Definition 1. *For any two users i and j in mobile social cloud G, the trust relationship between them, R, indicate the trust degree and the trust value of user j for user i, and can be defined as:*

$$tr_{ij} \triangleq R\langle Ex_{ij}, WEn_{ij}, \rho_{ij} \rangle \tag{1}$$

where Ex_{ij} is the expected trust value, WEn_{ij} is a weighted entropy, and ρ_{ij} is a utility weighted value.

In this paper, tr_{ij} is the basic elements of trust space, we call it *cloud-drop*. According to Definition 1, Ex_{ij} indicates the basic trust degree of j for i. WEn_{ij} reflects the importance of the trust relationship between users i and j for user i. ρ_{ij} reflects the intimacy level of user i and user j, and we show how to determine it in Section 4.4.

Definition 2. *For user i and any other user j in G_i, the local trust model indicates the trust relationships between user i and others, and can be defined as a tuple of:*

$$loc\_cloud_i \triangleq \langle \hat{tr}_{ij}, HEn_i \rangle \tag{2}$$

where $\hat{tr}_{ij}$ is the normalized value of tr_{ij}, i.e., $\hat{tr}_{ij} \triangleq R\langle \hat{Ex}_{ij}, \hat{WEn}_{ij}, \hat{\rho}_{ij} \rangle$ and HEn_i is the trust hybrid entropy and reflects the density of cloud drop.

3.3 Trust Transitivity

In our model, we also consider trust relationships between users: each user i keeps track of a trust relationship tr_{ij} to each of its neighbour nodes j. In social network, we assume trust relationships only exist between neighbours and users that are not directly connected cannot possibly have a trust relationship with each other. However, two such users may indirectly be connected to each other through a trust path in the network. Hence, we make the assumption that trust may propagate with appropriate discounting through the relationship path [23,24]. Furthermore, we assume that the trust distance indicates the length of the path from the source user to the target user, and the distance is denoted as the number of nodes in the path between two users. If the number of users equals to γ, we call γ-Distance trust. γ-Distance trust refers to the trust that is given to a user that is γ-Distance path connected to the user node in the path from the current user to the target user. In Fig. 3, there is a 2-distance trust between user i to target user j. If $\gamma = 0$, i.e., 0-Distance, we say there is a direct connection relationship from the user to the target user, and the trust is direct connection trust, correspondingly. In the paper, the direct connection trust can be denoted as 0-Distance trust, and all neighbor nodes have 0-Distance trust each other. On the other hand, we define the trust between unreachable nodes as ∞-Distance trust. For example, in Fig 3, the trust relationships of between user m and user j, user k and user l are ∞-Distance trust and 0-Distance trust, respectively.

In this paper, we compute the trust value along a relationships path as the product of the trust values of the links on that path. There may be more than one path between two indirect neighbour users, and each path has its own trust value. In other words, we take the position that "if i trusts j, and j trusts k, then i should have a somewhat more positive view of k based on this knowledge" [23]. For instance, there are two trust path between user k and user m in Fig. 2, i.e., $tr_{kl} : tr_{lm}$ and $tr_{kn} : tr_{nm}$, both are 1-Distance trust. In our model, trust discounting takes place by multiplying trust values along trust paths. We address this case in Section 5.

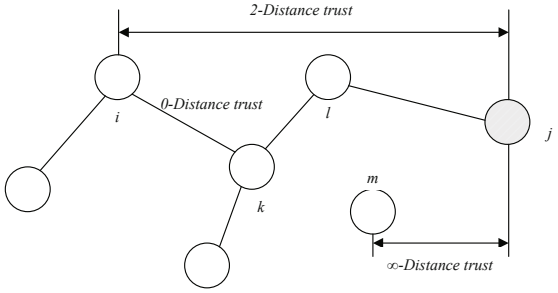

Fig. 3. γ-Distance trust

4 Computing Local Trust Value

Broadly speaking, trust means an act of faith, confidence and reliance in something that is expected to behave or deliver as promised [5,20]. Its a belief in the competence and expertise of others, such that you feel you can reasonably rely on them to care for your valuable assets [21]. Grandison and Sloman [22] have surveyed several existing trust models and they have defined the trust as "the firm belief in the capability of an entity to act consistently, securely and reliably within a specified context". They also claim that the trust is the composition of multiple attributes such as reliability, honesty, truthfulness, dependability, security, competence, timeliness, Quality of Service (QoS) and Return on Investment (ROI) in the context of an environment.

As mentioned above, we compute trust from user's connections. We consider the behavioral attributes such as call frequency, relevance, call moment, and satisfaction to compute local trust value, i.e., 0-Distance trust.

4.1 Call Frequency

Call frequency indicates the level of connections and the inter-user relationships among the users that directly connected. In other words, they are belonged to the same *cloud drop*, i.e., G_i. If the call frequency between user i and user j is greater than that between i and h, it indicates that user i trusts j more than h. For example, a user may trust his friend to whom he talks on the phone every day more than his colleagues at work to whom he talks on the phone for a significant time but with less frequency. We denote call frequency between users i and j as $Call_{freq}(i,j)$, and can calculate $Call_{freq}(i,j)$ as follows:

$$Call_{freq}(i,j) = \frac{Call_{num}(i,j)}{\sum_{k=1}^{N_i} Call_{num}(i,k)} \tag{3}$$

where $Call_{num}(i,j)$ denotes the number of call between users i and j, and any user k belongs to G_i.

4.2 Relevance

The relevance represents the the duration of inter-user relationship, i.e., the duration of call, among users. We let $Call_{rele}(i,j)$ denote the relevance degree of the relationship between users i and j. If $Call_{rele}(i,j)$ is longer than $Call_{rele}(i,k)$, we say a higher relevance and a higher reliability for users i and j. In this paper, we infer the value of relevance through the historical CDL. We assume that $DOWN_{rele}(i,j)$ denotes the total duration percent of all calls from user i to user j, and $UP_{rele}(i,j)$ the total duration percent of all calls from user j to user i. Let $Last(i,j)$ be the duration of each call from user i to user j. We, then, calculate $DOWN_{rele}(i,j)$ and $UP_{rele}(i,j)$ as shown in formula (4) and formula (5), respectively.

$$DOWN_{rele}(i,j) = \frac{\sum_{i,j \in G_i} Last(i,j)}{\sum_{\forall k \in G_i} (Last(i,k) + Last(k,i))} \tag{4}$$

$$UP_{rele}(i,j) = \frac{\sum_{i,j \in G_i} Last(j,i)}{\sum_{\forall k \in G_i} (Last(i,k) + Last(k,i))} \tag{5}$$

Obviously, the trust value between users i and j is various for different call patterns (i.e., user i send initiatively, or receive passively). To denote different relevances for different call patterns, we define a coefficient α ($0 \leq \alpha \leq 1$), which indicates the different importance for call relevance. And then, we obtain:

$$Call_{rele}(i,j) = \alpha UP_{rele}(i,j) + (1-\alpha) DOWN_{rele}(i,j) \tag{6}$$

4.3 Satisfaction

In a distributed social cloud environment, users may still rate each other after each communication. For example, each time user i communicates with user j, he may evaluate the call as positive ($= 1$) or negative ($= -1$). User i may rate a call as negative, for example, if the call is failed or interrupted. We define rat_{ij} as the sum of the ratings of the individual calls that user i has communicated with user j. Let $sat(i,j)$ and $unsat(i,j)$ be the satisfactory calls set and the unsatisfactory calls set, respectively. User i stores the rating value (i.e., 1) of satisfactory calls it has had with user j, $sat(i,j)$ and the rating value (i.e., -1) of unsatisfactory calls it has had with user j, $unsat(i,j)$. Then, rat_{ij} can be calculated:

$$rat_{ij} = \|sat(i,j)\| - \|unsat(i,j)\| \tag{7}$$

where $\|sat(i,j)\|$ and $\|unsat(i,j)\|$ are the absolute values of the sums of all elements in $sat(i,j)$ and $unsat(i,j)$, respectively. We define a local satisfaction value, ls_{ij}, as follows:

$$ls_{ij} = \begin{cases} \frac{max(rat_{ij},0)}{\sum_k max(rat_{ik},0)} & if \quad \sum_k max(rat_{ik},0) \neq 0; \\ 0 \quad if \quad \sum_k max(rat_{ik},0) = 0 \ \ \& \ \ |Neigh[i]| = 0; \\ p_i \quad if \quad \sum_k max(rat_{ik},0) = 0 \ \ \& \ \ |Neigh[i]| \neq 0; \end{cases} \tag{8}$$

where $p_i = 1/|Neigh[i]|$ and $|Neigh[i]|$ is the user number of direct neighbors of user i.

4.4 Call Moment

Call moment refers to the occurring time of the relationship among users and a different call moment implies a different trust relationship among users. In this paper, call moment is divided into *public time*, and *private time*. The trust value of call occurring in *private time* is higher than that of call occurring in *public time*. Generally, we define the work hours is the public time, otherwise, private time. We let $D_{public}(i,j)$ and $D_{private}(i,j)$ denote the call duration in *public time* and *private time* between users i and j, respectively. We can obtain $D_{public}(i,j)$ and $D_{private}(i,j)$ from the recent CDL. Let $Intimacy(i,j)$ denote the intimacy of users i and j, and we calculate $Intimacy(i,j)$ according to formula (9):

$$Intimacy(i,j) = \frac{D_{private}(i,j)}{D_{private}(i,j) + D_{public}(i,j)} \tag{9}$$

where $i, j \in G_i$.

To determine the different trust value according to $Intimacy(i,j)$, in this study, we divide $Intimacy(i,j)$ into four ranks. Generally, the rank of $Intimacy(i,j)$ is higher than that of $Intimacy(i,k)$ means a higher reliability and trust. To capture the nature, hence, we define the weighted value of call between users i and j, i.e., ρ_{ij}, and ρ_{ij} is determined depending on the scope of $Intimacy(i,j)$ as shown in Eq. (10).

$$\begin{cases} \rho_{ij} = 3 \cdot Intimacy(i,j) \quad if \quad Intimacy(i,j) > 0.75; \\ \rho_{ij} = 2 \cdot Intimacy(i,j) - 1 \; if \; 0.5 < Intimacy(i,j) \leq 0.75; \\ \rho_{ij} = 1 \quad if \quad 0.25 \leq Intimacy(i,j) < 0.5; \\ \rho_{ij} = 1 - 2 \cdot Intimacy(i,j) \quad if \quad Intimacy(i,j) < 0.25 \end{cases} \tag{10}$$

4.5 Computing Local Trust Value

As discussed above, local trust value is 0-Distance trust value, and we compute the value of 0-Distance trust according to formula (11).

$$Ex_{ij} = \rho_{ij}(w_1 \cdot Call_{freq}(i,j) + w_2 \cdot Call_{rele}(i,j) + w_3 \cdot ls_{ij}) \tag{11}$$

where w_1, w_2, and w_3 are nonnegative weight coefficients of the trust parameters such that $w_1 + w_2 + w_3 = 1$.

According to Definition 1, we normalize the value of Ex_{ij} as follows:

$$\hat{Ex}_{ij} = \frac{Ex_{ij}}{\sum_{k=1}^{N_i} Ex_{ik}} \tag{12}$$

We calculate $\hat{\rho}_{ij}$ and WEn_{ij} according to formulae (13) and (14), respectively:

$$\hat{\rho}_{ij} = \frac{\rho_{ij}}{\sum_{k=1}^{N_i} \rho_{ik}} \tag{13}$$

$$WEn_{ij} = -\hat{\rho}_{ij}\hat{Ex}_{ij} \log(\hat{Ex}_{ij}) \tag{14}$$

Assume non-influence for all users, we can obtain HEn from formula (15):

$$HEn_i = \sum_{k=1}^{N_i} WEn_{ik} \tag{15}$$

Hence, we obtain the local cloud model: $loc\_cloud_i \triangleq \langle \hat{tr}_{ij}, HEn_i \rangle$.

5 Propagation and Aggregation of Local Trust Values

5.1 Propagating Local Trust Values

In mobile cloud computing environment, users always can not obtain trust recommendation of strangers from their trusted neighbors directly. Hence, we need to propagate local trust values for indirect neighbor nodes.

This is a useful way to have each user gain a view of the network that is wider than his/her own experience. However, the trust values stored by user i still reflect only the experience of user i and his/her acquaintances. In order to get a wider view, user i may wish to ask his/her friends' friends. Furthermore, he/she can have a complete view of the network if he/she continues in this manner. Assume that local trust values are propagated through $n-2$ users from source to target users, i.e., $user_1$(source), $user_2$, $user_2$, $\cdots$, $user_n$(target), and the trust value from $user_i$ to $user_{i+1}$ is $tr_{i(i+1)}$. Hence, we compute the $(n-2)$-Distance trust value from $user_1$ to $user_n$ as follows:

$$\begin{aligned} & tr_{1n)}(Ex_{1n}, WEn_{1n}, \rho_{in}) = tr_{12} \bigotimes \cdots \bigotimes tr_{(n-1)n)} \\ &= \prod_{i=1}^{n-1} (Ex_{i(i+1)}, WEni(i+1), \rho_{i(i+1)}) \end{aligned} \tag{16}$$

where $\bigotimes$ is a logic multiplicative operator, and $Ex_{1n} = \prod_{i=1}^{n-1} Ex_{i(i+1)}$, $WEn_{1n} = min(\sqrt{\sum_{i=1}^{n-1} En^2_{i(i+1)}}, 1)$, and $\rho_{1n} = min(\rho_{12}, \rho_{23}, \cdots, \rho_{(n-1)n})$.

5.2 Aggregating Local Trust Values

In a distributed environment, more than one trust cloud of a stranger user can be considered in many cases. Therefore, we need to aggregate the normalized local trust values.

Assume that local trust values are aggregated in n local clouds, i.e., loc_cloud_1, loc_cloud_2, $\cdots$, loc_cloud_n, and the n trust cloud can be combined into one trust cloud as follows:

$$\begin{aligned} loc\_cloud(\bar{tr}, H\bar{E}n) &= loc\_cloud_1 \bigoplus \cdots \bigoplus loc\_cloud_n \\ &= \sum_{i=1}^{n} loc\_cloud_i(\hat{tr}_i, HEn_i) \end{aligned} \tag{17}$$

where $\bigoplus$ is a logic additive operator, $\bar{tr} = \frac{1}{n}\sum_{i=1}^{n} \hat{tr}_i$ and $HEn = \frac{1}{n}\sum_{i=1}^{n} HEn_i$.

We can obtain the global trust value by propagating and aggregating the local trust values.

6 Performance Evaluation

In order to measure the performance of our trust model, we build the framework of Fig. 1 based on users' CDL and personal information in a smartphone environment. Our simulation framework is constructed by two parts: local social network is implemented in client, and collection of personal information for global social network is processed in the server. The server computes the caller's trust value using our trust model and decide whether the call would be accepted by comparing the evaluating trust value with the predefined threshold value $Val_{threshold}$. In the paper, we define a node j is a "good" user for user i if $tr_{ij} \geq Val_{threshold}$. Otherwise, it is a "bad" user. In simulation, we apply our trust model into an agent-based recommendation system, where each user is denoted as an agent. User call records are extracted against agents. We assume that there are 1000 users and a total of 28,868 calls are extracted from all users. The extracted call information are used to construct local social network for each user and reflect call frequency, relevance, satisfaction, and call moment that are addressed in Section 4. During the simulations, agents interacted with each other for specific times. In each interact, the simulation system chose two nodes randomly, and the first is client and the other is server. To measure the intimacy value, we define the time interval [AM 8:00, PM 19:00] as *public time*, and the other is *private time*. The main simulation parameters are shown in Table 1.

Table 1. The numerical values of the main parameters

Parameter	Value
Number of user	1000
CDL	28,868
$Val_{threshold}$	0.5
α	0.7
Number of initial friend	20
w_1	0.4
w_2, w_3	0.3

We measure the performance of our trust model as compared to the profile-based trust approach [25] (P-Model for abbreviation), and the random approach (R-Model for abbreviation). To quantitatively measure the trust level of our model, we define expected trust density (ETD) as follows:

$$ETD = \frac{\sum_{i,j \in G} tr_{ij}}{Num_{link}} \tag{18}$$

where Num_{link} is a given total number of links of G.

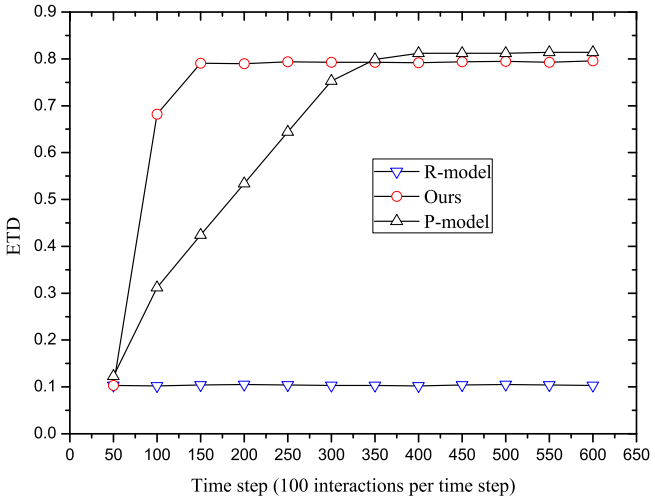

Fig. 4. ETD performance

The ETD characterizes the overall trust level of a mobile cloud environment, and a low ETD indicates the society formed by such mobile cloud environment is fragile and easy to collapse. Generally, the faster the ETD curve become horizontal, the better a trust model convergence is. Fig. 4 compare ETD performance of P-Model, R-Model, and our model with $Num_{link} = 35000$. From Fig. 4, we can find P-Model and our model are very similar and much higher than R-Model on ETD. The reason is due to R-model randomly choices node without trust, and lead to an equal distribution of "good" and "bad" nodes. Therefore, the performance on ETD of R-model is almost 0 on average. On the other hand, our model becomes horizontal faster than P-model, which means our model is easier to converge.

To measure the cooperative performance of our model, we analyze the probability of call request permission. A call request may be permitted or denied. A permissive global call depends on a cooperative social network environment. Therefore, we define the permissive probability, $Prob_{permission}$, to show the cooperative level of a mobile social cloud network. The greater the $Prob_{permission}$ is, the more cooperation a trust model is. Let Num_{call} and $Num_{permission}$ be the number of total call and the permissive call, respectively. We can calculate $Prob_{permission}$ as follows:

$$Prob_{permission} = \frac{Num_{permission}}{Num_{call}} \times 100\% \tag{19}$$

We obtain the simulation results shown in Fig. 5 by changing the number of links, Num_{link}, from 0 to 50000 with step 100. From Fig. 5, we can find that our model has a better cooperative performance than the other approaches.

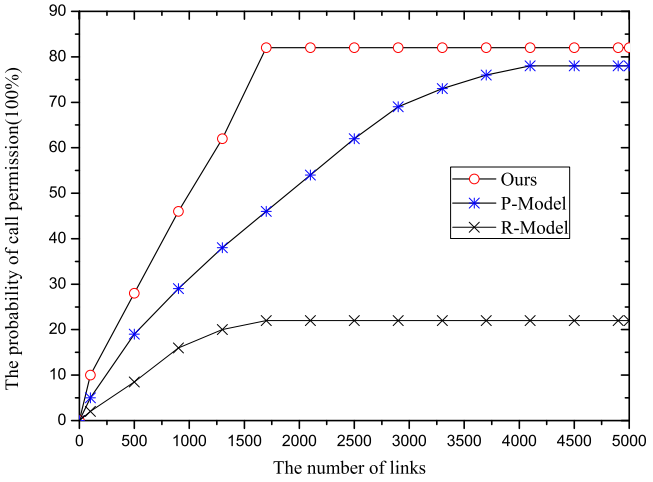

Fig. 5. Cooperative performance

Next, we analyze the difference of our trust model of the selecting recommendations as compared to P-Model, and R-Model. To evaluate the performance of our model, similarly to [25], we define an instantaneous utility function for an agent i following a recommendation from agent j on γ-Distance trust user k at time t as follows:

$$Utility(i, j, t) = \hat{Ex}_{ij} \tag{20}$$

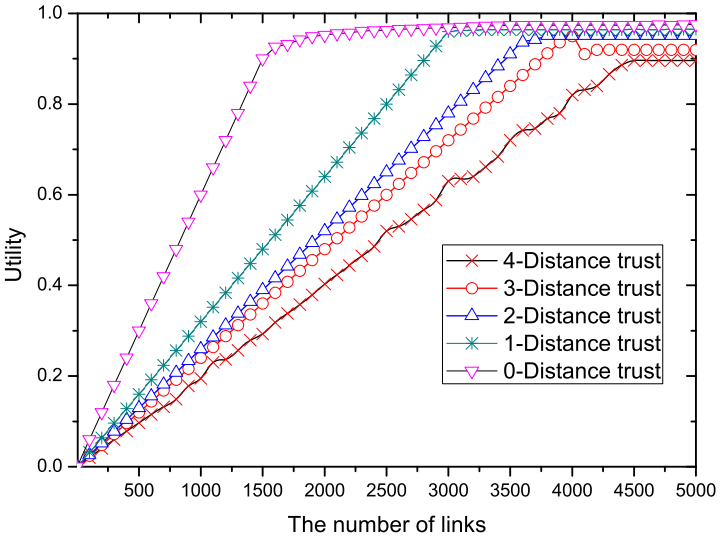

Fig. 6. Utility vs Num_{link}

For instance, for 0-Distance trust user k, $Utility(i,j,t)$ of user i is the $\hat{Ex}_{ij}$ of neighbor node j at time t. We consider the performance of the system to be the average of the utilities of the agents in the system:

$$Utility(t) = \frac{1}{N} \sum_{i \in G} \hat{Ex}_{ij} \tag{21}$$

where N is the number of agents in γ-Distance trust region. Similarity, we change the value of Num_{link} in the interval $[0, 50000]$ with step 100, and we obtain the simulating results shown in Fig. 6.

From Fig. 6, we can observe that each agent develops a trust value towards its neighboring nodes which reflects the similarity of their respective rating at begin. After some time, paths of high trust develop, connecting agents with similar profiles. As a result, the performance of the system, increases over time and reaches a stationary value as shown in Fig. 6, where the curves correspond to different values of γ. Increasing values of γ lead to curves approaching the stationary slower.

7 Conclusion

We have explained how local trust value is calculated based on user call behavioral attributes such as call frequency, relevance, satisfaction and call moment. We have proposed a novel quantitative trust management model. Furthermore, we have discussed the propagation and aggregation of local trust values for global trust model. We have demonstrated that our trust model performs better than the conventional R-Model and similar trust models such as P-Model through simulations. Here trust is measured in terms of four attributes. However, there are some more attributes such as honesty, context, accountability and auditability of social information to measure trust. These parameters are not discussed here. It is interesting to refine trust using these additional attributes.

Acknowledgment. This work is supported by the National Natural Science Foundation of China under grant numbers 61272151 and 61073037, National 973 Basic Research Program of China under grant number 2011CB302800, the Ministry of Education Fund for Doctoral Disciplines in Higher Education under grant number 20110162110043, and the Specialized Research Fund for Doctoral Program in Higher Education of Hunan Provincial Education Department under grant number CX2010B075.

References

1. Christensen, J.H.: Using RESTful web-services and cloud computing to create next generation mobile applications. In: Proceeding of the 24th ACM SIGPLAN Conference Companion on Object-Oriented Programming Systems Languages and Applications, Orlando, FL, USA, pp. 627–634 (2009)

2. Takabi, H.: Security and privacy challenges in cloud computing environments. IEEE Secur. Priv. 8(6), 24–31 (2010)
3. Heurta-Canepa, G., Lee, D.: A virtual cloud computing provider for mobile devices. In: Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services, vol. (6) (2010)
4. Chard, K., Bubendorfer, K., Caton, S., Rana, O.F.: Social Cloud Computing: A Vision for Socially Motivated Resource Sharing. IEEE Transactions on Services Computing 5(4), 551–563 (2012)
5. Costa, C., Bijlsma-Frankema, K.: Trust and Control Interrelations. Group and Organization Management 32(4), 392–406 (2007)
6. Kuada, E., Olesen, H.: A social network approach to provisioning and management of cloud computing services for enterprises. In: Proc. of Cloud Computing, pp. 98–104 (2011)
7. Golbeck, J., Hendler, J.: Film Trust: Movie recommendations using Trust in Web-based social network. In: CCNC 2006, pp. 1314–1315. IEEE 3rd Publication (2006)
8. Kim, S., Han, S.: The method of inferring trust in Web-based social network using fuzzy logic. In: Proc. of the International Workshop on Machine Intelligence Research, pp. 140–144 (2009)
9. Kikin-Gil, R.: Affective is effective: how information appliances can mediate relationships within communities and increase one's social effectiveness. Personal and Ubiquitous Computing 10(2-3), 77–83 (2006)
10. Counts, S.: Group-based mobile messaging in support of the social side of leisure. Computer Supported Cooperative Work 16(1-2), 75–97 (2007)
11. Pezzi, R.: Information Technology Tools for a Transition Economy (September 2009), http://www.socialcloud.net/papers/ITtools.pdf
12. Grob, R., Kuhn, M., Wattenhofer, R., Wirz, M.: Cluestr: Mobile Social Networking for Enhanced Group Communication. In: Proc. of GROUP 2009, USA, pp. 81–90 (2009)
13. Oulasvirta, A., Raento, M., Tiitta, S.: ContextContacts: redesigning SmartPhone's contact book to support mobile awareness and collaboration. In: Mobile HCI, pp. 167–174 (2005)
14. Farnham, S., Keyani, P.: Swarm: Hyper awareness, micro coordination, and smart convergence through mobile group text messaging. In: HICSS, vol. 3, pp. 1–10 (2006)
15. Kim, M., Seo, J., Noh, S., Han, S.: Identity management-based social trust model for mediating information sharing and privacy enhancement. Secur. Commun. Netw. 5(8), 887–897 (2012)
16. Kim, M., Park, S.: Group affinity based social trust model for an intelligent movie recommender system. Multimed. Tools Appl. 64(2), 505–516 (2013)
17. Balasubramaniyan, V.A., Ahamad, M., Park, H.: CallRank: combating SPIT using call duration, social networks and global reputation. In: Proceedings of Fourth Conference on Email and Anti-Spam, pp. 18–24 (2007)
18. Ankolekar, A., Szabo, G., Luon, Y., Huberman, B.A., Wilkinson, D., Wu, F.: Friendlee: a mobile application for your social life. In: Proceedings of the 11st International Conference on Human-Computer Interaction with Mobile Devices and Services, vol. (27) (2009), doi:10.1145/1613858.1613893
19. Roth, M., Ben-David, A., Deutscher, D., Flysher, G., Horn, I., Leichtberg, A., Leiser, N., Matias, Y., Merom, R.: Suggesting Friends Using the Implicit Social Graph. In: KDD 2010, pp. 233–241 (2010)
20. Lund, M., Solhaug, B.: Evolution in Relation to Risk and Trust Management. Computer, 49–55 (May 2010)

21. Gambetta, D.: Can We Trust Trust? Trust: Making and Breaking Cooperative Relations, pp. 213–237. Basil Blackwell (1988)
22. Grandison, T., Sloman, M.: A survey of trust in Internet applications. IEEE Communications Survey and Tutorials, 2–16 (2000)
23. Guha, R., Kumar, R., Raghavan, P., Tomkins, A.: Propagation of trust and distrust. In: WWW 2004: Proceedings of the 13th International Conference on the World Wide Web, pp. 403–412. ACM Press (2004)
24. Gray, E., Seigneur, J.-M., Chen, Y., Jensen, C.: Trust propagation in small worlds. In: Nixon, P., Terzis, S. (eds.) iTrust 2003. LNCS, vol. 2692, pp. 239–254. Springer, Heidelberg (2003)
25. Walter, F.E., Battiston, S., Schweitzer, F.: A model of a trust-based recommendation system on a social network. Auton Agent Multi-Agent Syst. 16, 57–74 (2008)