Frontiers of Information Technology & Electronic Engineering
www.zju.edu.cn/jzus; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

DGTM: a dynamic grouping based trust model for mobile peer-to-peer networks*#

Mei-juan JIA†1,2, Hui-qiang WANG1, Jun-yu LIN†‡3, Guang-sheng FENG1, Hai-tao YU4

(1*College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China*)
(2*College of Computer Science and Information Technology, Daqing Normal University, Daqing 163712, China*)
(3*Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*)
(4*College of Tourism, Guilin University of Technology, Guilin 541001, China*)
†E-mail: meijuan.jia@hrbeu.edu.cn; linjunyu@iie.ac.cn

Received Sept. 8, 2016; Revision accepted Nov. 20, 2016; Crosschecked Mar. 28, 2017

Abstract: The special characteristics of the mobile environment, such as limited bandwidth, dynamic topology, heterogeneity of peers, and limited power, pose additional challenges on mobile peer-to-peer (MP2P) networks. Trust management becomes an essential component of MP2P networks to promote peer transactions. However, in an MP2P network, peers frequently join and leave the network, which dynamically changes the network topology. Thus, it is difficult to establish long-term and effective trust relationships among peers. In this paper, we propose a dynamic grouping based trust model (DGTM) to classify peers. A group is formed according to the peers' interests. Within a group, mobile peers share resources and tend to keep stable trust relationships. We propose three peer roles (super peers, relay peers, and ordinary peers) and two novel trust metrics (intragroup trust and intergroup trust). The two metrics are used to accurately measure the trust between two peers from the same group or from different groups. Simulations illustrate that our proposed DGTM always achieves the highest successful transaction rate and the best communication overhead under different circumstances.

Key words: Mobile P2P networks; Trust management; Dynamic grouping; Super peer
http://dx.doi.org/10.1631/FITEE.1601535 **CLC number:** TP393

1 Introduction

The rapid proliferation of wireless networks and mobile portable devices has extended conventional peer-to-peer networks to mobile peer-to-peer (MP2P) networks. An MP2P network is organized according to the general P2P principles (Ranjan and Zhao, 2013), but it is different from conventional P2P networks. In an MP2P network, peers frequently join and leave the network, resulting in dynamic topology changes (Ou *et al.*, 2008). Moreover, there is no central administration in MP2P networks and peers are autonomous. Peers cannot communicate with each other via a well-established infrastructure, which makes them inherently insecure and untrustworthy (Castro *et al.*, 2009); an example is Skype, one of the most well-known P2P infrastructures. To deploy a mobile P2P system, a straightforward approach is to mount a P2P system over mobile ad hoc networks (MANETs) (Tan *et al.*, 2010; Spaho *et al.*, 2012), where the transitory sets of mobile peers dynamically establish their own network on the fly (Qureshi *et al.*, 2010). Thus, it is very challenging to construct a trust relationship between two peers in an MP2P network. Meanwhile, in mobile P2P networks, each

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (Nos. 61502118, 61370212, and 61402127) and the Natural Science Foundation of Heilongjiang Province, China (Nos. F2015029 and QC2015070)

# A preliminary version was presented at the 13th IEEE International Conference on Services Computing, June 27–July 2, 2016, San Francisco, USA

ORCID: Jun-yu LIN, http://orcid.org/0000-0003-4807-0609

peer acts as both a client and a server to share its resources with other peers, and communicates with others via unregulated, short-range wireless technologies. It is obvious that wireless P2P systems are different from wired ones. So, the trust management system should be decentralized and is expected to effectively aggregate trust ratings despite delays, connection loss, and malicious behaviors from peers (Zhu and Bao, 2007; Zhuge *et al.*, 2008).

To develop trust strategies, the relationship between peers has been exploited (Tian C *et al.*, 2010; Wu, 2011; Chen *et al.*, 2015; 2016). In Tian C *et al.* (2010) and Wu (2011), trust relationships were considered to maintain the stability of the network topology. In Chen *et al.* (2015; 2016), social trust and social reciprocity were leveraged to promote efficient cooperation among peers. It is found that in an MP2P network, peers with the same or similar interests are more capable of maintaining cooperation. This characteristic can help guarantee the stability of the trust relationship between peers. Based on this characteristic, some group-based trust models have been proposed (Wu, 2011; Tian C *et al.*, 2010; Jia *et al.*, 2016; Tian HR *et al.*, 2006). However, in the existing group-based trust models, the members in a group are fixed once the grouping is completed. The existing group-based trust models are not appropriate for MP2P networks.

In this study, we extend the previous conference paper (Jia *et al.*, 2016). We consider the original trust value of peers before grouping and consider the effect of movement velocity of peers. The main contributions are summarized as follows: we (1) propose a novel method to dynamically divide peers into groups based on their interests, and (2) present a model based on two new trust metrics, intragroup trust and intergroup trust. Intragroup trust is the trust between two peers from the same group; intergroup trust is the trust between two peers from different groups. Using the two metrics, we evaluate the trustworthiness of a peer in a dynamic MP2P network.

2 Related work

Because P2P systems do not have central administration and peers are autonomous, the peers are inherently insecure and untrustworthy (Tan *et al.*, 2010; Almenárez *et al.*, 2011). To deal with the trust issues in open and decentralized environments such as P2P systems and MP2P systems, many trust and reputation schemes have been proposed. According to the evaluation methods of these trust models, they can be divided into (1) global trust management, (2) local trust management, and (3) group-based trust management. In the following sections we review these models.

2.1 Global trust management

Under a global trust management scheme, each peer who participates in a network has a unique reliability (Chang and Kuo, 2009). EigenTrust (Kamvar *et al.*, 2003) and PowerTrust (Zhou and Hwang, 2007) are two of the most well-known global trust management models.

EigenTrust, proposed by Kamvar *et al.* (2003), relies on the notion that some peers in the network are pretrusted. This approach addresses the collusion problem by using transitive trust. However, in some cases, the pretrusted peers may not be trustworthy in the future, because they may be scored badly after some transactions. In addition, this approach requires strong coordination and synchronization of peers. This assumption may be overly optimistic in a distributed computing environment. Zhou and Hwang (2007) leveraged power-law feedback characteristics to develop a robust and scalable P2P reputation system, PowerTrust. They used a trust overlay network (TON) to model the trust relationships among peers. This design achieved high speed and accuracy of aggregation, robust defense against malicious peers, and high scalability of large-scale P2P applications. Zhou *et al.* (2008) proposed a gossip protocol for fast score aggregation. It enables light-weight aggregation and fast dissemination of global scores in a low time complexity $O(\log_2 n)$, but it is not effective in identifying malicious peers.

2.2 Local trust management

In local trust management, a peer calculates reliability by directly using evaluations received from a certain number of peers (Yang and Sun, 2016). PeerTrust (Xiong and Liu, 2004) and M-Trust (Qureshi *et al.*, 2012) are two of the most well-known local trust management schemes.

PeerTrust can identify the important trust parameters for evaluating trustworthiness of peers, and can address various malicious behaviors in a P2P community. However, the computation convergence rate is not guaranteed in large-scale P2P systems. In addition, the five factors used in their trust model are costly to retrieve. PET (Liang and Shi, 2005) is a model (Chang and Kuo, 2009) for sharing files in P2P networks, and evaluates reliability and risk of suppliers as resource shares. SFTrust (Zhang *et al.*, 2009) is a trust model based on the topology adaptation protocol, which was proposed in an unstructured P2P system. SFTrust separates trust between the service provided and feedback. The reliability of service and feedback was calculated respectively.

A robust distributed reputation and trust management scheme was proposed in M-Trust (Qureshi *et al.*, 2012). M-trust incorporates distributed trust rating aggregation algorithms that acquire trust ratings from direct and witness recommendations from distant peers. The scheme uses confidence in reputation, based on interactions among peers, to decrease the time required in computing trust ratings and reduce the space for storing trust ratings. However, setting threshold limits for selecting highly trustworthy recommenders in a dynamic MANET environment is not an easy task. Threshold limits need to be adjusted according to the network situation.

2.3 Group-based trust management

Sun and Tang (2007) proposed a multilayer and grouping P2P trust model. This model avoids the infinite iterations of global reputation. However, the groups are based on physical distance clustering. Thus, its performance cannot be guaranteed in MP2P networks. Tian HR *et al.* (2006) proposed a group-based reputation system GroupRep to infer the direct trust relationship between peers in P2P networks. However, such a reputation system is not suitable for large-scale MP2P networks due to the message overhead of global reputation aggregation. Largillier and Vassileva (2012) argued that many different contexts and groups could be formed based on a user's criteria or using methods that match user desires. Al-Oufi *et al.* (2012) extended the Advogato trust metric (Leskovec *et al.*, 2010) so that trustworthy users can be identified. Their approach can discover reliable users and unreliable users. However, their approach is based on some specific environments. Easa *et al.* (2012) considered two factors in their trust model, i.e., intermediate group confidence and group confidence between two groups. Wu (2011) proposed a stable group based trust management scheme (SGTM) to construct sufficient and reliable trust relationships. Though their experimental results illustrated that the model can handle peers joining and leaving the network, they did not present the methods to validate it. SuperTrust is a trust model for P2P networks based on a super peer (Tian C *et al.*, 2010). A feedback filtering algorithm was proposed to effectively filter fake, misleading, and unfair feedback in the referral, but peers joining or leaving networks/groups were not considered.

3 Dynamic grouping management strategy

In an MP2P network, each peer has high mobility, which means that the availability of peers frequently varies. We first define three roles of peers, based on which transaction information is effectively managed. Then we propose a dynamic grouping method to add a peer to the best-fit group in an MP2P network. As the topology of the MP2P network changes, we consider peer joining, leaving, and the movement velocity of peers in our grouping method.

3.1 Roles of peers

In each group, we define three roles for peers: super peer, ordinary peer, and relay peer.

Super peer (SP): An SP is a peer that maintains a trust table and a file list of all the peers in a group. A trust table records the trust information of all the peers in the group. When a peer requests some files, it can send the request to the super peer. The super peer advises the requesting peer which peers are trustworthy according to the trust table. The file list records the files of all peers. When a peer requests some files, it can send the request to the super peer. The super peer tells the requester which group member has the requested files.

Relay peer (RP): An RP is an ordinary peer who connects two adjacent groups. The transaction information between peers from different groups is stored in the relay peers. In Fig. 1, we present an example of transactions among different roles in an MP2P network. First, P7 requests a file owned by P9. P7 sends a query to the super peer P1. If P1 or one of the other peers in P1's group (i.e., P4 or

P8) has the requested file, P1 sends a response to P7. Note that a super peer maintains the file information for all peers in its group. Thus, the super peer knows if a peer has the requested file. If no one in P1's group has the requested file, P1 sends the query to the relay peers, e.g., P4 in Fig. 1. P4 sends the query to relay peers, P5 and P10, from different groups. The relay peer sends the query to the super peers in their groups, e.g., P2 and P3 in Fig. 1. Because P2 is the super peer of the group, it has a file list of all peers in its group. P2 finds that P9 has the requested file. P2 sends a response to P7 via back tracing (Yates *et al.*, 2012), to convey the information that P9 has the target file.

Ordinary peer (OP): An OP is a peer that is not a super peer or a relay peer. It can request sources from other peers and share resources with other peers. An ordinary peer updates the number of interests after each transaction and sends the information to the super peer of the group.

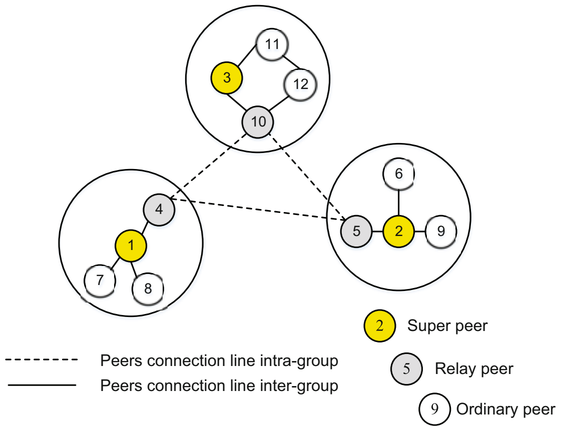
11
3
12
10
6
4
5
2
9
1
7
8
2 Super peer
Peers connection line intra-group
Peers connection line inter-group
5 Relay peer
9 Ordinary peer

Fig. 1 An example of groups

3.2 Dynamic grouping

In an MP2P network, the interest set of peer i is denoted by $I_{p_i}=\{a_1,a_2,...,a_k\}$ and the interest set of peer j is denoted by $I_{p_j}=\{b_1,b_2,...,b_k\}$. The similarity between peer i and peer j can be calculated as follows:

$$S_{p_i,p_j}=\cos\alpha=\frac{\sum_{m=1}^{k}a_m b_m}{\sqrt{\sum_{m=1}^{k}a_m^2\sum_{m=1}^{k}b_m^2}}. \qquad (1)$$

Phase 1 (initial phase): In the initial phase, the similarity of two peers is calculated with their interest values with Eq. (1). Because k is the number of attributes in a peer's interest set, k peers are randomly selected as the initial center peers. Then, we obtain k center peers and k corresponding initial groups. Given a peer, we can calculate its similarity with k center peers. The given peer is added to a center peer's group if the similarity between the given peer and the center peer is the smallest. By repeating this process, all peers are added to corresponding groups. Afterward, we update the center peer in each group by using the method adopted in K-means (Nayak *et al.*, 2015). Then, we can obtain k new groups by calculating the similarity between peers and the updated center peers. This process is terminated if the peers in each group stop changing.

We assume that $C_1,C_2,...,C_k$ are the peers that are randomly selected and k is the number of interests of a peer. Algorithm 1 describes the proposed scheme—dynamic grouping.

In the initial phase, the super peer is selected using the similarity with C_i. This is described in Algorithm 2.

Phase 2 (network operation phase): During the network operation phase, a peer may update its interests according to its request. If a peer successfully receives the requested files, the relevant interest value is increased by one. Otherwise, the relevant interest value is decreased by one.

If the successful transaction rate (STR) is less than a certain value, or many peers leave/join the network, following Algorithm 1, a new group is formed based on the peers' updated interests.

STR is the ratio of the number of successful transactions T^{s} to the number of all transactions T^{t}. A successful transaction means that the requesting peer can obtain the requested files from the serving peer.

STR is defined as

$$\mathrm{STR}=\frac{T^{\mathrm{s}}}{T^{\mathrm{t}}}. \qquad (2)$$

During the network operation phase, the super peer is selected according to the reliability of peers. A peer with the highest reliability will be selected as a super peer in a group. The reliability will be described in Section 4.

3.3 Time complexity analysis

In the dynamic grouping algorithm, we analyze the average time complexity and the best complexity.

Algorithm 1 Dynamic grouping

```
Require: $C_1, C_2, ..., C_k$ are the initial center peers which are randomly selected.
    $k$ is the number of attributes in a peer's interest set
Flag = true /*stop iteration*/
Unchanged = 0;
for ($i = 1$ to $k$) do
    $G_i = \{C_i\}$, /*add $C_i$ to corresponding groups*/
    $G_i^{'} = \varnothing$ /*$G_i^{'}$ denotes results of last grouping*/
end for
$V_1 = V - (\{C_1\} \cup \{C_2\} \cup ... \cup \{C_k\})$ /*remove center peers*/
while Flag do
    while ($V_1$ is not empty) do
        $\forall v \in V_1$
        Sim = 0
        Group = 1; /*initialize number of groups*/
        for ($i = 1$ to $k$) do
            $\text{Sim}_i = \text{Similarity}(v, C_i)$ /*calculate the similarity*/
            if Sim < $\text{Sim}_i$ then
                Sim = $\text{Sim}_i$ /*update the Sim*/
                Group = $i$ /*record the number of groups*/
            end if
        end for
        $G_{\text{group}} = G_{\text{group}} \cup \{v\}$ /*peer $v$ is added to a corresponding group*/
        $V_1 = V_1 - \{v\}$ /*delete peer $v$*/
        $G_{\text{group}} = \frac{1}{|G_{\text{group}}|}\sum_{i=1}^{|G_{\text{group}}|} g_{\text{group}}^i$ /*$g_{\text{group}}^i$ denotes the $i$th peer. Update the center peer*/
    end while
    if $G_1 = G_1^{'}$&&$G_2 = G_2^{'}$&&...$G_k = G_k^{'}$ /*no change to the group*/ then
        Unchanged++; /*the counter is added by 1*/
        if (Unchanged > $T$) /*no change to the groups*/ then
            Flag = false
        else
            Flag = true; /*another iteration*/
            for ($i = 1$ to $k$) do
                $G_i^{'} = G_i$ /*store last grouping result*/
                $G_i^{'} = \varnothing$ /*clear the last result*/
                $V_i = V$
            end for
        end if
    else
        Flag = false;
        Unchanged = 0; /*reset the counter to 0*/
        for ($i = 1$ to $k$) do
            $G_i^{'} = G_i$ /*store the last grouping result*/
            $G_i^{'} = \varnothing$
            $V_i = V$
        end for
    end if
end while
Ensure: $G_i$ ($i = 1, 2, ..., k$)
```

Algorithm 2 Super peer selection

```
Require: $C_1, C_2, ..., C_k$
for ($i = 1$ to $k$) do
    $\text{Super}_i = g_i^1$ /*$\text{Super}_i$ is the super peer of the $i$th group*/
    $\text{Sim}_i = \text{Similarity}(\text{Super}_i, C_i)$
    for ($j = 1$ to $|G_i|$) do
        if $\text{Similarity}(C_i, g_i^j) > \text{Sim}_i$ then
            $\text{Super}_i = g_i^j$
            $\text{Sim}_i = \text{Similarity}(C_i, g_i^j)$
        end if
    end for
end for
Ensure: $\text{Super}_1, \text{Super}_2, ..., \text{Super}_n$
```

In the best case, after the first iteration of the algorithm, the group is in a stable state, and the algorithm ends after $T-1$ iterations (T is the number of iterations required to achieve the stability of the group).

According to the definition of time complexity, the time complexity in the best case is $O(k) + O(Tkn + Tk)$, where $O(k)$ can be ignored, so the time complexity is $O(Tk(n+1))$. k is the number of groups, T is the number of iterations before the groups do not change, and n is the number of peers. $O(k)$ is the time complexity to join the initial cluster center of an empty group; $O(kn)$ denotes the time complexity of one iteration; $O(Tkn)$ denotes the required time complexity that a group does not change after T iterations; $O(Tk)$ denotes the time complexity of storing the latest group results.

Before T grouping is stable, the iterative algorithm needs S iterations of the unstable group; this indicates the number of iterations during which the group results are not the same in T successive times. So, the average time complexity of the algorithm is $O(k) + O((S+T)kn + (S+T)k)$. According to the algorithm's definition of time complexity, $O(k)$ can be ignored. So, the average time complexity is $O((S+T)k(n+1))$, where $O(Skn)$ denotes the time complexity before achieving stability of T grouping and $O((S+T)k)$ denotes the time complexity required to store the latest group results. It can be seen from the above analysis that, the time complexity of the dynamic grouping algorithm is related to the number of groups, the number of peers, and the number of iterations required by the algorithm.

3.4 Group management

MP2P networks have dynamic topologies. The main challenge is to maintain the stability of MP2P networks in the face of high peer mobility with peers joining and leaving. In DGTM, we design a strategy to process these scenarios.

3.4.1 Peers joining

A peer joining an MP2P network means that the peer joins a group that reflects its interests. An initial trust value is set for a new peer, which can inspire it to transact with other peers. When a single peer joins an MP2P network, the information about that peer's interaction with other peers is not available. So, the peer's similarity with the super peer of the group can be calculated. The peer will be added to the group to which it is most similar. When a number of peers join an MP2P network, the trust relationships among peers change, and new groups are generated following Algorithm 1.

3.4.2 Peers leaving

In DGTM, we propose three roles for peers, so we need to consider three kinds of situations. When many peers leave groups, new groups are generated following Algorithm 1.

1. Ordinary peers leaving

Peers broadcast leaving messages to the other peers in the same group. The other peers in the same group update the information of the neighbors and recalculate the trust values. Meanwhile, the super peer in the group updates the route tables and file lists.

2. Relay peers leaving

If a relay peer leaves a group, it broadcasts messages to the other peers in the same group. The leaving relay peer transfers its information to other relay peers in the same group. The new relay peer sends information to confirm the role. The super peer broadcasts messages about the new relay peer to all the member peers in the group after it receives the information from the new relay peer. According to the messages, all the member peers update their information about the relay peer.

3. Super peers leaving

In a group, the super peer manages the trust messages and the file lists of all members in the group. Thus, it is important to consider the case in which a super peer leaves. First, the super peer is required to broadcast its leaving message, and then the new super peer is selected based on the reliability of all peers. Once a new super peer is confirmed, all the trust messages and the file lists of the group are transferred to the new super peer. The new super peer responds to the information that it has received from the original super peer. After that, the initial super peer leaves. All the members in the group update their information about the new super peer. In our work, for simplification, we adopt a single super peer scheme. In our future work, we will consider a mechanism with a set of super peers in a group for robustness.

In MP2P networks, peers have high mobility due to joining, leaving, and the movement velocity. Peers that have a longer time to live and lower average movement velocity are more valuable in transactions. In Section 4.1, we will discuss the impact of the movement velocity of peers on our trust model.

To avoid data loss, out-of-sync data, and failure of an access point due to peers joining and leaving the network, we introduce the boundary agreement (perimeter refresh protocol, PRP) (Ratnasamy *et al.*, 2002).

4 Dynamic grouping based trust model

Based on our proposed dynamic grouping method, we propose the trust model DGTM to calculate the trust between two peers in MP2P networks. All peers are divided into groups according to our proposed dynamic grouping method. A super peer manages the trust messages and file lists of all the peers in its group. Thus, it is important to select the super peer.

4.1 Super peer selection for trust management

In DGTM, the peer with the highest reliability in a group is selected as the super peer. A peer's reliability results from its trust value, the remaining energy in its mobile device, and the dynamics of the peer. In this subsection, we define direct trust, indirect trust, remaining energy of peers, dynamics of peers, and reliability of peers.

Definition 1 (Direct trust, DT) DT is defined according to the successful transactions between peers in a time interval denoted by $\mathrm{DT}(p_i, p_j)$.

DT can be calculated as follows:

$$\mathrm{DT}(p_i,p_j)=\begin{cases}\frac{N^{\mathrm{s}}(p_i,p_j)}{N(p_i,p_j)}, & N(p_i,p_j)\neq 0,\\ 0, & N(p_i,p_j)=0,\end{cases} \tag{3}$$

where $N^{\mathrm{s}}(p_i,p_j)$ denotes the successful transaction number and $N(p_i,p_j)$ denotes the total number of transactions.

Definition 2 (Indirect trust, IDT) IDT is evaluated by the weighted average of DT, which is provided by p_i's neighbors who have transacted with p_j. It is denoted by $\mathrm{DT}(p_i,p_j)$.

IDT can be calculated as follows:

$$\mathrm{IDT}(p_i,p_j)=\frac{\sum_{m=1}^{n}W_i^m\cdot\mathrm{DT}(\mathrm{neig}_i{}^m,p_j)}{n}, \tag{4}$$

where $\mathrm{IDT}(p_i,p_j)$ is the indirect trust between peer p_i and peer p_j.

The number of peer p_i's neighbors is n and the mth neighbor of peer p is $\mathrm{neig}_i{}^m$. The weight of the mth neighbor of peer p_i is W_i^m, which can be computed as follows:

$$W_i^m=\frac{\mathrm{DT}(p,\mathrm{neig}_i^m)}{\sum_{m=1}^{n}\mathrm{DT}(p_i,\mathrm{neig}_i^m)}, \tag{5}$$

where $\mathrm{DT}(p,\mathrm{neig}_i^m)$ is the direct trust from peer p_i to peer neig_i^m.

Trust (TR) is a term that describes how much one peer believes in another peer. A peer's TR is defined as

$$\mathrm{TR}(p_i,p_j)=w\cdot\mathrm{DT}(p_i,p_j)+(1-w)\cdot\mathrm{IDT}(p_i,p_j), \tag{6}$$

where w is the weight of DT and $(1-w)$ is the weight of IDT.

TR ranges from 0 to 1. A TR of 0 means complete distrust, and a TR of 1 means complete trust.

Definition 3 (Remaining energy of a peer, RE) RE is the time remaining in a mobile peer's battery (Kassinen *et al.*, 2009). One typical challenge of MP2P applications is battery consumption. We follow the method in Kassinen *et al.* (2009) to evaluate RE.

RE is calculated as

$$\mathrm{RE}_i=\frac{\mathrm{BC}\cdot V_{\mathrm{avg}}}{P_{\mathrm{avg}}}, \tag{7}$$

where BC is the battery capacity of a mobile peer. The power P_{avg} is measured as an average of the power consumption during each 20-min interval on the two mobile devices. The average voltage level V_{avg} is reported by the Energy Profiler software.

Definition 4 (Dynamics of a peer, DYN) DYN is a measure that indicates the dynamics of a peer. DYN is determined by two factors: the failure rate of a peer and the time to live of the peer. The failure rate of peer i is denoted by lose_i, and it can be calculated as follows:

$$\mathrm{lose}_i=1-\frac{R_i}{V_i\cdot\Delta T+R_i}, \tag{8}$$

where R_i is the communication radius, V_i is the movement velocity of peer i, and ΔV is the update time. Therefore, the smaller the communication radius and the greater the movement velocity, the higher the failure rate.

DYN of peer p_i is calculated as

$$\mathrm{DYN}_i=\frac{1}{\mathrm{lose}_i}\cdot T_i, \tag{9}$$

where T_i is the time to live of peer i. The larger the DYN, the smaller the peer's dynamics, and the more stable the peer.

Definition 5 (Reliability of a peer, RP) RP is a measure that indicates whether a peer can provide reliable resources. In our proposed model, RP is determined by three factors: TR, RE, and DYN. The peer with the highest reliability will be selected as the super peer in a group. Because a super peer needs to manage the trust table, route table, and file list, the super peer is required to maintain more energy.

RP is calculated as

$$\mathrm{RP}_i=w_i\cdot\mathrm{RE}_i+w_j\cdot\mathrm{TR}(p_i,p_j)+w_l\cdot\mathrm{DYN}_i, \tag{10}$$

where w_i is the weight of RE, w_j the weight of TR, and w_l the weight of DYN.

4.2 Intragroup trust

Intragroup trust is the trust between two peers in a group. Peers in a group have similar interests. They accumulate much experience through their interactions. Therefore, sufficient and reliable trust relationships are constructed in the group without relying on any fixed networking infrastructure or centralized entities. So, in DGTM, if there is a transaction between two peers, the trust is calculated with Eq. (3).

If there are no transactions between two peers, the experience of the other peers must be considered. As shown in Fig. 1, P7 and P8 are in the same group. There are no transactions between them. They will store the transaction records of their neighbors. The intragroup trust between peers can be calculated with Eq. (10). In a group, the super peer has the highest reliability, so the trust between two peers is calculated without considering the super peer.

4.3 Intergroup trust

The interactions between peers in different groups are weaker than those of peers within a group. The overall trust is less than intragroup trust because of the limited interaction between groups. Intergroup trust is used to estimate the trust between two peers in different groups. If two peers p_a and p_b have transacted with each other, the intergroup trust is calculated according to Eq. (10). If there are no transactions between the two peers, the intergroup trust is calculated according to

$$\mathrm{TR}_{p_a,p_b}=\begin{cases}\dfrac{N^{\mathrm{s}}_{G_i,G_j}}{N_{G_i,G_j}}, & N_{G_i,G_j}\neq 0,\\ 0, & N_{G_i,G_j}=0,\end{cases} \tag{11}$$

where G_i is the group to which p_a belongs and G_j is the group to which p_b belongs. $N^s_{G_i,G_j}$ denotes the number of successful transactions between groups G_i and G_j. N_{G_i,G_j} denotes the total number of all transactions between groups G_i and G_j. TR_{p_a,p_b} is stored in a super peer.

When there are no transactions between peers, peers can send a request to the super peer to determine the intergroup trust.

5 Simulations and analysis

To evaluate the performance of the proposed trust evaluation and management model, we performed simulations to compare our proposed DGTM with three models: SGTM (Wu, 2011), M-Trust (Qureshi *et al.*, 2012), and PowerTrust (Zhou and Hwang, 2007).

SGTM is a stable group-based trust model. M-Trust is a distributed reputation- and trust-management scheme. PowerTrust is a classic global trust system.

5.1 Setting

In the simulations, the network topology structure is randomly initiated. We generate 200 mobile peers in a 1000 m×1000 m area and the experience time is set to 1800 s. We assume that two peers cannot communicate when the distance between them is more than 200 m. The mobile peers are moving continuously at 25 m/s. The mobility of peers is simulated using the random waypoint model (Jeyaraj and Subadra, 2014). It is a random model that is often used to simulate the movements of mobile users. The initial trust values of honest peers follow a normal distribution with $\mu=0.9$ and $\sigma=0.1$.

Originally, with similar interests and demands, peers join the MP2P networks to communicate and share resources with each other. After a period of exchanging, some peers may become resourceful, active, and sophisticated, while others may become selfish, irresponsible, and even malicious.

The parameters used in the simulations are listed in Table 1.

Table 1 Parameters for simulations

Parameter	Value
Peer number	200
Deployment area	1000 m×1000 m
Communication range	200 m
Maximum speed	25 m/s
Experience time	1800 s
Original trust value	$\mu=0.9$, $\delta=0.1$

5.2 Simulation results and analysis

For comparison, we evaluated the successful transaction rate (STR, defined in Section 3) and the communication overhead for each model. Each result was obtained from an average of 50 independent runs.

Communication overhead refers to the total number of messages that a peer generates and forwards in one second, including aggregating all trust, dynamic grouping, and group updating.

5.2.1 Simulation 1 (successful transaction rate)

In the first simulation, we compared the STR change with the mobility of peers.

Fig. 2a plots the STR when new peers are added to the simulations. We can observe that the STR values of all methods decline when the proportion of joining peers increases. It is obvious that the lower the trust relationship, the fewer the transactions between peers, and the lower the successful transaction rate. We can observe that DGTM delivers the highest STR values in all cases. When the proportion of new peers reaches 50%, the STR value of DGTM is around 94%, which is 2%, 8%, and 10% higher than that of SGTM, M-Trust, and PowerTrust, respectively.

Fig. 2b plots the STR when the peers leave the MP2P networks. We can observe that the STR values of all trust models decline when the number of leaving peers increases. It is obvious that when more peers leave, there are fewer transactions between peers, and thus the successful transaction rate is lower. DGTM delivers the highest STR values in all cases. When the proportion of leaving peers reaches 50%, the STR value of DGTM is around 90%, which is 10%, 17%, and 18% higher than that of SGTM, M-Trust, and PowerTrust, respectively. This is because the trust information for all peers is stored in the super peers. When a peer leaves, the super peer updates the trust table and broadcasts the updated information to all peers in the group. After obtaining the information, the peers update their trust information. This can guarantee that leaving peers will not affect the transactions between two peers in the group.

Fig. 2c plots the STR with the movement velocity of peers. We can observe that DGTM maintains the highest STR value, although the movement velocity of the peers increases. When the movement velocity of peers increases to 25 m/s, the STR value of DGTM is still the highest. The STR value of DGTM is 94.1%, which is 2%, 6%, and 9% higher than that of SGTM, M-Trust, and PowerTrust, respectively. Using DGTM, the peers are divided into groups according to their interests, and peers select other peers with which to transact based on the larger DYN.

5.2.2 Simulation 2 (communication overhead)

To make our simulation as close to the dynamic topology of MP2P networks as possible, we assigned every peer a time-to-live (TTL), whose value is from 50 to 100. After reaching the lifetime, the peer will not respond to any service request, and will not be counted in the statistics. With a new TTL, the peer comes alive again. We simulated scenarios with 500 to 2500 peers.

Fig. 3a shows the number of messages in DGTM, SGTM, M-Trust, and PowerTrust, when the number of peers increases. The average numbers of messages sent by PowerTrust, M-Trust, SGTM, and the proposed DGTM are 91.6, 70.6, 34.2, and 23.8, respectively.

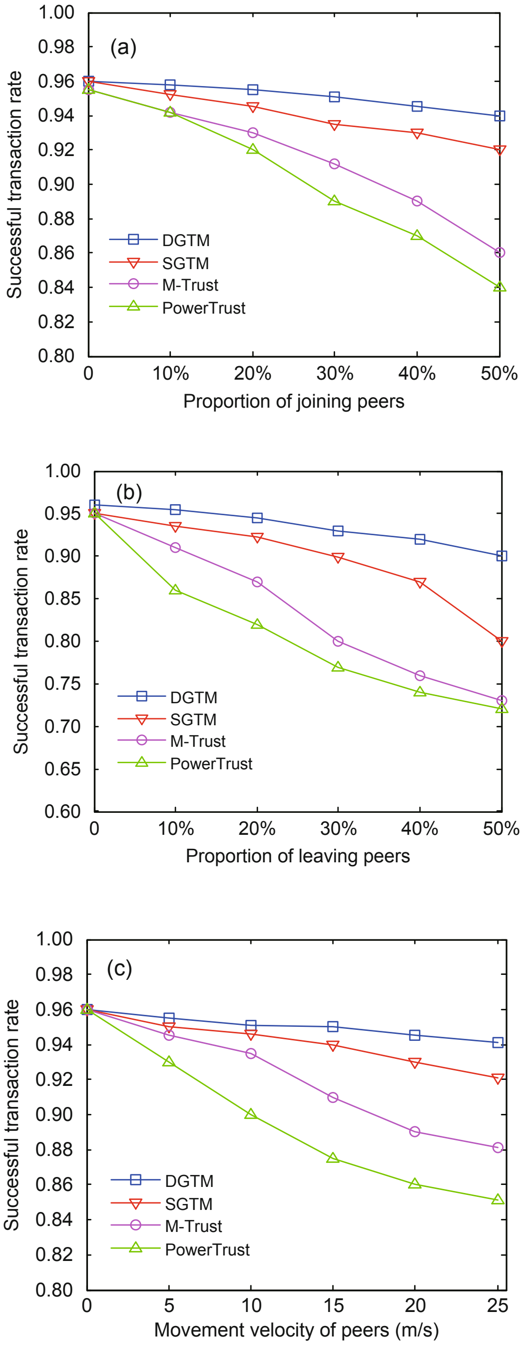

Fig. 2 STR with peers joining (a), peers leaving (b), and movement velocity (c)

We repeated the simulation in a system of the movement velocity of peers. Fig. 3b shows that our system needs 17 messages on average, whereas SGTM, M-Trust, and PowerTrust need 22.25, 36.25, and 46 messages on average, respectively, to perform the same task.

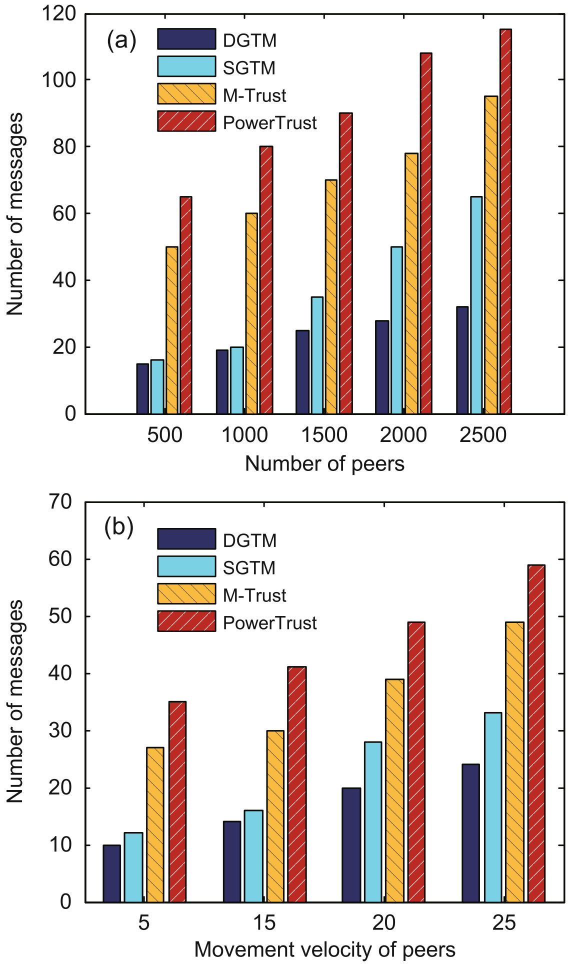

Fig. 3 Number of messages vs. the number of peers (a) and movement velocity (b)

From Figs. 2 and 3, we can observe that using DGTM, the peers experience a noticeably lower communication overhead. When there are fewer than 1000 peers and the movement velocity of the peers is less than 15 m/s, DGTM and SGTM show similar results. This is because DGTM and SGTM are both group based. The peers have stable relationships in a group.

In DGTM, peers are divided into groups according to similar interests. When a large number of new peers join the group, they lead to dynamic grouping, which results in stable trust relationships within a group. Furthermore, peers transact with peers with a lower movement velocity, which leads to a higher successful transaction rate and fewer communication messages.

So, our dynamic grouping model can better alleviate the communication overhead, whereas SGTM, M-Trust, and PowerTrust cannot. Therefore, DGTM is scalable in handling an even larger number of MP2P services and higher movement velocity.

6 Conclusions and future work

In this paper, we proposed an effective trust model for MP2P networks, DGTM, in which all peers in MP2P networks are divided into different groups. We focused on how to effectively create dynamic groupings when peers join and leave networks. Furthermore, two trust metrics, intragroup trust and intergroup trust, can accurately measure the trust between peers in MP2P networks. Therefore, DGTM can guarantee a stable successful transaction rate.

In DGTM, we adopt a single super peer scheme for simplicity. In our future work, we will consider a mechanism where a set of super peers is established in a group to create robustness. The information about group members will be stored in every super peer in the set. When a super peer leaves the group or has low reliability during network operation, other backup super peers will continue to manage the members of the group.

References

Almenárez, F., Marín, A., Díaz, D., *et al.*, 2011. Trust management for multimedia P2P applications in autonomic networking. *Ad Hoc Netw.*, **9**(4):687-697. http://dx.doi.org/10.1016/j.adhoc.2010.09.005

Al-Oufi, S., Kim, H.N., El Saddik, A., 2012. A group trust metric for identifying people of trust in online social networks. *Expert Syst. Appl.*, **39**(18):13173-13181. http://dx.doi.org/10.1016/j.eswa.2012.05.084

Castro, M.C., Kassler, A.J., Chiasserini, C.F., *et al.*, 2009. Peer-to-peer overlay in mobile ad-hoc networks. *In*: Shen, X.M., Yu, H., Buford, J., *et al.* (Eds.), Handbook of Peer-to-Peer Networking. Springer US, p.1045-1080. https://doi.org/10.1007/978-0-387-09751-0_37

Chang, B.J., Kuo, S.L., 2009. Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs. *IEEE Trans. Veh. Technol.*, **58**(4):1846-1863. http://dx.doi.org/10.1109/TVT.2008.2005415

Chen, X., Proulx, B., Gong, X.W., *et al.*, 2015. Exploiting social ties for cooperative D2D communications: a mobile social networking case. *IEEE/ACM Trans. Netw.*,

23(5):1471-1484.
http://dx.doi.org/10.1109/TNET.2014.2329956

Chen, X., Gong, X.W., Yang, L., *et al.*, 2016. Exploiting social tie structure for cooperative wireless networking: a social group utility maximization framework. *IEEE/ACM Trans. Netw.*, **24**(6):3593-3606.
http://dx.doi.org/10.1109/TNET.2016.2530070

Easa, F.R., Bafghi, A.G., Shakeri, H., 2012. A group-based trust propagation method. 2nd Int. eConf. on Computer and Knowledge Engineering, p.313-317.
http://dx.doi.org/10.1109/ICCKE.2012.6395398

Jeyaraj, J.A.S., Subadra, S., 2014. A study on dynamic source routing in ad hoc wireless networks. *Int. J. Eng. Trends Technol.*, **8**(7):401-410.
http://dx.doi.org/10.14445/22315381/IJETT-V8P269

Jia, M.J., Wang, H.Q., Ye, B., *et al.*, 2016. A dynamic grouping-based trust model for mobile P2P networks. 13th IEEE Int. Conf. on Services Computing, p.848-851.
http://dx.doi.org/10.1109/SCC.2016.121

Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H., 2003. The eigentrust algorithm for reputation management in P2P networks. Proc. 12th Int. Conf. on World Wide Web, p.640-651. http://dx.doi.org/10.1145/775152.775242

Kassinen, O., Harjula, E., Korhonen, J., *et al.*, 2009. Battery life of mobile peers with UMTS and WLAN in a Kademlia-based P2P overlay. 20th Int. Symp. on Personal, Indoor and Mobile Radio Communications, p.662-665.
http://dx.doi.org/10.1109/PIMRC.2009.5450083

Largillier, T., Vassileva, J., 2012. Using collective trust for group formation. *LNCS*, **7493**:137-144.
http://dx.doi.org/10.1007/978-3-642-33284-5_12

Leskovec, J., Huttenlocher, D., Kleinberg, J., 2010. Signed networks in social media. Proc. SIGCHI Conf. on Human Factors in Computing Systems, p.1361-1370.
http://dx.doi.org/10.1145/1753326.1753532

Liang, Z.Q., Shi, W.S., 2005. PET: a PErsonalized Trust model with reputation and risk evaluation for P2P resource sharing. Proc. 38th Annual Hawaii Int. Conf. on System Sciences, p.201b.
http://dx.doi.org/10.1109/HICSS.2005.493

Nayak, J., Naik, B., Kanungo, D.P., *et al.*, 2015. An improved swarm based hybrid K-means clustering for optimal cluster centers. 2nd Int. Conf. on Information Systems Design and Intelligent Applications, p.545-553.
http://dx.doi.org/10.1007/978-81-322-2250-7_54

Ou, Z.H., Song, M.N., Zhan, X.S., *et al.*, 2008. Key techniques for mobile peer-to-peer networks. *J. Softw.*, **19**(2):404-418 (in Chinese).
http://dx.doi.org/10.3724/sp.j.1001.2008.00404

Qureshi, B., Min, G., Kouvatsos, D., 2010. M-Trust: a trust management scheme for mobile P2P networks. IEEE/IFIP 8th Int. Conf. on Embedded and Ubiquitous Computing, p.476-483.
http://dx.doi.org/10.1109/euc.2010.79

Qureshi, B., Min, G., Kouvatsos, D., 2012. A distributed reputation and trust management scheme for mobile peer-to-peer networks. *Comput. Commun.*, **35**(5):608-618. http://dx.doi.org/10.1016/j.comcom.2011.07.008

Ranjan, R., Zhao, L., 2013. Peer-to-peer service provisioning in cloud computing environments. *J. Supercomput.*, **65**(1):154-184.
http://dx.doi.org/10.1007/s11227-011-0710-5

Ratnasamy, S., Karp, B., Yin, L., *et al.*, 2002. GHT: a geographic hash table for data-centric storage. ACM Int. Workshop on Wireless Sensor Networks and Applications, p.78-87.
http://dx.doi.org/10.1145/570738.570750

Spaho, E., Kulla, E., Xhafa, F., *et al.*, 2012. P2P solutions to efficient mobile peer collaboration in MANETs. 7th Int. Conf. on P2P, Parallel, Grid, Cloud and Internet Computing. http://dx.doi.org/10.1109/3pgcic.2012.50

Sun, Z.X., Tang, Y.W., 2007. Multilayer and grouping P2P trust model based on global reputation. *J. Commun.*, **28**(9):133-140 (in Chinese).

Tan, H., Wang, Y., Hao, X.H., *et al.*, 2010. Arbitrary obstacles constrained full coverage in wireless sensor networks. Proc. 5th Int. Conf. on Wireless Algorithms, Systems, and Applications, p.1-10.
http://dx.doi.org/10.1007/978-3-642-14654-1_1

Tian, C., Jiang, J., Hu, Z., *et al.*, 2010. A novel super-peer based trust model for peer-to-peer networks. *Chin. J. Comput.*, **33**(2):345-355 (in Chinese).
http://dx.doi.org/10.3724/sp.j.1016..2010.00345

Tian, H.R., Zou, S.H., Wang, W.D., *et al.*, 2006. A group based reputation system for P2P networks. *LNCS*, **4158**:342-351. http://dx.doi.org/10.1007/11839569_33

Wu, X., 2011. A stable group-based trust management scheme for mobile P2P networks. *Int. J. Dig. Cont. Technol. Appl.*, **5**(2):116-125.
http://dx.doi.org/10.4156/jdcta.vol5.issue2.13

Xiong, L., Liu, L., 2004. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Trans. Knowl. Data Eng.*, **16**(7):843-857.
http://dx.doi.org/10.1109/TKDE.2004.1318566

Yang, H.S., Sun, J.H., 2016. A study on hybrid trust evaluation model for identifying malicious behavior in mobile P2P. *Peer-to-Peer Netw. Appl.*, **9**(3):578-587.
http://dx.doi.org/10.1007/s12083-015-0411-6

Yates, J.S., Storch, M.F., Nijhawan, S., *et al.*, 2012. Apparatus for Executing Programs for a First Computer Architecture on a Computer of a Second Architecture. US Patent 8 127 121.

Zhang, Y.C., Chen, S.S., Yang, G., 2009. SFTrust: a double trust metric based trust model in unstructured P2P system. IEEE Int. Symp. on Parallel & Distributed Processing, p.1-7.
http://dx.doi.org/10.1109/IPDPS.2009.5161240

Zhou, R.F., Hwang, K., 2007. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing. *IEEE Trans. Parall. Distr. Syst.*, **18**(4):460-473.
http://dx.doi.org/10.1109/TPDS.2007.1021

Zhou, R.F., Hwang, K., Cai, M., 2008. GossipTrust for fast reputation aggregation in peer-to-peer networks. *IEEE Trans. Knowl. Data Eng.*, **20**(9):1282-1295.
http://dx.doi.org/10.1109/TKDE.2008.48

Zhu, H.F., Bao, F., 2007. Quantifying trust metrics of recommendation systems in ad-hoc networks. IEEE Wireless Communications and Networking Conf., p.2904-2908.
http://dx.doi.org/10.1109/WCNC.2007.538

Zhuge, H., Chen, X., Sun, X.P., *et al.*, 2008. HRing: a structured P2P overlay based on harmonic series. *IEEE Trans. Parall. Distr. Syst.*, **19**(2):145-158.
http://dx.doi.org/10.1109/TPDS.2007.70725