2012 15th International Conference on Network-Based Information Systems

Trustworthiness of Peers in P2P Overlay Networks

Ailixier Aikebaier
Seikei University
Tokyo, Japan
Email: alisher.akber@computer.org

Tomoya Enokido
Risho University
Tokyo, Japan
Email: eno@ris.ac.jp

Makoto Takizawa
Seikei University
Tokyo, Japan
Email: makoto.takizawa@computer.org

***Abstract*—In peer-to-peer (P2P) overlay networks, a group of multiple peers have to cooperate with each other. P2P systems are in nature scalable distributed systems, where there is no centralized coordinator. It is difficult for each peer to communicate with every other peer. An acquaintance peer of a peer is another peer with which the peer can directly communicate. Each peer has to obtain access and location information on resources through communicating with acquaintances. It is critical to discuss how each peer can trust an acquaintance since acquaintances may have obsolete information. There are subjective (direct) and objective (indirect) types of trustworthiness of a peer on an acquaintance. A peer obtains the subjective trustworthiness on an acquaintance through directly communicating with the acquaintance. Here, the more number of satisfiable replies a source peer receives from a acquaintance, the larger subjective trustworthiness on the acquaintance the source peer has. On the other hand, a peer obtains the objective trustworthiness on a target acquaintance through collecting subjective trustworthiness on the target acquaintance from other peers. Here, the subjective and objective types of trustworthiness on an acquaintance might be different. That is, other peers have different trustworthiness opinions on the target acquaintance. A peer decides on which type of trustworthiness to be taken based on the confidence. The confidence of a peer shows how much the peer is confident of its own trustworthiness opinion, i.e. subjective trustworthiness on the acquaintance. If a peer is confident of the trustworthiness opinion, i.e. the confidence is larger, the peer takes the subjective trustworthiness on the target acquaintance. Otherwise, the peer takes the objective trustworthiness.**

***Keywords*-P2P overlay networks; subjective trustworthiness; objective trustworthiness; confidence; trustworthiness-based group communication;**

I. Introduction

Peer-to-peer (P2P) systems are composed of peer processes (*peers*) interconnected in networks. There are many discussions on how to detect target objects like files in P2P overlay networks like flooding algorithms [8] and distributed hash tables (DHT) [4]. Furthermore, peers can autonomously join and leave networks and change services which the peers provide to other peers. Thus, P2P systems are distributed where there is no centralized coordinator like index and super peers [2]. Hence, each peer has to communicate with other peers to obtain information on target objects. In papers [12], the authors discuss not only how to detect a peer which holds a target object but also how to be granted access rights to manipulate the target object.

A peer p_s cannot communicate with every peer due to the scalability of P2P overlay networks. Hence, a peer with which a peer p_s can directly communicate is referred to as *acquaintance* peer. A peer p_s has to get access and location information on target objects through communicating with its acquaintances. Here, some acquaintance might hold obsolete information on the target objects due to propagation delay and be faulty. Hence, a peer p_s has to use only information obtained from trustworthy acquaintances. In this paper, we discuss how each peer trusts an acquaintance. We postulate that P2P communication is a model of individual-to-individual communication in human societies.

First, a peer p_s issues a service request q to an acquaintance peer p_t to obtain some service in the network. Then, the acquaintance p_t sends a reply r to the source peer p_s. If the reply r satisfies the request q, p_s recognizes the acquaintance p_s to be more trustworthy. For example, a peer p_s issues an SQL query to an acquaintance p_t. The SQL query is performed on the database system and then the acquaintance p_t sends a reply with a derived table to p_s. If the acquaintance p_t returns the derived table, the source peer p_s is satisfiable and recognizes p_t to be more trustworthy. Otherwise, p_s recognizes p_t to be less trustworthy.

If an acquaintance p_t could not handle the request q from a source peer p_s, e.g. does not have a database system, p_t may introduce p_s another peer p_u which holds a database system. Then, p_s issues the request q to p_u. The peer p_u sends a reply r to the source peer p_s. If the reply r satisfies the request q, p_s recognizes p_u to be more trustworthy. In addition, p_s recognizes the acquaintance p_t which introduces the trustworthy peer p_u to be more trustworthy. If the reply r does not satisfy the request q, p_s recognizes not only p_u but also the acquaintance p_t to be less trustworthy.

A source peer p_s obtains the trustworthiness of an acquaintance peer p_t on a service request by directly communicating with the peer p_t. This kind of trustworthiness is referred to as *subjective* trustworthiness S_{st} [12].

On the other hand, a source peer p_s can collect subjective trustworthiness on an acquaintance p_t from other peers. The more number of peers trust p_t, the more the source peer p_s trusts p_t. This concept is similar to the reputation concept [3], [5], [6]. In order to collect trustworthiness opinions in the network, a source peer p_s sends a trustworthiness

978-0-7695-4779-4 2012

DOI 10.1109/NBiS.2012.117

request to every acquaintance. On receipt of the trustworthiness request, each acquaintance p_u sends its subjective trustworthiness on the target peer p_t to p_s. Then, p_u forwards the trustworthiness request to its acquaintances. Thus, the trustworthiness request is distributed to peers by a kind of flooding algorithm [8]. Since the P2P overlay network is scalable, it takes time and spends communication overheads to distribute a trustworthiness request to every peer. In addition, some peer might be faulty and might have wrong, obsolete trustworthiness opinions on the target peer p_t. It is critical to discuss to which peer a trustworthiness request to be delivered in the network. A *trustworthiness domain* D_{st} is a subset of the peers in the network, from each of which a source peer p_s collects subjective trustworthiness on p_t. The average value of subjective trustworthiness values collected from peers in the domain D_{st} is referred to as *objective* trustworthiness O_{st} [12].

Next, suppose a source peer p_s obtains a pair of the subjective trustworthiness S_{st} and objective trustworthiness O_{st} on a target acquaintance p_t. If S_{st} and O_{st} are similar, p_s takes S_{st} or O_{st}. Otherwise, p_s has to decide on which type of trustworthiness, S_{st} or O_{st}, to be taken. We introduce the *confidence* concept F_{st} which shows how much the source peer p_s is confident of its own subjective trustworthiness S_{st}. The larger F_{st} is, the more often p_s takes the subjective trustworthiness S_{st}. We postulate a source peer is more confident of its own subjective trustworthiness S_{st} if p_s had more often communicated with p_t for a long time and S_{st} is more stable.

We first present the system model in section 2. In section 3, we discuss the subjective trustworthiness of an acquaintance peer based on the Fuzzy logics. In section 4, we discuss the objective trustworthiness of an acquaintance peer. In section 4, we discuss the confidence of each peer.

II. System Model

A. Acquaintance peers

A peer-to-peer (P2P) system S is composed of multiple peer processes (*peers*) p_1, ..., p_n which are interconnected in an overlay network. Since the P2P systems are scalable, a peer cannot know about the overall membership of the system S and which peers hold what objects and are granted what access rights [12]. A peer p_t with which a peer p_s can directly communicate is referred to as *acquaintance* peer of the peer p_s. The acquaintance relation is written as $p_s \rightarrow p_t$. We assume $p_s \rightarrow p_t$ is symmetric and reflexive. However, the acquaintance relation $p_s \rightarrow p_t$ is not transitive.

[Definition] A peer p_t is an *implicit* acquaintance of a peer p_s ($p_s \Rightarrow p_t$) iff $p_s \rightarrow p_u$ and $p_u \Rightarrow p_t$ for some peer p_u but $p_s \rightarrow p_t$ does not hold ($p_s \not\rightarrow p_t$) [Figure 1].

A peer p_s cannot directly communicate with an implicit acquaintance p_t. However, p_t can get an acquaintance of the peer p_s if an acquaintance p_u such that $p_s \rightarrow p_u \Rightarrow p_t$ and $p_s \not\rightarrow p_t$ introduces p_t to p_s. The peer p_s sends an acquaintance request to p_t. If p_t agrees on the acquaintance relation with p_s, p_s gets the acquaintance of p_t. A peer autonomously makes decision on which peer is an acquaintance. For example, if an acquaintancep_t gets less trustworthy, p_s recognizes p_t to be not an acquaintance peer. Thus, the relation $\rightarrow$ ($\subseteq S^2$) is dynamically changed.

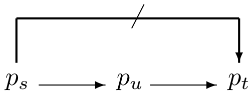

Figure 1. Subjective trustworthiness

B. Acquaintance base

Each peer p_s holds information on acquaintance peers. First, acquaintances of a peer p_s are stored in the acquaintance base $AB_s = \{p_t \mid p_s \rightarrow p_t\}$. A peer p_s may send a request to an acquaintance p_t to obtain acquaintances of p_t, i.e. implicit acquaintances. On receipt of the acquaintance request from the peer p_s, the acquaintance p_t may send all or some of the acquaintances to p_s. Thus, p_s gets an implicit acquaintance p_t by communicating with an acquaintance p_u, i.e. $p_s \rightarrow p_u \Rightarrow p_t$ and $p_s \not\rightarrow p_t$. Acquaintances which the peer p_s obtains from an acquaintance p_u are stored in the implicit acquaintance base $IB_s = \{ \langle p_t, p_u \rangle \mid p_s \rightarrow p_u \Rightarrow p_t$ and $p_s \not\rightarrow p_t$ for some peer $p_u\}$. A peer p_s obtains an acquaintance relation with a peer p_t such that $p_u \rightarrow p_t$ or $p_u \Rightarrow p_t$ from an acquaintancer p_u. The peer p_s stores an implicit acquaintance relation $p_s \Rightarrow p_t$ in the implicit acquaintance base IB_s.

If a peer p_s receives unsatisfiable replies from an acquaintance p_t, p_s recognizes a peer p_t not to be an acquaintance. Then, the relation $p_s \rightarrow p_t$ is removed in AB_s. On the other hand, if a peer p_s sends an acquaintance request to an implicit acquaintance p_t and the peer p_t sends a positive acknowledgment to p_s, the implicit acquaintance p_t gets an acquaintance of p_s. The peer p_t is stored in AB_s. If p_t is in IB_s ($p_s \Rightarrow p_t$), p_t is also removed in IB_s.

In addition, the sizes of the acquaintance base AB_s and the implicit acquaintance base IB_s are limited. Hence, if AB_s and IB_s overflow, some acquaintance p_u has to be removed in the acquaintance base AB_s and IB_s, respectively. For example, a least trustworthy acquaintance p_u is removed in AB_s. Here, if $p_s \Rightarrow p_t$ in IB_s, there is an acquaintance p_u of the peer p_s such that $p_u \Rightarrow p_t$. If so, IB_s is referred to as *consistent*. Each peer p_s might not have a consistent implicit acquaintance base IB_s.

III. Subjective Trustworthiness

A. Subjective trustworthiness

A peer p_s sends a request q to an acquaintance p_t to ask to do something. Here, p_s is referred to as *source* peer and the acquaintance p_t is referred to as *target* peer. On receipt of the request q from p_s, the target peer p_t performs the request q and sends a reply r to p_s. If the target peer p_t performs the request q, p_s can more trust the target peer p_t. However, if p_t does not perform the request q, p_s less trusts p_t. If p_t stops by fault, p_s does not receive any reply from p_t. If p_t suffers from Byzantine fault [7], p_s might receive a reply r from p_t but the reply r does not satisfy the request q. We assume that the trustworthiness of a source peer p_s on an acquaintance p_t is decided through request-reply interactions.

Next, even if a source peer p_s sends a request q to a target acquaintance p_t, p_t cannot send a reply r, for example, p_t does not provide the source peer p_s with the service r. However, p_t knows an acquaintance p_u of p_t which can provide other peers with the service r [Figure 2]. Then, p_t introduces the acquaintance p_u to the source peer p_s. p_s sends the request q to p_u. Suppose the target peer p_u sends a satisfiable reply r to the source peer p_s. Here, p_s recognizes the peer p_u to be more trustworthy as discussed here. In addition, p_s recognizes the acquaintance p_t which introduces the trustworthy peer p_u to be more trustworthy.

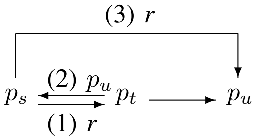

Figure 2. Subjective trustworthiness

The *subjective* trustworthiness S_{st} of a source peer p_s on a target peer p_t is defined in terms of the following parameters;

[Parameters of subjective trustworthiness]

1) Responsibility rsp_{st}.
2) Satisfiablity stf_{st}.
3) Quality of service (QoS) qos_{st}.

For each request-reply interaction from a source peer p_s to a target acquaintance p_t, if p_s receives a reply from p_t, rs_{st} is 1. Otherwise, rsp_{st} is 0. If p_s does not receive any reply from p_t for some time period, i.e. rsp_{st} = 0, p_s recognizes p_t to be faulty. Next, suppose p_s receives a reply r from the target acquaintance p_t. If r includes an answer on the request q, stf_{st} is 1. Otherwise, stf_{st} = 0. Even if the reply r includes an answer a, a might not satisfy the quality of service (QoS) required by the source peer p_s. For example, a source peer p_s would like to get a fully colored movie object but the target peer p_t sends just a monochromatic movie object to p_s. Here, qos_{st} = 0. If r satisfies the QoS requirement, qos_{st} is 1. rsp_{st} = 0 implies stf_{st} = qos_{st} = 0. In addition, stf_{st} = 0 implies qos_{st} = 0. Each interaction among a source peer p_s and a target acquaintance p_t is characterized in terms of a tuple $\langle rsp_{st}$, stf_{st}, $qos_{st}\rangle$ of the parameters. There are possible combinations of the parameters $\langle$1, 1, 1$\rangle$, $\langle$1, 1, 0$\rangle$, $\langle$1, 0, 0$\rangle$, and $\langle$0, 0, 0$\rangle$.

For each interaction with an acquaintance p_t, a source peer p_s obtains the parameters rsp_{st}, stf_{st}, and qos_{st}. The peer p_s records the parameters rsp_{st}, stf_{st}, and qos_{st}. Then, p_s takes statistical values $\langle\overline{rsp_{st}}$, $\overline{stf_{st}}$, $\overline{qos_{st}}\rangle$ of the parameters received. For each parameter a_{st} (0 leq a_{st} leq 1), the value $\overline{a_{st}}$ is calculated each time a new value a_{st} is obtained as follows, where $a \in \{$*rsp*, *stf*, *qos*$\}$:

1) $\overline{a_{st}}$ is an average value of parameter a_{st} in the record. That is, $\overline{a_{st}}$ = ($\overline{a_{st}}$ · (n -1) + a_{st}) / n where *n* is the total number of interactions.
2) $\overline{a_{st}}$ = ($\overline{a_{st}}$ · α + a_{st} · β) where $0 \leq \alpha \leq 1$, $0 \leq \beta \leq 1$, and $\alpha + \beta = 1$.

If the source peer p_s had communicated with a target acquaintance p_s for a longer time, a_{st} most recently obtained by p_s does not affect the the average value $\overline{a_{st}}$. For example, suppose a peer p_s has trusted an acquaintance p_t. Even if the target acquaintance p_t once fails to support p_s with required service, p_s still trusts p_t.

In the second way, if α is smaller than β, the current parameter a_{st} is more important than previous $\overline{a_{st}}$. This means, even if an acquaintance p_t had been trusted by a source peer p_s, p_s changes its trustworthiness opinion on p_t once p_t fails to support the required service.

In the paper [12], the satisfiability S_{st} shows the expected ratio at which a source peer p_s can get a satisfiability reply from a target peer p_t. In another way, the subjective trustworthiness S_{st} of a source peer p_s on an acquaintance p_t is defined on the Fuzzy logics. The subjective trustworthiness S_{st} is given as one of the Fuzzy variables, definitely trustworthy (*DT*), possibly trustworthy (*PT*), marginal (*M*), possibly untrustworthy (*PU*), and definitely untrustworthy (*DU*). The membership function $\mu_T(\langle\overline{rs_{st}}$, $\overline{st_{st}}$, $\overline{qos_{st}}\rangle)$ is given for each Fuzzy variable *T* $\in \{$*DT*, *PT*, *M*, *PU*, *DU*$\}$.

B. Expected subjective trustworthiness

Suppose $p_s \rightarrow p_u \Rightarrow p_t$ for some peer p_u and $p_s \not\rightarrow p_t$. We discuss how to estimate the subjective trustworthiness on an implicit acquaintance peer p_t given a pair of subjective trustworthiness S_{su} of p_s and S_{ut} of the acquaintance peer p_u. The *expected* subjective trustworthiness ES_{st} of the source peer p_s on the acquaintance peer p_t is obtained as shown in Figure 3.

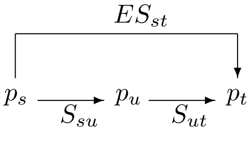

Figure 3. Implicit subjective trustworthiness

Suppose a peer p_u is an acquaintance of a source peer p_s and a target peer p_t is an acquaintance of p_u but the

Table I
EXPECTED SUBJECTIVE TRUSTWORTHINESS.

S_{su}	S_{ut}	ES_{st}
DT	*DT*	*DT*
DT	*PT*	*PT*
DT	*M*	*M*
DT	*PU*	*PU*
DT	*DU*	*DU*
PT	*DT*	*PT*
PT	*PT*	*PT*
PT	*M*	*M*
PT	*PU*	*PT*
PT	*DU*	*PU*
M	*DT*	*DT*
M	*PT*	*PT*
M	*M*	*DT*
M	*PU*	*PT*
M	*DU*	*DT*
PU	*DT*	*PU*
PU	*PT*	*PU*
PU	*M*	*M*
PU	*PU*	*PT*
PU	*PU*	*PT*
DU	*DT*	*DU*
DU	*PT*	*PU*
DU	*M*	*M*
DU	*PU*	*PT*
DU	*DU*	*DT*

$$\begin{tikzcd}
p_s \arrow[r, "S_{su}"'] \arrow[rr, bend left, "ES_{st}"] & p_u \arrow[r, "ES_{ut}"'] & p_t
\end{tikzcd}$$

Figure 4. Implicit subjective trustworthiness

Table II
EXPECTED SUBJECTIVE TRUSTWORTHINESS.

S_{su}	ES_{ut}	ES_{st}
DT	*DT*	*PT*
DT	*PT*	*PT*
DT	*M*	*M*
DT	*PU*	*PU*
DT	*DU*	*PU*
PT	*DT*	*PT*
PT	*PT*	*PT*
PT	*M*	*M*
PT	*PU*	*PT*
PT	*DU*	*PU*
M	*DT*	*PT*
M	*PT*	*PT*
M	*M*	*DT*
M	*PU*	*PT*
M	*DU*	*PT*
PU	*DT*	*PU*
PU	*PT*	*PU*
PU	*M*	*M*
PU	*PU*	*PT*
PU	*PU*	*PT*
DU	*DT*	*DU*
DU	*PT*	*PU*
DU	*M*	*M*
DU	*PU*	*PT*
DU	*DU*	*DT*

peer p_t is not an acquaintance of p_s, i.e p_t is an implicit acquaintance of p_s. Here, ES_{st} is given as S_{su} * S_{ut}.

If the source peer p_s definitely trusts the peer p_u, i.e. S_{su} = ***DT*** and S_{ut} = ***DT***, the source peer p_s is expected to definitely trust the target peer p_t. That is, the expected subjective trustworthiness ES_{st} is ***DT***. Next, suppose the source peer p_s definitely does not trust the target peer p_u, i.e. S_{su} = ***DU*** and p_u definitely does not trust p_t, i.e. S_{ut} = ***DU***. Here, p_s is expected to definitely trust p_t. That is, the expected subjective trustworthiness ES_{st} is ***DT***. Table I shows the expected subjective trustworthiness ES_{st} of a source peer p_s on an implicit acquaintance p_t given a pair of the subjective trustworthiness S_{su} and S_{ut}.

The source peer p_s can get the expected subjective trustworthiness ES_{st} from ES_{ut}, i.e. $p_s \rightarrow p_u \Rightarrow p_t$ [Figure 4]. Table II shows the expected subjective trustworthiness ES_{st} of a source peer p_s on an implicit acquaintance p_t given the subjective trustworthiness S_{su} and ES_{ut}.

IV. OBJECTIVE TRUSTWORTHINESS

A. *Objective trustworthiness*

A source peer p_s collects trustworthiness opinions on a target acquaintance p_t from other peers. We would like to discuss the objective trustworthiness O_{st} of a peer p_s on an acquaintance p_t. The objective trustworthiness O_{st} shows how a target acquaintance p_t is trusted by other peers in a P2P system S. The objective trustworthiness O_{st} is calculated on subjective trustworthiness collected from acquaintances of a target peer p_t. A collection of peers whose subjective trustworthiness on p_t is used to obtain the objective trustworthiness O_{st} is a *trustworthiness* domain D_{st}. Since the P2P system S is scalable, it is difficult to collect the subjective trustworthiness on the target peer p_t from every peer which know about p_t. One idea to calculate the objective trustworthiness O_{st} from the trustworthiness domain D_{st} is to get the average values of subjective trustworthiness of peers in D_{st}. Each subjective trustworthiness S_{ut} of a peer p_u on the target acquaintance p_t where p_u is in the domain D_{st} takes one of the Fuzzy values ***DT***, ***PT***, ***M***, ***PU***, and ***DU***. In this paper, we take a majority value in

D_{st}.

B. Trustworthiness-based broadcast algorithm

By using the flooding algorithm [8], the trustworthiness domain D_{st} is obtained. That is, a source peer p_s sends a trustworthiness request to every acquaintance p_u. On receipt of the request, the peer p_u sends the subjective trustworthiness S_{ut} to the source peer p_s if p_t is an acquaintance of p_u ($p_u \rightarrow p_t$). Otherwise, if $p_u \Rightarrow p_t$, p_u sends the expected subjective trustworthiness ES_{ut} to the source peer p_s. Then, p_u forwards the request to every acquaintance of p_u. Thus, the trustworthiness request is distributed to peers in the network.

The domain D_{st} of a peer p_s might include a peer p_u which does not have correct trustworthiness opinion on the target peer p_t. For example, a peer p_u has an inconsistent implicit acquaintance p_t. A peer p_u might be faulty. In order to get the more correct objective trustworthiness O_{st}, the source peer p_s has to collect the more correct subjective trustworthiness S_{ut} from a peer p_u. In addition, the communication overhead is increased since messages are broadcast in P2P overlay networks. We take the following approaches to efficiently collecting the more trustworthy subjective trustworthiness to obtain the objective trustworthiness O_{st} of a source peer p_s on a target acquaintance p_t:

[Trustworthiness-base protocol]

1) A source peer p_s sends a trustworthiness request q to every definitely or possibly trustworthy acquaintance p_u where S_{su} is *DT* or *PT*.
2) On receipt of the request q, if a peer p_u had ever received the request q, p_u neglects q. Otherwise, p_u sends the trustworthiness opinion T_{ut} on p_t to the source peer p_s, i.e.
   a) T_{ut} = S_{ut} if $p_u \rightarrow p_t$.
   b) T_{ut} = ES_{ut} if $p_u \not\rightarrow p_t$ but $p_u \Rightarrow p_t$.

   If $p_u \not\rightarrow p_t$ and $p_u \not\Rightarrow p_t$, p_u does not send a reply to p_s.
3) Then, the peer p_u forwards the request q to only definitely or possibly trustworthy acquaintance peers.
4) The steps 2) and 3) are iterated.

This is based on s a trustworthiness-based broadcasting (TBA) algorithms [1] [10], [11]. Each peer p_u does not forward the trustworthiness request q to an acquaintance which p_u does not trust. We can reduce the number of messages transmitted in the network. However, it takes time to distribute a trustworthiness request q to peers in the network. In order to reduce the response time, a request message q is assigned with a hop counter *q.h*. In the trustworthiness-based broadcasting algorithm, the peer p_u decrements the counter *q.h* by one on receipt of the request q. If *q.h* gets 0, p_u does not forward the request q. The initial value *q.h* which the source peer p_s gives to a request q shows the maximum number of peers which the request q can hop. If *q.h* is initially 1, a source peer p_s just delivers the request q to only its acquaintances. If *q.h* = 2, the request q is delivered to not only every trustworthy acquaintance p_u of p_s but also the acquaintance of p_u.

The source peer p_s thus collects replies of the trustworthiness request q from peers. Each reply r_u carries the trustworthiness information T_{ut} on a target peer p_t from a peer p_u. Here, the trustworthiness information T_{ut} is the subjective trustworthiness S_{ut} if $p_u \rightarrow p_t$ or the expected subjective trustworthiness ES_{ut} if $p_u \Rightarrow p_t$. One idea is to collect every trustworthiness information into one set *T* and then take a majority in the set *T*. Another way is to collect only subjective trustworthiness into the set *T* and take a majority in the set *T*.

There are the following approaches to collecting the replies of the request q:

1) The source peer p_s accepts a reply q_u only from a trustworthy peer p_u. Here, even if p_s receives a reply q_u from a peer p_u whose ES_{su} is neither *DT* nor *PT*, the source p_s neglects the reply q_u.
2) p_s accepts a reply q_u from every peer p_u.

If the peer p_u is trustworthy for the source peer p_s, i.e. ES_{su} is *DT* or *PT*, p_s can take the reply q_u with the subjective trustworthiness ES_{ut} from p_u.

V. Confidence

A peer p_s obtains the subjective trustworthiness S_{st} and the objective trustworthiness O_{st} on an acquaintance p_t. If the subjective trustworthiness S_{st} is similar to the objective trustworthiness O_{st}, the peer p_s can take the subjective trustworthiness S_{st}. However, p_s has to make a decision on which type of trustworthiness S_{st} or O_{st} to be taken if S_{st} is greatly different from the objective trustworthiness O_{st}. We would like to introduce a concept of *confidence* F_{st} on the subjective trustworthiness S_{st} which p_s obtained by itself through directly communicating with he target acquaintance p_t. The larger the confidence F_{st} is, the more often the subjective trustworthiness F_{st} is taken.

In this paper, we consider the following parameters to obtain the confidence F_{st} of a source peer p_s on a target acquaintance peer p_t:

[Parameters of confidence]

1) Communication time CT_{st}: A source peer p_s has been communicating with a target acquaintance p_t for time CT_{st}. The longer the source peer p_s has communicated with the target peer p_t, the more the source peer p_s is confident of the subjective trustworthiness S_{st} which p_s has obtained through communicating with p_t.
2) Communication frequency FR_{st}: The frequency FR_{st} shows how often a source peer p_s has communicated with a target acquaintance p_t. The more often p_s has communicated with p_t, the more p_s is confident of the subjective trustworthiness S_{st}.

3) Stability ST_{st}: If the subjective trustworthiness S_{st} is not so changed, the stability ST_{st} is lager. The larger ST_{st}, the more confident of the subjective trustworthiness ST_{st}.

The confidence F_{st} is thus given a tuple $\langle CT_{st}, FR_{st}, ST_{st}\rangle$ of the parameters. A source peer p_s issues a request to a target peer p_t. If p_s could get a satisfiable reply from p_t, the source peer p_s increases the subjective trustworthiness ST_{st} as discussed.

First, a source peer p_s would like to get service. The source peer p_s selects an acquaintance p_t by taking advantage of the subjective trustworthiness ST_{st} and objective trustworthiness OT_{st} with the confidence F_{st}. There are the following types of peers:

[Types of peers]

1) Self-confident peers.
2) Cooperative peers.
3) Non-confident peers.

If a source peer p_s is self-confident, the source peer p_s only uses the subjective trustworthiness ST_{st} as the trustworthiness T_{st} on an acquaintance p_t. A self-confident peer p_s is strongly confident of the subjective trustworthiness ST_{st} which the source peer p_s has obtained by itself. The source peer p_s selects an acquaintance p_t with the highest subjective trustworthiness ST_{st}. On the other hand, an non-confident peer p_s does not use the subjective trustworthiness ST_{st} for each acquaintance p_t and uses the objective trustworthiness OT_{st} as the trustworthiness T_{st}. A cooperative peer p_s takes usage of both the subjective trustworthiness ST_{st} and objective trustworthiness OT_{st} for each acquaintance p_t.

For each acquaintance p_t, a source peer p_s selects a target acquaintance p_t as follows:

1) If the confidence F_{st} is larger, the source peer p_s takes the subjective trustworthiness ST_{st}.
2) Otherwise, the source peer takes the objective trustworthiness OT_{st}.

Then, the source peer p_s takes an acquaintance p_t whose trustworthiness T_{st} is the maximum in a set A_s of acquaintances as a target peer.

VI. Concluding Remarks

In this paper, we discussed how each peer trusts an acquaintance in P2P overlay networks. First, we introduced two types of trustworthiness, subjective and objective types of trustworthiness. In this paper, the trustworthiness is given based on the Fuzzy logics. If the subjective trustworthiness and objective trustworthiness of a peer p_s on an acquaintance p_t are different, the source peer p_s has to decide on which type of trustworthiness to be taken. In this paper, we introduced the confidence F_{st} which shows how much p_s is confident of the subjective trustworthiness S_{st} which the source peer p_s has obtained by itself through communicating with the target acquaintance p_t. If the confidence F_{st} is larger, p_s takes the subjective trustworthiness S_{st}. Otherwise, p_s takes the objective trustworthiness O_{st}.

References

[1] A. Aikebaier, T. Enokido, and M. Takizawa, *Trustworthy Group Making Algorithm in Distributed Systems*, Human-centric Computing and Information Sciences (HCIS), *Vol.*1, *No.*1, *Article* 6, 2011, pp.1:6:1 - 1:6:15,

[2] E. Ayorak and A. B. Bener, *Super Peer Web Service Discovery Architecture*, Proc. of IEEE 23rd International Conference on Data Engineering 2007, pp.1360–1364.

[3] R. Chen, X. Chao, L. Tang, J. Hu, and Z. Chen, *CuboidTrust: A Global Reputation-Based Trust Model in Peer-to-Peer Networks*, Proceedings of the Autonomic and Trusted Computing, 2007, pp.203–215.

[4] A. Dtta, A. I. Stoica, and M. Franklin, *LagOver: Latency Gradated Overlays*, Proc. of IEEE 27th International Conference on Distributed Computing Systems, 2007, pp.13–20.

[5] F. K. Hussain, E. Chang, and T. S. Dillon, *Classification of Reputation in Peer-to-Peer (P2P) Communication*, Proc. of the International Conference on Parallel and Distributed Processing Techniques and Applications (*PDPTA*), 2004, pp.1429–1435.

[6] D. S. Kamvar, T. M. Schlosser, and H. Garcia-Molina, *The Eigentrust Algorithm for Reputation Management in P2P Networks*, Proc. of the 12th IEEE International Conference on World Wide Web, 2003, pp.640–651.

[7] L. Lamport, R. Shostak, and M. Pease, *The Byzantine Generals Problem*, Transactions on Programming Languages and Systems, *vol.*4, *no.*3, 1992, pp.382–401.

[8] A. Qayyum, L. Viennot, A. Laouiti, *Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks*, Proceedings of the 35th Annual Hawaii International Conference on System Sciences (*HICSS*), 2002, pp.298–306.

[9] J. Sabater and C. Sierra, *Reputation and Social Network Analysis in Multi-Agent Systems*, Proc. of the First International Joint Conference on Autonomous Agents and Multiagent Systems, 2002, Part 1, pp.475–482.

[10] A. B. Waluyo, D. Taniar, W. Rahayu, A. Aikebaier, M. Takizawa, and B. Srinivasan, *Trustworthy-based Efficient Data Broadcast Model for P2P Interaction in Resource-Constrained Wireless Environments*, Journal of Computer and System Sciences (*JCSS*), 2011.

[11] A. B. Waluyo, W. Rahayu, D. Taniar, and B. Srinivasan, *A Novel Structure and Access Mechanism for Mobile Broadcast Data in Digital Ecosystems*, IEEE Transactions on Industrial Electronics, vol.58, no.6, 2011, pp.2173–2182.

[12] K. Watanabe, Y. Nakajima, T. Enokido, and M. Takizawa, *Ranking Factors in Peer-to-Peer Overlay Networks*, ACM Transactions on Autonomous and Adaptive Systems(*TAAS*), *Vol.*2, *No.*3, *Article* 11, Sept. 2007, pp.11:1–11:26
(DOI : http://doi.acm.org/10.1145/1278460.1278465).